N. 135

DIRECTION

LE TECNOLOGIE CHE MUOVONO IL BUSINESS

SPECIALE
CYBERTECH EUROPE

OPENTEXT CYBERSECURITY
LA CONTINUITÀ AL PRIMO POSTO

BROTHER
LA SECURITY NEL PRINTING

QUALYS
ALLINEA IL RISCHIO CYBER
AL BUSINESS

DATA CENTER
L'AI CHIEDE PIÙ EFFICIENZA
E PRESTAZIONI

VERTIV
ONECORE RIDISEGNA
IL MODELLO INFRASTRUTTURALE

DATA MANAGEMENT
LE NUOVE TECNOLOGIE
CAMBIANO LE REGOLE

AXIANTE
STRATEGIE NELL'ERA DELL'AI

SIEMENS
due secoli di innovazione al servizio dell'industria

Floriano Masoero,
CEO e presidente di Siemens Italia

MERCATI VERTICALI **RETAIL ED E-COMMERCE:** STRATEGIE E TECNOLOGIE PER COMPETERE OGGI
SNOM LA TECNOLOGIA CHE RAFFORZA RETAIL E GDO
L'AI E IL RETAIL 5.0: L'EVOLUZIONE DELL'OMNICANALITÀ **a cura di IDC**

brother
at your side

Il nostro obiettivo è ridurre le emissioni del

65%

entro il **2030**

In Brother abbiamo a cuore l'ambiente e ci impegniamo costantemente per ridurre al minimo l'impatto delle nostre operazioni, eliminando gli sprechi senza perdere mai di vista la qualità dei prodotti.
Dalla progettazione dei prodotti, fino al riciclo delle cartucce toner, lavoriamo giorno dopo giorno per favorire un'economia sostenibile e ridurre le emissioni di CO2.

Vision 2050

CARBON NEUTRAL
Ridurre attivamente le emissioni di CO2 per l'intera catena del valore in tutte le operazioni aziendali e contribuire a creare una società carbon-free

RICICLO DEI MATERIALI
Massimizzare il riciclo dei materiali per garantire l'utilizzo sostenibile delle risorse naturali e ridurre al minimo il nostro impatto ambientale

PROTEGGERE LA BIODIVERSITÀ
Ridurre al minimo l'impatto delle operazioni aziendali sull'ecosistema e far crescere le nostre attività per ripristinare e preservare l'ecosistema

Programma di riciclo toner

Per promuovere l'economia circolare, in Brother abbiamo attivato per aziende e liberi professionisti un servizio di ritiro gratuito delle cartucce toner originali esauste, tramite corriere autorizzato. Ogni componente verrà rigenerato o riciclato: nulla andrà in discarica. Aderire è molto semplice: gli utenti possono richiedere dal nostro sito il ritiro gratuito delle cartucce toner Brother. Noi ci occuperemo del ritiro per poi riciclarle, contribuendo fattivamente alla sostenibilità ambientale.

Riciclando proteggiamo l'ambiente.

www.brother.it

DIRECTION
Anno XXI - numero 135
Ottobre 2025

Direttore responsabile: Riccardo Florio
Coordinamento editoriale: Paola Rosa

Ha collaborato: Fabrizio Pincelli, Stefano Uberti Foppa, Piero Todorovich

Immagini: Dreamstime.com
Stampa: New Press Edizioni Srl
Via Della Traversa, 22 - 22074 Lomazzo (CO)

Editore: Reportec Srl;
Via Monte San Michele, 163
20099 Sesto San Giovanni (MI)
Tel 339 3785157; https://reportec.it;
redazione@reportec.it

Il Sole 24 Ore non ha partecipato alla realizzazione di questo periodico e non ha responsabilità per il suo contenuto

Amministratore unico: Riccardo Florio
Iscrizione al tribunale
di Milano n° 212 del 31 marzo 2003

Diffusione cartacea + digitale 32.500 copie
Tutti i diritti sono riservati
Tutti i marchi sono registrati e di proprietà delle relative società

Reportec è una società fondata da Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi

AI, data center e **ESG** muovono il business

DI RICCARDO FLORIO
Direttore responsabile

Molti temi di grande attualità e interesse vengono approfonditi in questo numero di Direction. La **cover story dedicata a Siemens** mette in evidenza le prospettive aperte dall'AI per il comparto industriale italiano, chiamato a svolgere un ruolo da protagonista in Europa: ingegnerizzazione più rapida, controllo qualità assistito dai modelli, supply chain più reattive. Non retorica, ma risultati misurabili che migliorano competitività e margini.
Dal **Cybertech 2025**, appena conclusosi, di cui **Direction è stato media partner**, arriva un messaggio netto: l'AI è ormai parte integrante dei SOC. Significa rilevazione più tempestiva, analisi contestuale degli eventi, priorità d'intervento basate sul rischio e una difesa che diventa davvero operativa. **Le interviste** ad alcuni manager di primo piano mostrano come i vendor stiano ricalibrando ruoli, processi e metriche per rispondere alle nuove sfide e affrontare minacce più sofisticate con tempi di risposta coerenti con il business.
Il **tema ESG** si conferma centrale nel mondo dell'IT ed evolve da adempimento normativo a driver di business e competitività. È efficienza energetica, riduzione degli sprechi, trasparenza dei processi ma anche un linguaggio comune tra tecnologia, giurisprudenza e finanza che apre partnership e opportunità commerciali.
Da questo numero inauguriamo, inoltre, una **copertura continuativa dedicata ai Data Center**. Li seguiremo numero dopo numero perché sono l'infrastruttura che rende possibile l'AI e, più in generale, la trasformazione digitale del Paese. Disponibilità di potenza, densità di calcolo, raffreddamento, connettività: ciò che accade nei Data Center determina la velocità con cui l'innovazione arriva nelle aziende.
Chiudiamo con analisi dedicate a **Data management** e **Retail**. I dati non sono materia prima, ma capitale operativo: organizzarli e qualificarli riduce i tempi decisionali, migliora l'esperienza cliente, rende scalabili i modelli di servizio. Nel Retail, l'e-commerce cresce, l'esperienza d'acquisto viene ridefinita da AI, gestione dati e logistica sostenibile, per un'offerta che si avvicina alle esigenze reali dei territori.
Un numero ricco di contenuti e spunti per orientarsi meglio nel mondo delle tecnologie che muovono il business.

COVER STORY

6 **SIEMENS, due secoli di innovazione al servizio dell'industria**

FOCUS TECNOLOGIE

12 Data management: un mercato in crescita

14 L'evoluzione del data management incontra AI e ML

16 **Axiante.** Data management e AI

DATA CENTER

18 Sostenibilità dei data center oltre il PUE

20 **Vertiv** OneCore accelera il deployment dei data center

22 Capacità, potenza e AI ridisegnano il mercato dei data center

CYBERSECURITY

24 **Cybertech 2025** fa il punto sulla cybersecurity

28 **OpenText Cybersecurity.** La business continuity prima di tutto

30 **Brother.** La stampa, un grande rischio di sicurezza spesso sottovalutato

32 **Qualys** gestisce i rischi parlando il linguaggio del business

32 **ESET** cresce puntando sulla tecnologia

36 **Fortinet,** AI e cybersecurity

37 **Rubrik,** prevenzione data security

38 **Sophos,** cyber resilience

39 **Zscaler,** infrastrutture zero trust

INDICE

DIRECTION 135
OTTOBRE 2025

SPECIALE INNOVAZIONE

40 ESG, le nuove regole UE e le implicazioni per imprese e bilanci

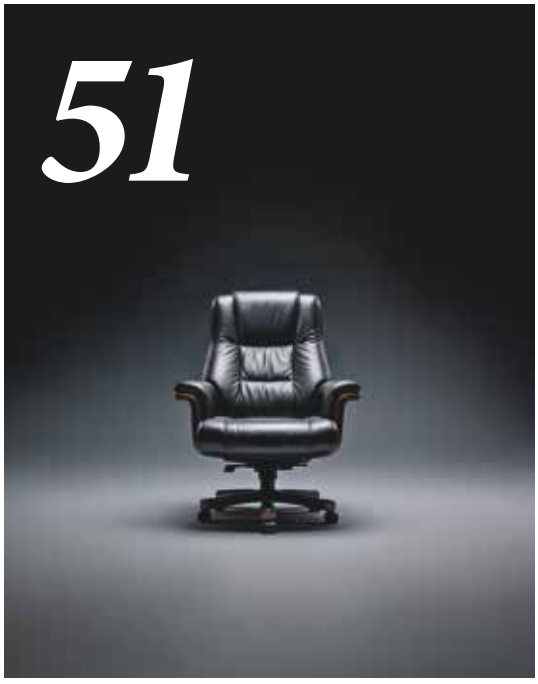
46 L'impatto ESG sui contratti tecnologici

ANALYTICS

48 Il contributo dell'intelligenza per dare valore ai dati

INSIGHT

50 I CEO guardano alle imprese di domani



MERCATI VERTICALI

57 **Retail ed e-commerce** strategie e tecnologie per competere oggi

62 **Snom** La tecnologia che rafforza retail e GDO

64 **IDC:** AI e retail 5.0: l'evoluzione dell'omnicanalità

SIEMENS
due secoli di innovazione al servizio dell'industria

Da oltre 175 anni Siemens guida l'innovazione industriale, unendo tecnologia e sostenibilità. Con il programma Siemens Xcelerator accelera la trasformazione digitale di industrie, reti e città in tutto il mondo

DI RICCARDO FLORIO

Siemens è un'azienda unica che, fin dalla sua fondazione a Berlino nel 1847, ha dimostrato una straordinaria capacità di innovare, di leggere i cambiamenti e di guidarli. In oltre 175 anni di storia ha consolidato una presenza globale in più di 200 Paesi, con 312mila dipendenti, di cui quasi 3mila in Italia, dove è attiva dal 1899. La missione dell'azienda è rimasta costante nel tempo: **coniugare tecnologia e innovazione per generare valore** per la società, l'economia e l'industria.

Negli ultimi decenni Siemens ha anticipato le grandi trasformazioni che hanno ridisegnato la manifattura e i processi industriali, dall'automazione dei primi impianti produttivi fino alla digitalizzazione delle fabbriche. Come una vera e propria tech company ha contribuito a portare sul mercato piattaforme e soluzioni capaci di rendere più efficienti i processi, di ridurre consumi ed emissioni e di creare valore lungo l'intera catena produttiva.

È il caso di tecnologie come il **Digital Twin**, che permettono di simulare e ottimizzare impianti e prodotti prima della loro realizzazione fisica o di **sistemi avanzati di automazione e controllo** che permettono di integrare macchine, software e dati in un unico ecosistema digitale. A queste si affiancano oggi le **applicazioni di intelligenza artificiale industriale**, un ambito in cui Siemens è apripista e protagonista grazie anche a partnership strategiche con realtà come Microsoft e Nvidia. L'AI industriale consente di sviluppare modelli predittivi, ottimizzare la manutenzione, ridurre sprechi ed emissioni e rendere i processi decisionali più rapidi e accurati.

È anche grazie a soluzioni di questo tipo che Siemens si è affermata come uno dei principali abilitatori dell'Industria 4.0, con applicazioni che spaziano dall'automotive al farmaceutico, dall'alimentare all'energia, fino ad arrivare alla più recente declinazione dell'Industria 5.0, dove automazione, digitalizzazione e intelligenza artificiale si combinano con obiettivi di sostenibilità ambientale, resilienza dei sistemi e centralità delle persone.

In Italia, dove il tessuto manifatturiero rappresenta un pilastro dell'economia nazionale, Siemens è partner di riferimento sia per grandi gruppi sia per PMI che puntano a innovare i propri modelli produttivi, ridurre l'impatto ambientale e restare competitivi in mercati sempre più globalizzati. **Transizione digitale, reti smart, efficienza energetica, intelligenza artificiale e mobilità sostenibile** rappresentano i pilastri strategici su cui il vendor concentra ricerca e sviluppo per trasformare industrie, infrastrutture, trasporti e reti. Ma la sola tecnologia non basta. Perché le imprese possano adottarla in modo rapido e sostenibile servono ecosistemi abilitanti. Con questa logica **Siemens ha lanciato Siemens Xcelerator, una piattaforma di business che mette a disposizione software, hardware e servizi digitali integrati**, creando un network di partner e soluzioni pensato per accelerare la trasformazione digitale di industrie, reti e città.

INDUSTRIAL AI: un cambio di paradigma

Direction intervista Floriano Masoero, CEO e Presidente di Siemens Italia, che spiega cosa può fare l'AI applicata all'industria e come l'Italia possa assumere una posizione di leadership in Europa

FLORIANO MASOERO, CEO E PRESIDENTE DI SIEMENS ITALIA

Come legge oggi il contesto industriale italiano ed europeo?

Oggi abbiamo un'opportunità rara, soprattutto in Italia e Germania. Sono i due Paesi industriali più forti d'Europa, il baricentro di un know-how che copre l'intero ciclo del valore: dalla progettazione al planning, dall'ingegneria alle operation e al service. Se riusciamo a mettere a fattor comune competenze di filiera e nuove tecnologie, possiamo costruire una propulsione industriale capace di ridefinire il ruolo dell'Europa nello scenario macroeconomico globale e in cui l'Italia non sia follower ma attore di primo piano. In questo quadro, grazie anche alla collaborazione con Microsoft, Siemens dà forma all'integrazione nativa tra intelligenza artificiale e mondo industriale promuovendo il concetto di Industrial AI.

Che cambiamenti porterà l'Industrial AI?

Non si tratta di un semplice upgrade tecnologico. È un cambio di paradigma, paragonabile al passaggio a Internet o al mobile. È una rivoluzione che permeerà l'industria al punto tale da diventare "invisibile", ma che costituirà il motore dei prossimi salti di produttività, qualità e time-to-market. Il potenziale è enorme e l'incremento di produttività derivante dall'adozione dell'AI Industriale potrebbe generare benefici economici che stimiamo tra gli 80 e i 100 miliardi di euro, se parametrati sul fatturato nazionale. Non va però scordato che l'AI industriale è molto differente da quella che utilizziamo sui nostri computer perché ogni errore può avere impatti diretti sulla produttività e persino sulla salute e sicurezza delle persone. Per questo motivo Siemens ha sviluppato un approccio "industrial grade", focalizzato su robustezza, precisione e affidabilità.

Come si integra questa nuova AI?

Un primo pilastro è **Siemens Industrial Copilot:** un'interfaccia conversazionale e uno stack applicativo che portano l'AI dentro l'ingegneria e la smart factory. Il Copilot accelera digitalizzazione e produttività, automatizza attività ripetitive, riduce errori e connette tra loro persone, OT e IT lungo la catena del valore. Ma ciò che ne esalta il valore è la sua disponibilità all'interno dell'ecosistema **Siemens Xcelerator** che realizza l'integrazione con applicazioni e casi d'uso specifici e offre la possibilità di estensione con soluzioni di terze parti. Per esempio Microsoft è uno dei partner dell'ecosistema.

Ma oltre l'interfaccia parlate anche di AI agentica. Perché?

Perché il punto di arrivo non è limitarsi a cercare informazioni, ma definire obiettivi, delegando compiti a una squadra di agenti specializzati. In due anni e mezzo siamo passati dall'attenzione per la sola AI generativa a un'**AI agentica, capace di eseguire task, orchestrare processi e interagire con macchine e dati** in modo naturale. È ciò che chiamiamo "automating automation" a significare che l'AI non assiste soltanto, ma opera sul sistema scegliendo gli agenti opportuni da ingaggiare. È la direzione che abbiamo intrapreso estendendo l'offerta con **Industrial AI Agents** integrati nell'ecosistema dei Siemens Industrial Copilot e aperti anche a terze parti.

Ci sono già applicazioni reali dell'AI Industriale?

Innumerevoli. Ne cito alcune. La società svedese **VA SYD** utilizza la soluzione Siemens SIWA Leak Finder di AI industriale per il rilevamento delle perdite d'acqua nella rete di distribuzione riuscendo a ridurre a meno dell'8% l'acqua non fatturata. **EPF**, realtà italiana specializzata in soluzioni di robotica e automazione, e l'azienda d'imbottigliamento **GAI Macchine** hanno realizzato impianti complessi sfruttando l'allenamento dell'AI nel Metaverso industriale.
Infine, le stesse piattaforme tecnologiche che ospitano l'AI possono essere utilizzate anche per altri progetti avveniristici. **Audi**, per esempio, ha deciso di virtualizzare i controllori dell'automazione in uno stabilimento automobilistico grazie ad app dedicate ed eseguite su Edge, conseguendo maggiore flessibilità, prestazioni superiori e semplificando la manutenzione.

Le aziende italiane come possono usufruire in tempi rapidi dei benefici portati dall'AI industriale?

Per riuscire a concretizzare le opportunità in tempi rapidi è essenziale adottare un **approccio progettuale basato su un framework standardizzato** che riunisca hardware e software e che faciliti la scalabilità. È possibile, per esempio, sfruttare soluzioni AI già industrializzate, capaci di risolvere problemi ricorrenti come il rilevamento dei difetti o la manipolazione di oggetti. Inoltre, è importante **valorizzare l'ecosistema di competenze** già disponibile, pensato per supportare aziende di ogni dimensione e settore.

L'AI industriale è una tecnologia appannaggio solo delle grandi aziende?

No. Uno degli obiettivi chiave di Siemens è rendere l'intelligenza artificiale accessibile a tutte le aziende, indipendentemente dalle dimensioni o dal settore. Anche le PMI possono trarre vantaggio da queste tecnologie, in un processo che possiamo definire di **democratizzazione dell'AI**. È una tecnologia democratica perché il paradigma cloud permette a un ufficio tecnico di cinque progettisti di usare, in prova o in esercizio, la stessa "cassetta degli attrezzi" di una grande impresa, senza investimenti iniziali proibitivi. Si può partire con piccoli progetti mirati per scalare verso attività avanzate di engineering, operations e service.

Come si coniuga l'Industrial AI con la sicurezza e la tutela dei dati riservati?

Si tratta di prerequisiti non negoziabili. Per questo motivo **l'uso dell'Industrial Copilot, in sede o da remoto, non espone i sistemi aziendali.** I dati incrementali usati per contestualizzare le risposte restano privati e sotto la piena governance del cliente. L'architettura rispetta policy e confini di rete, integra identity aziendale, logging e controlli di sicurezza by design. È qui che l'unione tra piattaforma cloud e dominio industriale fa la differenza: l'AI "vede" solo ciò che deve, quando serve e lo fa in modo tracciabile.

Qual è il passo successivo per Siemens?

La **maturità degli agenti AI**. Immaginate un orchestratore capace di comprendere la richiesta di un ingegnere, interrogare di conseguenza il progetto all'interno della nostra piattaforma integrata per l'automazione industriale (TIA Portal N.d.R.), incrociare manuali e specifiche, individuare problemi hardware, proporre la correzione, aggiornare lo schema elettrico e notificare il tutto al progettista. È un esempio reale del passaggio dall'AI che risponde all'AI che agisce sui processi industriali. La nostra roadmap su Industrial AI Agents e l'apertura dell'ecosistema su Xcelerator vanno esattamente in questa direzione.

Siemens ridisegna il futuro della **PRODUZIONE INDUSTRIALE**

Le nuove evoluzioni dell'AI preparano un futuro industriale all'insegna di fabbriche cognitive dotate di agenti autonomi che interagiscono tra loro e con le persone. Per sfruttare le nuove opportunità è bene indirizzarsi verso soluzioni integrate con il supporto di chi, da anni, opera attivamente in questo contesto tecnologico.

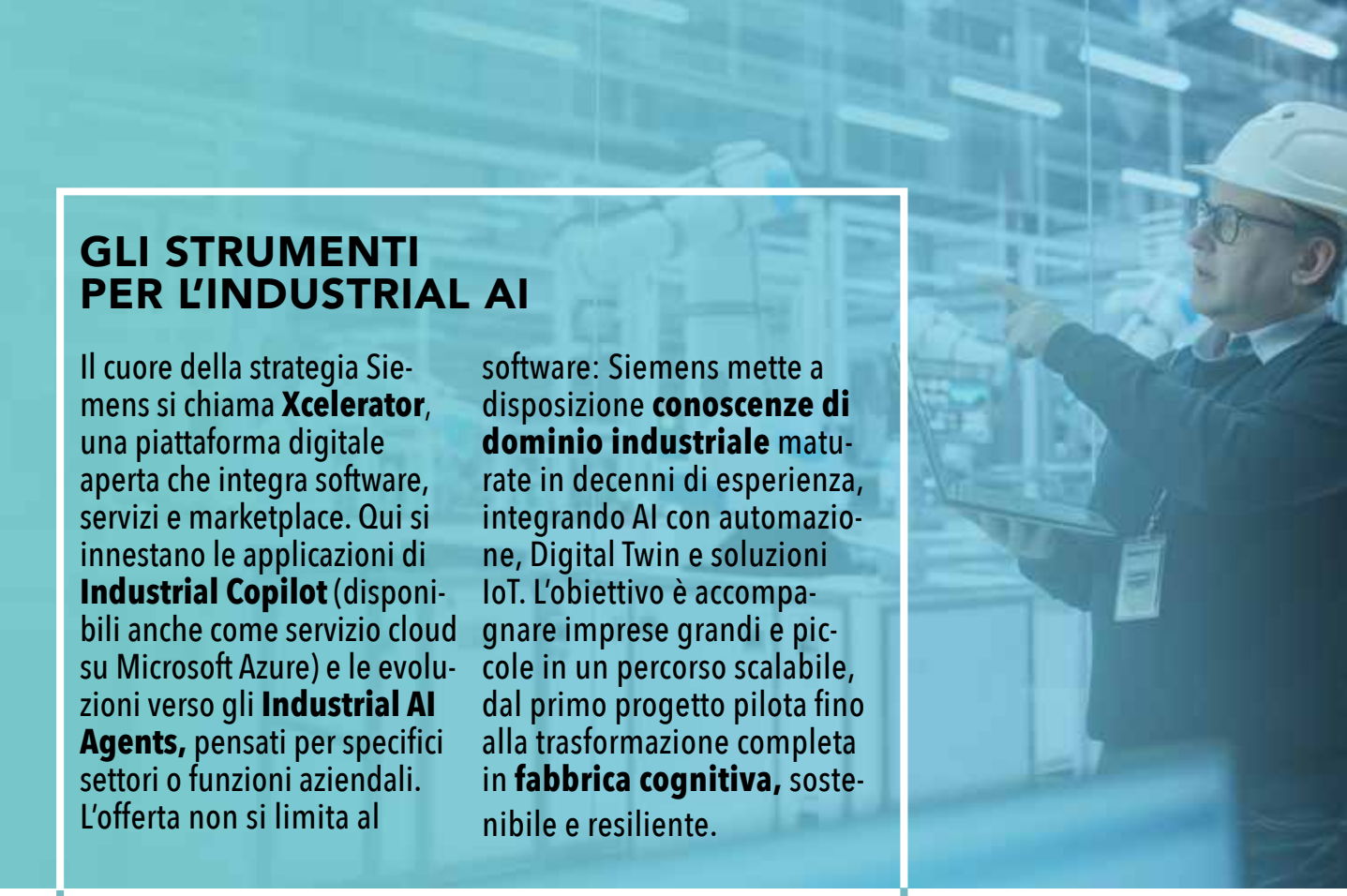
Il concetto di "industria intelligente" ha compiuto negli ultimi anni un balzo che va ben oltre l'automazione tradizionale. Oggi si parla di **Industrial AI**, un paradigma che non consiste soltanto nell'applicare algoritmi a processi esistenti, ma nell'integrare nativamente intelligenza artificiale e competenze di dominio industriale per trasformare l'intero ciclo di vita del prodotto: dal design al service.
Questa visione è parte di una traiettoria che ha già attraversato due transizioni epocali: la quarta rivoluzione industriale, segnata dalla digitalizzazione e dalla convergenza IT/OT e l'attuale fase che sempre più analisti chiamano Industria 5.0, in cui produttività, sostenibilità e centralità delle persone diventano priorità imprescindibili.

SIEMENS PIONIERE E LEADER NELL'AI INDUSTRIALE

Già dall'inizio degli anni '70, il **Dipartimento Centrale di Ricerca di Siemens** stava esplorando le potenzialità dell'AI applicata all'industria, anticipando di decenni le evoluzioni che oggi stanno trasformando il mondo produttivo.
L'impegno costante e strutturato, che ha reso Siemens un punto di riferimento per l'AI industriale a livello globale è oggi confermato dai dati: 3.700 domande di brevetto AI depositate, primo posto in Europa per brevetti AI (13° al mondo), oltre 500 famiglie di brevetti AI attivi, oltre 1.400 esperti di AI distribuiti in laboratori di ricerca in Europa, Stati Uniti e Asia.
Questi risultati consentono a Siemens di porre le basi per quelle che si prospettano le prossime due rivoluzioni nell'ambito dell'AI e di proporsi per **guidare le aziende nel processo decisionale** e accompagnarle lungo un percorso personalizzato e sostenibile.

SIEMENS IN ITALIA E NEL MONDO: I NUMERI DI UN PRESIDIO STRATEGICO

In Italia Siemens è presente dal 1899 e oggi conta **2.800 collaboratori**, con un **giro d'affari di circa 2 miliardi di euro.** Il quartier generale è a Milano, affiancato da centri di eccellenza a Bologna e Genova e da due **Digital Experience Center** a Milano e Piacenza, luoghi di sperimentazione e co-creazione con i clienti.
Le attività spaziano dalle soluzioni per l'industria digitale alle infrastrutture intelligenti, dalla mobilità alle tecnologie per la salute, coprendo l'intera catena del valore industriale e infrastrutturale. L'Italia è riconosciuta come mercato strategico, per dimensioni della manifattura e capacità di innovazione, in particolare nel percorso di trasformazione avviato dal PNRR.
Il posizionamento italiano si inserisce in un quadro globale imponente. Nell'anno fiscale 2024 Siemens ha registrato un **fatturato di 75,9 miliardi di euro** e un **utile netto di 9 miliardi.** Il Gruppo è **tra le prime dieci aziende software** a livello internazionale e investe in ricerca e sviluppo più di **6,3 miliardi di euro l'anno,** da cui solo nell'anno fiscale 2024 sono scaturite **5.250 nuove invenzioni e 2.900 domande di brevetto.**
Alla base di questa accelerazione c'è una strategia che combina acquisizioni mirate e partnership con i principali attori globali della tecnologia, da Microsoft a Nvidia, da Accenture a Sony e AWS.



GLI STRUMENTI PER L'INDUSTRIAL AI

Il cuore della strategia Siemens si chiama **Xcelerator**, una piattaforma digitale aperta che integra software, servizi e marketplace. Qui si innestano le applicazioni di **Industrial Copilot** (disponibili anche come servizio cloud su Microsoft Azure) e le evoluzioni verso gli **Industrial AI Agents,** pensati per specifici settori o funzioni aziendali. L'offerta non si limita al software: Siemens mette a disposizione **conoscenze di dominio industriale** maturate in decenni di esperienza, integrando AI con automazione, Digital Twin e soluzioni IoT. L'obiettivo è accompagnare imprese grandi e piccole in un percorso scalabile, dal primo progetto pilota fino alla trasformazione completa in **fabbrica cognitiva,** sostenibile e resiliente.

DALL'AUTOMAZIONE ALL'INTELLIGENZA AGENTICA ALLA PHYSICAL AI

Negli ultimi due anni l'attenzione pubblica si è concentrata sulla AI Generativa, resa popolare da modelli come GPT. Ma in ambito industriale lo scenario si è già spostato oltre: l'**Agentic AI** consente di passare da sistemi che forniscono risposte a sistemi che, in autonomia, eseguono task, orchestrano attività e interagiscono con macchine, software e persone in ambienti dinamici.

Una competenza che prepara già il passaggio futuro verso la **Physical AI** in cui l'integrazione tra intelligenza artificiale e robotica consentirà di interagire direttamente con il mondo fisico. In questo modo l'AI non sarà solo uno strumento, ma un vero e proprio agente di trasformazione.

Siemens ha costruito un **ecosistema completo** per semplificare l'adozione dell'AI che comprende: Competence center dedicati, modelli **software as a service, programmi di formazione** mirati; una rete di **partner certificati** per l'implementazione operativa.

SIEMENS INDUSTRIAL COPILOT

L'approccio sviluppato da Siemens con Industrial Copilot è un esempio concreto per "mettere a terra" nel mondo industriale e manifatturiero i benefici dell'AI.

Questa soluzione automatizza attività ripetitive come la gestione dei dati, la configurazione dei sensori e la reportistica, permettendo agli ingegneri di concentrarsi su lavori più complessi e a valore aggiunto. In tal modo l'AI diventa interfaccia naturale tra l'operatore e la fabbrica, capace di tradurre linguaggio naturale in azioni specifiche, di suggerire correzioni, di generare codice per PLC e di supportare l'ingegneria in tempo reale.

A questo si aggiunge la prospettiva degli Industrial AI Agents che operano come "specialisti" in aree specifiche (dal controllo qualità all'analisi dei sensori) coordinati da un orchestratore centrale.

UN'OPPORTUNITÀ PER L'ITALIA

Per un Paese manifatturiero come l'Italia, l'Industrial AI rappresenta un'occasione unica. Secondo lo studio *AI 4 Italy from theory to practice* realizzato da The European House - Ambrosetti insieme a Microsoft, l'adozione della sola AI generativa può generare fino a **312 miliardi di euro di valore aggiunto annuo** per il sistema-Paese, pari all'incirca al PIL della Lombardia.

La natura "cloud-based" delle soluzioni riduce la barriera d'ingresso, rendendo queste tecnologie accessibili non solo alle grandi aziende ma anche alle PMI. È proprio qui che

Siemens Italia sta concentrando parte delle proprie iniziative, mostrando come strumenti quali Industrial Copilot possano supportare l'engineering **in studi tecnici con pochi progettisti tanto quanto in stabilimenti di scala globale.**

VALORE AGGIUNTO E IMPATTO SUL BUSINESS

L'adozione di Industrial AI trova la sua naturale declinazione in un contesto di smart factory che permette di abilitare tre direttrici fondamentali di valore.

La prima è l'**efficienza**. L'AI riduce tempi di progettazione, velocizza la messa in servizio degli impianti e abilita manutenzione predittiva, con riduzioni dei fermi macchina che studi indipendenti stimano fino al 30% *(fonte: McKinsey, The state of AI in 2023: Generative AI's breakout year)*.

La seconda è la **flessibilità**, fondamentale per il manufacturing europeo e italiano, caratterizzato da produzioni ad alta variabilità. L'AI consente di simulare scenari alternativi, riprogrammare linee produttive e orchestrare supply chain in modo dinamico, un aspetto che Gartner individua come chiave per la resilienza delle aziende manifatturiere nei prossimi cinque anni *(fonte: Gartner, Predicts 2024: Future of Supply Chain Operations)*.

La terza è la **sostenibilità**, perché l'AI è i grado di analizzare consumi ed emissioni, creando le condizioni per ottimizzare l'uso delle risorse e supportare strategie di economia circolare.

Per Siemens, questo significa integrare Industrial AI nella piattaforma **Xcelerator**, dove le applicazioni vengono sviluppate, scalate e condivise in un ecosistema aperto che comprende partner e aziende.

VERSO UNA NUOVA IDEA DI FABBRICA

Tutto ciò pone le basi per costruire la **fabbrica del futuro**. Un futuro più vicino di quanto si possa pensare, in cui la fabbrica non sarà soltanto connessa o automatizzata ma **cognitiva**, all'interno della quale AI agentici collaboreranno con operatori, ingegneri e manager per prendere decisioni in tempo reale, personalizzare la produzione, ridurre sprechi e creare valore lungo tutto il ciclo di vita del prodotto.

È questo lo scenario in cui Siemens si propone come partner tecnologico e industriale, non limitandosi a fornire strumenti ma **costruendo, insieme alle imprese, un ecosistema aperto, data-driven e sostenibile**.

Un ecosistema in cui l'AI smette di essere tecnologia a sé stante e diventa parte integrante del DNA della manifattura.

ENGINEERING COPILOT FOR TOTALLY INTEGRATED AUTOMATION (TIA) PORTAL

Engineering Copilot for TIA Portal è l'assistente che si connette direttamente al TIA Portal con l'obiettivo di aumentare l'efficienza dei processi di ingegneria, ridurre il peso delle attività ripetitive, diminuire gli errori e introdurre l'automazione guidata dall'AI nei flussi di lavoro giornalieri. Attraverso un'interfaccia che permette l'interazione in linguaggio naturale, gli ingegneri dell'automazione possono generare rapidamente codice SCL o JavaScript, creare pannelli di visualizzazione per le interfacce uomo macchine (HMI), documentare il codice, tradurre testi e ottenere risposte a quesiti legati all'automazione. Questo consente di migliorare la qualità dei progetti e ridurre i tempi di sviluppo spostando l'attenzione verso compiti di maggior valore.

In prospettiva, Siemens Industrial Copilot si configura come un insieme di assistenti basati su intelligenza artificiale generativa, integrati attraverso l'intera catena del valore dei clienti e applicati a diversi settori industriali e casi d'uso.

Data management un mercato in crescita

Il data management si conferma come segmento del mercato IT in forte crescita e strategico per poter estrarre conoscenza e valore di business dalle grandi quantità di dati a disposizione delle imprese

DI PIERO TODOROVICH

Con la digitalizzazione progressiva dei processi e l'esplosione dei volumi di dati generati internamente all'ecosistema aziendale e da provider esterni, le capacità per gestire, governare e valorizzare le informazioni sono diventate un fattore critico per la competitività. Un'esigenza che oggi accumuna grandi e piccole imprese, ben rappresentata dalla crescita degli investimenti in infrastrutture, servizi e software nell'ambito del data management.

La crescita del mercato sull'onda del rinnovamento infrastrutturale

Il rinnovato interesse per sistemi e soluzioni di data management è confermato dai dati più recenti sulla spesa globale. Secondo il rapporto Enterprise Data Management Market (2025-2030) di *Grand View Research*, la spesa globale da parte delle grandi imprese, pari a 110,5 miliardi di dollari nel 2024, salirà a 221,6 miliardi entro il 2030, con una crescita media del 12,4% annuo. Questo sotto le spinte dei progetti di trasformazione digitale, dell'adozione del cloud computing e dell'adeguamento della gestione dei dati sotto i profili della sicurezza e della conformità.
Le sollecitazioni al rinnovamento delle infrastrutture dati esistenti ha vissuto una prima accelerazione nel periodo della pandemia, con l'esigenza per le imprese di garantire la continuità operativa, gestendo dati distribuiti e lavoro remoto. Negli ultimi due anni hanno avuto un ruolo nella crescita degli investimenti l'adozione di piattaforme dati cloud-based e di strumenti più efficaci per la data governance.
Tra i principali fattori per la crescita futura ci sono l'**esplosione dei big data** (con un volume di dati globale che gli analisti prevedono possa superare 180 zettabyte quest'anno), ma anche l'estensione dell'accesso e dell'utilizzo delle informazioni in azienda attraverso interfacce colloquiali basate su AI/ML e di GenAI.
Al pari di altre soluzioni per erogare dati analitici in self-service, l'implementazione richiede grandi capacità di governo sugli aspetti di sicurezza e privacy in accordo con normative come GDPR (in Europa), CCPA e HIPAA (negli USA) e future evoluzioni.

Italia: un panorama a luci e ombre

Il mercato italiano delle soluzioni di data management, unitamente a quello dei tool analitici ha una dimensione stimata per quest'anno tra i 3,5 e i 4 miliardi di euro, ma è caratterizzato da un parco installato da

soluzioni tecnicamente datate e frammentate. Grandi imprese, gruppi bancari e assicurativi sono pionieri nell'adozione delle soluzioni più avanzate, mentre molte piccole e medie imprese inseguono faticosamente l'innovazione, man mano che le emergenze della data protection e delle compliance normative sollecitano la migrazione verso strumenti più moderni ed efficaci per il governo del patrimonio dati.
Secondo le rilevazioni degli *Osservatori Digital Innovation del Politecnico di Milano*, la spesa delle aziende italiane in risorse infrastrutturali, software e servizi nell'ambito della gestione e dell'analisi dei dati, ha registrato nel 2024 una crescita pari al 20%. Sette aziende su dieci hanno avviato almeno un progetto di advanced analytics, ma solo quattro su dieci lo hanno fatto sulla base di una strategia unitaria di valorizzazione dei dati. Il 75% degli investimenti è appannaggio delle grandi imprese e solo il 6% ha riguardato la Pubblica amministrazione: una quota esigua che però ha registrato una crescita del 25% rispetto all'anno precedente. Anche la spesa per servizi e risorse infrastrutturali cresce con tassi superiori alla media, rispettivamente del 22% e 21%.
A spiccare maggiormente è risultata la domanda nei settori **utilities** (+28%) e **manifatturiero** (+23%).
Per quanto riguarda le quote assolute di spesa in italia, il **mondo finanziario** (banche e assicurazioni) è oggi in primo piano nella spesa per data management, con un terzo del totale, seguito dal settore manifatturiero per un quarto. La maturità delle realizzazioni resta però piuttosto bassa. Secondo il *Data Strategy Index 2024*, solo il 23% delle grandi imprese italiane si colloca a un livello avanzato nelle capacità di valorizzazione dei dati (era il 20% nel 2023). Per l'11% le realizzazioni sono giudicate immature. Il mercato italiano soffre la carenza di competenze specialistiche in ambiti di data engineering e data science, con una domanda che supera largamente l'offerta. Non aiutano la complessità normativa, con continui aggiornamenti, e il gap culturale delle PMI, dove la maturità digitale è ancora limitata.

IL MERCATO ITALIANO DEL DATA MANAGEMENT HA UN VALORE DI 4 MILIARDI DI EURO

SYSTEM INTEGRATOR E OPERATORI ITALIANI ATTIVI NEL DATA MANAGEMENT

Engineering Ha una divisione dedicata a big data e analytics che offre soluzioni end-to-end per la gestione e valorizzazione dei dati. L'azienda ha sviluppato competenze specifiche su piattaforme open source e soluzioni cloud.

Dedagroup Si posiziona come provider di soluzioni applicative e servizi IT con forte focus sul data management per settori specifici come sanità, pubblica amministrazione e utilities. L'azienda offre piattaforme proprietarie integrate con componenti di mercato.

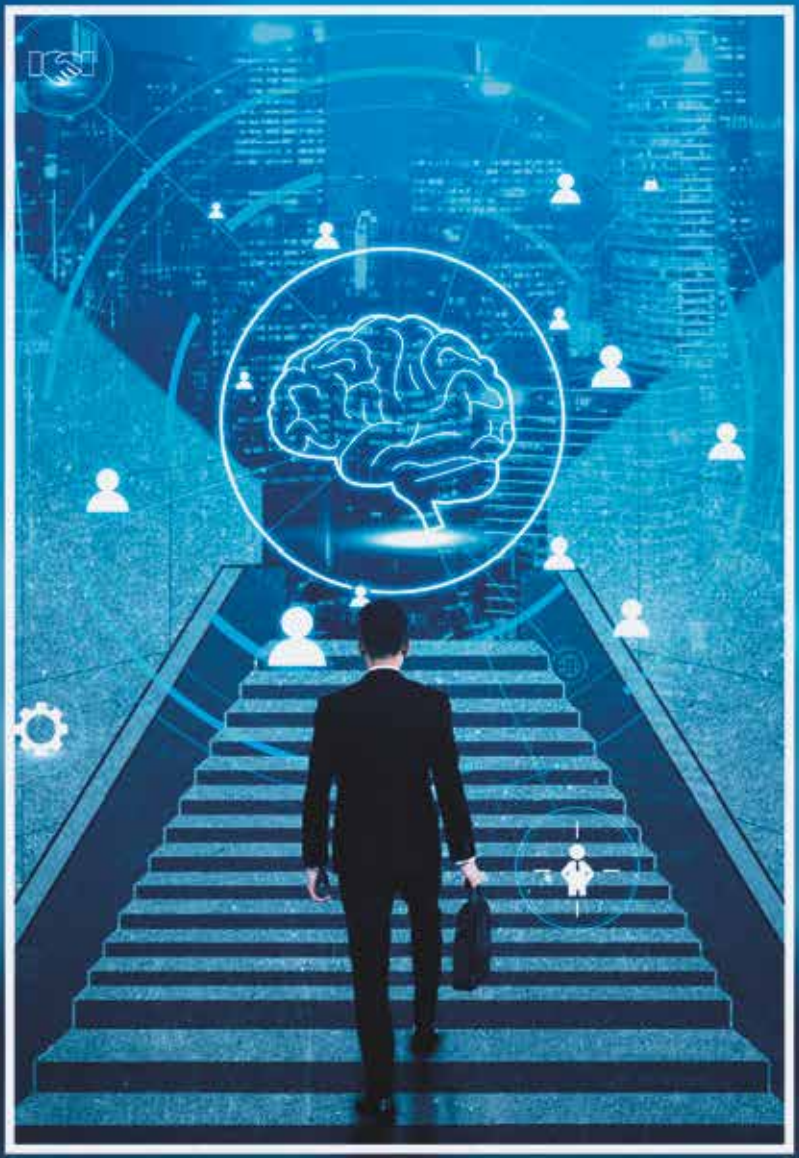
Lutech Nato dalla fusione di diverse realtà italiane, propone soluzioni integrate di data management con particolare focus su data governance e business intelligence, servendo principalmente il mercato enterprise italiano.

Reply Attraverso le sue diverse società specializzate come Data Reply e Machine Learning Reply offre servizi di consulenza strategica e implementazione sull'intero stack del data management: dalle architetture dati all'advanced analytics.

Sella Labs La divisione innovazione del Gruppo Sella ha sviluppato competenze avanzate in data management applicato al settore finanziario, con particolare attenzione a temi di data quality e governance.

Var Group System integrator italiano con competenze nel data management, offre servizi di consulenza e implementazione su piattaforme enterprise. L'azienda supporta le imprese nella definizione di strategie data-driven e nell'implementazione di soluzioni su misura.

L'evoluzione del data management incontra AI e ML



L'adozione del cloud e la disponibilità delle tecnologie AI/ML e Agentic AI promettono un data management sempre più intelligente, autonomo e adattivo nei fondamentali compiti di raccolta, organizzazione, conservazione, governo e sicurezza dei dati

Il data management sta vivendo una trasformazione profonda, alimentata dall'innovazione tecnologica e dal mutamento delle esigenze sui fronti del business e della sicurezza. Da una parte c'è la crescita esponenziale nella **quantità e varietà delle tipologie di dati** che devono essere gestiti, dall'altra le esigenze di **democratizzare l'accesso ai dati** per permettere alle line of business di trarre il massimo valore dai dati.

Il primo fattore alimenta la necessità di ambienti ibridi in cui convivono basi dati locali, centralizzate e su servizi multi-cloud, scelti in funzione delle esigenze prestazione, tutela e contenimento dei costi IT. Questo alimenta l'esigenza di strumenti per l'**unificazione semantica delle informazioni** in grado di rendere semplice l'accesso, l'analisi e l'elaborazione su fonti e archivi dati diversi.

Complessità a cui rispondono l'integrazione delle piattaforme con **strumenti di AI/ML e Agentic A**I capaci di semplificare la vita ai data manager, assolvendo con l'automazione molti compiti onerosi negli ambiti dell'integrazione, del monitoraggio, della qualità dei dati, della gestione, della sicurezza di accesso e di applicazione delle policy. Sul fronte della fruizione dei dati, le **capacità generative, tecniche di GenAI e strumenti di Retrieval augmented generation (RAG)** promettono di cambiare per sempre le modalità con cui le informazioni sono ricercate e utilizzate dagli utenti finali. I principali player nel mondo database stanno adeguando le loro piattaforme per poter aggiungere funzioni di ricerca conversazionale e contestuale su dati strutturati e non, generare viste dei dati a partire da domande in linguaggio naturale.

L'IMPATTO DELL'AI/ML NELLE CAPACITÀ CHIAVE DEL DATA MANAGEMENT

Master data management (MDM). Rientrano in questa categoria gli strumenti utili a mantenere versione unica e attendibile dei dati (anagrafiche clienti, prodotti, fornitori…) quindi garantirne la coerenza e la qualità nei processi su sistemi eterogenei e tra differenti reparti aziendali. L'introduzione delle tecnologie di AI/ML consente oggi di automatizzare le operazioni di matching e di deduplicazione dei dati. Altre innovazioni riguardano la semplificazione nelle gestioni multi-dominio e cloud-native con agenti intelligenti in grado di orchestrare operazioni di pulizia e sincronizzazione continua dei dati. Agentic AI e RAG (Retrieval augmented generation) permettono di ottenere viste sui dati critici per una gestione conforme alle normative.

Data integration – ETL. Sono gli strumenti fondamentali che servono per mettere insieme flussi e fonti dati eterogenei per renderli accessibili e utilizzabili in modo centralizzato. In quest'area tecnica del data management, le tecnologie di AI/ML implementate su alcune piattaforme rendono disponibili all'utente, in chiave end-to-end i suggerimenti per ottenere il giusto matching tra le diverse fonti di dati, automatizzando le operazioni di controllo su qualità e arricchimento dei dati.

Data quality. La qualità dei dati è fondamentale per qualsiasi iniziativa business di tipo data-driven. Quest'ambito funzionale contempla le funzioni di monitoraggio, controllo e correzione dei dati al fine di eliminare duplicazioni, errori e informazioni incomplete, migliorando quindi l'affidabilità delle informazioni. Gli algoritmi di ML riescono a rilevare in modalità automatica le anomalie, i duplicati e altre inconsistenze presenti nei dati, rendendo la gestione della qualità più efficace e meno soggetta agli errori umani.

Data governance. Riguarda le strategie, le regole, le responsabilità e i processi per una gestione dei dati più sicura e in linea con le normative di legge e le policy interne aziendali. Questo segmento si avvantaggia delle capacità di AI per i compiti del policy management. Agenti intelligenti sono in grado di monitorare, applicare e adattare le policy in tempo reale, in base al contesto normativo. Questo consente formalizzazioni più strutturate della governance e una rapida adozione delle normative a cominciare, per esempio, dall'EU Data Act (in vigore dal settembre 2025) in tema di portabilità e verificabilità dei dati.

Data security. Comprende i tool e le pratiche per proteggere i dati da accessi non autorizzati, quindi evitare violazioni e perdite, garantendo privacy e riservatezza. Capacità AI-driven aiutano a supportare il monitoraggio degli attacchi informatici, mentre agenti proattivi identificano e bloccano le violazioni prima che abbiano impatto sulla tutela dei dati o dei processi. L'AI permette anche una gestione automatizzata delle chiavi di cifratura utilizzate per la protezione più efficace dei flussi di dati, offre supporto alle capacità di auditing della sicurezza e nella governance permettendo reazioni più rapide ed efficaci.

Data Lifecycle Management: Serve alla gestione dell'intero ciclo di vita del dato: dalla creazione all'archiviazione, fino alla definitiva cancellazione in accordo con le policy aziendali e le normative di settore. Capacità di AI/ML permettono di supportare classificazioni automatiche e archiviazioni intelligenti dei dati sia su sistemi locali sia multicloud. L'agentic AI consente una gestione adattiva delle policy di data retention, non solo per il rispetto delle tempistiche di legge ma, per esempio, sulla base del loro valore d'uso e costi di gestione.

Database, data warehousing, data lake. Sono gli strumenti chiave per la raccolta, l'archiviazione e l'organizzazione dei dati a supporto delle attività di analisi, di reporting e di business intelligence d'impresa. Risorse in cloud e funzioni basate su AI/ML consentono di ottimizzare capacità, query e costi di gestione in funzione delle tipologie di dati e delle differenti esigenze di utilizzo. Sulla base dell'analisi predittiva, AI/ML e agentic AI possono orchestrare il bilanciamento ottimale tra workload locali e in cloud, offrire le capacità di supporto conversazionale RAG.

Data management e AI: strategie per un business più consapevole e competitivo

Dalla qualità dei dati alla data science, dalla governance alla privacy, fino alla spinta della generative AI, le imprese cercano sempre più strumenti e metodi per trasformare l'informazione in valore concreto, bilanciando innovazione e continuità. Matteo Longoni, business development manager di Axiante spiega come fare

DI FABRIZIO PINCELLI

Il data management e l'AI sono oggi leve decisive per guidare strategie e competitività. Ne abbiamo parlato con **Matteo Longoni, business development manager di Axiante**, che illustra sfide e opportunità per le imprese.

Negli ultimi anni il tema del data management ha assunto una centralità crescente. Come si è evoluto il vostro approccio in questo ambito?

Il nostro approccio si è evoluto insieme alla maturità del mercato. In Axiante abbiamo sempre considerato i dati fondamentali ma dieci anni fa nelle aziende mancava una consapevolezza diffusa. Oggi il contesto è cambiato: le grandi organizzazioni si sono evolute come maturità, ma ancora nel nostro lavoro la parte di education è fondamentale per renderle consci dell'importanza di sfruttare i dati per migliorare il processo decisionale. Il nostro ruolo è massimizzare queste potenzialità.

Quali sono i principali livelli di supporto che offrite alle aziende che vogliono valorizzare i propri dati?

Offriamo un supporto articolato su due livelli complementari per massimizzare il valore dei dati aziendali. In primo luogo, ci assicuriamo che i dati siano sempre disponibili, costantemente aggiornati e fruibili, velocemente e dinamicamente, attraverso architetture robuste che garantiscono qualità e coerenza. Questo, oltre che comportare scelte tecniche non banali, è fondamentale perché le decisioni strategiche non possono mai basarsi su dati obsoleti o incoerenti. Il secondo livello è quello analitico avanzato. Attraverso tecniche di data science e algoritmi di AI e approcci moderni di BI basati sul concetto di Self-Service Analytics, aiutiamo le aziende a scoprire insight nascosti e pattern significativi all'interno dei loro database. Quando si lavora con grandi volumi di dati, correlazioni importanti e anomalie critiche spesso rimangono invisibili a un'analisi superficiale, e devono poter essere esplorate in modo flessibile e interattivo: il nostro ruolo è fornire un sistema in grado di trasformare questi dati grezzi in indicazioni fruibili facilmente per azioni concrete per intervenire su aspetti critici o sfruttare opportunità.

Dal vostro osservatorio, quali differenze di maturità notate nei diversi settori industriali rispetto all'uso dei dati?

Il panorama è molto eterogeneo. Nel banking, l'utilizzo dei dati è ormai consolidato: modelli predittivi e sistemi di AI supportano risk management, churn analysis e fraud detection. In altri settori, invece, il concetto stesso di "data-driven" è ancora in fase embrionale e individuare i processi in cui i dati possono davvero fare la differenza non è scontato. Qui la tecnologia da sola non basta: è fondamentale un approccio strategico che coinvolga tutte le funzioni aziendali per identificare concretamente dove e come i dati possano generare valore misurabile, individuando a monte con quale obiettivo: maggiori ricavi, riduzione dei costi, nuove opportunità di business, maggiore competitività. Osserviamo inoltre una divisione dimensionale: le grandi imprese hanno maggiori probabilità di successo grazie a budget più consistenti e team dedicati, mentre le PMI spesso si trovano in difficoltà nell'avviare e portare a termine questi progetti.

Oltre alle complessità tecnologiche, ci sono criticità legate alla privacy e alla gestione del dato?

Certamente. In realtà, c'è una sfida di natura prettamente tecnica, legata a temi di modellazione e architettura dei sistemi di data management, ma quella principale è di natura culturale, legata anche al diverso livello di maturità digitale dei settori coinvolti. Facciamo un esempio concreto: un cliente di e-commerce è generalmente disposto a condividere i propri dati di navigazione per procedere a un acquisto o per ricevere raccomandazioni personalizzate. Al contrario, un'azienda manifatturiera che utilizza macchinari industriali spesso si mostra riluttante a garantire pieno accesso ai propri dati di utilizzo al fornitore, anche quando ciò permetterebbe di ottimizzare le prestazioni dell'impianto. Quindi la proprietà intellettuale dei dati e la definizione chiara dei diritti sul loro uti-

lizzo è un nodo centrale: senza accordi trasparenti che stabiliscano chi può accedere a quali informazioni e per quali scopi, anche la tecnologia più avanzata rimane inutilizzabile.

Oggi, l'offerta tecnologica è molto vasta. Quali scelte strategiche devono affrontare le imprese?

La vera sfida per le aziende non è accedere alla tecnologia, ma saperla orchestrare strategicamente per generare valore concreto. Ogni scelta deve essere valutata considerando l'allineamento con gli obiettivi di business, la governance dei rischi, la sicurezza dei dati, la scalabilità futura e l'effettiva adozione da parte degli utenti. In questo scenario complesso, la partnership con Axiante diventa determinante in quanto, monitorando con il nostro lavoro l'evoluzione del mercato e lavorando sul campo con progetti enterprise, abbiamo la capacità di trasformare la complessità tecnologica in soluzioni di business.

Le aziende chiedono sempre più spesso di conciliare innovazione e continuità. Come si gestisce questo equilibrio?

La chiave è la gradualità. Certamente i sistemi critici non si possono sostituire dall'oggi al domani, ma dobbiamo introdurre il concetto di evoluzione: far coesistere le nuove piattaforme con quelle esistenti e procedere con migrazioni progressive. Questo approccio preserva la continuità operativa, ma aiuta anche il processo di change management che deve inevitabilmente essere intrapreso in parallelo. Attraverso un percorso graduale, e che coinvolga i dipendenti, le organizzazioni possono metabolizzare il cambiamento senza subire traumi.

In settori regolamentati, dove la gestione del dato è particolarmente critica, quali accorgimenti vanno adottati?

Qui la chiave è la modellazione concettuale: definire con precisione chi può accedere ai dati, con quali permessi, per quanto tempo e attraverso quali processi di tracciabilità. Tuttavia, in questi contesti spesso si eredita un'architettura tecnologica consolidata e difficile da sostituire. Il modello dati e di governance diventa quindi cruciale per implementare anche su infrastrutture datate i nuovi requisiti normativi senza compromettere l'efficienza operativa degli utenti finali.

Quali sono i KPI fondamentali per misurare il successo di un progetto data-driven?

I KPI per progetti data-driven devono seguire una logica gerarchica che parte sempre dal business value. In questa direzione il parametro primario rimane l'impatto economico: ogni iniziativa deve generare benefici tangibili sui ricavi e sul profitto. A questa misurazione, si affiancano poi i KPI operativi specifici per ogni use case che viene implementato, come analisi di churn o di predictive maintenance. Infine, i KPI tecnici - come la qualità dei dati, la loro completezza e frequenza di aggiornamento - rappresentano il terzo livello. Questi ultimi due indicatori hanno pieno valore quando sono chiaramente collegati agli obiettivi di business.

Parliamo di AI. Quale contributo concreto può dare al processo decisionale?

L'AI si sta rivelando un alleato prezioso per chi deve prendere decisioni complesse. Il suo punto di forza non sta nel fornire risposte definitive, quanto piuttosto nell'aiutarci a vedere più chiaramente e più velocemente le possibili conseguenze delle nostre scelte. Attraverso capacità predittive e di simulazione, l'AI permette di esplorare diversi scenari e comprendere meglio l'impatto di ogni opzione sul tavolo. Anche le potenzialità della Gen AI si stanno rilevando enormi, ma la vera sfida sta ancora nel trovarle un ruolo efficace in relazione al contesto specifico dei processi decisionali.

Guardando al futuro, quali trend ritiene più significativi nella gestione dei dati?

La velocità dell'innovazione è impressionante. L'AI generativa continuerà a evolvere, ma altrettanto decisiva sarà la flessibilità nella modellazione dei dati, perché cresce il numero di funzioni aziendali che vogliono accedere alle informazioni. Parallelamente, la performance rimarrà centrale: in questa direzione, il quantum computing, pur ancora in fase sperimentale, promette calcoli drasticamente più rapidi in ambiti specifici. Una cosa però è certa: non sappiamo quali tecnologie domineranno tra dieci o quindici anni, ma, anche se in modalità probabilmente evolute rispetto alle attuali, i dati resteranno il fulcro del business.

Matteo Longoni
Business development manager di Axiante

Sostenibilità dei DATA CENTER oltre il PUE

Ridurre l'impronta di carbonio e rafforzare il bilancio di sostenibilità sta diventando un vincolo operativo, non solo reputazionale. Tra nuove metriche, obblighi europei di rendicontazione e obiettivi 24/7 carbon-free, il 2025 segna un cambio di passo per progettazione, approvvigionamento energetico e disclosure.

A CURA DELLA REDAZIONE

Per un decennio l'efficienza è stata raccontata quasi solo attraverso il **PUE (Power usage effectiveness)**. Nel 2025, però, il PUE medio ponderato dell'industria resta pressoché stabile attorno a 1,54, sesto anno senza progressi sostanziali: un segnale che i margini "facili" sono esauriti e che l'ottimizzazione va cercata in altre dimensioni come impronta di carbonio, acqua e riuso del calore. È qui che entrano in gioco metriche complementari: il **CUE per l'intensità di carbonio** e il **WUE per l'uso idrico**, indicatori esplicitamente promossi anche dalle linee guida del Dipartimento dell'Energia USA per la progettazione efficiente dei data center, che invitano a puntare al 100% di energia rinnovabile per il 100% del tempo e a minimizzare l'uso d'acqua con strategie di raffreddamento "dry" quando possibile. L'Open Compute Project, a sua volta, nel *Data Center Facility Sustainability Metrics* formalizza set di KPI per strutturare CUE e inventari di emissioni in modo confrontabile tra operatori e regioni.

Obblighi europei e reporting come requisito normativo

In Europa la sostenibilità è ormai materia regolata, con impatti diretti sui data center. La direttiva sull'efficienza energetica, nella versione riveduta, introduce **l'obbligo di monitorare e riportare le performance dei data center in un database europeo**, con indicatori su energia, temperatura, uso dell'acqua, quota rinnovabili e recupero di calore per siti sopra una certa soglia di consumo. La **Commissione europea per l'Energy efficiency directive (EED)** in un atto delegato ha esplicitato i KPI allineando la rendicontazione ai requisiti tecnici.

Sul fronte corporate, la **Corporate sustainability reporting directive (CSRD)** estende in profondità il perimetro del bilancio di sostenibilità e rende gli European sustainability reporting standards (ESRS) la base tecnica per la rendicontazione; per i gruppi extra UE con presenza significativa nel mercato europeo, l'entrata in vigore dei requisiti è stata confermata con tempistiche previste indicativamente a partire dal 2028-2029.
In parallelo, il **Climate neutral data centre pact** anticipa impegni di settore su energia 100% rinnovabile o carbon-free su base oraria entro il 2030, con un target intermedio al 75% entro fine 2025 e un allineamento crescente agli obblighi pubblici per superare gli audit basati su autoregolamentazione e orientarsi, invece, verso una rendicontazione conforme agli obblighi normativi.

IL PUE NON BASTA PIÙ: LA SOSTENIBILITÀ DEI DATA CENTER PASSA DA EMISSIONI, ACQUA E RIUSO DEL CALORE

Decarbonizzazione "reale" e transizione verso il 24/7 carbon-free

L'evoluzione del settore non si gioca solo sulla quantità annuale di rinnovabili contrattate, ma sulla **coerenza oraria tra consumo e generazione a zero emissioni**.
Pioniere di questo approccio, **Google** misura da anni l'allineamento orario 24/7 integrando contratti di acquisto di energia a lungo termine (PPA) e certificati granulari per avvicinare il consumo di ciascun data center alla produzione locale di energia a zero emissioni: un paradigma che sta diventando riferimento anche per altri hyperscaler e operatori europei. L'IEA, nel report *Energy demand from AI* , stima che il **consumo elettrico dei data center possa raddoppiare fino a circa 945 TWh entro il 2030** nello scenario base (quasi il 3% dei consumi globali) con una crescita media del 15% annuo nel periodo 2024-2030 trainata anche da AI e nuove applicazioni. In questo contesto, la decarbonizzazione "aggiuntiva", che porta nuova capacità rinnovabile in rete e la usa nelle stesse ore del consumo, diventa discriminante rispetto a un semplice bilancio annuale di certificati.

Come cambia il bilancio di sostenibilità per un operatore europeo

Un bilancio di sostenibilità completo non è più solo CO_2. L'uso idrico finisce sotto i riflettori dei regulator e delle comunità locali, con pressioni per scegliere tecnologie di raffreddamento che minimizzino i consumi nei periodi critici e per documentare il WUE con la stessa precisione del PUE.
In molte città europee, inoltre, cresce l'attenzione per il recupero di calore verso reti di teleriscaldamento, che la stessa direttiva europea considera tra i KPI da tracciare nel database dei data center e che rappresenta una leva che può migliorare il valore ambientale e sociale dei progetti. L'effetto pratico delle nuove esigenze di reporting è una pressione "a monte" sulle scelte tecniche.

La stabilità del PUE a 1,54 segnala che la vera frontiera competitiva si sposta su tre assi: approvvigionamento energetico **a basse emissioni nelle stesse ore del consumo**; architetture termiche capaci di **ridurre WUE** e stress idrico; **misurazioni granulari e auditabili delle emissioni** Scope 1-2-3 (dirette, da energia acquistata, altre emissioni) per alimentare un bilancio di sostenibilità che risponda a CSRD ed ESRS.
Gli hyperscaler stanno già incorporando questi vincoli in target ambiziosi al 2030: nel caso di Microsoft, per esempio, carbon negative e water positive, con investimenti su rimozione di CO_2 e riduzione dei consumi idrici rientrano tra gli obiettivi descritti e tracciati nel report di sostenibilità 2025 dell'azienda.
Per un operatore europeo, il bilancio di sostenibilità 2025-2026 dovrà **integrare indicatori operativi e obiettivi coerenti con gli standard ESRS e il database previsto dalla direttiva EED:** inventario CO_2 con l'indice CUE e la quota di energia carbon-free per sito misurata ora per ora (24/7); indice WUE di uso dell'acqua con evidenza della stagionalità e delle misure di risparmio nei picchi; piani di recupero e riuso del calore e di collegamento al teleriscaldamento; percentuale di energia acquistata tramite contratti a lungo termine (PPA) aggiuntivi; roadmap per le emissioni Scope 3 legate alla filiera dell'hardware e alle fasi di costruzione. Il tutto dentro un contesto di domanda elettrica in accelerazione, che rende imprescindibile legare i progetti di capacità a strategie di decarbonizzazione "ora per ora" e a un dialogo trasparente con i territori.

Vertiv OneCore accelera il deployment dei data center

Stefano Mozzato, vice president marketing EMEA di Vertiv, illustra le nuove esigenze di raffreddamento dei data center ad alta densità e spiega perché la necessità di ridurre i tempi di attivazione orienti verso architetture ibride prefabbricate come Vertiv OneCore.

DI RICCARDO FLORIO

Stefano Mozzato
vice president marketing EMEA di Vertiv

Partiamo da un chiarimento di fondo. Perché ritiene che il concetto di data center non sia ancora ben compreso, soprattutto in relazione all'AI generativa?

Sento troppo spesso chi si focalizza sull'impatto che il consumo energetico dei data center può avere, soprattutto in relazione all'incremento richiesto dall'intelligenza artificiale generativa, senza considerare la catena del valore che queste infrastrutture attivano. Il data center è costituito da dispositivi di calcolo che trasformano energia in contenuti al servizio delle persone, che ampliano la conoscenza e la produttività: dalle previsioni del tempo, ai servizi in ambito sanità, al supporto nel lavoro e nella vita quotidiana.
Il progresso di un Paese non può prescindere dalla tecnologia e il consumo energetico dei data center è un trade-off positivo rispetto all'energia che andrebbe comunque spesa per eseguire in modo meno efficace le attività su cui ha un impatto diretto o indiretto.

In termini di efficienza, la tecnologia ha davvero ridotto il rapporto tra energia impiegata e risultato ottenuto?

Sì. La crescente richiesta di capacità di calcolo rende i server sempre più compatti e richiede raffreddamento a liquido. Il mio primo lavoro 35 anni fa mi portò a operare sul raffreddamento a liquido di un Cray Supercomputer che ai tempi consumava 25 kW, e che aveva un ingombro pari a metà stanza. Oggi, un sistema di raffreddamento a liquido che raffredda rack da 130 kW occupa poco più del volume di un armadio a un'anta. Questo viaggio dell'ottimizzazione ci porta verso quella che definiamo "unit of computing" che integra i server con l'infrastruttura che li contiene e li raffredda.

È qui che si inserisce il vostro approccio denominato OneCore. Che cos'è e perché lo avete lanciato ad agosto?

Vertiv OneCore è una soluzione infrastrutturale prefabbricata ibrida pensata per elevate densità di elaborazione e raffreddamento che integra moduli di potenza, di raffreddamento e la superstruttura Vertiv SmartRun. È disegnata intorno all'architettura di Nvidia e risponde all'esigenza di accorciare i tempi di messa in opera dei data center rispetto ai metodi tradizionali che non risultano più congruenti con i cicli di innovazione tecnologica come, per esempio, la frequenza di rilascio delle nuove generazioni di server. Oggi può accadere che, quando il data center è pronto, si trovi a dover operare con sistemi che sono già di una o addirittura due generazioni precedenti.

Quanto si accorcia il percorso da decisione a messa in esercizio con OneCore?

Dal classico orizzonte di 12-24 mesi si può arrivare a 8-12 mesi.

In che cosa OneCore si differenzia dal data center modulare prefabbricato?

Il data center modulare continua a essere prodotto e adottato ed è costituito da moduli prefabbricati: costruiti, te-

stati, smontati, spediti e riassemblati. Vertiv OneCore parte, invece, dal bisogno di ridurre i tempi adottando un approccio ibrido: non più soli moduli, ma vere e proprie unità prefabbricate integrate su basamento metallico che noi chiamiamo "skid", già cablate e collaudate, pronte per l'installazione in sito. Le tre macro aree infrastrutturali coperte sono i Power Modules (comprensivi di interruttori, UPS, batterie, distribuzione), il white space (con server, cablaggi in fibra, alimentazione) e la parte di distribuzione superiore che chiamiamo Vertiv SmartRun.

Spieghiamo meglio come è fatta questa distribuzione in modalità "sopra rack"?

Un data center ad alta densità da 10 MW può alloggiare un'ottantina di rack da circa 130 kW ciascuno ma, alimentarli e raffreddarli tutti, diventa estremamente complesso. I Vertiv SmartRun sono superstrutture prefabbricate alte circa due metri che si installano sopra i rack e distribuiscono, in modo pre-assemblato e collaudato, alimentazione elettrica, connettività e raffreddamento a liquido. Questo approccio favorisce le attività di manutenzione e riduce tempi di cantiere ed errori, perché i componenti critici vengono montati e testati in fabbrica, in ambiente controllato, mentre le attività richieste in sito sono unicamente quelle di eseguire l'assemblaggio e il collegamento e il successivo collaudo.

OneCore può innestarsi su data center esistenti o resta "isola a sé"?

Vertiv OneCore va pensato come una suite, stile Microsoft Office 365 e ti consente di sfruttare al meglio tutte le potenzialità dei singoli elementi. Rispetto a un'infrastruttura esistente si possono usare i pilastri costitutivi che lo compongono come il PowerTrain, che è la linea che si estende dalla media tensione fino al chip, sia della Cooling chain che integra tutti gli elementi per la gestione del trasferimento di calore, dal riuso dello stesso per riscaldamento distrettuale o all'uso del Freecooling senza usare una goccia d'acqua nel processo.

Il calore rilasciato sulla Cooling chain può quindi diventare una risorsa?

Sì. Lo chiamiamo calore "nobile": il liquido di raffreddamento esce a circa 50 gradi ed entra nella cosiddetta Secondary Fluid Network e potrebbe alimentare reti di teleriscaldamento ove vi siano le reti di distribuzione o come incentivo alla loro realizzazione.

In Italia avete già collegato data center a teleriscaldamento?

In Italia no. Esistono recuperi di calore interni agli edifici, ma non collegamenti a teleriscaldamento veri e propri cosa che invece abbiamo in altri progetti fuori Italia. Non dipende solo da noi: servono condizioni territoriali e prossimità. Ad esempio, l'idea di spostare i data center lontano dalla città va in conflitto con l'uso del calore dove serve e dove può produrre un vantaggio per la comunità.

Qual è oggi il limite nello sviluppo dei data center?

Il limite non è la tecnologia, ma la capacità di implementarla e utilizzarla. Vertiv, in questi anni, ha saputo interpretare con lucidità le evoluzioni del mercato, investendo con anticipo rispetto alle esigenze che sarebbero poi emerse.
È un percorso iniziato già nei primi anni 2000, con i primi colocation data center, e sostenuto da continui investimenti in ricerca e sviluppo nelle nostre sedi italiane — oggi riconosciute come un modello di riferimento a livello mondiale. Nel tempo, abbiamo consolidato questa visione attraverso acquisizioni strategiche mirate a integrare tecnologie complementari, creando sistemi capaci di confluire in soluzioni complete come **Vertiv OneCore**. Tra le più significative ricordiamo alcune:

- **E+I Engineering (2021)**, specializzata in blindosbarre di distribuzione e sistemi elettrici modulari, oggi parte integrante delle nostre soluzioni integrate.
- **Cooltera**, frutto di una lunga collaborazione e ora pienamente integrata nel portafoglio Vertiv per il liquid cooling
- **Great Lakes**, che rafforza e sviluppa la nostra presenza nell'ambito del white space.
- **Waylay NV**, azienda leader nel digital twin e nel monitoraggio real time basato su intelligenza artificiale, destinata a ridefinire il paradigma dei servizi di continuità attraverso il monitoraggio predittivo.

Come vi rapportate allo sviluppo tecnologico nel white space?

Vertiv è specializzata in data center e la competenza che abbiamo maturato ci pone una generazione oltre il mercato. Abbiamo relazioni di collaborazione molto strette con i vendor specializzati nella componente di elaborazione come NVIDIA e Intel. Per esempio, qualche mese fa NVIDIA ha annunciato le proprie soluzioni rack a 800 Volt in corrente continua insieme alle nostre soluzioni in grado di alimentarle e che arriveranno in commercio nel 2026. Il nostro approccio è di vivere nel futuro per essere sicuri che quello che viene portato nel presente sia esattamente ciò che serve a risolvere i bisogni del cliente di oggi e di domani.

Capacità, potenza e AI ridisegnano il mercato dei DATA CENTER

Domanda AI driven, colli di bottiglia elettrici e nuove geografie della capacità delineano un settore in espansione ma frenato dall'accesso alla potenza.

Il 2025 è l'anno in cui la crescita del digitale incontra i limiti fisici della rete. Le analisi convergono su un punto: l'accesso alla potenza è la priorità assoluta per owner e operator, insieme alla gestione dei costi e alle problematiche legate alla supply chain. La combinazione tra carichi AI ad alta densità e tempi lunghi di allaccio alla rete sta ridisegnando la pianificazione di campus e moduli, orientando gli investimenti verso siti con time to power più prevedibile.

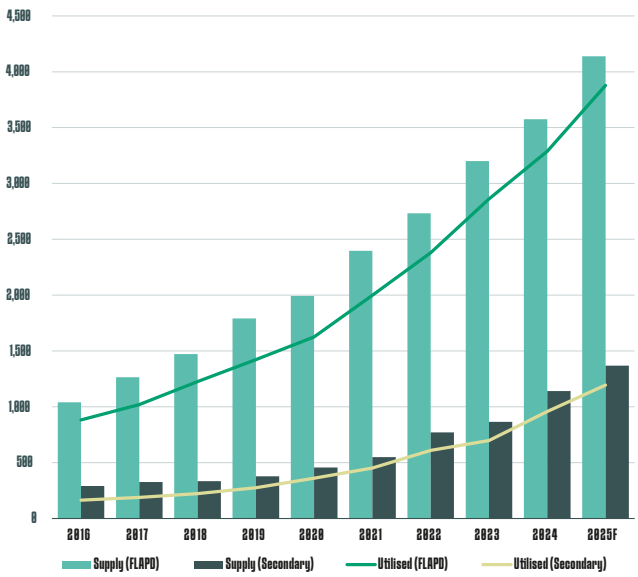
Vacancy compressa con l'ibrido che resta la norma

Dal lato dell'assorbimento, il mercato resta sotto pressione ma non uniforme con margini di saturazione di potenza IT e spazio. Un'analisi rilasciata a giugno 2025 da CBRE (Global Data Center Trends 2025) evidenzia una vacancy media globale al 6,6% nel primo trimestre 2025, in calo di oltre due punti su base annua; a Parigi il tasso scende dal 16,1% al 7,7% in dodici mesi, mentre la scarsità di potenza apre la strada a hotspot alternativi ai distretti storici. A livello continentale, Francoforte supera 1 GW di capacità operativa nel secondo trimestre 2025 ma il take up del primo semestre cala del 26% anno su anno a 272 MW, segnale di maggiore selettività negli impegni pluriennali. Il riequilibrio tra modelli di erogazione prosegue. Synergy Research stima 1.189 grandi data center hyperscale a fine primo trimestre 2025 e attribuisce agli hyperscaler il 44% della capacità mondiale, con trend verso quota 60% entro il 2030; la colocation non hyperscale pesa per il 22% e l'on prem il 34%. Nonostante la concentrazione, l'architettura ibrida (mix di on premise, colocation e cloud pubblico) resta dominante per i carichi regolati e a bassa latenza.

Capex in accelerazione e velocità di elettrificazione

Sul fronte degli investimenti, Dell'Oro Group prevede un capex cumulato di circa 1,2 trilioni di dollari al 2029, con crescita media annua del 21% e circa 50 GW addizionali trainati dagli acceleratori AI; metà della spesa farà capo agli hyperscaler. In Europa il 2025 è un anno record di nuova capacità in esercizio: 937 MW stimati, +43% sul 2024, oltre metà concentrata nei cinque hub FLAP D, con mercati adiacenti come Milano e Madrid in crescita a doppia cifra. Per chi pianifica oggi, la discriminante è la velocità di elettrificazione utile. L'incremento di densità spinto dall'AI impone architetture termiche in grado di sostenere 20–30 kW per rack e oltre senza sacrificare l'affidabilità. Gli "outage" con impatto sono in calo nel lungo periodo, ma nel 2025 quasi la metà resta legata alla catena della potenza, con gli UPS in prima linea, a conferma che la resilienza elettrica resta il vero differenziatore competitivo.

European market supply and utilisation, 2016-2025F (MW)



Source: CBRE Research, Q2 2025

DE-GUSTARE.IT
QUOTIDIANO ONLINE DI CIBO, VINO, BENESSERE E TURISMO

Dai più sapori alla vita

INQUADRA IL QRCODE
PER ISCRIVERTI ALLA NEWSLETTER DI

De-Gustare

CYBERTECH 2025

FA IL PUNTO SULLA CYBERSECURITY

Platea internazionale, sponsor di peso e un'agenda che mette al centro AI, difesa delle infrastrutture critiche, identità e compliance: l'edizione 2025 consolida il ruolo di Cybertech Europe come hub B2B di riferimento.

A CURA DELLA REDAZIONE

Si è chiusa a Roma l'edizione 2025 di Cybertech Europe, ospitata al centro congressi La Nuvola, con un riscontro di pubblico e di aziende che conferma la crescita dell'evento e il suo posizionamento nell'agenda europea della sicurezza digitale. La formula conferenza+expo ha favorito l'incontro tra C-level, responsabili della sicurezza, policy maker e vendor globali, con sessioni plenarie e momenti verticali dedicati ai settori regolati e alle infrastrutture strategiche, nel solco della tradizione che ha reso Cybertech una piattaforma internazionale per l'innovazione e il confronto professionale.
Direction è stata tra i media partner dell'evento, con una copertura dedicata ai momenti chiave della conferenza e dell'expo, interviste ai protagonisti e approfondimenti sui filoni tecnologici più rilevanti.
Sul palco hanno dominato alcuni assi ormai strutturali.

L'**AI PER LA SICUREZZA OPERATIVA**, inclusa la componente generativa, entra nei SOC con casi d'uso che vanno dalla correlazione alla risposta assistita.

L'**OT SECURITY** si conferma priorità per energia, trasporti e altre infrastrutture critiche, complice l'integrazione con cloud e 5G che impone modelli zero trust e telemetrie specialistiche.

IDENTITÀ E ACCESSO restano l'ossatura della difesa "identity-first", mentre threat intelligence e gestione continua dell'esposizione guidano la prioritizzazione del rischio in un'ottica orientata al business.

Sul **PIANO NORMATIVO** l'attenzione si concentra su NIS2, DORA e AI Act, con un approccio di compliance by design che allinea governance e supply chain europee.

In parallelo, si consolida un trend trasversale: la sicurezza sta assumendo i contorni più ampi della **CYBER RESILIENZA E DELLA GESTIONE DEL RISCHIO**. Non si tratta solo di prevenire e rilevare, ma di garantire continuità operativa, piani di risposta e ripristino orchestrati, governance del rischio integrata con gli obiettivi di business e comunicazione efficace verso board e supply chain.

Non sono mancati i filoni di frontiera, dal quantum alla space security, mentre temi come sovranità del cloud, DevSecOps e ransomware recovery hanno attraversato discussioni e showcase tecnologici dell'expo.

INFRASTRUTTURE CRITICHE

A CACCIA DI RESILIENZA

Servono telemetrie affidabili, controllo degli accessi e piani di ripristino dimostrabili per un'operatività senza interruzioni

Le infrastrutture critiche sono sistemi vivi in cui tecnologia e processo si sovrappongono a vincoli fisici, di sicurezza personale e di servizio pubblico. L'obiettivo non è soltanto ridurre la probabilità di un incidente informatico, ma assicurare che, qualora accada, la fornitura di energia non si fermi, i treni non rimangano in stazione, gli ospedali non sospendano triage e cartelle cliniche, i pagamenti non vadano in stallo. In questi contesti, **protezione del dato e continuità del servizio diventano la stessa cosa:** l'integrità delle informazioni alimenta le decisioni operative, mentre la disponibilità dei sistemi dipende dalla qualità con cui quelle informazioni sono raccolte, custodite e recuperate.

Dal campo al cloud senza perdere il controllo

L'interconnessione di impianti e reti con cloud, 5G e IoT ha ampliato la superficie d'attacco ma, soprattutto, ha reso più complessa la catena della fiducia. I sensori sul campo generano telemetrie che si muovono su segmenti di rete eterogenei, attraversano gateway, piattaforme di messaggistica e altre dove i dati vengono normalizzati, arricchiti e correlati con fonti esterne. La priorità è garantire che ogni passaggio **mantenga provenienza, coerenza e tempi certi.**

Il controllo degli accessi deve riflettere questa catena; servono identità forti per operatori e workload, principi di minimo privilegio, segregazione netta tra il dominio informatico (IT) e quello dell'operatività industriale (OT), federazione delle identità dove più ambienti cooperano. Il risultato atteso non è una barriera monolitica, ma una serie di controlli coerenti che accompagnano il dato dalla periferia alla decisione, riducendo gli errori di configurazione e impedendo ai cybercriminali i possibili movimenti laterali all'interno del perimetro aziendale.

La sicurezza industriale che si integra con i processi senza bloccarli

L'evoluzione della sicurezza OT ovvero associata agli impianti industriali non può limitarsi alla messa in sicurezza di PLC, SCADA e reti. L'obiettivo è **inserire la difesa dentro il ritmo operativo di impianti e reti, evitando azioni che interrompano la produzione** o i flussi operativi.

Il monitoraggio passivo del traffico industriale, l'inventario continuo degli asset e la rilevazione di anomalie di protocolli devono aiutare a individuare possibili anomalie senza "toccare" dispositivi critici o influenzare finestre di manutenzione molto ridotte.

In parallelo, il **dialogo con i sistemi di gestione del cambiamento e con le sale operative** diventa strutturale, perché un allarme che non distingue tra manutenzione programmata e comportamento malevolo genera falso rumore; così come una regola che scatta in orario di picco può bloccare più di quanto protegga.

L'integrazione con l'identità aziendale, infine, è ciò che consente di legare ogni azione a un soggetto verificato, mentre la segmentazione di rete e l'adozione di modelli zero trust impediscono che un singolo punto debole diventi un guasto sistemico.

L'AI, quando i dati sono affidabili, consente allora di accelerare la correlazione tra telemetrie OT e indicatori IT, mettendo in relazione eventi che, presi isolatamente, sembrano innocui, ma che insieme delineano un attacco in corso.

INTELLIGENZA ARTIFICIALE

MOTORE DELLA SICUREZZA OPERATIVA

Meno rumore, decisioni più veloci e coerenti, risposte più ordinate e misurabili, con la giusta dose di controllo umano e una chiara responsabilità sui risultati: le promesse dell'uso di AI nei SOC

Nei Security operation center l'adozione dell'AI non è un abbellimento tecnologico, ma un cambio di paradigma che tocca l'intera catena di valore: dalla normalizzazione dei log alla correlazione degli eventi, dal filtro al contenimento, fino alla comunicazione verso i team IT e il management. Il punto **non è sostituire gli analisti, bensì farli lavorare su problemi a maggiore impatto**, delegando alle macchine le attività ripetitive e ad alta intensità dati. Questo implica scelte architetturali chiare, una governance dei modelli, un'integrazione accurata con lo stack esistente e, soprattutto, metriche che rendano visibile il miglioramento operativo e il rischio residuo.

Dal "rumore" al segnale utile nei SOC

La promessa più concreta dell'AI nei Security Operation Center (SOC) è la **riduzione del rumore.** Modelli addestrati su grandi volumi di dati aiutano a correlare indicatori eterogenei e a raggruppare avvisi provenienti da diverse fonti che descrivono lo stesso incidente.
L'assistente AI è in grado di proporre una Timeline coerente, di evidenziare le dipendenze fra host, identità e processi e di suggerire le ipotesi più plausibili da verificare. È in questa fase che si gioca gran parte della diminuzione dei tempi di detection: meno falsi positivi, meno "alert fatigue", maggiore priorità agli eventi davvero rilevanti.
Affinché, però, tutto ciò possa funzionare è **richiesta la qualità del dato:** completezza, aggiornamento, coerenza semantica tra fonti sono i prerequisiti che abilitano la correlazione intelligente.

Filtro e risposta automatizzata con controllo umano

La **selezione degli eventi di sicurezza rilevanti** è l'altro collo di bottiglia che l'AI è in grado di affrontare bene. I modelli classificano gli eventi per severità e affidabilità, propongono le "next-best-action" e producono automaticamente report descrittivi comprensibili anche dei manager. Nei SOC più avanzati, l'automazione esegue procedure operative standard (i cosiddetti playbook) di contenimento su scenari ricorrenti quali: isolamento di endpoint compromessi, revoca di token sospetti, forzatura del cambio password, blocco di domini e hash noti.

QUANTUM COMPUTING E CYBERSECURITY

Il quantum computing introduce una discontinuità che la sicurezza non può ignorare: gli algoritmi crittografici più diffusi potrebbero diventare vulnerabili quando capacità quantistiche sufficienti saranno disponibili. L'orizzonte operativo si chiama **crittografia post-quantum**, un insieme di schemi progettati per resistere ad attacchi quantistici e selezionati perché implementabili su larga scala. Il rischio immediato non è solo teorico, perché modelli "harvest now, decrypt later" spingono attori malevoli a raccogliere oggi dati cifrati con l'aspettativa di decifrarli domani; per alcuni settori con obblighi di riservatezza di lungo periodo, la finestra di esposizione è già aperta.

La chiave in tutto ciò è il **principio "human-in-the-loop": l'AI può orchestrare e pre-compilare, ma l'azione finale deve restare approvata da un analista**, con soglie e policy differenti a seconda del rischio e del contesto. Questo compromesso riduce i tempi senza generare effetti collaterali ingestibili in produzione. Laddove l'organizzazione sia pronta, alcune classi di playbook possono passare in "auto-pilot" fuori dall'orario di ufficio, lasciando agli esperti la revisione a posteriori.

NORMATIVA EUROPEA E GOVERNO DELLA SICUREZZA

NIS2, DORA e AI Act non sono solo normative, ma strumenti per rendere la sicurezza misurabile e governabile. La **loro forza sta nella capacità di allineare obiettivi tecnici e linguaggio del board**, definendo responsabilità, requisiti minimi e pratiche verificabili lungo tutta la filiera. I modelli più efficaci attribuiscono sponsorship a livello esecutivo, integrano la sicurezza nel risk management aziendale e chiariscono i ruoli tra operatività, controllo e audit. Un impatto rilevante riguarda la supply chain: le norme spostano il focus dai confini aziendali al ciclo di vita del fornitore, introducendo due diligence, requisiti contrattuali, attestazioni periodiche e meccanismi di escalation.

Integrazione con gli stack esistenti

Il valore nasce anche dall'integrazione profonda con gli strumenti già in campo. L'AI deve poter "vedere" telemetrie ricche e aggiornate provenienti da SIEM (Security Information and Event Management) e data lake di sicurezza, interrogare in tempo reale EDR/XDR, sistemi di gestione dell'identità e infrastrutture cloud e orchestrare esecuzioni tramite sistemi SOAR (Security orchestration, automation and response) o piattaforme di automazione equivalenti.

In pratica, l'**adozione segue percorsi incrementali**. Si parte spesso da assistenti che accelerano le indagini per poi spostare l'asticella verso l'automazione di azioni di contenimento in casi d'uso ad alta ripetitività e basso rischio operativo.

Un altro passo cruciale è l'unificazione del contesto. Collegare criticità tecniche e impatto business consente, infatti, all'AI di proporre priorità che riflettono davvero il rischio per l'organizzazione, e non solo la "rumorosità" dell'evento.

DALLA CYBERSECURITY ALLA CYBER RESILIENZA

Il passaggio dal "non deve accadere" al "deve continuare a funzionare" è ormai sancito. La cyber resilienza ribalta la prospettiva spostando il focus sulla **garanzia di continuità dei servizi essenziali e di un ritorno alla normalità rapido**, tracciabile e ripetibile. Questo approccio integra tecnologia, processi e governance in un unico modello operativo, in cui orchestrazione, ripristino testabile e priorità basate sul rischio diventano routine. L'orchestrazione della risposta collega rilevamento, decisione ed esecuzione, definendo chi approva cosa, con quali soglie e in quali tempi; l'automazione accelera le azioni ricorrenti, mentre il controllo umano presidia gli snodi critici. In questo modo le metriche smettono di essere esercizi di stile e diventano veri e propri strumenti decisionali.

Metriche che contano per un percorso praticabile

Senza misure condivise l'AI resta però un mero esercizio di stile. Di conseguenza, oltre alle definizioni classiche di MTTD (Mean Time To Detect) e MTTR (Mean Time To Restore) è utile spostare la conversazione su indicatori leggibili da tutta l'organizzazione: per esempio la riduzione del tempo di analisi per classe d'incidente, la percentuale di falsi positivi eliminati e la variazione del rischio residuo su asset critici. Collegare queste metriche agli obiettivi operativi (SLA applicativi, disponibilità di servizi, obblighi normativi) è ciò che consente di dimostrare il ritorno dell'investimento.

Per ottenere risultati tangibili è, inoltre, utile **seguire una roadmap realistica**. Si parte da casi d'uso ristretti e ad alta ripetitività, con dataset solidi e playbook già in produzione. Si innesta l'AI come acceleratore dell'analisi per poi estendere le automazioni di risposta dove il rischio è governabile, mantenendo approvazioni umane e limiti chiari.

In parallelo va costruita la disciplina associata a data governance, alla modalità di costruzione e implementazione dell'AI e ai controlli di qualità e di trasparenza delle decisioni, finché **l'AI diventa un componente naturale del SOC, non un progetto a latere**. Quando le metriche mostrano che il tempo di detection si accorcia, i falsi positivi calano e il rischio residuo scende su asset ad alta priorità, allora l'adozione ha senso anche per il board e per chi deve garantire continuità operativa.

OpenText: la business continuity prima di tutto

DI RICCARDO FLORIO

PIERPAOLO ALÌ, DIRECTOR SOUTHERN EUROPE, OPENTEXT CYBERSECURITY SPIEGA PERCHÉ LA BUSINESS CONTINUITY DEVE ESSERE AL CENTRO DELLA SICUREZZA ALL'INSEGNA DI UN MODELLO DI CYBER RESILIENZA CAPACE DI CONIUGARE ATTIVITÀ PREVENTIVA, IDENTIFICAZIONE DELLE MINACCE E CAPACITÀ DI RISPOSTA

Quali devono essere gli obiettivi prioritari in materia di sicurezza per un'azienda?

La priorità è la continuità operativa. La sicurezza non è un fine in sé, ma la condizione perché servizi e processi restino disponibili, i dati rimangano integri e gli SLA siano rispettati anche durante un incidente. In un contesto in cui catene digitali e fornitori sono interdipendenti, l'azienda deve essere in grado di erogare servizi senza interruzioni, preservare la fiducia dei clienti e proteggere la propria capacità di generare ricavi. **Prevenzione e capacità di restare operativi** sono parti del medesimo disegno strategico: la maturità della sicurezza di un'azienda non si misura soltanto dai tentativi bloccati, ma dalla capacità di continuare a funzionare quando qualcosa va storto, limitando l'impatto economico e reputazionale.

Dal punto di vista tecnologico, come si affrontano i rischi in modo efficace?

Le tecnologie sono essenziali e devono intervenire, innanzitutto, in chiave preventiva, ma non è sufficiente un impianto fondato su regole statiche e "signature". I cyber criminali cambiano continuamente tattiche e tecniche di movimento laterale con una velocità che impone **piattaforme capaci di combinare analytics avanzati, AI e threat intelligence**, con una telemetria ampia che includa utenti, endpoint, server, workload cloud e traffico di rete. Serve la capacità di distinguere ciò che conta dal rumore, portando in superficie i segnali deboli che anticipano un incidente. Il contributo della tecnologia va però sostenuto integrandola all'interno di processi chiari, con ruoli e responsabilità definiti, metriche condivise con il business e tempi decisionali compatibili con le finestre operative.

Cosa serve oltre alla prevenzione?

La capacità di essere cyber resilienti. Dobbiamo assumere che l'invulnerabilità al 100% non esista. Neppure per chi utilizza le migliori tecnologie disponibili. L'obiettivo è **ridurre la probabilità di compromissione** e, se accade, garantire che l'azienda continui a erogare servizi senza impatti percepiti dai clienti,

mentre i "runbook" di risposta riportano rapidamente la normalità. Questo richiede segmentazione e isolamento selettivo, orchestrazione del ripristino, replica dei dati, comunicazione coordinata verso stakeholder interni ed esterni e una disciplina di esercitazioni periodiche. In questa prospettiva, RPO (Recovery Point Objective) e RTO (Recovery Time Objective) cesano di essere metriche solo IT e diventano KPI di business, perché definiscono la perdita di dati ammissibile e il tempo di indisponibilità compatibile con gli obiettivi economici.

OpenText come abilita in pratica questo modello?

Mettiamo insieme tre dimensioni complementari. La prima è la visibilità "oltre il perimetro",: visibilità esterna, analisi comportamentale interna e risposta coordinata. All'esterno partiamo dall'analisi globale degli indicatori di minacce: **OpenText Adversary Signals (già ArcSight cyDNA)** osserva su scala Internet l'infrastruttura e le tracce operative degli attori di minaccia, anticipando tattiche e metodi prima che giungano alle porte dell'azienda. All'interno dell'organizzazione, **OpenText Core Threat Detection and Response** effettua analisi comportamentali (UEBA) con machine learning non supervisionato per evidenziare comportamenti anomali di utenti, endpoint e workload, riducendo il rumore nel SOC e spostando il focus sugli eventi realmente rilevanti, integrandosi nativamente con gli ecosistemi di sicurezza Microsoft. La threat intelligence operativa **BrightCloud** alimenta reputazione di domini e IP, rilevazione di phishing e classificazioni Web in tempo reale. Infine, per garantire continuità e ripartenza veloce, le tecnologie **Carbonite** e **Webroot** nel portafoglio OpenText abilitano backup, replica e disaster recovery orchestrati.

Accesso e gestione dell'identità che ruolo hanno nella cyber resilienza?

L'identità è il nuovo perimetro e non riguarda più soltanto le persone. Oggi parliamo di identità di utenti, dispositivi, applicazioni, API e workload. Tutte queste identità definiscono la superficie di attacco reale. La cyber resilienza richiede un **modello IAM** che tenga insieme autenticazione forte, controllo degli accessi basato sul rischio, governance delle identità secondo il principio del minimo privilegio e una correlazione continua con i segnali comportamentali. È qui che si sommano tre esigenze: **ridurre l'esposizione preventiva**, **riconoscere tempestivamente gli abusi d'identità** e **limitare l'effetto domino** in caso di compromissione. In OpenText facciamo lavorare in modo coerente e coordinato le soluzioni di access management, identity governance e autenticazione avanzata con il motore di analisi comportamentale: l'anomalia non è solo un alert, diventa un input per modificare in tempo reale le decisioni di accesso, rafforzare la verifica o isolare un contesto finché l'analisi non è conclusa.

E per la protezione dei dati?

È un altro tassello complementare e imprescindibile della cyber resilienza. A queste esigenze OpenText dedica una serie di soluzioni specifiche (in precedenza riunite all'interno del brand Voltage - N.d.R.) e siamo l'unico vendor che, grazie a tecnologie di mascheramento brevettate, non si limita a cifrare i dati in condizione di riposo o in transito, ma anche durante l'uso pur preservandone la referenzialità funzionale.

Parliamo di compliance, a partire da NIS2

NIS2 rende cogente una gestione del rischio strutturata e la capacità di notificare gli incidenti entro finestre temporali precise, con tracciabilità e auditabilità delle evidenze. La nostra piattaforma supporta l'intero ciclo: misure preventive e di detection documentabili; telemetria e correlazioni utili per le notifiche tempestive agli stakeholder; meccanismi di replica e ripristino per garantire la resilienza del servizio. In questo modo tecnologia e governance si rafforzano a vicenda e l'allineamento ai requisiti normativi diventa più lineare. Inoltre, NIS2 richiede pratiche di sviluppo e codice sicuro lungo tutto il ciclo di vita del software: in questo ambito OpenText garantisce copertura con le soluzioni **Fortify**, da anni riconosciute come riferimento di mercato per la sicurezza applicativa.

L'AI è amica o nemica della sicurezza?

È entrambe le cose. L'AI oggi potenzia anche i criminali, dalla generazione di codice alla social engineering. Ma, **se ben adottata, è un moltiplicatore di difesa:** consente di riconoscere pattern anomali invisibili alle regole statiche e di passare da un approccio reattivo a uno preventivo. Serve però un salto di maturità: protezione rigorosa di credenziali e proprietà intellettuale, autenticazione forte, segregazione dei privilegi, responsabilità individuale e cultura della sicurezza guidata dal top management. OpenText porta un'esperienza pluridecennale di machine learning applicato alla security e la incorpora nelle sue soluzioni per renderla realmente efficace e fruibile dalle aziende.

La **stampa**, un grande rischio di **sicurezza** spesso sottovalutato

Connessione alla rete, memoria interna e sistemi operativi proprietari rendono multifunzione e stampanti endpoint che possono rappresentare una facile via di accesso per i cybercriminali. Un efficace sistema di difesa è l'approccio Triple Layer Security proposto da Brother, basato su protezione del dispositivo, del documento e della rete

DI FABRIZIO PINCELLI

Per anni le stampanti sono state considerate semplici periferiche di output, ma l'evoluzione tecnologica le ha trasformate in veri endpoint intelligenti, connessi alla rete, dotati di memoria, firmware e sistemi operativi proprietari. Questa metamorfosi ha introdotto nuove superfici d'attacco e implicazioni dirette in termini di governance, compliance e gestione del rischio di cybersecurity. Al punto che, secondo una ricerca *IDC*, oltre un quarto dei responsabili IT dichiara di aver subito **violazioni legate a dispositivi di stampa non protetti** nell'ultimo anno, segno che la sicurezza di stampa è ancora troppo spesso sottovalutata.

Tre livelli di sicurezza

Brother ha adottato il modello **Triple Layer Security**, un framework a tre livelli (dispositivo, documento e rete) che affronta la protezione dei dati in modo sistemico e coerente lungo l'intero ciclo di vita informativo. L'obiettivo è garantire che la sicurezza non si esaurisca nel perimetro logico, ma si estenda fino all'output fisico, assicurando la confidenzialità e l'integrità del dato dalla generazione alla stampa.

Livello 1: l'endpoint fisico sotto controllo

Il primo livello riguarda la sicurezza del dispositivo, intesa come hardening dell'endpoint fisico e del software residente. Ogni stampante multifunzione è un sistema embedded completo, con interfacce di amministrazione, porte di comunicazione e firmware aggiornabile. Se non correttamente gestiti, questi elementi rappresentano vettori di compromissione. Brother applica **misure di protezione multilivello**: firma digitale dei firmware, blocco delle impostazioni critiche, restrizione delle funzioni per utente e autenticazione obbligatoria tramite badge NFC, smart card o credenziali Active Directory. Questa gestione dei privilegi consente di **controllare puntualmente l'accesso alle funzioni di stampa**, copia e scansione, assicurando che solo utenti autorizzati possano operare sui dispositivi.

Nei modelli più avanzati, l'assenza di dischi rigidi interni riduce la persistenza dei dati, mentre nei sistemi che ne dispongono la crittografia hardware AES-256 e la cancellazione automatica dei file temporanei eliminano il rischio di recupero forense. Tuttavia, la robustezza tecnologica non sostituisce la corretta configurazione: password predefinite, firmware obsoleti o protocolli non cifrati restano le cause più comuni di esposizione.

Livello 2: protezione e tracciabilità del dato

Il secondo livello del modello riguarda la **sicurezza dei documenti, ovvero la protezione dei dati che transitano nel flusso di stampa e scansione**. Le vulnerabilità più frequenti

derivano da job lasciati incustoditi nei vassoi di uscita o da trasmissioni in chiaro sulla rete. Soluzioni come **Secure Print e Secure Print+** consentono di trattenere i lavori in coda fino all'autenticazione fisica dell'utente, riducendo drasticamente il rischio di accesso accidentale o doloso ai documenti. La cifratura delle comunicazioni tra PC, server e stampante tramite protocolli TLS o SSL garantisce la protezione dei dati in transito, mentre la scansione verso cartelle di rete o indirizzi e-mail utilizza canali protetti (SMBv3, SFTP, HTTPS). L'integrità dei documenti è ulteriormente salvaguardata tramite firme digitali e password di protezione per i PDF.

Nei **contesti enterprise**, l'integrazione con piattaforme di document management o soluzioni di **Managed print services (MPS)**, come **Pagine+** di Brother, consente una tracciabilità completa delle operazioni. Sistemi di watermarking, log di audit e report centralizzati permettono di associare ogni stampa o scansione a un utente identificato, garantendo accountability e conformità al GDPR. In caso di incidenti o data breach, l'audit trail fornisce elementi di prova forense indispensabili per ricostruire l'origine dell'anomalia.

Livello 3: il perimetro invisibile della stampa

Il terzo livello, la **sicurezza di rete**, è probabilmente il più delicato, perché la stampante è a tutti gli effetti un nodo connesso. Senza adeguati controlli, può essere sfruttata come punto d'ingresso per attacchi laterali o esfiltrazioni di dati. Brother integra nei propri dispositivi firewall interni, **filtri IP e protocolli di autenticazione IEEE 802.1X**, che consentono di validare la legittimità del dispositivo sulla rete prima di concedergli accesso. L'adozione di protocolli cifrati come HTTPS e IPPS sostituisce le connessioni in chiaro, mentre IPsec assicura la protezione a livello di pacchetto.

La **segmentazione VLAN** rappresenta un ulteriore livello di difesa: isolare i dispositivi di stampa in reti dedicate riduce la possibilità di propagazione di minacce in caso di compromissione. Inoltre, l'integrazione con sistemi di logging centralizzati come Syslog e SNMPv3 consente di rilevare in tempo reale comportamenti anomali o tentativi di accesso non autorizzato. L'obiettivo è far rientrare i dispositivi di stampa all'interno delle politiche di sicurezza e monitoraggio già applicate a server, endpoint e apparati di rete.

Cloud, BYOD e obsolescenza tecnologica

La complessità aumenta con la diffusione di modelli di lavoro ibridi e BYOD. Ogni dispositivo personale che accede a una rete aziendale rappresenta un potenziale vettore di rischio. La stampa mobile o cloud, se non adeguatamente protetta, può diventare un canale d'ingresso per malware o un punto di fuga di informazioni sensibili. Soluzioni come **Brother Cloud Secure Print** affrontano questo scenario garantendo la trasmissione cifrata dei job e l'autenticazione dell'utente, preservando la coerenza con le policy di sicurezza aziendali anche fuori dal perimetro tradizionale.

Un ulteriore elemento di vulnerabilità deriva dall'obsolescenza tecnologica. Dispositivi non aggiornati o privi di supporto per protocolli moderni non solo aumentano il rischio di exploit, ma rendono più difficile la conformità alle normative sulla protezione dei dati. In questi casi, la mitigazione passa da strategie di asset management e segmentazione, oltre che da politiche di sostituzione programmata del parco macchine. Anche la diversità dei modelli in uso può complicare la gestione delle policy di sicurezza, richiedendo piattaforme di controllo centralizzato capaci di uniformare la configurazione e gli aggiornamenti.

La sicurezza di stampa come parte della governance IT

Sul piano organizzativo, la sicurezza della stampa deve essere integrata nella governance IT aziendale. Occorrono procedure di onboarding e decommissioning dei dispositivi, policy di gestione delle credenziali e formazione degli utenti. La sicurezza tecnologica, infatti, perde efficacia se non è accompagnata da comportamenti consapevoli: documenti sensibili lasciati nei vassoi di uscita o credenziali condivise tra colleghi rappresentano vulnerabilità tanto gravi quanto una vulnerabilità software. È quindi necessario un approccio che combini strumenti, processi e cultura della sicurezza.

Qualys gestisce i rischi parlando il linguaggio del business

DI RICCARDO FLORIO

PER IL CEO SUMEDH THAKAR LA DOMANDA CHE CONTA NON È QUALE TECNOLOGIA ADOTTARE, MA QUANTO INVESTIRE PER ABBATTERE IL RISCHIO ECONOMICO. IL PASSAGGIO È DALLA MERA VISIBILITÀ ALLA REMEDIATION, FINO AL RISK OPERATIONS CENTER CHE RENDE LA GESTIONE DEL RISCHIO UN PROCESSO OPERATIVO

"Tre anni fa nessuno avrebbe previsto il cambiamento così profondo in così poco tempo portato dall'AI. Questo insegna che non sappiamo quale tecnologia sarà davvero dirompente nei prossimi anni. Ma c'è una domanda che per ogni azienda rimarrà sempre la stessa: quanto denaro dobbiamo spendere in cybersecurity per gestire il rischio dell'organizzazione?"

Sumedh Thakar, CEO di Qualys, riporta la conversazione sul terreno che interessa al board e alla direzione finanziaria. **La sicurezza**, spiega, è essenzialmente **un esercizio di risk management:** si investe una certa cifra per ridurre una certa probabilità di perdita dovuta ad attacchi digitali. È un linguaggio di business, non di tecnologia, mentre lo scenario da affrontare diventa sempre più critico.

Se vent'anni fa, infatti, si scansionava la rete ogni trimestre e si dava all'IT tre mesi per sistemare tutto, oggi gli attacchi si succedono alla velocità delle ore, non dei mesi. Oggi la cybersecurity coinvolge sempre più stakeholder, incluso il CFO, e il tema chiave, secondo Thakar, è quanto velocemente si correggono i problemi perché la sola scansione, in assenza di remediation, non riduce il rischio.

Oltre l'attack surface verso la risk surface

Il mercato resta concentrato sul tema della **gestione della superficie di attacco,** ma per Thakar non basta.

"Occorre spingersi oltre, verso ciò che chiamiamo risk surface management. L'errore tipico è spendere mezzo milione di dollari per coprire una superficie d'attacco che, magari, tradotta in perdita attesa, ne vale 50mila. È qui che CFO e consiglio di amministrazione incalzano chiedendo qual è il modo corretto di pensare alla sicurezza e come allineare ogni cosa al risk management in termini economici. Questo è l'aspetto su cui si focalizza Qualys".

Il punto, insiste il CEO di Qualys, è accettare che l'infrastruttura IT si è molto espansa, il codice distribuito è esploso e il numero di vulnerabilità scoperte ogni giorno cresce più in fretta dei budget.

> ***Il ROC introduce un modello operativo di gestione del rischio che riunisce tecnologia, quantificazione economica e remediation***

*"In qualunque momento, solo una piccola parte dei problemi rilevati, spesso meno del 5%, genera un **rischio economico per l'azienda.** La priorità deve essere quella di individuare questa frazione e ridurla prima degli attaccanti".*

Misurare, comunicare, mitigare

Thakar sintetizza il ruolo che deve avere il partner tecnologico in gestione del rischio in tre verbi: misurare, comunicare, mitigare; con il secondo che appare il più trascurato.
*"Molti strumenti misurano, alcuni aiutano a correggere. **Quasi nessuno ti aiuta a comunicare il rischio.** Eppure è decisivo. Se dici alle persone IT 'ecco migliaia di vulnerabilità da correggere', ti detesteranno perché hanno altre priorità; ma sono costretti a farlo, impiegano enormi energie, sistemano tutto e l'unico 'grazie' che ricevono è un nuovo elenco altrettanto lungo. Se invece la conversazione fosse 'se risolvete queste 50 criticità riducete dell'80% il rischio di perdere 500 milioni di euro', il messaggio cambia completamente ed è infinitamente più efficace".*
La stessa logica vale con il CFO.
*"**Il CFO non vuole sentir parlare di sigle tecniche come MFA o ZTNA**, vuole Euro. Se una business unit fattura 500 milioni l'anno e un attacco può costare 10 milioni al giorno, ciò che conta è quanto possiamo abbassare la probabilità di quell'evento e a quale costo. Se con 300mila dollari portiamo un rischio su scala 0-100 da 80 a 40 questo sblocca i budget".*
Nella comunicazione con il board, aggiunge, non esiste il rischio zero. Va chiarito cosa si **mitiga** con tecnologia e processi, cosa si **accetta** e quale quota si **trasferisce** all'assicurazione cyber: questa deve essere la grammatica del rischio, che va resa operativa nella sicurezza come in qualunque altra area aziendale.

Dalla visibilità alla remediation continua

La strategia di Qualys nasce da una convinzione semplice: la **conoscenza del rischio da sola non rende più sicuri.**
*"La differenza la fa la capacità di **remediation** prima degli attaccanti. Se arrivano prima loro, hai una compromissione; se arriviamo prima noi, difendiamo l'azienda".*
In linea con questo principio Qualys ha introdotto da tempo nel vulnerability management il **collegamento tra detection e patching automation** portando nella cybersecurity un tema considerato appannaggio dell'IT e arrivando a distribuire, nel solo 2024, 113 milioni di patch negli ambienti dei clienti, tramite i propri agent.
Oggi Qualys serve **oltre 10mila clienti** con **circa 2.600 dipendenti** nel mondo, ma la sfida, sottolinea Thakar, è soprattutto metodologica: spostare il baricentro delle metriche dalla conta di vulnerabilità e configurazioni errate alla **riduzione di rischio quantificata** in termini economici.

Nasce il Risk Operations Center (ROC)

*"Il concetto di SOC (Security operations center) è ben formalizzato nel mercato per correlare segnali e rilevare le violazioni post-attacco, ovvero dopo che un aggressore è riuscito a entrare nel perimetro aziendale. Mancava l'equivalente pre-breach, capace di orchestrare persone, processi e strumenti per un esercizio ripetibile di **risk management operativo**".*
Per questo Qualys ha introdotto il **ROC, il Risk Operations Center**: un modello operativo che parte da un **inventario degli asset** affidabile, **aggregazione dei fattori di rischio** dai diversi tool (anche non Qualys), **contestualizzazione con threat intelligence** e, soprattutto, c**ontestualizzazione di business.**
*"Se una business unit ha un risk score pari a 900 su una scala di 1000 e un'altra di 750, si è soliti partire dalla prima per eliminare il rischio. Ma se la prima business unit fattura 2 milioni e la seconda 500 milioni, la priorità va, invece, invertita. Da ciò si comprende come **portare la quantificazione economica nel flusso decisionale cambi la remediation**".*
Ultimo tassello, la **compliance**: il rischio di fermo per non conformità fa parte del rischio d'impresa e in larga misura nasce da lacune cyber.
Il ROC punta, dunque, a unire le componenti tecniche, la quantificazione economica e la remediation in un unico workflow.
*"In Qualys abbiamo creato la nostra versione di ROC che viene messa a disposizione tramite il cloud. Lo chiamiamo **Enterprise True Risk Management** perché si tratta di gestire il rischio reale e non solo di individuare i problemi. La nostra piattaforma è aperta ed è in grado di acquisire dati provenienti non solo da Qualys, ma **anche da altri strumenti di terze parti inclusi i nostri competitor**, da Tenable, a Rapid7 a ServiceNow. Perché i clienti non vogliono stravolgere il loro stack, ma chiedono invece di valorizzare ciò che hanno in modo più automatizzato e orientato al rischio".*

ESET cresce puntando sulla tecnologia

DI RICCARDO FLORIO

SPINTA DALLA SOLIDITÀ DELLE PROPRIE SOLUZIONI, L'AZIENDA SLOVACCA CONSOLIDA LA POSIZIONE NEL MID-MARKET E ACCELERA VERSO L'ENTERPRISE, CON SERVIZI GESTITI, FORMAZIONE E CLOUD COME LEVE DI CRESCITA. L'INCONTRO CON PAVOL HOLÉCZY, PRESIDENT EMEA REGION DELL'AZIENDA

All'ultimo piano di un moderno edificio di Bratislava, decine di esperti di cybersecurity analizzano flussi di sicurezza provenienti da oltre 110 milioni di "sonde" della rete LiveGrid distribuite in tutto il mondo, valutano gli scenari di minaccia, individuano le vulnerabilità e predispongono avvisi e contromisure in tempo reale. Sono gli specialisti del **Security operation center di ESET**, la più importante azienda tecnologica della Slovacchia, fornitore globale di soluzioni per la protezione e la sicurezza informatica. Fondata nel 1992 e diventata nota in tutto il mondo per l'efficacia dell'antivirus Nod32, Eset ha progressivamente ampliato il proprio raggio d'azione fino a proporsi come vendor di cybersecurity a spettro più ampio.

Oggi ESET propone la piattaforma unificata di sicurezza **ESET Protect,** che copre endpoint, server, mobile e workload cloud con prevenzione multilivello, EDR/XDR **(ESET Inspect)**, protezione email e Cloud Office Security per Microsoft 365, più cifratura, gestione delle patch e servizi MDR. Il portafoglio è completato da threat intelligence e formazione per la security awareness, con delivery cloud-first e opzione on-prem.

Nel 2024 ha registrato ricavi globali pari a 691 milioni di euro, confermando un percorso di crescita sostenuto che, nel 2025, potrebbe superare gli 800 milioni. È un'azienda interamente privata, ancora guidata dai fondatori, che punta sul valore tecnologico delle soluzioni sviluppate in casa e sulla propria identità di vendor europeo, radicato nel Vecchio continente e allineato ai requisiti normativi dell'Unione.

In Italia, l'azienda è guidata da Fabio Buccigrossi e opera quasi esclusivamente tramite il Canale, mettendo a disposizione delle aziende un SOC dedicato presente sul nostro territorio che fornisce sevizi di assistenza in lingua italiana con copertura 24/7, erogati da personale locale.

Pavol Holéczy, President Emea Region di ESET illustra progetti e strategie della società.

Quali sono i vostri piani per il prossimo futuro?

Nei prossimi cinque anni vogliamo consolidare la posizione raggiunta sul mercato. Il focus sarà sulla crescita dei servizi e sulla formazione delle persone. Il pilastro principale sono i professional service: vogliamo poter gestire l'ambiente del cliente con competenza diretta, anche in lingua locale, come avviene già in Italia, perché lo riteniamo decisivo. In parallelo investiremo sulla formazione del personale e sulla consapevolezza della sicurezza sia a livello individuale sia aziendale.

Quali sono oggi gli ostacoli principali?

La sfida più grande è convincere clienti ed ecosistema della reale necessità e delle opportunità. Non si tratta di "spuntare caselle" per ottenere una polizza cyber, ma di mettere in campo misure effettive. Per una media impresa, il costo della nostra soluzione è marginale rispetto al rischio. Spesso non è una questione di budget, ma di comprensione dell'urgenza. Al di là della tecnologia, questa è la vera missione per i prossimi cinque anni.

In ottica strategica, nel medio periodo rafforzerete la presenza nel mid-market o punterete con più decisione sull'enterprise?

Non è un aut-aut. Conosciamo la nostra storia e da dove veniamo, ma dal punto di vista commerciale siamo passati dall'essere percepiti come vendor consumer a un fornitore di sicurezza a pieno titolo. Siamo molto forti nelle PMI e nel mid-market, ma senza rinunciare all'enterprise. "Enterprise" può significare cose diverse a seconda dei Paesi ma, oltre alle soluzioni pronte, abbiamo una divisione corporate che realizza progetti su misura anche per organizzazioni molto grandi. Il cliente più grande con cui lavoriamo su tecnologie avanzate, non solo endpoint, conta circa 85mila postazioni.

Quali priorità e difficoltà comporta questa strategia?

L'ampiezza dell'approccio è una sfida, ma i percorsi di go-to-market possono variare. La priorità è restare il più vicini possibile a clienti di ogni dimensione. La collaborazione con il Canale è molto produttiva, in Italia e altrove: più comunichiamo insieme verso l'utente finale e più il cliente ci vede direttamente, maggiore è il successo. È così che operiamo.

La sovranità è uno dei vostri elementi distintivi. Essere europei sta avendo riscontro presso i clienti?

Sì, in modo evidente. Abbiamo comunicato bene questo aspetto perché fa parte della nostra identità: siamo a capitale privato, siamo cresciuti nella regione, abbiamo guadagnato la fiducia del mercato e siamo riconosciuti per un approccio etico. Su questo costruiamo valore e rilevanza, con una forte presenza locale.

Molta cybersecurity si sposta nel cloud. Cosa fate e cosa farete per seguire questo trend?

Oltre il 90% di ciò che vendiamo in ambito B2B è già cloud o comunque in versione cloud. Manteniamo l'opzione on-premise, ma spingiamo verso il cloud perché non è solo una tendenza ma offre vantaggi concreti per i clienti.

Uno dei vostri tratti distintivi nella prevenzione delle minacce?

Conta il modo in cui comprendiamo il panorama delle minacce: ricerca, casi reali e un'ampia esperienza in ambienti multivendor. Questa comprensione si riflette nell'efficacia della nostra a tecnologia; abbiamo visto situazioni in cui i dispositivi protetti da noi non sono stati intaccati mentre altri venivano compromessi. In più, stiamo investendo molto nella formazione e nell'assicurare che le soluzioni siano configurate correttamente perché anche questo è un aspetto chiave della prevenzione.

Pensate che il mercato abbia una percezione di voi non all'altezza del vostro valore tecnologico?

Se è così non rappresenta un problema ma un'opportunità. Fino a poco tempo fa eravamo percepiti come focalizzati sugli endpoint per l'utenza domestica, ma abbiamo dimostrato di saper cambiare questa percezione. Ci focalizziamo sul valore della nostra tecnologia e non sul marketing. Condividiamo la nostra competenza in modo mirato al mercato e vogliamo essere la prima scelta per il Canale che comprende questo valore. Al tempo stesso, puntiamo su clienti soddisfatti come vettore di riconoscibilità.

In futuro le acquisizioni faranno parte della vostra strategia?

È un tema molto discusso. Finora abbiamo sviluppato pressoché tutto in casa. Per alcune componenti lavoriamo con partner e quando aggiungiamo nuove funzionalità valutiamo anche questa strada. Come dice spesso il mio capo, il diavolo è nei dettagli: serve la soluzione giusta al prezzo giusto. Se la troveremo saremo interessati. Finora non abbiamo trovato l'equilibrio per acquistare nell'area in cui non eravamo coperti adeguatamente dai partner, ma l'ipotesi è sul tavolo più di quanto non sia mai stata in passato.

L'impatto dell'AI sulla cybersecurity

Cesare Radaelli, senior director channel account Italy & Malta di Fortinet, spiega perché l'AI semplifica le operazioni, accelera la risposta e migliora la comprensione di minacce e rischi per i diversi stakeholder

Cesare Radaelli, senior director channel account Italy & Malta di Fortinet

Oggi come e dove si può usare concretamente l'AI a supporto della cybersecurity?

L'AI è un tema a 360 gradi. L'uso dell'AI nel SOC è un aspetto, ma c'è anche l'AI che deve proteggere se stessa e quella applicata alle soluzioni. L'approccio di Fortinet copre dall'AI generativa all'AI operativa che entra nel SOC, con un'attenzione mirata area per area. Parlando di AI generativa, è una tecnologia che utilizziamo già da qualche anno: è integrata nelle nostre soluzioni e ci ha permesso di alzare l'asticella non solo nei controlli in tempo reale contro minacce zero-day, ma soprattutto nell'usabilità delle piattaforme. Oggi è particolarmente evidente come l'AI sia abilitante per chi si torva a gestire un SOC, perché introduce velocità di reazione e qualità dell'analisi. All'interno dei SOC l'AI interviene a livello di soluzioni, protezione e gestione e, su ciascuno di questi aspetti, Fortinet concentra investimenti significativi che trasferiamo poi al mercato attraverso le nostre soluzioni.

L'AI è integrata nella vostra piattaforma o la proponete anche come soluzione autonoma?

Entrambe le cose. Abbiamo sviluppato FortiAI, una soluzione stand-alone che si può acquistare per supportare la gestione, la razionalizzazione degli eventi e l'assegnazione degli allarmi in ingresso. In parallelo, integriamo AI — generativa e non — all'interno delle nostre soluzioni per migliorarne qualità e tempi di risposta. Per noi è un motivo di orgoglio il numero di brevetti registrati: in EMEA sono circa 1.400 di cui oltre 500 riguardano specificamente l'intelligenza artificiale. L'investimento non è solo massivo ma anche sempre più attento a un utilizzo dell'AI reso fruibile ed etico.

Sul fronte dell'automazione abilitata dall'AI, a che punto siete in Fortinet?

Siamo molto avanti, soprattutto per l'uso nel SOC. Mettiamo a disposizione degli operatori un'interfaccia non solo grafica ma anche vocale, che aumenta il livello di interazione e consente di effettuare "deep dive" estremamente puntuali, fino a proporre le azioni per ostacolare o bloccare la minaccia. Cambia il paradigma rispetto a quando l'operatore doveva esaminare serie infinite di log e basarsi su motori di correlazione che producono risultati "prelavorati" da interpretare nel contesto. Oggi l'operatore riceve un supporto enorme e trae un beneficio concreto dall'intelligenza artificiale.

Le competenze richieste agli operatori si abbassano o si spostano su un altro piano?

La visione di competenza resta fondamentale, anche tecnica e di alto profilo. L'AI consente però di sopperire alla scarsità di personale perché una parte del lavoro viene ridotta drasticamente e, nel contempo, permette di elevare il livello di analisi per gli specialisti che conoscono anche il business dell'azienda. Invece di avere molte persone dedicate al monitoraggio e al controllo dei flussi "prelavorati", posso contare su un gruppo più vicino al business, capace di correlare la minaccia con il rischio aziendale e di valutare, per esempio, l'impatto su un servizio critico o capire quando ci trova di fronte a decisioni da demandare a livelli superiori.

Questo avvicina quindi la security al risk management?

Esatto. Ci avviciniamo al risk management e a interlocutori come i CFO che un tempo non volevano nemmeno sentir parlare di security. Con il supporto dell'intelligenza artificiale l'operatore può produrre rapidamente report specifici indirizzati ai vari stakeholder interni. Dal potenziale incidente e dal suo possibile impatto si arriva in tempi brevi a una reportistica che, con linguaggio adeguato a ciascun interlocutore, rende evidente in modo semplice, intuitivo e grafico che cosa è accaduto, come è accaduto e che cosa è stato impattato. In questo modo riusciamo ad avvicinare la complessità della security al CFO, al COO, ai direttori di produzione e agli altri responsabili aziendali.

Prevenzione e data security per una piena resilienza

Giampiero Petrosi di Rubrik spiega perché la data security rappresenta l'ultima linea di difesa e come affrontare il tema della prevenzione e ripartenza assistita dall'AI.

Partiamo dalla resilienza oltre la sicurezza tradizionale.

Il primo punto, per affrontare la resilienza in modo corretto, è essere preparati. In concreto, la preparazione significa conoscere la tipologia dei dati che trattiamo e ciò che accade al loro interno. Rubrik è specializzata nella data security che rappresenta la "last line of defense" nello stack di sicurezza: se l'attacco supera i vari layer e arriva alla componente dati, è lì che entriamo in gioco. Non ci limitiamo a restituire una copia dei dati e a riportare l'azienda in produttività dopo un attacco, ma operiamo anche nel cosiddetto "peace time", osservando come evolvono dati e data center. Se quotidianamente si gestiscono i dati con una soluzione come la nostra, diventa possibile comprendere come cambiano e, grazie a un motore di threat intelligence nativo, intercettare comportamenti anomali o l'arrivo di malware, prevenendo potenziali attacchi.

Come è possibile intervenire in caso di attacchi zero day?

La preparazione consente, anche in caso di zero-day in cui mancano indicatori di compromissione in tempo reale, di verificare tutte le copie storicizzate e individuare rapidamente quella pulita, senza dover fermare tutto per attivare SOC o altre funzioni al solo scopo di capire quale dato sia utile al ripristino. Questa capacità definisce il nostro Cyber RTO (Recovery Time Objective). In un attacco non sai quali movimenti laterali siano avvenuti prima della sua manifestazione e quindi non conosci il perimetro della compromissione se non hai uno strumento che, analizzando il dato giorno per giorno, ti indichi il raggio d'azione, i dati potenzialmente sensibili coinvolti e la recuperabilità del business.

Con tempi medi di scoperta della compromissione nell'ordine dei 200 giorni come evitate di ripristinare copie di dati che non siano già compromessi?

Proteggiamo i dati e le applicazioni aziendali con uno store che, in base alla retention, consente di co<ntrollare l'evoluzione del dato. Quando effettuiamo la copia di backup il nostro motore di threat monitoring, collegato al nostro security cloud, scarica tutti gli indicatori di compromissione (IoC) aggiornati e li utilizza in tempo reale durante l'ingestion dei dati di backup. Questi IoC vengono anche da collaborazioni esterne, per esempio con Mandiant. Con un modello di backup "incremental forever", tutto ciò che conosciamo al momento della fase di ingestion ci permette di marcare come pulito quanto risulta non toccato dagli indicatori. Il punto critico è lo zero-day, dove l'IoC non è ancora noto. Nel momento in cui subiamo l'attacco, analizziamo l'accaduto, lavoriamo con i centri di ricerca, con il SOC, definiamo gli IoC e, con lo stesso motore, eseguiamo una scansione accelerata sui dati già acquisiti. In questo modo identifichiamo la copia di backup più vicina nel tempo e non compromessa, evitando restore inutili o dannosi.

L'AI vi aiuta in questo processo?

Assolutamente sì, e in più modi. L'AI ci aiuta nell'analisi conoscitiva e nell'apprendimento dei cambiamenti che avvengono sui dati e supporta la gestione operativa del rollback attraverso componenti di automazione costruite per accelerare il rientro in produzione. Abbiamo annunciato due progetti basati sull'intelligenza artificiale. Il primo, più recente, è Agent Rewind, un agente AI già annunciato che sarà disponibile nel prossimo futuro. L'obiettivo è aiutare le aziende nel rollback di azioni eseguite dagli agenti AI che si rivelino errate. Uno dei problemi più rilevanti nella gestione aziendale degli agenti è, infatti, proprio la possibilità che prendano decisioni autonome i cui esiti non siano quelli attesi.

Il secondo progetto?

L'altro progetto è Annapurna, già disponibile da tempoi. Un fattore critico nell'adozione dell'intelligenza artificiale in azienda è la perdita di controllo dal punto di vista della sicurezza. Noi, che ci occupiamo di contenere i dati, di classificarli, del controllo degli accessi e delle integrazioni con gli asset di rete, forniamo al modello un ambiente sicuro: una sorta di data lake controllato in modo che al modello AI vengano fornito solo le informazioni ritenute opportune, secondo le policy aziendali.

Perché è meglio nessuna risposta che una risposta sbagliata?

Si, ma anche per evitare di trattare dati che l'azienda non desidera esportare o utilizzare fuori dai confini stabiliti.

Gianpiero Petrosi, regional vp sales engineering Southern Europe di Rubrik

Cyber resilience
oltre la cybersecurity

Marco D'Elia, country manager di Sophos Italia, descrive una cyber resilience fondata su prevenzione e risposta rapida per garantire continuità operativa

Marco D'Elia, country manager di Sophos Italia

Qual è la vostra visione della cyber resilience con il superamento della cybersecurity?

Cyber resilience significa ammettere che esiste un rischio e che non è possibile eluderlo del tutto, ma anche essere capaci di prevenirlo e soprattutto di rispondere in modo tempestivo per evitare la non operatività, quindi per scongiurare situazioni disastrose. La cyber resilience oggi si applica affiancando alla tecnologia, che resta fondamentale, capacità operative e processi: il software di endpoint protection si è evoluto, riducendo il numero di rischi che arrivano da gestire, ma questo da solo non basta.

All'interno dei SOC come si declina questa proposizione?

Non è sufficiente contare solo sulla tecnologia: bisogna affiancare il lavoro dei SOC. La differenza, al di là dell'uso di strumenti di AI generativa anche all'interno del SOC per fornire supporto, sta nell'architettura e nell'apertura della piattaforma. Sophos si sta differenziando anche grazie all'acquisizione di Secureworks (avvenuta a febbraio 2025 N.d.R.), per costruire un sistema di protezione che si basa su concetti di SIEM e di SOAR, fornendo risposte automatiche a eventi predeterminati e, soprattutto, aperto a includere qualsiasi tecnologia preesistente. Oggi integriamo più di 350 applicazioni. Una piattaforma di questo tipo deve essere omnicomprensiva.

Cosa suggerite a chi decide di dotarsi di un SOC?

Un aspetto che suggeriamo sempre a chi valuta un SOC riguarda i criteri di scelta. La qualità e la potenza di un SOC sono direttamente proporzionali al numero di persone e di risorse coinvolte e, soprattutto, al numero di "device" gestiti nel mondo. Chi difende, senza un'ampia base osservativa, è "cieco": fatica a capire cosa stia accadendo sul fronte dell'offesa. Più dispositivi proteggi, migliore è la visibilità su ciò che accade attraverso "gli occhi" dei device sotto protezione. Se un vendor tutela solo device in Europa avrà una visibilità più limitata rispetto a chi protegge centinaia di milioni di utenti a livello globale. Oggi Sophos vanta oltre 35mila utenti e clienti MDR sotto protezione e questo consente, per esempio, che un attacco rilevato in Corea venga messo a fattor comune in tempo reale a beneficio di chi sta lavorando per proteggere un'azienda italiana.

Oltre la parte di detection, la risposta è oggi centrale. Come l'affrontate e quale ruolo ha l'AI?

La risposta si basa sull'uso di strumenti di AI e, soprattutto, sull'esperienza che gli utenti e i team maturano. Sophos fornisce,per esempio, Playbook progettati per affrontare attacchi già noti; questo tipo di tecnologia è efficace, ma non protegge dagli zero day. Nel caso di un attacco nuovo per il quale non esiste un Playbook, bisogna capire subito quale risposta dare. Sophos garantisce, per contratto, una risposta entro 38 minuti dal momento dell'attacco, che è il tempo medio di risposta certificato dai nostri Labs.

Riuscite già oggi con l'AI a modificare in modo dinamico le policy a fronte di un attacco o di una minaccia reale?

Nel febbraio 2024 abbiamo rilasciato una tecnologia chiamata AI Assistant, all'interno della nostra piattaforma XDR, che consente esattamente questo. Si tratta di AI che intercetta rapidamente gli exploit e le aree di debolezza e, con grande rapidità, propone l'azione correttiva o interviene direttamente per conto dell'utente, se autorizzata.

Per esempio isolando accessi o parti della rete?

Sì. Questo è un utilizzo virtuoso dell'AI integrata nel software e nella piattaforma. L'industria sta andando chiaramente in questa direzione.

Spesso però il rischio viene dall'interno e dalle identità compromesse?

Abbiamo molteplici servizi, tra cui un servizio di Identity Threat Detection e di gestione delle minacce legate al furto d'identità. È un servizio erogato nella nostra piattaforma MDR ed è una delle tecnologie ottenute a seguito dell'acquisizione di Secureworks. In questo modo realizziamo un vero e proprio identity management integrato nel software.

La sicurezza parte dallo zero trust

Elena Accardi di Zscaler ci guida verso un modello di sicurezza di resilienza by design che non regala fiducia a niente e nessuno

Elena Accardi, country manager di Zscaler per Italia, Grecia, Malta e Cipro

Zscaler vanta oggi in Italia una presenza territoriale radicata, con oltre 40 professionisti ben distribuiti su tutto il territorio e solide alleanze e partnership. Parlare di Zscaler, sostiene Elena Accardi, country manager di Zscaler per Italia, Grecia, Malta e Cipro, significa affrontare il tema della trasformazione, che non si può fare in assenza di consolidate relazioni con partner e system integrator. Senza dimenticare le tech alliance con cui Zscaler sviluppa la propria proposizione core dello Zero Trust.
Tra le alleanze, ricorda Accardi, vi sono aziende come Rubrik e CrowdStrike, che svolgono un ruolo importante soprattutto nei progetti Zero Trust end-to-end su clienti enterprise altamente regolamentati. Le collaborazioni in relazione al tema dell'AI prevedono molti vendor che si inseriscono con soluzioni evolute di SIEM e, ricorda Accardi, aziende come Vectra AI, con cui Zscaler sviluppa con il proprio motore di AI intelligence per le attività di detection. L'interoperabilità con le soluzioni EDR consente poi alle aziende clienti di valorizzare investimenti già effettuati.

AI tra detection e protezione dei dati

L'AI viene affrontata su due piani. Da un lato, Zscaler sviluppa con il proprio motore di AI un layer di intelligence orientato alla detection, lavorando in interoperabilità con soluzioni SIEM evolute. Dall'altro, protegge l'uso stesso di AI e GenAI con le soluzioni di AI data protection, intervenendo, per esempio, sul fenomeno dello Shadow AI (l'uso non autorizzato da parte dei dipendenti di motori di AI) o bloccando l'upload di informazioni riservate o confidenziali quando necessario, attivando azioni di "prompt response". L'AI viene impiegata anche in chiave difensiva, con strumenti pensati per consentire alle aziende di individuare le possibili anomalie e utilizzare queste tecnologie rivoluzionare in piena sicurezza.

Le caratteristiche di un'infrastruttura Zero Trust

Ciò che resta rilevante nella proposizione di Zscaler è progettare un'infrastruttura che segue il principio dello Zero Trust assistita dall'AI, quindi in grado di tutelarsi da eventuali attacchi e di limitare i danni. Seguire i principi Zero Trust vuol dire, di fatto, predisporre un principio di "resilienza by design", che permette di costruire e progettare una rete al riparo da possibili movimenti laterali all'interno dell'infrastruttura aziendale.
La grande differenza tra un'infrastruttura tradizionale e un'infrastruttura Zero Trust, ricorda Elena Accardi, è che quando un utente accede a un'infrastruttura tradizionale ha la libertà di muoversi lateralmente al suo interno: inizialmente e prioritariamente all'interno del data center, ma anche al suo esterno verso le reti di partner e fornitori. In un'infrastruttura Zero Trust, sostiene Accardi, il paradigma è completamente diverso perché il data center diventa un target da raggiungere dopo essere stati autorizzati, esattamente come qualsiasi asset o applicazione.
Nel modello di infrastruttura Zero Trust di Zscaler, un utente, per accedere all'asset di interesse, effettua una chiamata ai POP di Zscaler passando attraverso Zscaler ZCC (Zscaler Client Connector, un'applicazione leggera installata sul dispositivo dell'utente). La soluzione di Zscaler verifica l'accesso, controlla la destinazione desiderata di quell'utente attraverso l'interoperabilità con sistemi, per esempio, di EDR e, solo dopo averne validato l'accesso, concede a quello specifico utente di accedere unicamente a quell'applicazione attraverso un tunnel diretto.
Se un attaccante entra con un'identità legittima ma compromessa, spiega Accardi, la resilienza by design mantiene l'attaccante all'interno di quell'unico tunnel, limitando al minimo il danno e impedendo qualsiasi movimento laterale, come succederebbe invece in un'infrastruttura tradizionale. Un altro aspetto importante in un'infrastruttura Zero Trust è l'isolamento degli indirizzi IP: in assenza di indirizzi IP pubblici non vengono esposte reti né contenuti e si è più difficilmente attaccabili.
Tra le ragioni per cui Zscaler viene scelta, afferma Accardi, vi è anche la sua natura di piattaforma multitenant, che assegna a ogni cliente una propria area isolata: anche nel caso in cui Zscaler dovesse subire un attacco, questo non si trasferirebbe ai propri clienti, come invece potrebbe accadere con alcuni MSSP.
Questo è importante perché, sostiene la manager, *"oggi non si compra più sicurezza, ma si compra fiducia e reputazione"*.

ESG, le nuove regole UE e le implicazioni per imprese e bilanci

Direttive come la CSRD, gli ESRS aggiornati e la Tassonomia UE ridefiniscono gli obblighi di Environmental, Social and Governance per oltre 50.000 aziende. Le imprese devono attrezzarsi per nuove regole, assurance esterna e trasparenza finanziaria. Molte le sfide e gli impatti operativi, ma anche le opportunità

DI FABRIZIO PINCELLI

Nel corso degli ultimi anni il tema **ESG (Environmental, Social and Governance)** ha fatto un percorso radicale: da elemento facoltativo, presente solo in bilanci sociali e report volontari, è diventato un perno normativo su cui le autorità europee stanno costruendo un nuovo modo di regolamentare le imprese.
Le recenti **riforme UE** hanno trasformato il concetto di sostenibilità da contenuto etico e reputazionale a obbligo legale con impatti concreti su governance, bilancio e relazione con stakeholder.
L'innovazione normativa guida oggi il cambiamento: non più sostenibilità vista come scelta comunicativa, bensì come **ingrediente strategico e obbligato per operare nei mercati europe**i.
Le aziende che non si adegueranno rischiano sanzioni, perdita di credibilità e difficoltà nell'accesso al credito.

La rivoluzione CSRD e il suo ambito di applicazione

Il punto centrale di questa trasformazione normativa è la **Corporate Sustainability Reporting Directive (CSRD)**, che ha sostituito la precedente NFRD è stata pubblicata nel dicembre 2022 ed è entrata in vigore il 5 gennaio 2023. Con la CSRD cambia radicalmente la platea di imprese obbligate alla rendicontazione: non più solo le grandi aziende di interesse pubblico con oltre 500 dipendenti, ma molte più realtà di grandi dimensioni, **comprese le PMI quotate e le filiali europee di gruppi multinazionali**. Più in dettaglio, la direttiva si applica in modo progressivo: dal 2024 per le grandi aziende già soggette alla NFRD, dal 2025 per le altre grandi imprese, dal 2026 per le PMI quotate e dal 2028 per le filiali europee di multinazionali extra-UE. Si stima che oltre 50.000 imprese dovranno preparare il bilancio di sostenibilità, rispetto alle circa 12.000 coinvolte precedentemente.

Un altro aspetto fondamentale introdotto dalla CSRD è l'obbligo di redigere i bilanci secondo gli standard **ESRS (European Sustainability Reporting Standards)**. Questi standard impongono criteri rigorosi per la comparabilità, la verificabilità e la coerenza dei dati ESG. Inoltre, assume rilievo centrale il principio della doppia materialità: le aziende devono rendicontare non solo come i temi inerenti all'ESG influenzino la performance finanziaria, ma anche come le proprie attività incidano su ambiente e società.

Le aziende devono quindi dotarsi di sistemi adeguati per raccogliere dati su emissioni, consumo energetico, uso dell'acqua, politiche sociali e parametri di governance, e farlo in modo coerente e controllabile. Non si tratta più di dichiarazioni "soft" bensì di un documento con valore legale soggetto a revisione esterna, analogo al bilancio finanziario.

Aggiornamenti ESRS e linee guida operative

Le novità normative più recenti riguardano l'evoluzione degli ESRS. L'EFRAG ha pubblicato nei mesi scorsi le implementation guidance (IG1–IG3), con indicazioni su materialità, catena del valore e punti dati (datapoints) da raccogliere, utili per interpretare i requisiti tecnici standard. Inoltre, nel 2025 sono state pubblicate exposure drafts (luglio 2025) per la revisione e la semplificazione degli ESRS, con l'intento di rendere gli standard più attuabili e calibrati alle realtà aziendali, in particolare per PMI e imprese con meno maturità ESG. Questo processo di revisione può influire su regole tecniche e tempistiche: le imprese in fase di implementazione devono monitorare attentamente le modifiche strutturali che verranno approvate e recepite dalla Commissione europea.

Un altro elemento focale del nuovo sistema è la **Tassonomia UE**, che definisce gli standard con cui un'attività economica può essere qualificata come sostenibile. Le imprese devono indicare la percentuale di ricavi, investimenti in attività fisse (CAPEX) e spese operative (OPEX) conformi a questi criteri. Modifiche recenti da parte di delegated acts nel 2024–2025 hanno aggiornato le attività incluse e ridefinito soglie operative. Le imprese devono adeguarsi a questa evoluzione, poiché la classificazione "verde" delle proprie attività incide direttamente sulla rendicontazione e sulla credibilità nei confronti degli investitori.

Lo scorso mese di luglio la Commissione europea ha annunciato di aver adottato una serie di misure per semplificare l'applicazione della tassonomia dell'UE. L'obiettivo è **ridurre gli oneri amministrativi per le imprese dell'UE**, rafforzando in tal modo la competitività dell'UE e preservando nel contempo gli obiettivi climatici e ambientali fondamentali.

SFDR e trasparenza finanziaria

Nel contesto della finanza sostenibile, la **Sustainable Finance Disclosure Regulation (SFDR)** continua a legare i bilanci aziendali alla trasparenza del mondo finanziario. Le autorità europee (ESAs) hanno rilasciato Q&A aggiornate e linee guida sui prodotti finanziari, sugli indicatori PAI (principal adverse impacts) e sulla disclosure obbligatoria, creando una pressione diretta sulle imprese affinché forniscano dati ESG robusti e confrontabili.

Le informazioni rese dalle aziende

diventano materia prima per i gestori di fondi e gli strumenti finanziari ESG: se i dati aziendali non sono affidabili o allineati agli standard, l'accesso a capitali "verdi" può risultare compromesso. In **Italia**, l'implementazione della CSRD è stata recepita tramite un decreto legislativo (n.125/2024) che adatta le disposizioni europee alla normativa nazionale. La **Consob** ha intensificato l'attività di vigilanza sulle società quotate, emettendo avvisi, consultazioni e linee guida per adeguare i regolamenti degli emittenti alle nuove regole ESG. Le società quotate dovranno garantire che la comunicazione ESG **non contenga affermazioni generiche**, ma dati quantitativi e verificabili: il rischio reputazionale e normativo è reale per chi non si adegua. Le novità normative hanno impatti concreti anche per imprese italiane, incluse PMI che fino ad oggi non affrontavano la rendicontazione ESG obbligatoria. Nei settori manifatturiero, moda, agroalimentare, l'allineamento a standard rigorosi può favorire l'accesso a mercati internazionali dove i buyer e le catene del valore già richiedono certificazioni ESG spinte.

Tecnologia e competenze: ingredienti essenziali

Per assolvere agli obblighi CSRD / ESRS aggiornati non bastano buone intenzioni: servono infrastrutture tecnologiche avanzate. Le imprese devono dotarsi di piattaforme digitali (cloud, IoT, sistemi di analytics) per raccogliere e integrare i dati ESG. L'intelligenza artificiale e il machine learning possono supportare l'analisi predittiva, la gestione della catena di fornitura e la qualità dei dati raccolti.
Parallelamente, è fondamentale investire nel capitale umano: figure come sustainability managers, analisti ESG e data scientist diventano centrali. Le competenze devono includere conoscenze normative, gestione dati, metriche ESG e auditability.
L'obbligo normativo è severo, ma offre vantaggi reali. Un bilancio ESG certificato e trasparente consente di dialogare con gli stakeholder con maggiore credibilità, attrarre investimenti responsabili, ridurre il costo del capitale e migliorare la reputazione nei mercati internazionali. Le imprese che anticipano le regole e costruiscono processi interni virtuosi possono trasformare la compliance in innovazione strategica.
Non conformarsi significa esporsi a rischi legali, sanzioni, perdite reputazionali e difficoltà nell'accesso ai capitali. Inoltre, in un contesto in cui investitori, consumatori e istituzioni attribuiscono crescente valore alla sostenibilità verificabile, aziende poco trasparenti rischiano di essere escluse dalle rotte del mercato "verde".

BILANCIO AMBIENTALE E DI SOSTENIBILITÀ E REPORT DI SOSTENIBILITÀ: LE DIFFERENZE

Nel dibattito sulla sostenibilità i termini **"bilancio ambientale"**, **"bilancio di sostenibilità"** e **"report di sostenibilità"** vengono spesso confusi, ma non sono equivalenti.
Il **bilancio ambientale** è un documento volontario e specialistico, focalizzato esclusivamente sugli impatti ecologici di un'impresa: emissioni, consumi energetici, rifiuti, uso delle risorse naturali. Nasce come strumento tecnico per rendicontare le relazioni tra azienda e ambiente e non comprende necessariamente aspetti sociali o di governance.
Il **bilancio di sostenibilità** ha un respiro più ampio e integra la prospettiva ESG. Oltre ai dati ambientali, rendiconta politiche sociali, inclusione, diritti umani, relazioni con il territorio, composizione degli organi di governance. È spesso redatto secondo standard riconosciuti come i GRI e, con l'entrata in vigore della CSRD, diventa obbligatorio per migliaia di imprese europee, assumendo lo stesso livello di formalità e revisione di un bilancio finanziario.
Il **report di sostenibilità**, infine, rappresenta la versione più narrativa e comunicativa della rendicontazione. Spesso include storie, obiettivi e casi studio oltre ai dati, ed è destinato a un pubblico ampio: clienti, comunità, investitori. Può affiancare il bilancio di sostenibilità come strumento di storytelling e trasparenza, ma non sempre è soggetto a standard tecnici o revisione esterna.
In sintesi, il bilancio ambientale è un documento settoriale, il bilancio di sostenibilità è lo strumento regolamentato e completo, mentre il report di sostenibilità svolge la funzione di narrazione accessibile. Con la CSRD e gli standard ESRS la distinzione tenderà a ridursi: il bilancio diventa vincolo legale, il report la sua espressione comunicativa.

Come ridurre consumi ed eliminare sprechi con le **tecnologie clean**

Sempre più essenziali per le imprese che intendono individuare e ridurre consumi eccessivi, le cleantech migliorano l'efficienza permettendo di tagliare i costi e abbattere l'impatto ambientale. Dal manifatturiero al retail, sensori, analytics e AI guidano una trasformazione che non è solo tecnologica ma (soprattutto) culturale

Nell'ambito delle sfide energetiche e climatiche che devono affrontare le imprese, le **cleantech** non sono più solo una voce di bilancio o una dichiarazione di intenti: sono strumenti che **consentono di individuare praticamente dove si hanno consumi eccessivi**, perché si verificano e come intervenire per migliorare l'efficienza e ridurre costi. Vediamo quali "tecnologie pulite" possono aiutare le aziende a mappare i consumi, tradurre i dati in azioni e misurare i risparmi.

Mappatura dei consumi e strumenti analitici

Le imprese che vogliono tagliare consumi inutili devono prima di tutto conoscere con precisione la loro **"anatomia energetica"**: quali macchine o reparti assorbono più potenza, in quali fasce orarie si concentrano i picchi, dove si verificano dispersioni termiche o inefficienze nei processi. Qui entrano in **gioco sensori, sub-metering e piattaforme di gestione energetica**. Installando contatori di seconda e terza classe a livello di singola linea produttiva, di singolo quadro elettrico o di specifico impianto di climatizzazione, le aziende possono acquisire dati ad alta granularità: consumi istantanei, profili temporali, fattori di potenza e frequenza di avvio di carichi pesanti. Questi dati, aggregati su piattaforme cloud e combinati con i dati di produzione e di occupazione, permettono di **tracciare i "pattern" che rivelano sprechi** - ad esempio frigoriferi che lavorano a vuoto nelle ore notturne o forni che restano in temperatura oltre il necessario - e di definire priorità d'intervento.
Le soluzioni di energy management basate su algoritmi permettono di andare oltre il semplice reporting, trasformando dati grezzi in insight operativi. Le piattaforme moderne con funzioni di **machine learning possono identificare anomalie, prevedere picchi futuri e suggerire azioni correttive in tempo reale**, come lo spegnimento temporaneo di carichi non essenziali, la riallocazione della produzione in fasce orarie a minor costo energetico o l'attivazione automatica di sistemi di accumulo. L'**adozione di digital twin** per impianti critici consente inoltre di simulare scenari "what-if" – quale risparmio si ottiene abbassando di un grado la temperatura di processo, o quanto si riducono i picchi se si interviene su un singolo ventilatore – senza interrompere la produzione effettiva.
Le tecnologie cleantech non esauriscono il loro valore nella sola "intelligenza" dei dati: esistono interventi fisici che le aziende possono attivare con ritorni rapidi. L'efficientamento degli edifici attraverso **coibentazioni**, **sistemi HVAC** più moderni e **lampade LED** a controllo dinamico rimane una leva importante, soprattutto se affiancata a sistemi di controllo automatico che modulano consumi in funzione dell'occupazione reale. La cogenerazione e il recupero di calore nei processi industriali permettono di sfruttare energia che altrimenti verrebbe

dispersa. L'integrazione tra misurazione, analisi e intervento operativo è ciò che avvalora l'argomento del risparmio: quando una misura identifica un problema e la macchina lo corregge automaticamente, il risultato è misurabile e replicabile.

Un mercato in rapida crescita

Dal punto di vista del mercato, la domanda per questi prodotti e servizi è cresciuta rapidamente negli ultimi anni. Secondo le stime di *Grand View Research*, il mercato globale delle tecnologie pulite ha raggiunto nel 2024 916,20 miliardi di dollari in termini di fatturato aggregato e le previsioni indicano che il valore complessivo raggiungerà i 1.844,70 miliardi di dollari entro il 2030, con un CAGR del 12,7% dal 2025 al 2030. In particolare, *Global Market Inside* indica un mercato globale degli Environmental management systems (EMS) di circa 12-13 miliardi di dollari nel 2024, con proiezioni che lo vedono crescere fino a 28-30 miliardi di dollari entro il 2034, con un CAGR prossimo all'8,5%, segnalando una domanda forte per software e servizi che orchestrano sensori, dati e controllo degli impianti. **Questa crescita è alimentata sia dalla pressione regolatoria che dalla volontà delle imprese di ridurre costi energetici e impronta di carbonio**.

Anche gli investimenti nella transizione energetica continuano a sostenere l'ecosistema cleantech. Pur con oscillazioni geografiche e politiche, i flussi di capitale verso energie rinnovabili, accumulo e tecnologie di rete sono rimasti elevati nel 2024 e nel 2025: un report di *Bloomberg* evidenzia come gli investitori privilegino soluzioni che combinano riduzione dell'intensità carbonica e ritorno economico misurabile. Questi capitali alimentano sviluppo di prodotti, scalabilità delle piattaforme e adozione su scala industriale.

CLEANTECH: IL VALORE NASCE DA DATI PRECISI, INTEGRAZIONE, AI E SERVIZI SU MISURA ANCHE PER LE PMI

DAI SENSORI ALL'AI, COSÌ L'EFFICIENZA DIVENTA INTELLIGENTE

La forza delle cleantech non sta solo nella novità, ma nella capacità di connettere tecnologie esistenti, analisi dati e automazione. Il primo passo è la misurazione: sensori e sistemi di sub-metering permettono di rilevare i consumi di una singola linea, di un compressore o di un reparto, individuando sprechi e anomalie che un tempo restavano nascosti. Ma il vero salto avviene con gli **Energy management systems**, piattaforme che aggregano i dati in tempo reale, li integrano con produzione e manutenzione e li trasformano in mappe comprensibili, fino ad attivare direttamente correzioni automatiche.
A potenziarne l'efficacia è l'intelligenza artificiale, che grazie al **machine learning** riconosce pattern anomali, prevede picchi futuri e suggerisce azioni correttive difficili da cogliere per l'occhio umano. Sempre più diffusi sono anche i **digital twin**, repliche virtuali di impianti e macchinari che consentono di simulare scenari – come ridurre una temperatura di processo o anticipare la manutenzione – calcolando risparmi ed effetti ambientali prima di intervenire sul reale. L'ultimo tassello è il **demand response**: collegando i sistemi di consumo ai mercati energetici, le aziende possono modulare i carichi in base a prezzi e segnali di rete, trasformandosi da consumatori passivi in attori attivi. In questa integrazione – dalla misura all'analisi, dalla previsione all'azione – si gioca la vera potenza delle cleantech, ovvero la capacità di coniugare efficienza, competitività e sostenibilità.

I 4 elementi chiave delle cleantech company

Le cleantech company che offrono il maggior valore alle imprese sanno combinare quattro elementi: **misurazione di qualità** (hardware affidabile), **integrazione** (API con ERP e sistemi di controllo), **analytics avanzati** (ML, anomaly detection, previsioni di consumo) e **capacità di esecuzione sul campo** (project management per retrofit, commissioning e mantenimento). È in questa intersezione che nascono le **soluzioni "as-a-service"** che permettono anche a PMI di accedere a tecnologie prima riservate alle grandi aziende: contratti di rendimento energetico, modelli di servizio che prevedono la condivisione del risparmio e finanziamenti che ammortizzano l'investimento iniziale.
Un altro trend che accelera l'efficacia degli interventi è l'integrazione con mercati e servizi di flessibilità energetica. Le aziende dotate di **sistemi di controllo intelligenti** possono partecipare a meccanismi di demand response, modulando i carichi in momenti di prezzo elevato o quando la rete richiede stabilizzazione, ottenendo ricavi aggiuntivi e riducendo il costo totale dell'energia. Anche l'**uso di sistemi di accumulo** e la collaborazione con aggregatori sono leve che trasformano un centro di consumo in un attore attivo del sistema elettrico, con benefici economici e ambientali.

Chiari KPI e formazione per abbattere gli sprechi

Non vanno trascurati i vincoli: molte realtà sono rallentate da barriere interne come la **scarsa alfabetizzazione energetica dei team operativi,** la frammentazione dei dati e la reticenza a investire in manutenzioni preventive. La digitalizzazione, se proposta senza una chiara roadmap di change management, rischia di produrre report che rimangono consultati e non convertiti in azioni. Perciò le migliori cleantech company **abbinano la tecnologia a servizi di consulenza** che accompagnano il cliente nella definizione di KPI energetici, nella formazione del personale e nella strutturazione di processi che standardizzano la risposta a allarmi e opportunità. Guardando al prossimo futuro, le prospettive rimangono positive: la decarbonizzazione della generazione, la caduta dei costi delle tecnologie pulite e la crescente normazione su disclosure e reporting ESG spingono le aziende a dotarsi di strumenti più sofisticati per il controllo dei consumi. Tuttavia, la trasformazione non è solo tecnica; è gestionale e culturale. Le imprese che riusciranno a integrare i dati energetici nei processi decisionali quotidiani - pianificazione della produzione, ciclo di vita dei macchinari, politiche di manutenzione predittiva - saranno quelle in grado di convertire l'investimento in risparmio reale e in vantaggio competitivo.

MANUFACTURING E RETAIL, USE CASE CONCRETI

Quando si parla di cleantech si pensa spesso a concetti astratti, ma concreti use case nel manufacturing e nel retail mostrano la loro efficacia. Nelle **fabbriche**, i sistemi di monitoraggio hanno rilevato consumi anomali legati ai compressori d'aria: perdite non rilevate o pressioni eccessive possono generare sprechi da decine di migliaia di euro l'anno. Sensori e modelli predittivi permettono di intervenire subito, riducendo dispersioni e pianificando manutenzioni preventive. Nei **forni industriali**, invece, lo spreco deriva dal mantenimento della temperatura anche quando non serve: digital twin e intelligenza artificiale simulano scenari di spegnimento o modulazione, calcolando i benefici prima di agire. Nel **retail**, l'impatto riguarda soprattutto la refrigerazione. Un supermercato medio gestisce centinaia di frigoriferi e banchi frigo, responsabili di gran parte della spesa energetica. Il monitoraggio intelligente rileva anomalie come apparecchi accesi durante la chiusura o guarnizioni usurate che costringono i motori a lavorare di più. Correggere queste situazioni riduce i consumi e allunga la vita degli impianti. Anche l'illuminazione è sotto osservazione: sensori di presenza e controllo dinamico dei LED adattano la luce alle reali esigenze, evitando reparti illuminati a piena potenza senza clienti. La vera novità sta nell'**automazione** e nella misurabilità: i dati raccolti prima e dopo gli interventi documentano i risparmi, rafforzando fiducia e trasparenza. Così, sia nel manufacturing sia nel retail, **le cleantech generano risparmi, migliorano la sostenibilità e offrono un vantaggio competitivo**, perché dimostrare con dati concreti l'impegno ambientale rafforza la reputazione e la relazione con clienti e stakeholder.

L'impatto ESG sui **contratti tecnologici**

L'integrazione di clausole ESG nei contratti di outsourcing IT, cloud e servizi digitali è ormai imprescindibile e determina un ripensamento critico del ruolo dei responsabili legali in azienda così come della relazione con fornitori e imprese rispetto a temi quali sostenibilità e governance.

A CURA DI CATERINA ALESSIA DIBITONTO

Avvocato, componente Commissione innovazione dell'Ordine degli avvocati di Milano

Il tema ESG (Environmental, Social, Governance) è oggi trasversale in ogni ambito del Diritto, inclusi gli aspetti della contrattualistica correlati alla tecnologia. Peraltro, l'universo ampio della sostenibilità e della corporate social responsability ci invita a una riflessione sul cambiamento strategico che il nostro modo di approcciare il lavoro sta vivendo.

La regolamentazione europea (come la CSRD – Corporate Sustainability Reporting Directive) impone, infatti, obblighi di rendicontazione ESG anche attraverso l'intera supply chain e, pertanto, le imprese hanno il "constraint" di dimostrare la conformità ESG non solo al loro interno, ma anche nei confronti dei loro partner tecnologici.

La relazione con fornitori e partner

I fornitori di tecnologia IT (cloud provider e outsourcer) sono, a tutti gli effetti, partner del business e, come tali, condividono con l'impresa anche i rischi e le responsabilità relative agli indici ESG.

L'adempimento di **prevedere clausole contrattuali che siano a garanzia del rispetto di standard ESG** anche nel contratto di servizi tecnologici diventa un "necesse est". Di conseguenza, l'integrazione delle clausole ESG all'interno del contratto di matrice tecnologica soddisfa l' esigenza di rendere sostenibili anche i servizi digitali (come outsourcing IT, cloud computing, servizi software). In tal modo, la relazione commerciale tra fornitori/partner commerciali e imprese si arricchisce di uno scenario che apporta maggiore tutela a entrambe le parti e che ha impatti rilevanti sui rapporti commerciali e sulla gestione del rischio commerciale.

Chi si occupa degli affari legali e della contrattualistica all'interno dell'azienda, nell'attuare il suo piano di azione utilizza la sua cassetta degli attrezzi che è composta da strumenti tecnici il cui utilizzo andrebbe diffuso con una campagna di sensibilizzazione all'interno della categoria. Uno di questi è, come già detto, prevedere un **kit della contrattualistica ESG-oriented**. Così facendo, si integrano nella strategia aziendale gli indici ESG perché il **contratto** costituisce il documento che cristallizza le relazioni commerciali e, dunque, **fornisce un indirizzo chiaro al business.**

Le azioni compiute con la previsione e poi la messa in atto di questo "to do" si realizzano in obiettivi concreti.

Per fare questo il responsabile legale accompagna l'impresa nell'integrazione degli obiettivi ESG nella governance, nei processi decisionali e nel reporting, agevola un approccio "beyond compliance" e ne diffonde la cultura, fa parte del CdA e contribuisce a decidere strategie

condivise, collabora con funzioni interne (CSR, HR, Risk management, Investor relations) al fine di condividere le strategie decise a livello apicale.

Le ricadute delle clausole ESG sui contratti

L'integrazione delle clausole ESG nella contrattualistica tecnologica ha ricadute in diversi ambiti cruciali.
Innanzitutto, nella gestione della **relazione commerciale tra il fornitore e cliente** in cui si determina un vero e proprio cambio di paradigma.
Inoltre, nel **lavoro del gruppo** poiché richiede un approccio interdisciplinare che metta a fattor comune gli aspetti legale, tecnico, di compliance e sostenibilità.
Infine, **verso i competitor** diventando un adempimento che evita di perdere opportunità commerciali, anche se non ancora un obbligo normativo a tutto tondo.
L'impatto che questa previsione riveste nel rapporto contrattuale tra le parti ha degli effetti positivi (allineamento valoriale e strategico tra committente e fornitore e un miglioramento della reputazione e riduzione del rischio ESG), ma **comporta anche rischi e criticità** quali, per esempio, potenziali contenziosi per inadempienze o violazioni ed esclusione di fornitori non conformi, con impatto sulla competitività.

ESG: DAI DATA CENTER GREEN ALLA TUTELA DEI DATI, FINO A ETICA E ANTICORRUZIONE, L'IMPRESA SOSTENIBILE SI COSTRUISCE SU AMBIENTE, PERSONE E GOVERNANCE RESPONSABILE

Tipologie di clausole ESG nei contratti tecnologici e strumenti giuridici

Per comprendere meglio il tema possiamo esaminare alcuni esempi in relazione a ognuno dei temi espressi nell'acronimo ESG.
Alla componente **Environmental** sono ascrivibili clausole ambientali quali, per esempio, l'adozione di data center "green" ovvero alimentati da energie rinnovabili, il monitoraggio e la riduzione della carbon footprint digitale, gli obblighi di reporting ambientale (per esempio la Power Usage Effectiveness o PUE).
Tra le clausole **Social** rientrano la protezione dei dati personali e della privacy (prevista come cluster del "diritto sociale digitale"), il rispetto dei diritti dei lavoratori nella supply chain, l'inclusione di criteri DEI (Diversity, Equity, Inclusion) nelle policy relative al personale che opera nell'organizzazione.
Le clausole di **Governance** includono l'obbligo di conformità a standard ESG internazionali (per esempio ISO 26000, GRI Standards), l'adozione di codici etici e di politiche anti-corruzione.
La gestione delle clausole ESG inserite nel contratto di servizi tecnologici va **effettuata con l'utilizzo di strumenti giuridici,** per esempio gli ESG-SLA (Service level agreement), gli audit ESG con cadenza periodica che possono essere fatti anche da terze parti, la previsione di clausole di manleva e di clausole di risarcimento per danni reputazionali ESG, la redazione di smart contract in ambito blockchain per automatizzare la verifica dei KPI ESG.

Verso la standardizzazione

Il trend attuale suggerisce un percorso verso la standardizzazione dell'uso delle clausole ESG all'interno dei template internazionali dei contratti di tecnologia e questo passaggio mette **l'Italia in una condizione di parità operativa.** Si tratta di un trend molto positivo assieme, per esempio, alla collaborazione tra dipartimenti di uffici legali, uffici compliance e IT finalizzata a una migliore definizione di contratti sostenibili e alla previsione delle clausole ESG anche in contratti di intelligenza artificiale e IoT.
Il cambiamento in atto necessita, tuttavia, un certo grado di flessibilità a carico del responsabile legale aziendale e una necessaria formazione a riguardo.
La sostenibilità, oramai, non è più una opzione ma una necessità che innesca anche un moto di minore instabilità nel futuro delle nuove generazioni.

Il contributo dell'intelligenza per dare **valore ai dati**

L'intelligenza artificiale sta trasformando radicalmente il data management, passando da un approccio passivo basato su supervisione umana a sistemi proattivi capaci di auto-organizzarsi e generare valore in modo autonomo, con benefici concreti per il business

DI PIERO TODOROVICH

La moderna azienda ha di fronte un paradosso: le quantità di dati utili al business continuano a crescere, ma la capacità di estrarne valore non migliora, e spesso si riduce. Secondo gli analisti di *Gartner*, AI/ML, Agent AI e dati "AI-ready" hanno il potere di cambiare questo stato di cose e portare una trasformazione profonda nel modo in cui sono oggi gestite e utilizzate le informazioni aziendali. Alle capacità di raccolta e archiviazione si affianca l'intelligenza che serve a organizzare i dati per generare risultati. Questa evoluzione segna il passaggio da un data management passivo a un ecosistema proattivo in cui l'AI è motore d'innovazione e di efficienza.

Dall'automazione della gestione dati ai suggerimenti

Il data management tradizionale richiede una intensa supervisione umana: cataloghi da aggiornare manualmente, regole di qualità da definire caso per caso, policy di governance rigide. L'introduzione di AI/ML e Agentic AI ribalta il paradigma portando a sistemi che apprendono continuamente, prendono decisioni contestuali e si adattano dinamicamente. L'Agentic AI rappresenta un salto qualitativo: **mentre i sistemi ML tradizionali richiedono supervisione costante, gli agenti AI operano in modo semi-autonomo**, definendo obiettivi, pianificando strategie e coordinando gli strumenti per raggiungere i risultati anche senza l'intervento umano. Una dote utile, per esempio, per la correzione dei dati, fonte di costi ingenti per le imprese. Algoritmi di **anomaly detection** apprendono cosa è "normale" e cosa non lo è, segnalando le incongruenze. I sistemi più avanzati non solo rilevano gli errori, ma applicano correzioni basate sui pattern appresi e propongono consolidamenti dei record duplicati. Un caso concreto: un retailer con milioni di record cliente su sistemi CRM ed e-commerce identifica automaticamente che "Via G. Garibaldi 15" e "V. Garibaldi, 15" sono lo stesso indirizzo. Il risultato? Visione cliente unificata, migliore personalizzazione nelle attività di marketing e nessuno spreco nelle postalizzazioni.

La proliferazione delle fonti di dati rende difficile trovare le informazioni giuste al momento giusto. L'AI rivoluziona questo aspetto **generando automaticamente metadati** attraverso le capacità semantiche per analizzare nomi di colonne e le relazioni tra tabelle. I sistemi più sofisticati costruiscono grafi di conoscenza che mappano le relazioni, supportando le query in linguaggio naturale. Ma la più sorprendente innovazione sta nei **suggerimenti contestuali**. Un data scientist che, per esempio, lavorasse sulla churn prediction può ricevere suggerimenti sui dataset rilevanti già usati da altri team, su correlazioni sconosciute individuati dal sistema o altri avvisi per problemi di qualità. Questo può ridurre da settimane a giorni il time-to-insight, con incrementi di produttività rilevanti.

L'ADOZIONE? MEGLIO GRADUALE E "HUMAN IN THE LOOP"

L'adozione delle risorse AI/ML e Agentic AI nell'ambito del data management si avvantaggia di approcci graduali che partono da use case specifici ad alto impatto sul business e con rapido ROI. Secondo le raccomandazioni **"Stop Experimenting And Start Scaling Your AI Efforts"** di Forrester è fondamentale il giusto bilanciamento tra automazione e controllo umano, iniziando con modalità "human-in-the-loop" ed evolvendo verso una maggiore autonomia. La formazione è cruciale per permettere ai team di comprendere e collaborare con i nuovi strumenti; passare da operazioni manuali alla supervisione di sistemi che operano in modo autonomo e saper interpretare i risultati. Gli strumenti non sostituiscono i professionisti dei dati ma li liberano dalle attività a più basso valore per lasciare tempo a quelle più utili a fare dei dati un asset strategico per il business.

Dalla governance proattiva alla compliance automatizzata

La governance è l'area dove l'Agentic AI mostra il potenziale più trasformativo. Regolamenti come GDPR impongono obblighi stringenti e la compliance manuale è costosa e rischiosa. I sistemi AI automatizzano la classificazione dei dati sensibili, implementano policy enforcement dinamico e generano audit trail completi. Gli agenti avanzati possono **gestire autonomamente i diritti previsti da GDPR degli interessati**. Quando un cliente richiede la cancellazione dati, l'agente identifica tutte le occorrenze attraverso sistemi diversi, verifica gli obblighi legali ed esegue la rimozione, documentando il processo. Queste funzioni hanno permesso ad alcuni istituti finanziari europei di ridurre da giorni a ore il tempo di evasione delle richieste, eliminando il rischio degli errori umani.

L'infrastruttura dati è una voce di costo significativa del data management, sia con risorse locali sia utilizzando il cloud. L'AI consente **l'ottimizzazione predittiva, analizzando pattern di accesso, stagionalità e correlazioni,** i sistemi prevedono quali dati saranno necessari e quali possono essere archiviati. Questa capacità permette **tiering sofisticati dei dati**, con il pre-caricamento dei dataset associati alle attività in fase di avvio e suggerimenti per l'eliminazione definitiva dei dati che non hanno più valore. Una multinazionale della distribuzione ha riportato riduzioni del 30% nei costi cloud storage, senza impatto sulle performance. L'ottimizzazione può includere anche **scheduling di job** non urgenti durante le ore di minor costo e il dimensionamento dinamico dei cluster.

L'Agentic AI abilita sistemi autonomi capaci di gestire processi complessi end-to-end. Un agente può, per esempio, **orchestrare l'onboarding di nuove fonti dati**: connettere, profilare, generare schemi di mappatura, configurare pipeline, catalogare e notificare l'inserimento ai team. Sono preziose le **capacità di self-healing**: se una pipeline fallisce, l'agente AI diagnostica il problema, tenta la correzione o passa la palla all'essere umano fornendogli l'analisi dettagliata. Microsoft riporta casi d'uso in cui l'Agentic AI ha consentito una riduzione del 50% del carico operativo e accuratezza del 99,9% nelle richieste gestite.

I **CEO** guardano alle imprese di domani

Lo studio annuale di IBM sulle future linee di sviluppo strategico che i CEO daranno alle loro aziende nei prossimi anni, realizzato in collaborazione con Oxford Economics, identifica cinque aree di cambiamenti strutturali, organizzativi e competitivi, con indicazioni pratiche per realizzarli. In una competizione "fluida", l'AI impatta fortemente processi e tecnologie e spinge a una revisione di modelli, culture, architetture e relazioni che definiranno il modo di essere impresa nei prossimi anni

DI STEFANO UBERTI FOPPA

È ormai da anni evidente come le diverse turbolenze politiche, sociali, climatiche nonché le continue innovazioni sul fronte tecnologico e altro ancora, si trasformino in una disruption economica e nel cambiamento costante di modelli competitivi, anche da poco consolidati. È una situazione di fluidità divenuta ormai normalità dei mercati.

Proprio per questo il **CEO Study di IBM**, considerato dai top manager mondiali come uno tra gli indicatori più interessanti per fissare le future linee di svilup-

po strategico focalizzando il rapporto tra tecnologie digitali e organizzazioni di impresa, rappresenta uno strumento molto utile per inquadrare le future direzioni di cambiamento competitivo delle aziende.
Tra i valori primari dello studio vi è il campione di riferimento: per questa edizione 2025, scritta in collaborazione con **Oxford Economics**, sono stati coinvolti circa 2.000 CEO di 33 differenti aree geografiche e 24 settori di industria, il tutto nel primo trimestre di quest'anno. Oltre a questa base d'indagine, sono state realizzate "conversations" con CEO di clienti basate su priorità strategiche e tematiche di business, leadership, tecnologie, partnership, enterprise transformation.
Tra i topics che emergono dallo studio come elementi strutturali di cambiamento vi è inevitabilmente l'**intelligenza artificiale**, l'indispensabile infrastruttura per liberare le competenze dai task routinari accelerando processi di innovazione. L'accelerazione nell'adozione di soluzioni di AI impatta già ora, e sempre più sarà in futuro, sull'efficienza e la produttività, facendo emergere in impresa i vantaggi competitivi da sfruttare. *"Chi decide di seguire un approccio minimale, troppo cauto, alle scelte tecnologiche di AI decide* - scrivono i ricercatori - *di rinunciare a una nuova capacità competitiva"*. È il ricorso a una pervasiva distribuzione di AI in impresa, che entra in modo continuo e capillare nel ridisegno dinamico dei processi e nella ricerca di nuova efficienza, che potrà consentire all'azienda di sviluppare un nuovo modello competitivo. Gli **Agenti AI** supporteranno nei prossimi anni i CEO e il top management nell'individuare i potenziali impatti sul mercato prima che questi si consolidino. Tecnologie autonomous, adaptive, di continua governance tecnologica e infrastrutturale stanno cambiando il modo di sviluppare il business. Ben **il 61% dei CEO ha dichiarato che sta adottando Agenti AI** e preparando l'organizzazione a un nuovo modello diffuso di gestione. Interessante notare la comparazione delle risposte "Top CEO priorities" sul triennio 2023-25, con la voce "Accuratezza delle previsioni", passata dalla 15ma posizione di un paio di anni fa al primo posto nel 2025, a testimonianza di quanto importante sia oggi il supporto tecnologico per l'analisi intelligente dei dati da cui prendere le corrette decisioni.

Cinque punti per cambiare l'azienda

Dalle risposte sono state quindi elaborate 5 focalizzazioni che rappresentano una roadmap sulla quale i CEO svilupperanno le proprie strategie future:

1. **Fai del coraggio la tua forza**. Come operare in modo sicuro in un periodo di cambiamenti drastici?
2. **Abbracciare la "distruzione creativa" alimentata dall'AI.** Solo chi realizzerà una trasformazione profonda potrà essere nei prossimi anni parte attiva di mercati che saranno completamente ridefiniti.
3. **Realizzare un ambiente dati dinamico**. Molte aziende non hanno ancora le basi per abilitare la trasformazione oggi, bisogna pensare a cosa serve per alimentare le tecnologie di domani.
4. **Concentrarsi sul ROI lasciando la sindrome del "perdersi qualcosa".** Pur nella necessaria sperimentazione di progetti a base AI è necessario focalizzare il ROI.
5. **Prendere in prestito il talento che non si può comprare**. L'AI generativa e gli agenti AI stanno creando nuovi posti di lavoro più velocemente di quanto le aziende riescano a coprirne.

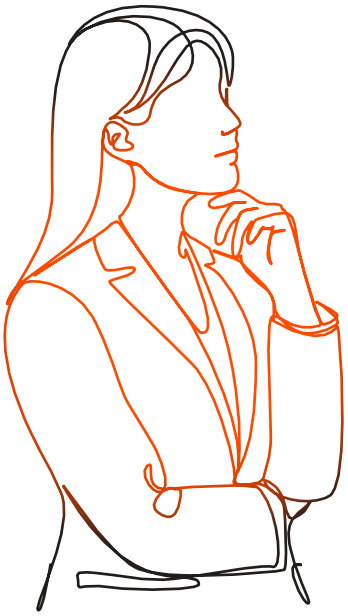
PUNTO 1

FARE DEL CORAGGIO LA FORZA DELLA TRASFORMAZIONE

In periodi di cambiamenti profondi serve accettare livelli di rischio ma con delle certezze di fondo

Dato interessante che emerge dall'indagine è che ben **il 64% del campione ha dichiarato di voler accettare nuovi rischi** rispetto alla possibilità di perdere capacità competitiva. Questo spinge i CEO a investire in nuove tecnologie anche se non si ha una chiara comprensione del valore che queste possono apportare all'organizzazione. Insomma la paura di restare indietro è tanta (il 37% afferma anche che quando si tratta di nuove adozioni tecnologiche è meglio essere veloci e sbagliati piuttosto che giusti e lenti): la maggioranza delle imprese sta introducendo team con il mandato di sperimentare, accelerare l'innovazione, **accettare il fallimento del micro progetto ma andare avanti.** La capacità di innovare genera fiducia nel brand. Il 65% dei CEO afferma infatti che creare e mantenere la fiducia dei clienti avrà un impatto maggiore sul successo dell'azienda rispetto a qualsiasi altra caratteristica del prodotto o del servizio. **In tutti i settori è emerso come la fedeltà dei clienti sia il fattore chiave di differenziazione** che guida il ROI. Ma il concetto di coraggio si deve diffondere in azienda attorno a punti fermi: consapevolezza di disporre di un disegno organizzativo flessibile; competenze di livello e anche, come emerso nel 67% delle risposte dei CEO, dalla capacità di attingere rapidamente a budget dedicati all'innovazione, cosa ancora oggi difficile da ottenere.

COME FARE



IL CORAGGIO DEL CAMBIAMENTO

Non fermarsi all' "Abbastanza buono". Serve inspirare un approccio ambizioso e diffonderlo in azienda attraverso obiettivi chiari e comprensibili che portino a una collaborazione vera attraverso le strutture organizzative a silos. Va sposato un cambiamento radicale.

Creare un'innovazione "liquida". Bisogna creare connessioni organizzative e integrazioni tecnologiche tra le diverse esigenze aziendali, tra le competenze presenti e quelle da ricercare, avviando una trasformazione attraverso investimenti mirati.

Aspettarsi l'imperfezione. Non serve fissare fino nel dettaglio il processo di budgeting o di definizione dell'infrastruttura tecnologica sulla situazione competitiva attuale. Serve piuttosto focalizzare un modello organizzativo e tecnologico basato sull'adattabilità continua, senza cercare la perfetta efficienza. Va monitorato l'effetto di ogni cambiamento sull'organizzazione, sulle relazioni con i clienti e sul coinvolgimento dei dipendenti per migliorare i modelli e orientare al meglio i futuri processi decisionali.

PUNTO 2

ABBRACCIARE LA "DISTRUZIONE CREATIVA" ALIMENTATA DALL'AI

I CEO stanno realizzando una piattaforma che possa rigenerare dal legacy nuovi modelli ed ecosistemi?

Esiste la consapevolezza nei CEO (68%) che l'intelligenza artificiale stia ridefinendo in maniera strutturale i propri core business. Solo però chi approccerà un modello di "distruzione creativa" potrà nei prossimi anni essere parte attiva di mercati completamente ridefiniti. È in atto ormai da tempo, ma accelerato dalla diffusione di software AI, una ridefinizione strutturale di ogni settore, con aziende che "softwarizzano" i propri prodotti e servizi e in cui l'AI gioca sempre più un ruolo primario nell'ingaggio immersivo, personalizzato, del cliente e nella sua fidelizzazione. Il 61% pensa che il vantaggio competitivo sarà appannaggio di chi possiederà la più evoluta AI generativa, usando il corretto modello di AI per le differenti tipologie di lavori e figure professionali. Anche il ridisegno dinamico dei processi e la loro governance automatizzata dall'AI in rapporto a cambiamenti di modelli competitivi repentini nonché alla capacità di sviluppare velocemente progetti di innovazione, sarà la risposta più efficace. Si creeranno nuove modalità di relazione persone-sistemi AI, con raccomandazioni operative e acquisizione di nuove competenze da entrambe le parti: nelle persone, che agiranno sulla base di alcune raccomandazioni dai sistemi AI frutto dell'analisi continua dei dati; e da parte dei sistemi di AI attraverso l'analisi costante dei comportamenti e degli output delle persone nelle loro modalità operative e di integrazione lavorativa con il resto dei sistemi aziendali.

COME FARE

DISEGNARE UNA "DISTRUZIONE CREATIVA"

Pensare come una start up. È da tempo che si teorizza questo modello. Ma l'AI sta accelerando questa impostazione: serve sviluppare un modello orientato alla trasformazione dinamica, incoraggiando i team all'adozione di strategie non consolidate; introdurre criteri di misurazione e iterare ciò che si è imparato per evitare l'esecuzione di piani a lungo termine che rischiano di diventare presto obsoleti.

Evitare un modello di lock-in. La storia insegna che il lock-in tecnologico è pericoloso per l'evoluzione anche organizzativa dell'azienda. Servono tecnologie di AI open source per favorire l'interoperabilità e garantirsi la libertà di adattare i modelli alle esigenze aziendali.

Progettare un motore di analisi basato sull'AI. Definire chiaramente come gli AI Agent operano e chi sono i responsabili della validazione del loro lavoro. Stabilire metriche e sistemi di monitoraggio per valutare l'efficacia dell'AI e, cosa molto importante per non delegare errori e meriti ai sistemi di AI, creare una "cultura della responsabilità". Fondamentale è ad esempio determinare dove è appropriato che l'AI automatizzi il processo decisionale e dove invece dovrebbe svolgere un semplice ruolo di supporto.

REALIZZARE UN AMBIENTE DATI DINAMICO

PUNTO 3

Molte aziende non hanno ancora le basi per abilitare la trasformazione oggi, pensiamo a cosa serve per alimentare le tecnologie di domani

Durante gli ultimi anni l'arrivo di numerose ondate tecnologiche, pensiamo solo al cloud ma anche alla nascita di applicazioni e servizi sempre più intelligenti che hanno "aperto" l'azienda a clienti, partner, fornitori, ecc, hanno determinato una forte frammentazione, con software e hardware non sempre integrati in imprese con tipiche strutture a silos. Questa è l'opinione di circa il 50% degli intervistati. E il punto di riaggregazione non può che partire dai dati, con una data quality governata da cui si possa partire per sostenere progetti di innovazione. Il 68% dei CEO sostiene infatti che un'ampia e integrata data architecture di impresa sia l'elemento primario per collaborazioni cross funzionali e supporto a progetti di innovazione, mentre il 72% afferma che sfruttare i dati proprietari aziendali è fondamentale per sbloccare il valore dell'AI generativa. Non serve un modello di centralizzazione dei dati, peraltro impossibile da realizzare. Serve piuttosto definire identificazioni coerenti e condivise, strutturate e soprattutto gestite, dando al dato un valore strategico: se le soluzioni di AI diventeranno la base strategica che impatterà molte aree dell'azienda, è chiaro che la qualità e la governance del dato per istruire sistemi di AI generativa indirizzati alle varie aree aziendali risulteranno imprescindibili. Solo da un ambiente dati coerente e dinamico nella sua evoluzione potranno partire gli adeguati supporti tecnologici e di processo che connoteranno l'innovazione futura.

COME FARE

UN AMBIENTE DATI EFFICACE

Padroneggiare i fondamentali. Serve la consapevolezza della necessità di un passaggio da dashboard e report statici a informazioni più conversazionali e predittive basate sull'AI. Identificare le varie fonti dati presenti in azienda, facendo una check quality in termini di stato attuale, utilità, lacune e punti deboli. Bisogna creare una visione unificata, distribuita e democratica dei dati organizzativi, con deleghe di aggiornamento, funzionalità self service, virtualizzazione, integrazione tra i diversi data base.

Collegare le persone al flusso dei dati. Creare un data fabric per integrare Agenti AI nelle operazioni quotidiane, automatizzando le attività di routine, aumentando il processo decisionale umano e supportando il lavoro di alto valore. Va definito un framework per la data quality basato su elementi di accuratezza, completezza e coerenza. Va utilizzata una piattaforma dati cloud-native per la collaborazione real time tra i silos aziendali e per rendere i dati più accessibili. Punto strategico, la security: va definito un framework di sicurezza dei dati che garantisca protezione e che l'accesso sia limitato a persone autorizzate.

Istruire gli agenti di AI, poi studiarli. Va sviluppato un framework di formazione per fornire agli Agenti AI i dati e le informazioni necessari per automatizzare i flussi di lavoro end-to-end. L'istruzione dell'Agente deve comprendere anche gli elementi peculiari dell'organizzazione, inclusi aspetti etici non generici ma pratici, policy di sicurezza e privacy, nonché i risultati attesi in termini di customer experience. Vanno definiti anche cicli di feedback in cui gli agenti AI possano fornire suggerimenti per migliorare qualità, accessibilità dei dati e ottimizzazione sui processi aziendali.

Nell'ambito dell'AI, le imprese hanno fino a oggi sperimentato iniziative, spesso con la paura di "perdersi qualcosa" in questa fase tecnologica iniziale.
Risultato: negli ultimi tre anni i CEO hanno dichiarato che solo il 25% delle iniziative di AI ha confermato il ROI atteso, e che solo il 16% dei progetti si è esteso a livello dell'intera impresa. Oggi e sempre più in futuro, ha dichiarato quindi il 65% dei CEO, le aziende si affideranno a progetti di intelligenza artificiale basati fortemente sul ROI, e ben il 68% ha affermato che la propria impresa già dispone di metriche chiare per misurare il ROI dell'innovazione.
Tuttavia, come emerge dalle Top CEO priorities 2025, la focalizzazione CEO per i prossimi anni riguarderà una maggiore "Accuratezza nelle previsioni" della domanda e in generale nel prevedere le variabili competitive. Questo richiederà un diverso orizzonte temporale e nuove metriche per la definizione e la misurazione del ROI. Sono infatti numerosi i campi di applicazione in azienda per l'AI: dalla creazione di una maggiore soddisfazione e fidelizzazione dei clienti alla riduzione delle violazioni della sicurezza e delle sanzioni per la conformità; fino alla generazione di nuove opportunità di cross o upselling.
Quindi l'impatto dell'AI sui risultati aziendali nelle diverse unit potrebbe anche essere non così evidente da rilevare e misurare. Ad esempio, il 51% dei CEO prevede che nuovi processi di automazione a base AI miglioreranno la customer experience nel 2026, rispetto al solo 16% del 2024. Non sarà facile misurarla!

PUNTO 4

CONCENTRARSI SUL ROI ABBANDONANDO LA SINDROME DEL "PERDERSI QUALCOSA"

Pur nella necessaria sperimentazione di progetti a base AI è necessario focalizzare il ROI

COME FARE

CONCENTRARSI SUL ROI MA... ESTENDERE I KPI

Bilanciare l'eccessivo ottimismo con il concreto potenziale. Dare priorità a iniziative basate sul ROI. Raccordare le prestazioni dei team di innovazione che usano Agenti AI con i risultati ottenuti. Vanno ampliati i Kpi per misurare il ROI dell'innovazione, includendo metriche che rilevino il valore dei dati, il rendimento dell'innovazione e il tempo risparmiato (rispetto ai metodi tradizionali) per ottenere insight utili.

Concentrarsi sull'orizzonte dell'innovazioni. I Kpi devono essere disegnati secondo un modello di individuazione di valore di innovazione. Emergeranno poi opportunità per "scaricare a terra" risultati concreti, e a quel punto si potranno indirizzare le risorse verso questi obiettivi di business.

Non disperdere gli investimenti. Il fallimento o la scarsa incisività di un progetto fa parte del gioco. Procedere oltre senza insistere oltre misura. Serve un processo formale di project management per monitorare cosa funziona e cosa no. In questo modo anche i diversi team potranno condividere le esperienze. I Kpi predefiniti sia su base "ROI produttività" sia su "ROI di valore di innovazione", devono essere il riferimento per decidere se proseguire modificare o annullare i progetti.

PUNTO 5

PRENDERE IN PRESTITO IL TALENTO CHE NON SI PUÒ COMPRARE

L'AI generativa e gli agenti AI stanno creando nuovi posti di lavoro più velocemente di quanto le aziende riescano a coprirne

I CEO intervistati hanno dichiarato che il 31% della propria forza lavoro avrà bisogno di nuovi percorsi di formazione entro i prossimi tre anni. Il 54% ha affermato che sta cercando assunzioni in ruoli correlati all'intelligenza artificiale, ruoli che non esistevano solo un anno fa. Mancano le corrette competenze spesso in posizioni delicate. E per queste figure servono adeguati incentivi. Si sta facendo nuova formazione a figure professionali presenti in azienda, assumendone di nuove e usando anche gli stessi Agenti AI per rafforzare il processo formativo e colmare il gap di competenze. Importante e delicato in questa fase è il ricorso, dichiarato dai CEO, al proprio ecosistema di partner specializzati in queste tecnologie ma che non potrà essere davvero calato nella dimensione organizzativa e culturale dell'azienda senza un diretto intervento delle persone interessate e dei diversi team aziendali. Natualmente management e top management compreso.

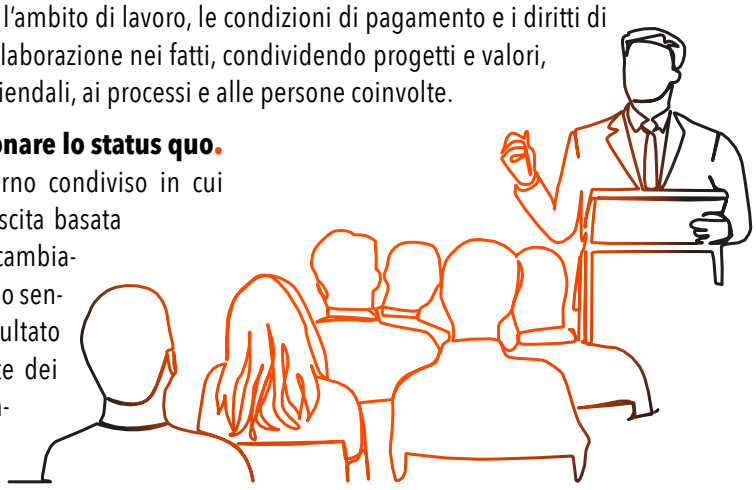
COME FARE

CERCARE NUOVE COMPETENZE, APRIRE L'IMPRESA

Conoscere i punti deboli e sfruttare i punti di forza. Gli Agenti AI possono essere usati per un'analisi della forza lavoro, evidenziando punti forza e carenze. In questi ambiti vanno scelti i talenti, sia tecnologici sia di business, presenti in impresa, gente che abbia il desiderio di misurarsi con il nuovo e la trasformazione. Serve anche creare un gruppo misto di competenze business-IT che abbia mandato di innovare in armonia con il quadro organizzativo e di business generale.

Rafforzare le partnership strategiche. L'integrazione con l'ecosistema dei partner, spesso tecnologicamente all'avanguardia nelle soluzioni di AI, è essenziale. Vanno definiti con chiarezza ruoli, responsabilità, termini e condizioni della partnership, inclusi l'ambito di lavoro, le condizioni di pagamento e i diritti di proprietà intellettuale. Deve essere una collaborazione nei fatti, condividendo progetti e valori, aprendo in sicurezza, l'accesso ai sistemi aziendali, ai processi e alle persone coinvolte.

Utilizzare i talenti esterni per rivoluzionare lo status quo. Serve costruire un ambiente esterno-interno condiviso in cui sia comune la mentalità orientata alla crescita basata su competenze tecniche che accelerino il cambiamento. Anche le competenze esterne devono sentirsi ingaggiate nel raggiungimento del risultato aziendale e devono fare pienamente parte dei team impegnati in una profonda trasformazione aziendale.



MERCATI VERTICALI

Retail ed **e-commerce** strategie e tecnologie per competere oggi

In un periodo in cui in Italia il retail vive una fase di maturità e l'e-commerce cresce, l'esperienza d'acquisto viene ridefinita da AI, gestione dati, logistica sostenibile e customer service evoluto. Per essere vincenti bisogna essere innovativi e saper integrare tecnologia e relazione umana

DI FABRIZIO PINCELLI

L'accelerazione tecnologica e, soprattutto, i mutamenti nelle aspettative dei consumatori hanno obbligato il retail e l'e-commerce a subire una trasformazione radicale. Il cliente digitale non cerca solamente un prodotto a buon prezzo, ma un'esperienza fluida, un servizio affidabile, trasparenza e un rapporto che si va costruendo nel tempo. **In Italia**, come mostrano gli ultimi dati, **il settore è in forte espansione**, ma entra in una fase di consolidamento: crescite positive, ma con margini che derivano dall'innovazione, non più solo dalla mera espansione. In questo contesto, le imprese stanno agendo principalmente su alcuni fronti critici: **gestione dei dati** e **AI**, iniziative di **attrazione del cliente**, **logistica** e **customer service**. Vediamo come.

Mercato: il contesto italiano

Secondo i dati raccolti dagli *Osservatori del Politecnico di Milano* e da *Netcomm*, nel 2025 l'e-commerce B2C in Italia supererà i 62 miliardi di euro con una crescita del +6 % rispetto al 2024. Di questi, oltre 40 miliardi riguardano prodotti (+6 %) e circa 22 miliardi i servizi, che salgono a un tasso leggermente più elevato (+8 %). Gli utenti digitali sono ormai 35,2 milioni, con un aumento di 1,5 milioni rispetto all'anno precedente. **Food & grocery** e **beauty & pharma** sono i settori che crescono più della media, ciascuno con +7 %. Anche **abbigliamento**, **informatica** ed **elettronica di consumo** e **arredamento/home living** crescono, ma con ritmi leggermente inferiori (attorno al +5-6 %). La quota dell'online nei consumi retail totali di prodotti raggiunge l'11,2 %, segno che, pur con spazi di crescita, la penetrazione digitale sta già maturando.

Da evidenziare che il numero di **imprese italiane con un sito e-commerce** è aumentato del 3,4% rispetto al 2024, raggiungendo le 91.000 realtà, con una crescita marcata delle società di capitale (+8,5%). Anche in questo caso, i dati evidenziano la maturazione del settore e l'integrazione di strategie digitali avanzate. A dominare sono **le micro e piccole imprese**, mentre le aziende italiane che operano nell'e-commerce sono distribuite principalmente in Lombardia, Lazio e Campania, con Milano, Roma e Napoli come principali hub.

Le nuove abitudini degli utenti

Gli acquirenti online consultano mediamente **4 touchpoint** prima di effettuare un acquisto. Di questi, 2 sono legati a contenuti prodotti direttamente dai brand, come i loro siti web o app (50,3%) e i loro e-commer-

ce (44,2%). I restanti 2 touchpoint sono invece riferiti a contenuti indipendenti, tra cui motori di ricerca (55,7%), recensioni (50%) e comparatori (40%). I **social media** rimangono una fonte importante di orientamento per circa un acquisto su quattro (29,8%), insieme ai **punti vendita** e al **retail media online**, mentre le **notifiche push** segnano un leggero calo. Inoltre, in base alla categoria di prodotto, si osservano preferenze specifiche: ad esempio, l'**uso di AI** e **chatbot** è particolarmente rilevante nell'elettronica e nell'editoria, mentre il retail media offline è più influente nel settore alimentare. Ogni categoria ha quindi un set di touchpoint prioritari, con il sito del brand e l'e-commerce che prevalgono nell'abbigliamento.

Il **Retail Report 2025** di **Adyen** rivela che il 34 % degli utenti europei che comprano online ha usato l'AI per fare acquisti, un dato in aumento del 47 % rispetto al 2024. Adesione maggiore dalla **Gen Z**, ma con incrementi significativi registrati anche tra le fasce più mature come i **Baby Boomer**. Questi numeri confermano che l'AI non è più un esperimento, ma sta entrando nel quotidiano dell'esperienza di acquisto.

Gestione dei dati e uso dell'AI

A conferma del ruolo che ha assunto l'AI, le aziende stanno investendo sempre più nella raccolta e nella gestione dei dati dei clienti. Tali dati spaziano da quelli transazionali, come storici di acquisto e resi, fino a quelli comportamentali e demografici: preferenze, frequenza d'uso, dispositivo, località geografica. Strumenti come **customer data platform, analytics avanzati** e **dashboard** integrate permettono di avere una visione unica del cliente, abilitando segmentazioni dettagliate e comunicazioni personalizzate.

L'intelligenza artificiale entra con forza in queste strategie. L'**AI predittiva** serve per anticipare comportamenti, come l'abbandono del carrello, la probabilità di ripetere l'acquisto, la predisposizione ad acquistare un determinato prodotto. L'**AI generativa** supporta, invece, la creazione automatica di contenuti personalizzati: email, raccomandazioni prodotto, suggerimenti nelle app e sui siti web. **Chatbot conversazionali** (basati su AI), forniscono richieste semplici, rispondono a FAQ, gestiscono il supporto iniziale, lasciando i casi più complessi al servizio umano.

Tuttavia, l'utilizzo di dati e AI comporta rischi da non sottovalutare: la **privacy** resta centrale. Gli utenti chiedono trasparenza su quali informazioni vengono raccolte, come vengono utilizzate, se ci sono bias negli algoritmi, come vengono esercitati i diritti di accesso, rettifica e cancellazione. Le normati-

L'AI SI ADEGUA ALLO STATO EMOTIVO DEL CLIENTE

La nuova frontiera nel dialogo con il cliente è l'**intelligenza artificiale emozionale (Emotion AI)**. Sistemi di machine learning evoluti, combinando Natural language processing (NLP), analisi vocale, riconoscimento facciale e sentiment analysis, riescono a rilevare in tempo reale stati emotivi, così da permettere alle macchine di modulare risposte non solo corrette sul piano semantico, ma anche empaticamente adeguate.

Nel customer service, l'integrazione dell'Emotion AI in chatbot e virtual assistant consente di **identificare segnali di frustrazione o insoddisfazione** attraverso parametri testuali e prosodici, attivando escalation verso operatori umani qualificati. Questa capacità riduce i tassi di churn e ottimizza indicatori come il Net Promoter Score (NPS). Parallelamente, nei contact center avanzati, l'analisi emotiva in tempo reale guida la personalizzazione del tono e dello stile.

Nel retail, **sistemi di riconoscimento facciale e vocale** permettono di correlare le reazioni emotive dei clienti a variabili ambientali, come layout e posizionamento dei prodotti, consentendo un'ottimizzazione dinamica delle strategie di merchandising. L'integrazione con i programmi di loyalty offre inoltre la possibilità di calibrare campagne promozionali sulla base delle emozioni effettivamente rilevate, incrementando il tasso di conversione. Sul fronte tecnologico, l'affidabilità dei modelli dipende dalla qualità e dalla diversità dei dataset di training: un requisito indispensabile per mitigare bias culturali e linguistici. L'adozione di modelli di continuous learning migliora la capacità predittiva e l'adattamento a contesti complessi. Tuttavia, la raccolta di dati biometrici introduce criticità legate a privacy e sicurezza: anonimizzazione, crittografia e privacy by design diventano prerequisiti imprescindibili, soprattutto in ottica di conformità al GDPR. La convergenza tra Emotion AI, sistemi IoT e Large language model (LLM) apre scenari di interazione multimodale, in cui gli algoritmi non solo comprendono il contenuto delle richieste, ma anticipano bisogni latenti attraverso una valutazione empatica. Una prospettiva che promette vantaggi competitivi, ma che richiede un equilibrio rigoroso tra innovazione e governance etica dei dati.

ve come il GDPR impongono obblighi stringenti che non possono essere ignorati. Diverse ricerche mostrano come, se l'utente percepisce un uso scorretto o eccessivo dei dati, la fiducia si riduce rapidamente. Per esempio, in uno studio la *Cornell University* ha misurato gli impatti su traffico e redditività per 6.286 siti web di 24 settori, coprendo 10 mesi prima e 18 mesi dopo l'entrata in vigore del GDPR. Nella ricerca sono stati isolati gli **effetti a breve e lungo termine del GDPR sul comportamento degli utenti**. I risultati hanno mostrato che il GDPR ha avuto un impatto negativo medio sull'utilizzo online per sito web; in particolare, le visite settimanali sono diminuite del 4,88% nei primi 3 mesi e del 10,02% dopo 18 mesi dall'entrata in vigore.

A 18 mesi dall'entrata in vigore del GDPR, questi cali si sono tradotti in **perdite di fatturato medie di circa 7 milioni di dollari** per i siti di e-commerce e di quasi 2,5 milioni di dollari per i siti web basati su annunci pubblicitari. Va però evidenziato che l'impatto del GDPR è variato a seconda delle dimensioni del sito, del settore e dell'origine degli utenti, con alcuni siti e settori di grandi dimensioni che hanno beneficiato del regolamento.

GDPR E FIDUCIA DIGITALE: L'IMPATTO SUI DATI E SUL BUSINESS

Analisi degli effetti della normativa su traffico e ricavi (Studio Cornell University)

IMPATTO IMMEDIATO

-4,88%

Calo medio delle visite settimanali nei primi 3 mesi dal GDPR

EFFETTO A LUNGO TERMINE

-10,02%

Riduzione media del traffico per sito dopo 18 mesi

CONSEGUENZE ECONOMICHE

-7 M$
-2,5 M$

Rispettivamente per e-commerce e per siti pubblicitari

Più personalizzazione per attrarre clienti

Le imprese stanno sviluppando strategie multidimensionali. La personalizzazione è ormai una parola d'ordine: non solo messaggi su misura, ma esperienze digitali differenziate. Il sito o l'app adeguano offerte, suggerimenti, layout in base ai comportamenti pregressi. Alcune aziende integrano **realtà aumentata, visualizzazioni immersive, video interattivi, "shop the look" o prove virtuali**, per rendere più coinvolgente il processo decisionale. L'**omnicanalità** è un'altra frontiera: il cliente vuole poter passare dal digitale al fisico e viceversa senza discontinuità. Soluzioni di click & collect, ritiro in negozio per ordini online, politiche di reso fluide che permettono di restituire articoli acquistati online in negozio fisico sono ormai mainstream per molti retailer. Anche la **fidelizzazione** evolve: programmi fedeltà digitali, incentivazioni per clienti abituali, offerte personalizzate, retargeting intelligente, notifiche push studiate per momento e contesto.

Il **retail media** rappresenta una leva nuova: è la pubblicità fatta all'interno dei canali del retailer stesso (app, sito, punto vendita digitale), che usa dati proprietari per proporre ai marchi campagne mirate. In Italia, diversi importanti brand del retail hanno iniziato a sperimentare **digital signage, campagne personalizzate su display in store e piattaforme dedicate.** Come risultato hanno osservato un incremento medio del valore dello scontrino quando hanno implementato soluzioni di digital signage personalizzato che hanno portato ad allungare la permanenza del cliente nei punti vendita.

Un'altra dimensione è quella dell'**omnicanalità estesa**: integrare retail media digitali con esperienze negli store fisici, con piani promozionali sincronizzati, con offerte che si attivano online ma che hanno effetto anche fisico. Le aziende che operano così non solo aumentano il coinvolgimento, ma **raccolgono dati più ricchi**, migliorano la personalizzazione e possono **modulare le strategie** in modo dinamico. Secondo i dati raccolti da *Morgan Stanley*, il mercato globale del retail media potrebbe raggiungere 130 miliardi di dollari entro il 2025, grazie al boom della pubblicità che i retailer stanno generando grazie all'uso dei propri dati clienti.

Logistica: ottimizzazione, sostenibilità, e performance

La logistica resta uno degli elementi decisivi per il successo del retail e, soprattutto oggi, dell'e-commerce: il tempo di consegna, la precisione nella gestione dell'ordine, il modo in cui vengono gestiti i resi hanno impatti concreti sulla soddisfazione del cliente e sulla fedeltà. In Italia, come si è detto, sono state spedite 186 milioni di unità solo nel primo trimestre del

TIKTOK SHOP STA RIDEFINENDO LE REGOLE DELL'E-COMMERCE

TikTok non è più solo una piattaforma di condivisione video. Negli Stati Uniti, nell'ultimo anno, le vendite tramite il suo servizio di shopping sono cresciute del 120%, con una rete di oltre 750 categorie di venditori e più di 70 milioni di prodotti disponibili. Un fenomeno che segna l'avanzata del social commerce, dove l'acquisto va oltre l'atto transazionale per diventare un'esperienza integrata nei contenuti e nelle community.
"Il social commerce è la fusione di contenuti, cultura e commercio – spiega **Chris Kastenholtz, CEO Global di Pulse Advertising** –. *Trasforma il pubblico in acquirenti attraverso l'esperienza in tempo reale, non solo tramite elenchi di prodotti. Mentre l'e-commerce classico è transazionale, il social commerce è emotivo, integrato e in rapida evoluzione".* A differenza dello shopping online tradizionale, che richiede a brand e retailer di costruire e promuovere le proprie piattaforme, TikTok Shop concentra l'intero percorso d'acquisto dentro l'app. I creator diventano veri e propri ambasciatori dei prodotti, presentandoli alle loro community già fidelizzate. Bastano due click: uno per aprire la scheda del prodotto direttamente dal video, l'altro per confermare l'acquisto, senza mai uscire da TikTok. Un flusso lineare, che riduce la dispersione tipica dei funnel digitali e si affida a una comunicazione post-vendita essenziale ma chiara.
Il modello è già consolidato in Cina, dove tutte le fasce d'età utilizzano il social commerce, mentre **in Occidente la spinta arriva soprattutto da Gen Z e Millennial.** Si tratta di utenti che privilegiano lo smartphone per i propri acquisti e seguono trend e creator come principali fonti di ispirazione. Le cifre spese per singolo ordine restano contenute, ma i tassi di riacquisto sono elevati, soprattutto in categorie come beauty, moda e benessere.
Per i brand, l'opportunità è significativa. *"I vantaggi* – continua Kastenholtz – *sono conversioni rapide grazie al checkout integrato, l'accesso a nuove audience, la fiducia generata dai creator e la reattività alle tendenze in tempo reale"*. Prodotti venduti in kit, edizioni limitate o offerte speciali sono particolarmente adatti a questo modello, che gioca sull'**urgenza e sul valore percepito**.
Se la Cina è già un mercato maturo, capace di vendere online di tutto, dagli snack alle automobili, in Europa il percorso è appena iniziato. Ma la direzione è chiara: il social commerce si candida a diventare la forma prioritaria di acquisto online, unendo intrattenimento, relazione e shopping in un unico ambiente digitale.

2024, con un incremento del 13,5% rispetto allo stesso periodo dell'anno prima, segno che la domanda si espande, ma che serve capacità operativa e infrastrutturale adeguata.
Un'esperienza d'acquisto fluida non può prescindere da consegne rapide, precise e sostenibili. I **magazzini automatizzati**, gestiti da **software di orchestrazione** e popolati da **robot mobili**, consentono di processare ordini con maggiore efficienza, riducendo errori e tempi di evasione.
Le tecnologie di **machine learning** migliorano la previsione della domanda e ottimizzano la gestione delle scorte, evitando sprechi e ritardi. Parallelamente, la **distribuzione last-mile** sta sperimentando nuove soluzioni più sostenibili, dai corrieri elettrici ai punti di ritiro automatici o i locker intelligenti che permettono al cliente di ritirare l'ordine in qualsiasi momento, riducendo costi e impatti ambientali.
Le **tecnologie predittive** aiutano a gestire le scorte, limitare rotture di stock (out of stock) e ottimizzare l'allocazione del magazzino, evitando sprechi o costi eccessivi di stoccaggio. Anche il packaging viene rivisto per minimizzare impatto ambientale e costi.
Un aspetto che emerge è che la **logistica** non è più vista solo come un semplice costo, ma è **un driver di differenziazione**: i clienti sono disposti a pagare di più o scegliere un retailer che offre consegne rapide, consegne in giornata, o almeno una delivery affidabile. Al contrario, ritardi, ordini sbagliati, prodotti danneggiati compromettono la reputazione, specialmente con la facilità con cui i feedback online si diffondono. Anche la **tracciabilità** è diventata un elemento distintivo: grazie a piattaforme basate su **blockchain** e **sensori IoT**, i consumatori possono monitorare in tempo reale lo stato della spedizione e avere garanzie sull'autenticità e sulla provenienza dei prodotti. Questo rafforza la fiducia e apre la strada a un modello di retail più trasparente e responsabile.

Customer service: evoluzione verso il valore aggiunto

Il **servizio clienti** si sta trasformando da funzione reattiva a preventiva. Le aziende stanno adottando chat automatizzate, AI, sistemi di routing intelligenti che indirizzano il cliente al

servizio più adeguato, riducono i tempi di risposta e aumentano la soddisfazione complessiva. In questo scenario i chatbot assumono un ruolo strategico: da semplici strumenti di automazione sono diventati **assistenti digitali** capaci di accompagnare l'utente lungo l'intero percorso d'acquisto. Oggi non si limitano a rispondere a domande frequenti, ma interagiscono in tempo reale, forniscono raccomandazioni mirate e guidano le decisioni con conversazioni naturali e contestuali, disponibili su siti, app e piattaforme di messaggistica.

Il dato è significativo: il 44% dei consumatori utilizza i chatbot per raccogliere informazioni prima di acquistare, mentre il 60% dei Millennial è disposto a concludere l'ordine direttamente all'interno della chat. Segnali che evidenziano un'accettazione crescente di questi strumenti, soprattutto quando l'esperienza è personalizzata.

Esistono due principali tipologie di chatbot: quelli basati su regole, pensati per gestire richieste semplici, e quelli potenziati dall'intelligenza artificiale, capaci di comprendere il linguaggio naturale, apprendere dai dati e offrire consigli su misura. A questi si affianca una nuova generazione alimentata dall'**Agentic AI**, in grado di anticipare i bisogni, prendere decisioni autonome e interagire proattivamente su più canali, integrandosi con l'intervento umano quando necessario.Oggi l'assistenza post-vendita è diventata una componente fondamentale per gestire bene i resi, garantire trasparenza nello stato dell'ordine e offrire supporto multi-canale (telefono, chat, social, app). Tutti elementi che impattano in modo sostanziale sul sentiment del cliente. In caso di problemi, una **risposta rapida e umana rimane un differenziale importante**: quando un chatbot non basta, l'intervento umano deve essere pronto, per evitare frustrazione. L'efficacia del customer service diventa anche tema di reputazione digitale: recensioni, feedback, rating incidono direttamente sul traffico, sulla fiducia e sul tasso di conversione.

Due universi convergenti

Retail ed e-commerce non sono più due universi a sé: si intersecano sempre di più, l'esperienza del cliente digitale influenza il punto vendita fisico, la logistica diventa parte integrante della promessa al cliente, il servizio clienti è leva di fidelizzazione più che di costo, la sicurezza è prerequisito. Per avere successo oggi, le imprese devono riuscire a costruire un ecosistema coerente, centrato sul cliente, sostenibile, tecnologico ma umano.

I dati italiani mostrano mercati in crescita, ma maturi: non basta espandere, bisogna eccellere. Innovazione, cultura organizzativa, investimento in tecnologie abilitanti come AI, analytics, logistica avanzata e sicurezza sono i fattori che rivestono un ruolo sempre più determinante per competere in un mercato dominato da un'economia incerta e da clienti sempre più esigenti.

ECCO COME AVERE CLIENTI PIÙ FEDELI

"La personalizzazione non è più un optional, ma un elemento chiave della relazione tra brand e cliente. I chatbot moderni non si limitano a rispondere, ma interagiscono, imparano e costruiscono esperienze uniche su larga scala". Ad affermarlo è **Vittorio D'Alessio, country manager Italy di Infobip**. Per il retail, si tratta di un'opportunità concreta per migliorare la customer satisfaction, ridurre i carrelli abbandonati e aumentare la fidelizzazione. Perché un progetto di chatbot funzioni davvero, puntualizza Infobip, è essenziale partire dagli obiettivi e dall'analisi dei punti critici del customer journey. Solo così si può creare uno strumento in grado di risolvere problemi concreti e accompagnare l'utente in ogni fase dell'acquisto. La coerenza con l'identità del brand diventa un fattore determinante: la "voce" del chatbot deve riflettere lo stile aziendale, che sia empatico e informale per un marchio lifestyle o più sobrio e professionale nel lusso o nell'elettronica.

Il valore offerto al cliente è un altro tassello decisivo. Non basta fornire risposte rapide: un chatbot efficace deve suggerire prodotti, proporre promozioni personalizzate e diventare un vero alleato nelle decisioni d'acquisto. Per questo è cruciale l'integrazione omnicanale, che consenta di muoversi senza frizioni tra sito, app, social e piattaforme di messaggistica, mantenendo il contesto della conversazione.

La tecnologia sottostante deve essere flessibile e scalabile, capace di crescere con l'azienda e di orchestrare interazioni intelligenti tra intelligenza artificiale e operatori umani. Infine, l'implementazione non si esaurisce con il lancio: l'analisi dei dati e dei feedback consente di affinare costantemente l'esperienza. Un chatbot ben monitorato, alimentato dall'AI, diventa col tempo un asset sempre più strategico.

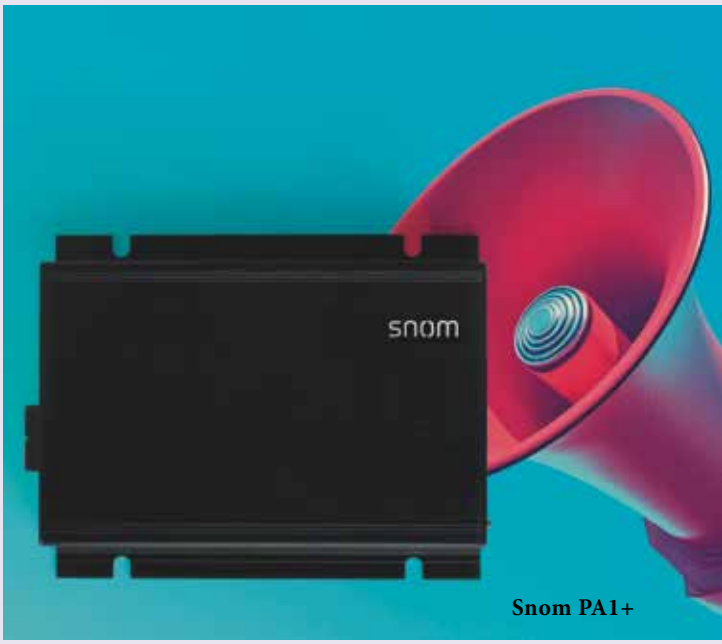
Nel panorama competitivo attuale, i chatbot personalizzati sono molto più di una soluzione tecnologica: rappresentano una leva per creare relazioni più profonde, tempestive e su misura, ponendo le basi per un retail più vicino alle aspettative del consumatore digitale.

La tecnologia che rafforza **retail** e **GDO**

Le soluzioni di comunicazione Snom forniscono un supporto ai punti vendita connessi semplificando la gestione, aumentando il livello di sicurezza e migliorando l'esperienza dell'utente

A CURA DELLA REDAZIONE

Snom M900



Snom PA1+

Il settore della distribuzione moderna vive un momento cruciale. Da un lato c'è la necessità di offrire un'esperienza fluida e sicura ai clienti, dall'altro l'urgenza di contenere i costi e di affrontare criticità crescenti come i furti e la gestione delle emergenze. In questo contesto, la tecnologia non è più un supporto accessorio ma un elemento che incide direttamente sui risultati economici e operativi delle aziende

Ridurre i costi operativi e semplificare la gestione

L'introduzione di soluzioni di comunicazione integrate consente di abbattere i costi legati a infrastrutture multiple e a interventi tecnici frequenti. Le s**tazioni multicella DECT, come lo Snom M900**, garantiscono copertura continua su grandi superfici senza necessità di cablaggi complessi. Questo significa meno investimenti iniziali e una manutenzione più snella, grazie anche agli aggiornamenti software che possono essere inviati da remoto. Nella pratica quotidiana, i dipendenti possono spostarsi liberamente tra corsie, magazzini e piani diversi restando sempre collegati, con un impatto immediato sull'efficienza del lavoro e sul servizio offerto al cliente.

Proteggere i margini attraverso la sicurezza

Uno dei problemi più gravi per il settore è la perdita dovuta ai furti: nel 2023, in Italia, il fenomeno ha comportato un danno stimato di 4,6 miliardi di

Gateway Beacon Snom M9B

euro. In questo scenario, strumenti tecnologici dedicati offrono un contributo concreto. Le **cuffie DECT professionali** permettono al personale di scambiarsi informazioni in modo discreto e di reagire tempestivamente in caso di comportamenti sospetti. A queste si aggiunge **il gateway di localizzazione DECT/Bluetooth Snom con Tags**, che consente di monitorare in tempo reale la posizione di merci o oggetti di valore e di generare allarmi immediati se vengono rilevati spostamenti non autorizzati. L'effetto è duplice: si riduce il rischio di perdite economiche e si migliora la percezione di sicurezza all'interno del punto vendita.

Snom E303

Reagire con tempestività alle emergenze

La gestione delle emergenze è un altro ambito in cui la tecnologia fa la differenza. I **telefoni Snom E303**, installati in aree strategiche, consentono di stabilire, con la pressione di un solo tasto, un collegamento diretto con operatori qualificati. Sono dispositivi semplici, immediati e facilmente riconoscibili, che riducono i tempi di reazione e garantiscono al personale uno strumento affidabile in caso di situazioni critiche.
Anche i **terminali cordless rugged come lo Snom M85** contribuiscono a rafforzare la protezione dei dipendenti: grazie alle funzioni di allarme automatico, come il laccetto antistrappo e la modalità "man down", permettono di intervenire rapidamente qualora un lavoratore si trovi in difficoltà. Migliorare la sicurezza interna, infatti, non significa soltanto tutelare le persone, ma anche contenere i costi legati a infortuni o interruzioni dell'operatività.

Snom M85

Migliorare l'esperienza del cliente

Un punto vendita ben organizzato è anche un luogo in cui i clienti percepiscono attenzione e rapidità di servizio. I **terminali IP e le cuffie cordless DECT** rendono possibile un coordinamento costante tra i dipendenti, sia in corsia sia nei reparti di supporto. In questo modo, le richieste vengono gestite senza ritardi e i flussi di lavoro interni risultano più fluidi. Ma non solo; soluzioni per la **diffusione di messaggi al pubblico come lo Snom PA1+** consentono di trasmettere annunci promozionali e informazioni di servizio utili alla clientela. La comunicazione efficiente non è dunque solo un vantaggio per l'azienda, ma si traduce in un miglioramento tangibile dell'esperienza d'acquisto.

Efficienza e sostenibilità grazie all'automazione

Le piattaforme IP di nuova generazione consentono di integrare le telecomunicazioni con i sistemi di automazione dell'edificio e quindi controllare illuminazione, climatizzazione e qualità dell'aria direttamente dai terminali telefonici. Soluzioni come lo Snom PA1+, dotato di relè, rendono ancora più immediato il controllo di serrature e porte elettriche, che possono essere attivate da remoto via SIP premendo un pulsante del telefono. Questo tipo di integrazione contribuisce a ridurre i consumi energetici e a rendere la gestione del punto vendita più sostenibile e immediata. Per le aziende della GDO, si traduce in un abbattimento dei costi di esercizio e in una semplificazione delle operazioni quotidiane, aspetti fondamentali in strutture di grandi dimensioni.

Tecnologia come motore operativo

Mettere insieme comunicazione, sicurezza, gestione delle emergenze e automazione significa trasformare la tecnologia in un vero motore operativo per la GDO. Non si tratta più soltanto di strumenti per migliorare l'organizzazione interna, ma di soluzioni che hanno un impatto diretto sui margini economici, sulla sicurezza del personale e sull'esperienza del cliente. Investire in queste integrazioni significa garantire continuità operativa, sostenibilità e competitività, elementi che oggi fanno la differenza tra un punto vendita che subisce le sfide del mercato e uno capace di affrontarle con successo.

AI E RETAIL 5.0: L'EVOLUZIONE DELL'OMNICANALITÀ

La spesa IT nel settore retail si dimostra resiliente e l'AI è un grande abilitatore dell'integrazione omnicanale, incrementando l'efficienza operativa e migliorando l'esperienza del cliente

Nel 2025, il panorama europeo del settore del retail è profondamente influenzato da nuove pressioni normative, volatilità macroeconomica e aspettative dei consumatori in continua evoluzione. In questo complesso scenario economico, i retailer sono chiamati ad adottare un **approccio sempre più flessibile** e guidato dai dati, capace di mitigare i rischi, cogliere opportunità di crescita e garantire continuità operativa tra i diversi canali. Di fronte alle sfide macroeconomiche e politiche, unitamente all'evoluzione continua delle aspettative dei consumatori, l'adozione dell'**AI** e l'integrazione **omnicanale** diventano non solo un'opportunità per le aziende, ma una necessità per il successo futuro nel retail.

L'Intelligenza artificiale diventa sempre più agentica, non senza costi

Nel cuore della rivoluzione Retail 5.0, non tutte le intelligenze artificiali sono create allo stesso modo. L'Intelligenza Artificiale è diventata il principale motore della spesa IT a livello globale. In Europa, la spesa per soluzioni AI è destinata a raggiungere i 144,6 miliardi di dollari entro il 2028, con un tasso di crescita annuo composto (CAGR) del 30,3%. A livello globale, i principali casi d'uso dell'AI agentica riguardano l'ottimizzazione delle catene di approvvigionamento, la gestione dei prezzi dinamici e la personalizzazione delle esperienze dei clienti, migliorandone la soddisfazione e la fidelizzazione. In Europa invece, il 37% delle aziende retail ha già avviato alcuni progetti **Agentic AI**, sebbene ancora in fase sperimentale, mentre il 24% dichiara di star già sviluppando alcuni use cases orientati all'accelerazione operativa (sia del negozio che online) e al miglioramento dell'esperienza di acquisto e di supporto al cliente in tempo reale (tra ricerca e selezione di prodotti tramite mobile app all'assistenza personalizzata in negozio). Se da un lato gli AI agents svolgono compiti specifici come suggerire prodotti o rispondere a domande, dall'altro l'Agentic AI si muove su un altro livello: agisce con autonomia, prende decisioni strategiche, anticipa i bisogni dei

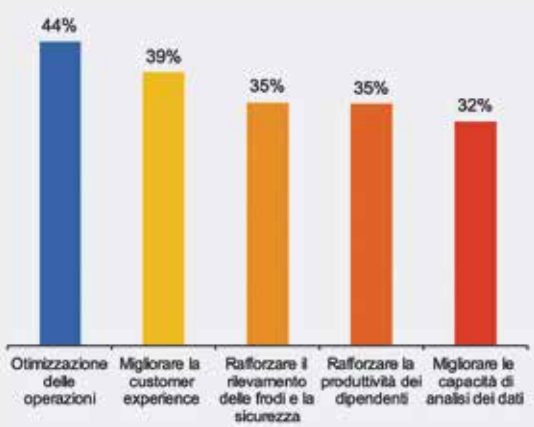
clienti e orchestra l'intera esperienza d'acquisto. È la **differenza tra un assistente (chatbot) che esegue ordini e un agente** che pianifica, propone alternative, e agisce per il successo del brand. Per i retailer, questa distinzione non è solo tecnica, è l'inizio di un vero e proprio cambio di paradigma, che ha il potenziale di trasformare il settore retail, integrando esperienze omnicanale e personalizzate. Con l'adozione dell'AI, i retailer possono ottimizzare operazioni, riducendo mansioni ripetitive, e efficientando il tempo e le competenze del personale a vantaggio di una maggiore sicurezza e prontezza di risposta alle aspettative dei consumatori moderni. Nonostante i benefici, l'implementazione dell'AI agentica presenta però anche sfide significative. I retailer devono affrontare costi infrastrutturali elevati e la necessità di competenze specializzate. Tuttavia, le opportunità offerte dall'AI sono immense, con la possibilità di migliorare la sicurezza, prevenire le frodi e ottimizzare le operazioni. Il 35% dei retailer sta già utilizzando l'AI per la sicurezza e la prevenzione delle frodi, dimostrando l'importanza di queste tecnologie per proteggere i dati dei clienti e mantenere la fiducia del brand.

Omnicanalità e integrazione restano fondamentali, così come la cultura aziendale

L'**integrazione omnicanale** tra sistemi nuovi e quelli già esistenti è essenziale per offrire esperienze di acquisto fluide. I consumatori si aspettano di poter interagire con i brand

PRIORITÀ E INVESTIMENTI IN AI, AUTOMAZIONE E AGENTIC AI NEL RETAIL A LIVELLO GLOBALE

Principali aree di investimento in AI e automazione nel retail



Le Funzioni aziendali al centro degli investimenti tecnologici per il 2025 nel retail

© 2025 IDC

attraverso diversi canali, senza interruzioni. Il 47% dei retailer sta investendo in tecnologie per migliorare l'integrazione dei dati e la visibilità dell'inventario in tempo reale. Questo approccio consente ai retailer di offrire opzioni di acquisto flessibili, come il "click-and-collect" e la consegna a domicilio, aumentando la convenienza e la velocità di gestione degli ordini.

Allo stesso tempo, la flessibilità dell'architettura IT si afferma come leva strategica per l'innovazione nel retail. Sempre più aziende riconoscono il valore di piattaforme **unified commerce**, capaci di abilitare un'innovazione rapida senza i vincoli imposti dai sistemi legacy. Queste architetture modulari permettono di integrare facilmente nuove funzionalità — dalla ricerca intelligente basata su AI al voice commerce, fino al potenziamento delle app mobile — offrendo ai retailer la possibilità di sperimentare, adattarsi e scalare soluzioni in tempi ridotti.

Tuttavia, la tecnologia da sola non basta. Per quanto fondamentali siano l'Intelligenza Artificiale, l'automazione e le architetture digitali flessibili, il vero cambiamento richiede anche un allineamento culturale e una trasformazione operativa profonda. Solo integrando l'innovazione tecnologica con una visione condivisa, competenze adeguate e processi agili, i retailer potranno affrontare con successo le sfide del mercato e costruire un futuro realmente sostenibile, centrato sul cliente. Ancora una volta, la collaborazione tra IT e funzioni di business costituisce una condizione necessaria per misurare e ottenere risultati tangibili e sempre più orientati alla sostenibilità.

ORNELLA URSO
Associate Research Director, IDC Manufacturing Insights EMEA

> L'AI STA TRASFORMANDO IL VOLTO DEL SETTORE RETAIL, A VANTAGGIO DI UNA CUSTOMER EXPERIENCE PERSONALIZZATA E DI OPERAZIONI SEMPRE PIÙ EFFICIENTI.

Scansiona il QrCode per accedere al Report "Industry Market Trends: Europe Retail, 2025". Per informazioni, rivolgersi alla redazione.

Reportec

È ANCHE

bizIT.it

bizIT.it è la rivista digitale che ti aggiorna con notizie, analisi, report, approfondimenti, interviste e case study dedicati all'ICT e alla tecnologia

Iscriviti alla newsletter e ricevi direttamente nella tua casella email le riviste Direction e Partners

Redazione: REPORTEC srl | Via San Michele, 163
20099 Sesto San Giovanni (MI)
redazione@reportec.it | www.reportec.it

INNOVAZIONI, TECNOLOGIE E NUOVE PROSPETTIVE

opentext™
Cybersecurity

LA NOSTRA FORZA È LA VOSTRA SICUREZZA

OpenText Cybersecurity, divisione di OpenText, offre il più ampio portafoglio di soluzioni modulari sul mercato per rafforzare la resilienza del tuo business attraverso il cloud e ambienti ibridi, sfruttando l'automazione guidata dall'intelligenza artificiale

IDENTIFICARE ogni minaccia con la potenza dell'AI

GOVERNARE l'accesso e l'identità con una gestione Zero Trust

PROTEGGERE la privacy e i dati strutturati e non strutturati

BLOCCARE ogni tipo di minaccia e rispondere in modo rapido e proattivo

RAFFORZARE la sicurezza delle applicazioni con analisi del codice e test

opentextcybersecurity.it