CLOUDFLARE

2026

Report Cloudflare Security Signals

Resilienza autonomica

PREFAZIONE DI MICHELLE ZATLYN

Tutto sta cambiando.

L'IA sta passando dalla fase pilota alla produzione, i sistemi autonomi (AS) stanno accelerando il processo decisionale e l'economia digitale si sta evolvendo in tempo reale. Per i leader pronti ad agire, questo ritmo di cambiamento crea opportunità reali.

La resilienza è diventata il nuovo vantaggio competitivo. Man mano che i sistemi intelligenti rimodellano l'economia digitale, i leader possono progettare difese per anticipare il cambiamento, mettere a punto sistemi che si adattano e trasformare la volatilità in un vantaggio.

Cloudflare gestisce una delle più grandi reti globali al mondo, che copre più di 330 città in oltre 120 paesi. Proteggiamo milioni di proprietà Internet, blocchiamo oltre 230 miliardi di attacchi informatici ogni giorno e gestiamo 2,5 miliardi di richieste bot al giorno. Da questo punto di vista, vediamo sia i rischi che le opportunità che plasmano Internet.

Il Report Cloudflare Security Signals 2026 fornisce approfondimenti pratici di cui i leader hanno bisogno oggi, mappando le forze che stanno rimodellando il panorama digitale, in modo da poter governare i sistemi intelligenti, modernizzarli in modo sicuro e creare resilienza dal nucleo.

La nostra missione è aiutare a realizzare un Internet migliore. Nel 2026, questo significa aiutarti a operare con sicurezza e fiducia, su scala automatizzata.

Michelle Zatlyn
Co-fondatrice, Presidente
e Co-chair, Cloudflare

RIEPILOGO

Per le aziende odierne altamente interconnesse e automatizzate, il modello "absorb shocks and recover" non funziona più.

Questo approccio si basa sul presupposto ingenuo che possiamo prevedere con precisione e prepararci per ogni interruzione specifica. I sistemi IA agiscono in modo autonomo; le piattaforme cloud concentrano i carichi di lavoro critici; le supply chain si estendono in profondità negli ecosistemi opachi. In questa nuova realtà, i leader della sicurezza richiedono **resilienza autonomica: sistemi che, oltre a resistere allo stress, si regolano, si adattano e si riprendono in tempo reale**.

Ma mentre molte organizzazioni sembrano mature, moderne e ben governate, la resilienza autonomica non è visibile in uno stato stazionario. È un risultato di leadership rivelato solo in condizioni di stress prolungato e grave.

Questo report si basa su una semplice premessa: i maggiori rischi che le aziende dovranno affrontare nel 2026 non derivano da evidenti debolezze. Emergono da linee di faglia nascoste, aree che sembrano solide nelle normali operazioni, ma si fratturano quando aumentano la velocità, la scala o le turbolenze.

In questi capitoli, forniamo ai dirigenti un progetto per far emergere questi punti deboli prima che si manifestino. Ogni sezione offre domande mirate per accendere il dibattito interno e scoprire la fragilità nascosta all'interno delle proprie organizzazioni. In un'era di intelligence, autonomia e velocità, il successo appartiene ai leader che progettano le loro imprese in modo che percepiscano, si adattino e si auto-correggano sotto stress, proteggendo al contempo i risultati critici man mano che le condizioni cambiano.

Sei linee di faglia critiche

Queste linee di faglia non sono isolate. La pressione in un'area può intensificare la debolezza nelle altre.

1 Domare l'algoritmo: governare l'IA su larga scala

I programmi IA spesso appaiono disciplinati, governati e basati sul valore. Tuttavia, sotto esame, molti leader non sono in grado di spiegare chiaramente dove è in esecuzione l'IA, quali dati tocca o chi è responsabile quando i risultati falliscono. I progressi in superficie spesso mascherano un divario di visibilità e proprietà che viene esposto quando le autorità di regolamentazione, i clienti o gli incidenti esercitano pressioni.

2 Attendibilità su scala automatizzata: autonomia ingegneristica

I sistemi autonomi funzionano bene quando le condizioni sono prevedibili. Sotto stress, le decisioni si muovono più rapidamente della supervisione umana e l'attendibilità viene presupposta anziché progettata. Questo punto critico verifica se la delega è stata deliberata o se l'autorità sia passata silenziosamente alle macchine senza confini chiari, responsabilità o controllo in tempo reale.

3 Supply chain shadow: esporre le dipendenze nascoste

Le aziende appaiono diversificate e ricche di partner, ma dipendono da livelli di servizi di terzi e di quarti di cui non hanno piena visibilità. Quando si verifica un'interruzione, il primo errore spesso non è la risposta, ma la scoperta. Questa linea di faglia rivela se il rischio di dipendenza è intenzionale e visibile o ereditato e opaco.

4 Segnali di intenti: dall'intelligence alla previsione

Mentre i programmi di intelligence basati sui dati spesso sembrano completi, le informazioni che arrivano troppo tardi non riescono a plasmare le decisioni. Questa linea di faglia separa le organizzazioni che utilizzano i primi segnali per perfezionare continuamente le decisioni, rafforzare l'anticipazione e affinare la risposta nel tempo, da quelle che apprendono solo dopo che il danno è stato fatto.

5 La trappola del debito: l'architettura legacy come rischio strategico

Le architetture legacy possono apparire stabili nelle operazioni giornaliere. Sotto la moderna velocità di attacco e il controllo normativo, diventano fragili, consumando tempo, talento e resilienza più velocemente di quanto le organizzazioni possano adattarsi. Questa linea di faglia rivela se l'architettura consente l'evoluzione o, al contrario, la limita silenziosamente.

6 Miraggio del cloud: disaccoppiamento del rischio a cascata

Le strategie cloud promettono scalabilità ed efficienza, ma i piani di controllo condivisi e le strette dipendenze concentrano i guasti. Quando lo stress colpisce, i sistemi cadono insieme. Questo verifica se la resilienza è progettata per il contenimento o se viene semplicemente data per scontata attraverso i piani di ripristino. Le organizzazioni mature limitano l'impatto e diventano più tolleranti ai guasti con ogni interruzione.

Indice

1

Domare l'algoritmo: governare l'IA su larga scala

Domare l'algoritmo: governare l'IA su vasta scala

L'adozione dell'IA sta accelerando più velocemente di quanto i modelli di governance aziendale possano adattarsi. Quella che era iniziata come una sperimentazione isolata è diventata incorporata nei flussi di lavoro, negli strumenti degli sviluppatori, nelle interazioni con i clienti e nel software di terzi che le organizzazioni utilizzano ma non controllano direttamente. Ma prima che l'IA agisca in modo indipendente, visibilità, proprietà e vincoli devono già essere presenti. Una volta che le decisioni si muovono su scala automatizzata, queste domande non possono più essere discusse.

Sebbene la maggior parte dei team esecutivi riconosca l'IA come un problema a livello di consiglio di amministrazione, pochi sono in grado di articolare chiaramente dove viene utilizzata l'IA, quali dati tocca o come viene gestito il rischio all'interno dell'azienda. Questo divario tra consapevolezza e controllo dell'IA è ora uno dei punti ciechi più consequenziali nella leadership moderna.

La domanda non è più se l'IA offra valore. Si tratta di sapere se la leadership ha una visibilità sufficiente per governare l'impatto dell'IA su resilienza, attendibilità, costi e responsabilità su larga scala.

L'IA non è più sperimentale. Opera nel cuore dell'azienda e deve essere governata con lo stesso rigore riservato alle finanze, alla gestione dei rischi e alle normative. In questo ambiente, la fiducia è il vero fattore di differenziazione.

La velocità vince. Aspettare le autorizzazioni significa restare indietro.

L'accessibilità dell'IA ha cambiato radicalmente il modo in cui la tecnologia entra nell'organizzazione. I dipendenti e i team non aspettano più l'approvazione centralizzata. Gli strumenti IA vengono adottati in modo silenzioso, tramite estensioni del browser, funzionalità SaaS integrate, API e piattaforme per sviluppatori, spesso con buone intenzioni e guadagni immediati in termini di produttività.

La conseguenza è prevedibile: l'IA si diffonde più velocemente della governance. In effetti, il 98% dei dipendenti utilizza app non autorizzate nei casi d'uso di shadow AI e shadow IT.[1]

Gli strumenti non autorizzati introducono controlli di sicurezza incoerenti e pratiche di gestione dei dati poco chiare e diffondono la responsabilità. Per i consigli di amministrazione, questo crea una realtà scomoda. Il rischio dell'IA è materiale, ma spesso scarsamente quantificato e privo di chiare responsabilità.

Questo non riflette un fallimento della disciplina. Si tratta di una discrepanza strutturale tra i modelli di approvazione legacy e la curva di adozione senza problemi dell'IA.

La governance non può più essere una fase di approvazione. Deve diventare un sistema sempre disponibile basato su protezioni, visibilità continua e standard scalabili alla stessa velocità dell'adozione dell'IA.

I dati sono la vera ricompensa, ma anche il rischio maggiore.

I sistemi IA traggono valore dall'accesso: ai dati, ai modelli e alle decisioni a valle. Sotto la pressione di risposte rapide, le organizzazioni spesso espandono l'accesso più velocemente di quanto non rafforzino i controlli.
I confini dei privilegi di accesso sfumano. I flussi di dati diventano opachi.
I servizi meno attendibili si avvicinano alle informazioni sensibili. Il 97% delle organizzazioni che hanno segnalato un incidente di sicurezza legato all'IA nel 2025 non disponeva di adeguati controlli di accesso all'IA.[2]

I framework di sicurezza tradizionali non sono stati progettati per catturare i rischi nativi dell'IA come la manipolazione dei prompt, la conservazione involontaria dei dati o l'uso improprio dei modelli. Di conseguenza, molte organizzazioni possono certificare la conformità senza comprendere veramente l'esposizione basata sull'IA.

Framework come NIST AI RMF e ISO/IEC 42001 forniscono indicazioni, ma la vera certezza deriva dal modo in cui vengono implementati e applicati. Ogni sistema IA è un sistema di dati prima di essere un sistema intelligente. Se i leader non sono in grado di mappare i flussi di dati, i percorsi di uso improprio e le modalità di errore, non sono pronti per la scalabilità.

> “Uno schema si ripete ogni volta che il processo decisionale viene automatizzato: i risultati si muovono più velocemente della responsabilità. L'IA non crea questo divario: lo espone. Quando la responsabilità non è chiara, la **governance diventa puramente formale**, indipendentemente da quanto siano raffinati i criteri”.
>
> Joe Sullivan, ex CSO, Uber

Shadow AI è shadow IT su scala automatizzata.

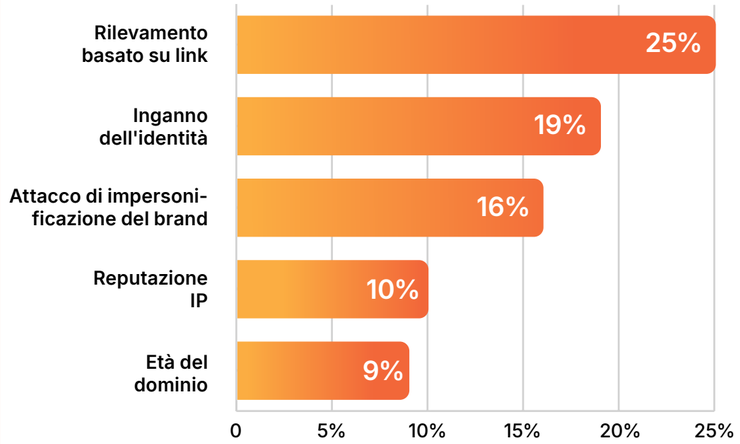
L'IA può proliferare in modo invisibile tra dipendenti, appaltatori, team di prodotto e vendor di terzi senza attivare una revisione formale. Questo crea un divario di verificabilità proprio nel momento in cui le autorità di regolamentazione richiedono maggiore trasparenza.

I governi e le autorità di regolamentazione richiedono sempre più inventari IA documentati, derivazione dei dati tracciabile e spiegabilità per le decisioni automatizzate. L'incapacità di dimostrare il controllo sta rapidamente diventando un errore di conformità, non solo un problema di maturità.

Le organizzazioni leader che stanno colmando questo divario stanno passando da audit episodici a controlli continui, combinando registrazione completa, raccolta automatizzata di prove e controlli per rilevare l'utilizzo non autorizzato dell'IA in tempo reale.

Se le attività dell'IA non possono essere registrate, spiegate e dimostrate, non possono essere difese dalle autorità di regolamentazione, dai clienti o dal consiglio di amministrazione.

Principali categorie di minacce nel rilevamento delle e-mail



Le percentuali non si sommano al 100% poiché le e-mail possono avere più categorie di minacce.

Fonte: Cloudflare Radar

Gli attacchi basati su link e l'inganno dell'identità dominano le moderne minacce e-mail. Queste campagne sfruttano i segnali di attendibilità piuttosto che le vulnerabilità tecniche. Poiché l'IA riduce i costi di produzione di inganni convincenti e personalizzati, la governance deve estendersi oltre la supervisione dei modelli all'autenticazione, all'integrità delle identità e alla tracciabilità delle decisioni.

> La governance sembra sempre adeguata **finché non si verifica un imprevisto**. Con l'IA, quel momento arriva prima e con un impatto più vasto. Le organizzazioni che gestiscono al meglio questa sfida trattano l'IA non tanto come uno strumento, quanto come una supply chain: ne tracciano l'origine, le responsabilità e l'influenza, anche quando opera al di fuori del perimetro aziendale".
>
> Kate Kuehn, Global Head of Cybersecurity Strategy, World Wide Technology

La regolamentazione risiede nel codice, non solo nei criteri.

Le giurisdizioni di tutto il mondo si sono mosse con decisione verso regimi di governance dell'AI applicabili che bilanciano innovazione e responsabilità. Solo negli Stati Uniti, i legislatori statali hanno presentato 1.208 disegni di legge relativi all'IA, che si sono tradotti in 145 nuove leggi promulgate in un solo anno.[3] Le sanzioni si estendono sempre più oltre le multe alla responsabilità personale e fiduciaria.

Questo segnala un cambiamento più ampio: la governance dell'IA viene riformulata come un rischio aziendale e una responsabilità di leadership e non un criterio tecnico discrezionale. Le organizzazioni che progettano la governance dell'IA come infrastruttura trasformano l'attendibilità in un fattore di crescita, non in un vincolo.

> Stiamo assistendo alla più grande proliferazione di shadow IT nella storia, poiché i dipendenti adottano servizi e agenti IA non governati. A differenza del tradizionale shadow IT SaaS, queste funzionalità IA sono difficili da rilevare o bloccare; possono assumere identità di utenti reali, integrarsi in attività standard e operare su scala automatizzata. Il mandato del CISO non è quello di bloccare questa adozione, ma di progettare funzionalità IA sicure che eliminino la necessità di strumenti non governati".
>
> Michael Goodman, Vicepresidente/ Chief Digital e Security Officer (CD e SO), Hitachi

DOMANDE PER LA DIRIGENZA

Esporre i punti ciechi per la governance dell'IA

Su scala automatizzata, la proprietà poco chiara, la visibilità limitata e le protezioni deboli diventano responsabilità aziendali, rendendo così queste domande imperativi della leadership.

D1

Chi è formalmente responsabile della governance dell'IA a livello dirigenziale?

E dove inizia e dove finisce questa autorità? Questa responsabilità è strutturata a livello operativo, o viene data per scontata finché qualcosa non va storto?

D2

Quali vincoli definiscono oggi un comportamento IA accettabile nella nostra organizzazione?

Questi vincoli sono chiaramente articolati, espliciti, applicabili e coerenti fra i team o si basano in gran parte sulla fiducia che la nostra forza lavoro rispetti i criteri?

D3

Come determiniamo se l'uso dell'IA è appropriato, non solo conforme?

Gli usi dell'IA sono conformi ma disallineati con l'obiettivo aziendale, l'etica o la tolleranza al rischio? Governiamo i risultati o solo l'accesso e gli strumenti? Come possiamo identificare ciò che è conforme da quello che non lo è?

D4

In caso di audit, saremmo in grado di presentare una mappatura completa e condivisa dell'uso dell'IA a livello aziendale?

Oppure le definizioni, l'utilizzo non autorizzato e l'esposizione di terzi farebbero emergere delle lacune nella nostra comprensione?

D5

Con l'accelerazione dell'adozione dell'IA, il nostro modello di governance rimane coerente?

Oppure si frammenta tra funzioni, vendor e aree geografiche? La governance è trattata come un framework statico o come un sistema operativo dinamico?

2

Attendibilità su scala automatizzata: autonomia ingegneristica

Attendibilità su scala automatizzata: autonomia ingegneristica

Le aziende stanno vivendo la trasformazione più decisiva dai tempi dell'Internet commerciale. Siamo andati oltre gli strumenti assistiti dall'IA nell'era dell'"impresa autonoma", in cui gli agenti IA e i flussi di lavoro degli agenti eseguono processi aziendali end-to-end con un intervento umano minimo o nullo. Questa linea di faglia presuppone che i sistemi IA siano già integrati e agiscano in modo autonomo. A differenza della sfida della governance dell'IA che si concentra su visibilità, supervisione e responsabilità, questa linea di faglia affronta ciò che accade dopo che l'autorità è già stata delegata alle macchine. La domanda non è più dove viene utilizzata l'IA o chi la possiede; è se l'attendibilità resiste quando le decisioni vengono prese senza che gli esseri umani siano coinvolti.

Gartner prevede che entro il 2026 quasi la metà delle applicazioni aziendali dovrebbe incorporare agenti IA specifici delle attività, rispetto all'adozione a una cifra solo un anno prima.[4] Questo cambiamento offre velocità ed efficienza senza precedenti, introducendo anche un rischio strutturale: le decisioni aziendali ora superano la supervisione umana.

L'attendibilità non può più essere periodica, manuale o retrospettiva. In un ambiente autonomo, deve essere continua, verificabile e applicata su scala automatizzata. Per garantire questo futuro, è necessario un cambiamento fondamentale, ovvero da un approccio basato su "fidarsi ma verificare" a "fidarsi fin dall'ideazione" e, in definitiva, a sistemi che diventano più affidabili man mano che vengono testati.

Il "paradosso della velocità", quando l'azienda si muove più velocemente della supervisione

La sicurezza tradizionale presuppone di avere tempo a disposizione. Viene generato un avviso. Un essere umano indaga. Si prende una decisione. I sistemi autonomi eliminano questa finestra. Gli agenti IA possono eseguire migliaia di azioni, come la riconfigurazione dell'infrastruttura, il ribilanciamento dei portafogli e l'adeguamento delle supply chain, in pochi millisecondi. Se un agente è compromesso, disallineato o semplicemente sbagliato, l'impatto viene realizzato prima che un essere umano possa intervenire.

Questo è il paradosso della velocità: la stessa autonomia che guida il valore fa crollare anche il margine di errore. Gli autori di attacchi lo capiscono. Il phishing, l'impersonificazione e la manipolazione basati sull'IA prendono sempre più di mira i flussi di lavoro automatizzati anziché le persone.

L'implicazione è chiara: la sicurezza non può stare al di fuori del sistema. Deve essere incorporata nel livello decisionale stesso, governando l'obiettivo, non solo l'accesso. Questa linea di faglia non riguarda la previsione degli attacchi. Si tratta di garantire che quando i propri sistemi agiscono, lo facciano entro i confini deliberatamente progettati dalla leadership.

Il nuovo piano di controllo per IA autonoma

1. L'identità deve estendersi oltre gli esseri umani

Le identità non umane (agenti IA, account di servizio, bot) ora superano gli utenti umani per ordini di grandezza. I bot sono responsabili di circa il 30% del traffico HTTP servito da Cloudflare,[5] e un sorprendente 92% di tutti i tentativi di accesso osservati da Cloudflare provengono da bot: spesso attacchi di sottrazione e uso illecito delle credenziali.[6] Tuttavia, la maggior parte delle aziende continua a governare l'identità come se le persone fossero gli attori principali.

Il rischio è acuto. I sistemi IA vengono spesso distribuiti senza autenticazione complessa, autorizzazione granulare o controlli del ciclo di vita. Quando compromessi, operano con un impatto su scala automatizzata.

Ogni agente IA deve avere un'identità crittografica verificabile, governata attraverso la gestione dell'identità delle macchine. Le credenziali devono essere di breve durata, sensibili al contesto e revocabili in tempo reale. L'autonomia senza identità è abdicazione.

Distribuzione delle richieste HTTP tramite bot (automatizzata) e umani

Fonte: Cloudflare Radar

Non operiamo più su un Internet incentrato sugli umani. Gli algoritmi interagiscono sempre più con gli algoritmi, spesso senza la supervisione umana diretta. I modelli di governance basati sull'autenticazione degli utenti e i controlli di accesso dei dipendenti non sono allineati con questa realtà.

2. I sistemi probabilistici richiedono protezioni deterministiche

I sistemi IA ragionano in modo probabilistico. La sicurezza non può farlo Sebbene gli agenti possano ottimizzare, negoziare o consigliare, le regole che disciplinano ciò che sono autorizzati a fare devono essere assolute. I criteri non possono essere dedotti, devono essere applicati.

Questo richiede:

- Policy-as-code che definisce i vincoli non negoziabili
- Livelli di applicazione in tempo reale che intercettano l'obiettivo prima dell'esecuzione
- Separazione tra processo decisionale e autorizzazione

La vera autonomia esiste solo dove i confini sono espliciti, applicati e progettati in anticipo.

> I giudizio umano rimane essenziale, ma non viaggia più alla velocità richiesta dai sistemi. In ambienti in cui le macchine interagiscono in modo continuo, l'**attendibilità deve essere stabilita, imposta e verificata fin dall'ideazione**, proprio come i sistemi di sicurezza a cui ci affidiamo senza farci caso, finché non si guastano".
>
> Oliver Newbury, Senior Advisor, TPG

3. La fiducia richiede osservabilità, non ipotesi

Man mano che i sistemi IA si adattano, vanno alla deriva e apprendono, la certezza di ieri diventa rapidamente irrilevante. Senza una profonda osservabilità, i leader non possono distinguere tra comportamento autonomo e legittimo e manipolazione.

L'utilizzo non autorizzato e spesso invisibile dell'IA aumenta ulteriormente il rischio introducendo modelli, flussi di dati e logiche decisionali non governati nelle operazioni principali.

Il caso economico

L'integrazione dell'IA e dell'automazione nelle operazioni di sicurezza offre rendimenti finanziari misurabili. Le organizzazioni che utilizzano queste funzionalità in modo estensivo risolvono le violazioni 80 giorni più velocemente e riducono i costi medi delle violazioni di 1,9 milioni di dollari rispetto a quelle che non lo fanno.[7]

Il vantaggio va oltre la riduzione dei costi. Adottando solide protezioni, i leader acquisiscono la fiducia necessaria per distribuire l'automazione più in profondità nei flussi di lavoro critici per i ricavi, migliorando la reattività, la velocità del capitale e la differenziazione competitiva. Un'autonomia ben governata diventa un fattore di crescita, non solo un controllo del rischio. La sicurezza su scala automatizzata non è un sovraccarico. È il prezzo per scalare l'autonomia senza fragilità.

Il sistema di leadership per l'autonomia

L'ascesa dei sistemi autonomi sta ridefinendo il ruolo del CISO e, per estensione, le responsabilità di tutti i dirigenti. La leadership della sicurezza non riguarda più la protezione dei sistemi dopo che sono state prese le decisioni; si tratta di orchestrare l'attendibilità in ambienti in cui le macchine agiscono in modo indipendente.

Un CISO ha ricordato la prima volta che un sistema IA ha interrotto da solo una transazione multimilionaria. La decisione era corretta, ma ha suscitato una domanda più profonda nella sala del consiglio: chi aveva effettivamente autorizzato la macchine a effettuare quella chiamata? La tecnologia era in anticipo rispetto alla governance.

Questo cambiamento richiede scelte chiare da parte della dirigenza: dove è consentita l'autonomia, dove gli esseri umani restano coinvolti, quale trasparenza è richiesta tra modelli e dati e come viene misurato il rischio quando le macchine prendono decisioni.

Le metriche basate sui tempi di risposta umani non sono più sufficienti. I leader devono monitorare il rischio autonomo, l'integrità delle decisioni e la deriva sistemica. Tuttavia, solo il 15% circa dei consigli aziendali riceve regolarmente metriche di rischio e prestazioni legate all'IA.[8]

Con la diffusione dell'autonomia, la sicurezza, la conformità e la tecnologia non possono più operare in compartimenti stagni. La sicurezza influenza la velocità dei ricavi. La conformità determina l'accesso al mercato. La tecnologia definisce la responsabilità. L'attendibilità su scala automatizzata non è un programma di sicurezza: è un sistema di leadership che unifica resilienza, governance, innovazione e reputazione sotto un unico mandato esecutivo.

> **L'automazione cambia la velocità delle decisioni, ma cambia anche il raggio d'azione degli errori. La domanda per i leader è "Come possiamo progettare responsabilità e attendibilità in sistemi che agiscono in autonomia?"**
>
> **Kevin Jones, Global Chief Information Security Officer, Bayer**

DOMANDE PER LA DIRIGENZA

Passare dall'automazione all'autonomia

Queste domande espongono se la leadership abbia intenzionalmente progettato dei limiti su come le decisioni vengono prese su scala automatizzata e su come il rischio viene gestito in tempo reale.

D1

Quali decisioni aziendali vengono già prese dai sistemi autonomi?

Quali decisioni stiamo deliberatamente mantenendo per gli esseri umani? Tale confine è progettato, documentato e rivisitato o è implicito e alla deriva?

D2

Quando le macchine agiscono in autonomia, chi è responsabile in tempo reale: il proprietario del sistema, il titolare dell'attività di business o lo sponsor esecutivo?

La proprietà del rischio autonomo è chiaramente definita mentre il sistema è in funzione o viene esaminata solo dopo che qualcosa va storto?

D3

Dove vengono eseguite le decisioni dal software anziché dalle persone?

Dove abbiamo allentato i controlli sul software? Le macchine sono tenute a standard più elevati rispetto agli umani o si fidano di più?

D4

Possiamo spiegare e giustificare un'azione autonoma nel momento in cui si verifica?

Oppure, si manifesta giorni dopo durante le revisioni degli incidenti? L'obiettivo è osservabile su scala automatizzata o ricostruito sotto pressione?

D5

Il nostro modello di attendibilità scala in modo automatizzato?

Se l'autonomia raddoppiasse entro il prossimo anno, il nostro modello di attendibilità assorbirebbe l'accelerazione o fallirebbe sotto il suo peso? L'attendibilità è progettata per la scalabilità e la velocità o è ereditata dalla governance dell'era umana?

3

Supply chain shadow: esporre le dipendenze nascoste

Supply chain shadow: esporre le dipendenze nascoste

La nostra economia iperconnessa non è più definita da ciò che si controlla, ma da quello che può distruggerti e che non si vede nemmeno. Molti leader hanno rafforzato il proprio perimetro, modernizzato l'infrastruttura e rafforzato la governance, ma i rischi più consequenziali ora vivono oltre la loro linea di vista, incorporati in ecosistemi di terze, quarte ed ennesime parti che non possiedono né influenzano completamente. La scomoda verità: si può essere operativamente maturi e tuttavia sistematicamente fragili.

Le supply chain shadow non sono casi limite; sono il risultato naturale dell'assemblaggio digitale su larga scala. Ogni integrazione SaaS, chiamata API, libreria open source e servizio IA aggiunge un altro livello di rischio ereditato. La domanda della leadership non è più "Abbiamo un rischio per la supply chain?" ma "Capiamo quale guasto esterno potrebbe bloccare le entrate, erodere la fiducia o innescare un controllo normativo domani?"

L'impatto è già materiale. Le violazioni della supply chain hanno una media di 4,91 milioni di dollari, superiore alla media globale delle violazioni di 4,44 milioni di dollari.[9] La scelta strategica per i leader è considerare il rischio della supply chain come un esercizio di conformità e accettare sorprese periodiche, oppure trattarlo come un'esposizione operativa in tempo reale che richiede visibilità continua, garanzia di runtime e protezioni architettoniche.

Il rischio che non è mai stato approvato

Le moderne supply chain non si fermano più ai vendor diretti. Si estendono a piattaforme SaaS, servizi cloud native, provider di modelli IA, componenti open source e livelli di infrastruttura in subappalto che operano ben oltre la linea di vista dell'approvvigionamento. I guasti in qualsiasi punto di questo web esteso, che si tratti di una violazione, di un'interruzione o di un mancato rispetto della conformità, possono sfociare rapidamente in danni ai clienti, esposizione alle normative e interruzioni sistemiche.

La sfida principale è la visibilità e l'IA sta accelerando sia il rischio che l'opacità. La maggior parte delle organizzazioni non può vedere le proprie supply chain digitali estese, per non parlare di governarle in tempo reale. Ogni modello di IA, API e flusso di lavoro automatizzato espande silenziosamente le dipendenze oltre la supervisione tradizionale. Gli audit sono statici mentre il rischio è dinamico.

Quando i sistemi sono assemblati, non costruiti

Un'auto moderna è costruita da centinaia di fornitori e le parti hardware, i chip e il software provengono da molti vendor, ognuno con le proprie supply chain. Un piccolo difetto nascosto può diventare un problema di sicurezza a velocità autostradale, motivo per cui le case automobilistiche investono molto nella tracciabilità e nei test continui.

L'IT enterprise ora rispecchia questo modello. Un'applicazione può dipendere da decine di strumenti SaaS, servizi cloud, API, librerie open source e modelli IA, ciascuno con i propri responsabili del trattamento secondari. L'azienda vede l'interfaccia, non i livelli sottostanti. Questa è la supply chain shadow.

La differenza è la disciplina. Nel settore automobilistico, le parti vengono tracciate e i richiami sono precisi. Nell'IT, quando una libreria o un componente IA viene compromesso, molte organizzazioni si affrettano prima a scoprire se sono esposte. I questionari annuali non possono tenere il passo con i sistemi che cambiano settimanalmente. Visibilità e garanzia continua stanno diventando essenziali per i sistemi digitali quanto il controllo qualità lo è per le automobili.

Tre forze stanno accelerando questo rischio:

- **Trust-by-proxy è diventato il modello operativo predefinito.** Le aziende si fidano dei loro vendor. I vendor si fidano dei loro fornitori. Poche parti verificano l'intera catena. I problemi di concorrenza e la visibilità interna limitata fanno sì che le supply chain secondarie vengano raramente divulgate in dettaglio.
- **L'IA ha introdotto un nuovo, opaco livello di dipendenza.** I dipendenti si affidano sempre più a strumenti IA generativa e servizi IA incorporati che espongono i dati sensibili a modelli di quarti. I team di rischio di terzi spesso non hanno chiarezza su come questi modelli utilizzano i dati, conservano le informazioni o si addestrano sugli input aziendali, aumentando i rischi normativi, di proprietà intellettuale e di sovranità dei dati.
- **Le aspettative normative si stanno rafforzando.** In tutto il mondo, le autorità di regolamentazione si stanno muovendo in modo deciso dalla guida all'applicazione. Ci si aspetta sempre più che le organizzazioni dimostrino visibilità sulle dipendenze di terzi e quarti, in particolare quando sono coinvolti dati personali o finanziari o infrastrutture critiche. In futuro, i leader dovranno non solo valutare il rischio dei vendor, ma anche quantificare il rischio operativo derivante da supply chain estese. Il risultato? Un divario crescente tra ciò che le autorità di regolamentazione si aspettano e ciò che le organizzazioni possono attualmente dimostrare.

I 10 brand più impersonati nelle campagne di phishing

1	Windows	6	Amazon
2	SANS	7	Instagram
3	Microsoft	8	Costco
4	Stripe	9	YouTube
5	Facebook	10	iCloud

Fonte: tentativi di impersonificazione osservati da Cloudflare Email Security

I brand più impersonati non sono bersagli casuali. Sono piattaforme fondamentali integrate nei flussi di lavoro aziendali: provider di identità, sistemi di pagamento, piattaforme cloud, sistemi operativi. Gli autori di attacchi sfruttano la familiarità e la dipendenza, trasformando un'infrastruttura digitale attendibile in un vettore di attacco. Le supply chain shadow non sono solo esposizione operativa; sono identità ed esposizione del brand.

Dall'assicurazione statica alla trasparenza continua

Risolvere il problema della supply chain shadow non richiede più burocrazia. Necessita di un modello operativo diverso. Il futuro della garanzia della supply chain è la trasparenza continua: visibilità in tempo reale su ciò che è effettivamente in esecuzione, connesso e scambia dati in tutto l'ecosistema.

Un CISO ha descritto di aver scoperto un fornitore critico solo dopo che il traffico insolito è apparso nei log di rete. Il vendor era legittimo, ma nessuno si rendeva conto di quanto fosse profondamente radicato. La lezione era semplice: non puoi governare ciò che non puoi vedere.

Questo cambiamento è già in corso. Le distinte base del software (SBOM) e la Vulnerability Exploitability eXchange (VEX) si stanno spostando da artefatti di conformità a segnali operativi. Aspettati che l'approvvigionamento richiederà sempre più non solo contratti, ma divulgazioni in tempo reale e leggibili da una macchina che mappano componenti, dipendenze e sfruttabilità man mano che cambiano.[10]

Allo stesso tempo, l'applicazione si sta avvicinando al punto in cui si manifesta il rischio. I controlli a livello di rete e connettività consentono alle organizzazioni di osservare il comportamento, rilevare flussi di dati non autorizzati e identificare i fornitori shadow man mano che si verificano attività.

La garanzia della supply chain diventa una capacità operativa piuttosto che una revisione periodica. L'attendibilità viene continuamente verificata. Il rischio è emerso in anticipo. La governance si muove allo stesso ritmo dell'ecosistema che intende proteggere.

Fidati, ma verifica continuamente

Il 30% delle violazioni nel 2025 era legato al coinvolgimento di terzi, il doppio rispetto all'anno precedente[11], a dimostrazione di quanto profondamente le relazioni della supply chain influenzino l'esposizione al rischio oltre i tradizionali confini interni.

Tuttavia, le organizzazioni leader condividono un modello comune: trattano il rischio della supply chain come un sistema, piuttosto che come una funzione di conformità. Insistono nel sapere quali applicazioni esistono e come si connettono. Richiedono trasparenza per fluire lungo la supply chain, non fermarsi al primo contratto. Utilizzano segnali a livello di rete per scoprire le attività shadow anziché fare affidamento sull'autocertificazione. Applicano i principi Zero Trust all'accesso da macchina a macchina non solo agli utenti. E rivalutano continuamente il rischio dei vendor in base al comportamento, non alla reputazione.

Il guadagno è tangibile. L'85% delle organizzazioni leader nella modernizzazione delle applicazioni sta tagliando attivamente gli strumenti ridondanti e lo shadow IT per ridurre la superficie d'attacco della supply chain e migliorare la velocità operativa.[12] Queste non sono modifiche tecniche; sono scelte di leadership su quanta incertezza un'organizzazione è disposta a tollerare nei sistemi da cui dipende ogni giorno.

> Il rischio raramente deriva dalle dipendenze che tutti si aspettano, **emerge da quelle che nessuno può vedere**. Quando la visibilità è incompleta, gli audit offrono conforto ma poca protezione. La vera resilienza deriva da architetture che rivelano le loro dipendenze mentre operano".
>
> Tim Brown, CISO, SolarWinds

> Gli ecosistemi interconnessi premiano la velocità e la specializzazione, ma distribuiscono anche il rischio in modi che i contratti non possono catturare. L'analisi operativa, non le scartoffie, è ciò che in definitiva contiene l'esposizione".
>
> Sandip Wadje, Global Head of Emerging Technology Operational Risks and Intelligence, BNP Paribas

DOMANDE PER LA DIRIGENZA

Governare il rischio incontrollato

Il rischio della supply chain non può più essere gestito. È qualcosa con cui le organizzazioni convivono. Decidi se quel rischio è visibile e governato o opaco e presunto.

D1

Quali processi aziendali critici metteremmo in pausa se una dipendenza chiave dovesse guastarsi?

Sapremmo perché si è guastata? Possiamo tracciare entrate e impatto sui clienti in base a dipendenze specifiche in tempo reale, o scopriremo l'esposizione solo dopo che il danno è stato causato?

D2

Come risponderemo alle domande normative o del consiglio di amministrazione sul rischio dell'ecosistema?

Possiamo rispondere a domande su questi rischi senza indicare un contratto? Abbiamo visibilità tecnica sul percorso operativo del rischio dei vendor?

D3

Dove abbiamo ridotto la visibilità nella supply chain per preservare velocità, convenienza o relazioni con i vendor?

Sono scelte deliberate? Chi ha deciso di accettare questi compromessi? Quali dipendenze sono effettivamente "off-limits" al controllo?

D4

Con quale rapidità possiamo determinare se una vulnerabilità appena divulgata ci riguarda?

La responsabilità per la risposta è assegnata in modo chiaro? Il rilevamento dell'esposizione viene misurato in minuti, giorni o settimane?

D5

Stiamo gestendo il rischio della supply chain come una disciplina continua o un audit periodico?

Il nostro modello si evolve alla stessa velocità del nostro ecosistema o ci rassicura semplicemente sul fatto che i controlli dell'anno scorso sono stati rivisti?

4

Segnali di intenti: dall'intelligence alla previsione

Segnali di intenti: dall'intelligence alla previsione

Uno sguardo ai titoli dei giornali comunica che le attività degli avversari continuano a proliferare, a velocità e scala sempre maggiori. Con la ricognizione assistita dall'IA e i kit di strumenti, sempre più criminali informatici sono capaci di attacchi più grandi e sofisticati che mai. Inoltre, la finestra tra l'emergenza delle minacce e l'impatto sul business è sempre più breve, poiché il tempo medio impiegato da un avversario per iniziare a spostarsi lateralmente è sceso a soli 48 minuti.[13]

Una volta considerata una capacità discrezionale, l'intelligence delle minacce è diventata fondamentale. Il 52% delle organizzazioni ora mantiene team interni dedicati di intelligence delle minacce informatiche (CTI).[14] Nel panorama delle minacce in rapida evoluzione, l'intelligence è cresciuta da una funzione di sicurezza a una capacità di leadership. Il successo si misura dalla capacità di analizzare i dati CTI all'interno di un contesto aziendale, decifrando i segnali dal rumore e traducendo la conoscenza in previsioni fruibili.

L'intelligence delle minacce non significa più semplicemente accumulare conoscenze. Si tratta di sapere cosa conta davvero, *in tempo utile per agire.*

Dal feed tattico al segnale strategico

Le minacce moderne sono ad alta velocità, ad alto volume e sempre più modellate dalla geopolitica, dagli incentivi economici e dalle vulnerabilità specifiche del settore. In questo ambiente, l'intelligence delle minacce non può più essere trattata come una funzione di sicurezza opzionale o limitata a controlli formali di feed esterni generici. Il contesto, a livello aziendale, industriale e globale, è importante e i dirigenti devono richiedere informazioni che colleghino direttamente le attività delle minacce all'impatto aziendale, all'esposizione operativa e al rischio strategico.

Chiaramente, ci sono troppe attività sul fronte degli aggressori per rimanere al passo con tutto. La difesa richiede velocità e abilità e spesso entrambe scarseggiano. Sebbene la tua strategia di sicurezza debba affrontare e riconoscere l'intero inventario di attività e passività sotto la tua protezione, l'utilizzo dell'intelligence per comprendere non solo gli elementi tecnici delle minacce, ma anche il loro contesto, ti consente di ottimizzare il tuo programma di sicurezza per dare priorità alla riduzione del rischio in aree che hanno maggiore impatto sulla tua organizzazione.

Decidere cosa è importante per l'organizzazione generalmente implica l'allineamento del consiglio di amministrazione e della leadership su come integrare i principi aziendali fondamentali, le forze di mercato, le normative e i contributi delle parti interessate. Questo contesto è prezioso quando si valuta l'intelligence delle minacce, poiché fornisce all'azienda il contesto necessario per determinare quali dati CTI sono più utili.

È in questo modo che l'intelligence delle minacce può essere utilizzata per "eliminare" informazioni estranee (vulnerabilità irrilevanti o gruppi di aggressori che prendono di mira specificamente settori dissimili) in modo che tu possa concentrare le tue risorse dove possono avere il maggiore impatto in base al panorama delle minacce specifico per la tua organizzazione. Senza un impatto concreto sulle scelte strategiche, l'intelligence delle minacce si riduce a mero inquinamento informativo.

Principali settori presi di mira dagli attacchi DDoS nel 2025

Classificazione	Settore
1	Gioco d'azzardo e gaming
2	Telecomunicazioni
3	Tecnologia e servizi
4	Servizi bancari e finanziari
5	Vendita al dettaglio

Questa classifica è una media degli attacchi DDoS osservati a livello globale sia a livello di rete che a livello applicazione. La tecnologia e i servizi sono al primo posto per gli attacchi a livello di rete. Gaming e il gioco d'azzardo sono al primo posto per gli attacchi a livello applicazione.

Fonte: Cloudflare Radar

Le attività degli attacchi non sono distribuite in modo uniforme. Gli avversari danno la priorità ai settori legati alla leva economica, alla stabilità delle infrastrutture e alla rilevanza geopolitica. La concentrazione in settori specifici riflette l'obiettivo strategico, non la casualità. Un'intelligence efficace anticipa dove la pressione si intensificherà e allinea le difese di conseguenza.

L'intelligence delle minacce è diventata non negoziabile

Man mano che l'intelligence delle minacce matura, il suo obiettivo si sposta dagli indicatori tecnici alla rilevanza aziendale. I dirigenti ora la utilizzano per chiarire quali minacce sono realmente importanti, in che modo i cambiamenti geopolitici e del settore alterano l'esposizione e dove esiste la fragilità tra operazioni, partner e persone. La domanda non è più se investire nell'intelligence delle minacce, ma quale tipo di intelligence l'organizzazione stia privilegiando e per la quale stia pagando.

Per inquadrare le conversazioni sul budget, considera dove la CTI offre il massimo valore alla tua organizzazione:

- **Convalida** dell'allineamento degli investimenti in sicurezza al profilo di rischio dell'organizzazione
- **Riduzione** del rumore operativo concentrando le difese sulle minacce più critiche
- Riduzione **proattiva** del rischio, rispetto alla risposta reattiva agli incidenti dopo che si sono verificati

Per il CFO, l'intelligence delle minacce non è giustificata dal volume degli avvisi, ma dalla sua capacità di ridurre la probabilità e l'impatto di interruzioni significative dell'attività: tempi di inattività, frodi, interventi normativi o danni alla reputazione. A livello organizzativo, questo richiede chiarezza. Accordi ad hoc e funzioni di intelligence con risorse insufficienti non possono fornire approfondimenti di livello dirigenziale, né i risultati che consentono.

Che sia fornita tramite un team interno, partner fidati o un modello ibrido, il mandato è lo stesso: l'intelligence deve essere tempestiva, contestuale e pertinente per le decisioni. L'intelligence che spiega solo cosa è successo ieri fa ben poco per proteggere il futuro. I provider che offrono una nuova visibilità, come una visione precoce dell'infrastruttura, delle intenzioni e della preparazione degli avversari, offrono un vantaggio strutturale.

> Gli indicatori spiegano cosa è già successo; l'intento spiega cosa accadrà dopo. L'intelligence più preziosa collega comportamento, contesto e motivazione: **trasformando segnali isolati in previsioni** su cui i leader possono agire prima che si verifichino danni".
>
> Menny Barzilay, Cofondatore e CEO di Percepto

Orientarsi nel panorama delle minacce del 2026

Molte delle linee di faglia discusse in questo capitolo si riflettono nel Report sulle minacce 2026 di Cloudflare. Basato sui dati della rete globale di Cloudflare, che protegge il 20% del web, il report aiuta i leader a concentrarsi sui rischi che richiedono azione, non solo consapevolezza.

Utilizza una lente semplice: sforzo dell'aggressore rispetto all'impatto. Le minacce più importanti sono quelle che creano un impatto aziendale fuori misura con il minimo sforzo. Nel 2026, questo si presenta in tre modelli:

- L'**industrializzazione degli attacchi:** il passaggio dalle violazioni manuali alla scalabilità automatizzata e senza problemi nell'infrastruttura cloud di un'organizzazione
- **Intrusioni identity-first:** la transizione del ransomware in un evento di accesso piuttosto che in un'irruzione
- **Connettività della supply chain:** l'armamento del tessuto connettivo tra gli ambienti SaaS e API-first

Scarica il Report sulle minacce del 2026 di Cloudflare.

Scarica il report

L'ingrediente mancante: la modellazione delle minacce

Se l'integrazione dell'intelligence delle minacce ottimizza ogni aspetto della sicurezza, la sua sinergia con la modellazione delle minacce la trasforma in un vero e proprio motore strategico per l'intera azienda.

Mentre sempre più organizzazioni tengono conto del rischio nel processo decisionale e includono la riduzione del rischio nei loro obiettivi strategici a lungo termine, solo il 37% delle organizzazioni ha formalizzato e documentato con successo i propri processi di modellazione delle minacce.[15] La modellazione delle minacce fornisce una tassonomia comune che allinea il CISO, la dirigenza e il consiglio di amministrazione attorno a ipotesi di rischio condivise. Fornisce chiarezza sull'assegnazione di priorità agli asset, sulla probabilità di compromissione e sull'impatto aziendale in caso di controlli non riusciti.

La visione ottenuta negli esercizi di modellazione delle minacce è intenzionalmente di alto livello; i consigli di amministrazione chiedono chiarezza sul rischio sistemico, sulle tendenze emergenti delle minacce e sul fatto che l'organizzazione sia posizionata sul lato giusto della linea di faglia delle minacce. Attraverso la modellazione delle minacce, i rischi intrinseci vengono misurati in base alla probabilità e alla gravità dell'impatto sulla base delle priorità dell'organizzazione. Fattori come i controlli di sicurezza e i risultati degli audit, in combinazione con l'analisi dell'intelligence delle minacce, forniscono calcoli del rischio residuo.

L'inserimento dei dati CTI nel processo di modellazione delle minacce consente un'ulteriore messa a punto, fornendo una base per attività come la convalida dei controlli e la ricerca delle minacce, entrambi elementi essenziali in una posizione di sicurezza proattiva. Inoltre, l'intelligence pertinente al settore può confermare se le difese sono rafforzate contro gli avversari più probabili e fornire ai responsabili delle decisioni forti indicatori per il budget e la pianificazione strategica.

Senza modellazione delle minacce, l'intelligence rimane operativa. Grazie a questa, l'intelligence diventa strategica.

> Una buona intelligence riduce il rumore. Una grande intelligence cambia le decisioni. La differenza è se aiuta i leader ad anticipare le mosse, non solo a spiegarle".
>
> Troy Wilkinson, Venture Advisor, YL Ventures

Solo il

37%

delle organizzazioni ha formalizzato e documentato con successo i propri processi di modellazione delle minacce.[16]

DOMANDE PER LA DIRIGENZA

L'intelligence delle minacce come disciplina di leadership

L'intelligence delle minacce, se eseguita correttamente, collega sicurezza, rischio, operazioni, finanza e strategia in una visione esecutiva coerente dell'esposizione e degli intenti.

D1

Stiamo proteggendo ciò che è familiare o ciò che ha l'impatto maggiore?

Abbiamo allineato esplicitamente le nostre difese alle minacce che potrebbero interrompere entrate, operazioni o attendibilità quest'anno?

D2

Siamo davvero in grado di vedere gli intenti degli avversari in tempo utile?

Quali sono i punti ciechi in cui l'intelligence fallisce, lasciando che siano i danni a segnalare la presenza di un attacco? Stiamo guidando il ciclo delle minacce o lo stiamo seguendo?

D3

I briefing sulle minacce guidano le decisioni o semplicemente condividono le informazioni?

Queste informazioni cambiano le priorità, gli investimenti o la propensione al rischio in tempo reale?

D4

Quali decisioni o processi aziendali fallirebbero per primi se un individuo attendibile venisse compromesso?

Abbiamo progettato flussi di lavoro presumendo che il giudizio umano possa essere manipolato o impersonato?

D5

Con quale rapidità riusciamo a ricalibrarci quando gli avversari cambiano i loro schemi d'attacco?

Quali meccanismi sono in atto per avvisarci di un cambiamento imminente prima che l'azienda lo percepisca?

5

La **trappola del debito:** l'architettura legacy come rischio strategico

La **trappola del debito:** l'architettura legacy come rischio strategico

Nel 2026, il debito tecnico rappresenta un rischio aziendale materiale che erode silenziosamente la competitività. Le organizzazioni erano già messe a dura prova nel 2025, gestendo più di 130 nuove vulnerabilità ogni giorno, quasi il 40% delle quali era valutato alto o critico.[17] Poiché l'impiego dell'IA come arma rende indifendibili le architetture legacy, le organizzazioni con stack frammentati rischiano di rimanere intrappolate in un ciclo di sicurezza reattiva, innovazione limitata ed esposizione aggravata.

Il debito tecnico è diventato una superficie d'attacco esposta, che aggrava il rischio più rapidamente di quanto i team umani possano rispondere. Coloro che si modernizzano in modo decisivo non solo ridurranno il rischio, ma sbloccheranno la velocità, l'attendibilità e l'adattabilità necessarie per competere nell'economia basata sull'IA.

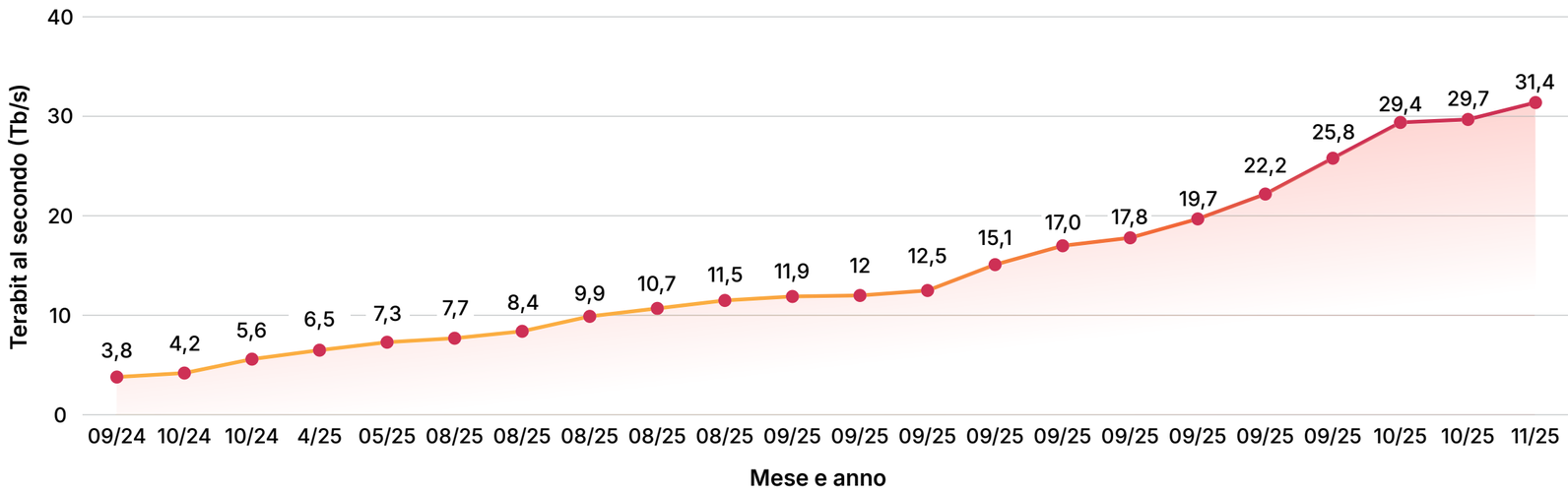
Quando la velocità espone una debolezza strutturale

Il cambiamento determinante del 2026 non è il volume delle vulnerabilità: è la velocità con cui vengono sfruttate. L'IA agentica ha ulteriormente ridotto la finestra tra divulgazione e sfruttamento, consentendo agli avversari di identificare e rendere operativi gli exploit in pochi giorni e, sempre più, in poche ore.

I dati sono inequivocabili. Nel 2025, sono state osservate 884 vulnerabilità sfruttate attivamente e il 29% ha mostrato prove di sfruttamento lo stesso giorno in cui sono state pubblicate.[18] La scala è altrettanto senza precedenti. React2Shell, una delle vulnerabilità più note dell'anno, ha registrato oltre 1 miliardo di tentativi di sfruttamento in soli 11 giorni.[19]

Escalation senza predisposizione dell'architettura

Attacchi DDoS da record mondiale



Fonte: Cloudflare Radar

In poco più di un anno, il più grande attacco DDoS registrato è quasi decuplicato. I sistemi centralizzati e strettamente accoppiati non sono mai stati progettati per questa scala. Il debito tecnico ora si traduce direttamente in fragilità sistemica sotto la pressione della scala automatizzata.

Gli ambienti legacy stanno crollando sotto pressione. Gli errori gravi si verificano spesso quando le dipendenze condivise si interrompono contemporaneamente. Anni di soluzioni temporanee hanno generato un debito oscuro: integrazioni nascoste, API fragili e sistemi troppo rischiosi da aggiornare. Questi ambienti non sono stati creati per le minacce legate su scala automatizzata o per la verifica continua.

Ciò espone anche i limiti dei cicli di patch di 30, 60 e 90 giorni. Le minacce vengono sfruttate in poche ore, non in trimestri. La protezione deve spostarsi verso l'esterno all'edge, riducendo l'esposizione prima ancora che i sistemi vulnerabili vengano toccati.

> Gli autori di attacchi non distinguono tra vecchi e nuovi sistemi; **cercano anelli deboli**. Il debito tecnologico aumenta silenziosamente il numero di questi collegamenti fino a quando la difesa non diventa un gioco di probabilità".
>
> Jerry Perullo, fondatore, Adversarial Risk Management

Il ciclo della scarsità di innovazione

Le organizzazioni con stack obsoleti sono intrappolate in un ciclo di scarsità di innovazione. Man mano che l'infrastruttura diventa più fragile, gli incidenti di sicurezza aumentano. Con l'aumento degli incidenti, più budget e talenti vengono dirottati alla manutenzione. Il risultato è un bacino di capacità di crescita in diminuzione.

L'impresa globale media spreca più di 370 milioni di dollari all'anno a causa della sua incapacità di modernizzare in modo efficiente sistemi e applicazioni legacy obsoleti e inefficienti.[20] Gli studi stimano che circa il 31% delle risorse tecnologiche sia dedicato alla risoluzione del debito tecnologico.[21] La vera innovazione (nuovi prodotti, iniziative IA, automazione) riceve solo il 7%. Questa non è stagnazione; è regressione.

Mentre i leader utilizzano l'IA per accelerare la differenziazione, i ritardatari stanno pagando un "tasso di interesse" crescente sul vecchio codice che limita la velocità, la resilienza e l'opzionalità strategica.

Perché gli stack legacy falliscono sotto la pressione dell'IA

La sicurezza moderna presuppone automazione, integrazione e controllo in tempo reale. I sistemi legacy presuppongono intervento manuale, configurazioni statiche e protezione basata sul perimetro. Questa discrepanza sta diventando pericolosa man mano che l'IA cambia il modello economico sia dell'attacco che della difesa.

Le architetture obsolete lottano con patch lente e con tempi di inattività pesanti, visibilità limitata tra API e flussi di dati, strumenti frammentati che non riescono a coordinare la risposta e basi deboli per le operazioni basate sull'IA. Tutto questo spesso costringe a un compromesso tra rischio informatico e rischio operativo, una tensione familiare tra CTO e CISO quando l'applicazione di patch potrebbe interrompere l'attività. Il risultato è un ritardo e il ritardo è esattamente ciò che sfruttano le minacce su scala automatizzata.

Le organizzazioni stanno ritardando l'adozione dell'IA non perché manchino di ambizione, ma perché la loro infrastruttura non può supportarla in modo sicuro. Nel frattempo, i concorrenti con architetture modernizzate consentono alle iniziative IA di portare avanti la modernizzazione, utilizzando carichi di lavoro reali per giustificare e accelerare il rinnovamento dell'architettura. Ad esempio, il 62% delle organizzazioni leader nell'innovazione delle applicazioni trova "molto facile" monitorare il proprio attuale livello di conformità alla sicurezza, rispetto al 35% di quelle in ritardo.[22]

370 milioni di dollari

sprecati ogni anno a causa dell'incapacità di modernizzare in modo efficiente sistemi e applicazioni legacy obsoleti e inefficienti[23]

La divisione della leadership

La differenza tra leader e ritardatari è la disciplina decisionale. Le organizzazioni che sfuggono alla trappola del debito fanno scelte difficili in anticipo. Centralizzano l'autorità di modernizzazione, allineano la sicurezza alla resilienza aziendale e trattano l'architettura come una risorsa strategica. Il 73% dei "leader" della modernizzazione ha centralizzato il processo decisionale con poche persone, rispetto a solo il 36% dei "ritardatari".[24] Coloro che falliscono rimangono intrappolati nella paralisi guidata dai comitati, in cui le vulnerabilità si muovono più velocemente delle decisioni e i rischi si aggravano mentre i piani sono dibattuti all'infinito.

Il debito tecnico spesso rispecchia il debito organizzativo. La proprietà frammentata, la responsabilità poco chiara e le decisioni differite creano la stessa fragilità nei modelli di leadership e operativi che esiste nell'infrastruttura legacy. Nel 2026, quella fragilità non sarà più sostenibile.

Modernizzazione come riduzione del rischio: riacquisto del tempo

Per sfuggire alla trappola del debito, è necessario considerare la modernizzazione come un mandato di resilienza, piuttosto che un ciclo di aggiornamento IT. La modernizzazione riduce i rischi riducendo la superficie d'attacco attraverso il consolidamento, consentendo l'applicazione di patch e la risposta automatizzate e rendendo la difesa e le operazioni basate sull'IA praticabili su larga scala. Altrettanto importante, riassegna la scarsa capacità ingegneristica a lavori di alto valore invece di una manutenzione continua.

Le organizzazioni che hanno successo non si modernizzano ricostruendo tutto; creano una base stabile e unificata in cui sicurezza, prestazioni e innovazione si rafforzano a vicenda. Con questa base in atto, i sistemi possono essere perfezionati, ridimensionati e adattati rapidamente, senza accumulare nuovi livelli di fragilità.

Il cambiamento richiesto non è incrementale. Richiede allineamento esecutivo e un'azione decisa. L'architettura legacy deve essere trattata come un rischio aziendale quantificato, non come un inconveniente tecnico. L'autorità decisionale per la modernizzazione deve essere centralizzata. Le iniziative IA consentono il rinnovamento dell'architettura piuttosto che attendere condizioni perfette. Le piattaforme devono essere consolidate per ridurre la complessità e ripristinare la visibilità.

In definitiva, la modernizzazione riguarda il recupero del tempo: tempo per innovare, tempo per rispondere e tempo per competere prima che il rischio crescente eroda il vantaggio.

73%

dei "leader" della modernizzazione ha centralizzato il processo decisionale con solo poche persone, rispetto a solo il 36% dei "ritardatari".[25]

DOMANDE PER LA DIRIGENZA

Il costo composto del legacy

Il debito tecnico drena velocità e resilienza. Molte aziende spendono di più per mantenere il passato che per costruire il futuro.

D1

Quali capacità aziendali sono oggi limitate dal debito tecnico?

Chi è responsabile della loro risoluzione e quali sono le tempistiche per ridurre tale rischio?

D2

Quale quota della spesa per la sicurezza mantiene il legacy rispetto a quella che costruisce la resilienza?

Qual è il nostro mix target nei prossimi 12-24 mesi?

D3

Quali iniziative prioritarie sono ritardate dai limiti dell'architettura?

Quali entrate, efficienza o guadagni di rischio stiamo rinviando di conseguenza?

D4

Quali sono le tre principali iniziative per ridurre il debito tecnico quest'anno?

Come misureremo i progressi e riterremo responsabili i leader?

D5

Quali sono i maggiori ostacoli alla riduzione del debito tecnico?

Sono limiti di budget, lacune di talenti, priorità in competizione o proprietà poco chiare? Quale rimuoveremo per primo?

6

Miraggio del cloud: disaccoppiamento del rischio a cascata

Miraggio del cloud: disaccoppiamento del rischio a cascata

Man mano che le aziende si consolidano su un minor numero di piattaforme cloud per muoversi più velocemente, molte stanno aumentando silenziosamente il rischio sistemico. Le strategie mono-cloud semplificano le operazioni ma concentrano i domini di guasto, mentre il multicloud viene spesso trattato come una casella da spuntare piuttosto che come una strategia di resilienza ingegnerizzata.

Le recenti interruzioni hanno reso inevitabile una verità: la resilienza non è determinata da quanti cloud utilizza un'organizzazione, ma da come la sua architettura si guasta. Nel 2026, i leader devono andare oltre l'ideologia del cloud e adottare la resilienza fin dall'ideazione: architetture realizzate per contenere i guasti, limitare l'impatto e preservare la fiducia sotto pressione.

Quando la velocità silenziosamente diventa fragilità

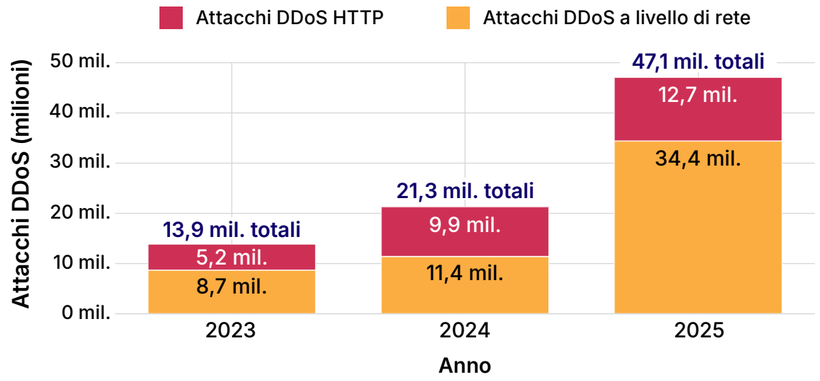
L'impresa moderna non intendeva costruire sistemi fragili. L'adozione del cloud prometteva velocità, elasticità e affidabilità, ma ha anche introdotto un rischio di concentrazione più silenzioso: meno visibile, più sistemico e più difficile da mitigare sotto stress.

Le interruzioni odierne non derivano solo da guasti di un singolo provider. Un singolo incidente del provider può ancora essere il fattore scatenante, ma gli eventi più dirompenti si verificano quando le dipendenze condivise falliscono in tandem: sistemi di identità, piani di controllo, pipeline di distribuzione e servizi di rete che sono alla base di tutto il resto. I dati pluriennali di Uptime Institute mostrano che circa due terzi delle interruzioni segnalate pubblicamente coinvolgono fornitori IT o di datacenter di terzi, inclusi colossi del cloud e di Internet, società di telecomunicazioni e colocation.[26]

La business continuity è ancora troppo spesso incentrata sul recupero, focalizzata sul ripristino del servizio piuttosto che sul contenimento del guasto. Nel tempo, le dipendenze a più livelli trasformano gli ambienti in sistemi strettamente accoppiati in cui piccoli guasti possono verificarsi a cascata. Questa fragilità di solito diventa visibile solo durante una crisi.

Pressione permanente

Attacchi DDoS per anno e tipo



Fonte: Cloudflare Radar

Le attività DDoS sono più che triplicate in due anni. L'interruzione su larga scala non è più episodica, è continua. In ambienti strettamente accoppiati, la pressione esterna sostenuta espone dipendenze nascoste e amplifica i piccoli guasti in eventi sistemici. La resilienza deve presupporre uno stress costante, non un raro guasto.

> Il cloud crea scalabilità: **ma non automaticamente resilienza**. Se i tuoi sistemi si guastano insieme, non hai progettato la ridondanza. Hai progettato la correlazione.
>
> Mark Hughes, Global Managing Partner for Cybersecurity Services, IBM

Il vantaggio è chiaro. Le organizzazioni che progettano e testano i guasti ottengono risultati materialmente migliori. Una grande azienda di servizi finanziari ha ridotto le interruzioni del 40% e ridotto i tempi di risoluzione di quasi il 60% dopo aver modernizzato l'architettura, migliorato l'osservabilità e l'ingegneria per la preparazione ai guasti.[27]

Oggi le interruzioni riguardano meno l'interruzione del cloud e più l'erosione dell'indipendenza. Il vero rischio è l'accoppiamento architettonico. La resilienza ora richiede l'isolamento intenzionale, i limiti dell'impatto e il trattamento del contenimento dei guasti come principio di progettazione fondamentale.

L'illusione del mono-cloud: efficienza senza contenimento

Per molte organizzazioni, le strategie mono-cloud sono diventate la scelta predefinita nella ricerca dell'efficienza. Gli strumenti standardizzati riducono la complessità, accelerano la distribuzione e riducono i costi operativi. Il compromesso è il rischio di concentrazione. Lo stesso consolidamento che guida l'efficienza può anche centralizzare i guasti.

I principali provider di servizi cloud sono spesso estremamente resilienti, ma il rischio maggiore oggi è architettonico e operativo. Quando identità, applicazione dei criteri, osservabilità e pipeline di distribuzione si basano tutti sullo stesso piano di controllo o limite di attendibilità, la resilienza diventa un presupposto piuttosto che una proprietà integrata. Un singolo errore, sia dal lato del provider che dal lato del cliente, può propagarsi ampiamente se il progetto non lo contiene. Possono esistere piani di ripristino, ma spesso non esiste un vero contenimento. Quando qualcosa si interrompe, il rischio che si interrompa tutto il resto è molto alto.

I dati del settore rafforzano questa realtà. La ricerca di Gartner mostra che la maggior parte dei guasti del cloud derivano da problemi operativi e di configurazione errata piuttosto che da difetti dell'infrastruttura principale. Le analisi basate sui sondaggi Gartner attribuiscono circa l'80% dei guasti alla sicurezza del cloud a una configurazione errata e le proiezioni suggerivano che entro l'anno scorso, fino al 99% dei guasti dell'ambiente cloud avrebbe comportato un errore umano in qualche parte nella catena.[28] La lezione non è che gli esseri umani sbagliano, lo faranno sempre, ma che le architetture devono essere progettate per assorbire tali errori in modo sicuro.

L'implicazione pratica è chiara. La resilienza deve essere progettata, non data per scontata. Questo significa progettare sia per il contenimento che per il ripristino, separare le dipendenze critiche, aggiungere protezioni e policy-as-code per ridurre l'impatto degli errori e testare regolarmente scenari di errore. Il rischio di concentrazione non è scomparso nell'era del cloud. È salito nello stack. Le organizzazioni che rimangono resilienti sono quelle che garantiscono che un singolo guasto non diventi un evento sistemico.

Il mito del multicloud: ridondanza senza indipendenza

Il multicloud è spesso posizionato come l'antidoto al rischio di concentrazione. In pratica, ricrea spesso la stessa fragilità, solo appoggiandosi a fornitori diversi. La maggior parte degli ambienti multicloud condivide provider di identità, pipeline CI/CD, strumenti di governance e dipendenze SaaS. Quando questi livelli condivisi falliscono, la promessa di indipendenza svanisce all'istante. Questo è il motivo per cui le revisioni post-incidente rivelano così spesso che i sistemi "ridondanti" non sono mai stati veramente indipendenti.

La resilienza non riguarda il numero di cloud presenti in un diagramma. Si tratta di quali livelli falliscono indipendentemente sotto pressione e quali no.

Ingegneria per il contenimento, non per la perfezione

La progettazione autonoma inizia con l'aspettativa che i sistemi si guasteranno e si concentra sul mantenere i guasti limitati e utili durante il processo di apprendimento. L'obiettivo non è solo quello di resistere agli shock, ma di migliorare grazie a questi.

Il contenimento è ciò che lo rende possibile. Significa che un guasto in un'area non si diffonde automaticamente ad altre. Un errore isolato ha una portata limitata, una causa chiara e un impatto gestibile. Non trascina con sé identità, criteri, dati e operazioni.

Le organizzazioni che utilizzano l'IA e l'automazione hanno notevolmente ridotto i cicli di vita delle violazioni di **80 giorni** e ridotto i costi medi delle violazioni di

1,9 milioni di dollari[29]

Si manifesta nell'architettura attraverso l'indipendenza tra i livelli di identità, criteri ed esecuzione, la separazione dei piani di controllo e il comportamento sicuro per impostazione predefinita in condizioni di incertezza. Le interruzioni sono inevitabili. La priorità è mantenerli locali, spiegabili e in grado di sopravvivere e utilizzarli per rafforzare il sistema. Le organizzazioni leader non sono quelle con zero incidenti, ma quelle che limitano con successo l'impatto di ogni singolo evento.

Il contenimento come vantaggio per la crescita

Sebbene spesso visto come un'assicurazione, il disaccoppiamento dei livelli supporta velocità e crescita. Il report Cost of a Data Breach 2025 di IBM ha rilevato che le organizzazioni che utilizzano l'IA e l'automazione hanno notevolmente ridotto i cicli di vita delle violazioni dei dati di 80 giorni e ridotto i costi medi delle violazioni dei dati di 1,9 milioni di dollari.[30]

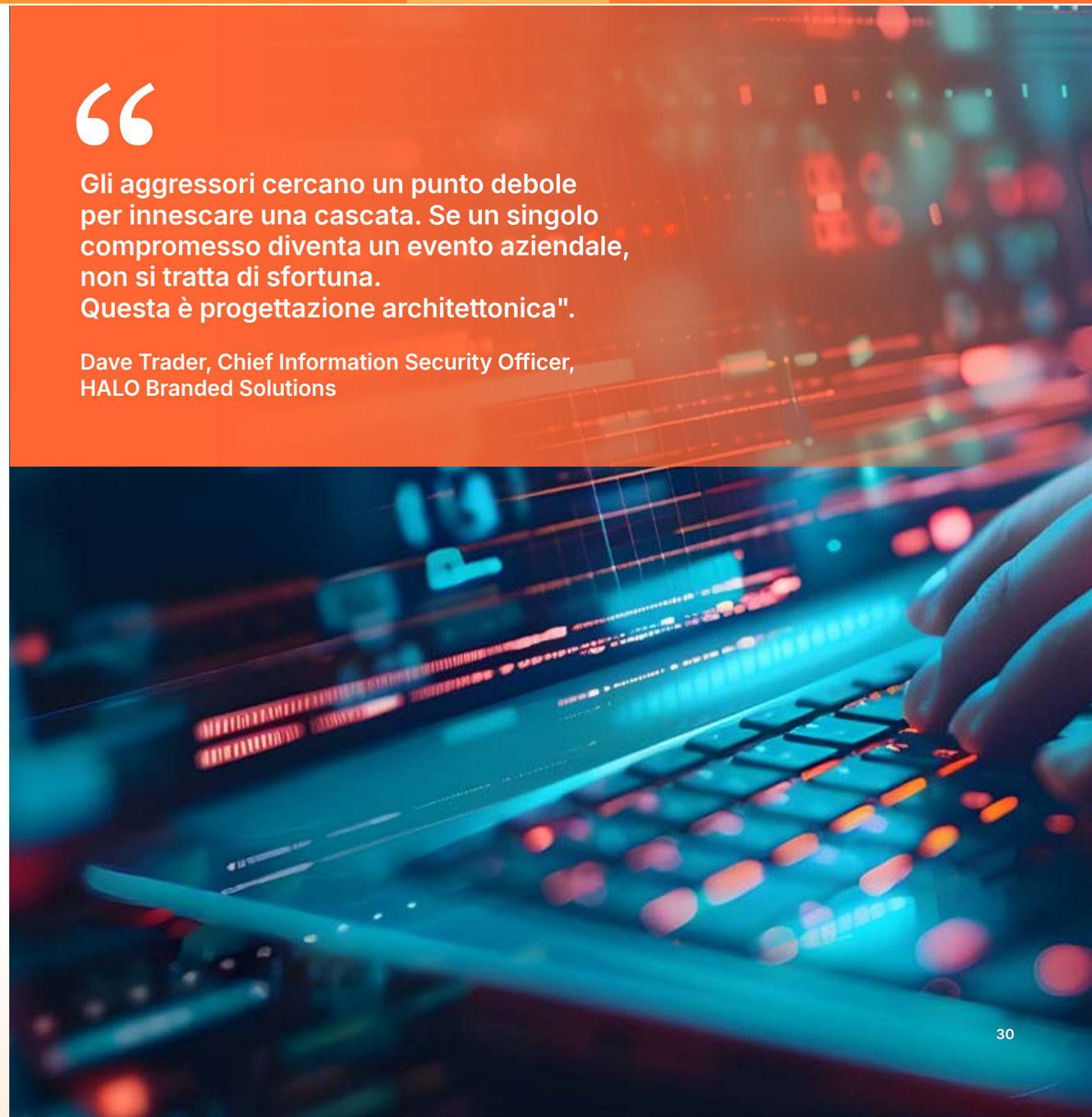
Limitando la portata dell'impatto, i leader preservano la fiducia di clienti, autorità di regolamentazione e investitori e mantengono l'agilità necessaria per un'adozione dell'IA più sicura, un ingresso più rapido nel mercato e un minor numero di escalation dei dirigenti. Quando il guasto è contenuto, i leader mantengono la capacità decisionale.

Il contenimento non è difensivo. Consente movimenti più rapidi e un approccio più oculato al rischio in un ambiente instabile.

Pianificare la tolleranza ai guasti a livello dirigenziale

Poiché i sistemi digitali sono alla base della strategia aziendale, la decisione di separare o accoppiare l'infrastruttura diventa una decisione aziendale ad alto rischio.

I vertici aziendali devono spostare il focus dalla velocità di ripristino all'individuazione dei processi che non possono permettersi un guasto simultaneo. Questo richiede chiarezza su piani di controllo condivisi, dipendenze di identità e pipeline, oltre a prove di test in modalità di errore, non solo sui tempi di attività. La gestione del contenimento spetta al consiglio di amministrazione perché il guasto sistemico è un rischio aziendale; non può essere delegato. Deve essere progettato deliberatamente dall'alto in modo che nessun singolo guasto diventi un evento a livello aziendale e ogni incidente rafforzi il sistema.



> **Gli aggressori cercano un punto debole per innescare una cascata. Se un singolo compromesso diventa un evento aziendale, non si tratta di sfortuna. Questa è progettazione architettonica".**
>
> **Dave Trader, Chief Information Security Officer, HALO Branded Solutions**

DOMANDE PER LA DIRIGENZA

Quando un servizio condiviso si guasta, l'architettura lo contiene?

Discusse insieme, queste domande rivelano se l'azienda può contenere le interruzioni in tempo reale o se la stabilità dipende ancora dalla speranza, dall'eroismo e dalla ripresa post-incidente.

D1

Quali sistemi critici possono guastarsi senza bloccare l'azienda?

Lo abbiamo dimostrato attraverso i test o è teorico?

→

D2

Se il sistema di gestione delle identità o una piattaforma principale subisse un disservizio, quali flussi di entrate verrebbero interrotti?

Conosciamo l'impatto in anticipo o solo dopo l'interruzione?

→

D3

Il multicloud sta riducendo i rischi o semplicemente aggiungendo complessità e costi?

Dove abbiamo ridotto la dipendenza e dove rimane?

→

D4

Stiamo misurando il contenimento o solo il tempo di recupero?

I nostri KPI premiano la prevenzione o la pulizia reattiva?

→

D5

Possiamo spiegare la nostra ultima interruzione al consiglio o alle autorità di regolamentazione?

L'impatto è stato limitato dalla progettazione o da una circostanza fortuita?

CONCLUSIONI

I principi di leadership per un vantaggio duraturo

In un mondo modellato da decisioni basate sull'IA, sistemi autonomi ed ecosistemi digitali profondamente interdipendenti, la resilienza non è più sufficiente. Il vantaggio verrà dalla capacità dei sistemi di rilevare lo stress, adattarsi in tempo reale, contenere i guasti e continuare a funzionare senza attendere l'intervento umano. Questo è ciò che chiamiamo resilienza autonomica.

Questo report non è un inventario delle minacce. Definisce un mandato di leadership: identificare e affrontare le faglie incorporate nelle imprese moderne. Queste debolezze strutturali possono sembrare gestibili in condizioni stazionarie, ma emergono in modo affidabile sotto pressione senza un'azione decisiva. Funzionano con l'adozione dell'IA, la dipendenza dal cloud, l'architettura legacy, l'intelligence delle minacce e i modelli operativi realizzati per un'era più prevedibile.

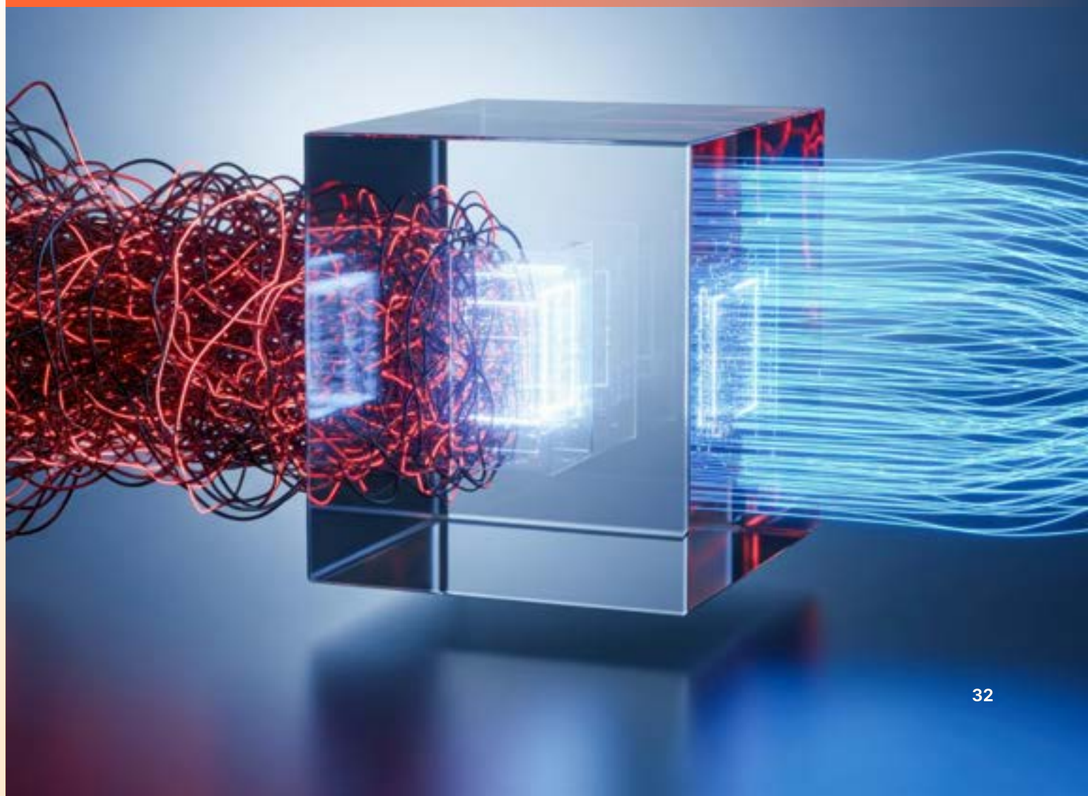
Affrontare queste linee di faglia non è compito del solo CISO. La resilienza autonomica è una responsabilità della dirigenza, modellata dal modo in cui i team dirigenziali stabiliscono le priorità, assegnano l'autorità e progettano sistemi che si autoregolano. Le organizzazioni autonomiche si distinguono per i principi che i loro team di leadership incarnano costantemente:

- **Proprietà condivisa del rischio sistemico rispetto alla responsabilità delegata.** Il rischio sistemico è di proprietà del team dirigente, non delegato nell'organigramma. La responsabilità è esplicita, la proprietà è condivisa in tutta la dirigenza e i consigli di amministrazione si impegnano attraverso scenari e compromessi reali, non generazione di report statici.
- **Esecuzione incorporata nei sistemi rispetto all'intento dichiarato.** Le decisioni contano solo se vengono eseguite su scala automatizzata. Il controllo su modelli, dati, prompt e azioni autonome deve risiedere dove avviene l'esecuzione. Tutto ciò che dipende dalla documentazione, dall'allineamento o dal processo manuale non è scalabile.
- **Indipendenza strutturale rispetto alla convenienza a breve termine.** Ciò che sembra efficiente in condizioni di calma spesso crea fragilità sotto stress. I team resilienti danno autonomicamente priorità a contenimento, reversibilità e separazione. I sistemi sono progettati in modo che i guasti rimangano locali, osservabili e correggibili. La capacità di prevenire le cascate diventa un vantaggio strategico.
- **Attendibilità dimostrabile anziché controllo presunto.** L'attendibilità deve essere continuamente dimostrabile, non implicitamente assunta. I leader richiedono visibilità sul comportamento del sistema, controlli applicabili sulle identità umane e di macchine e prove di integrità su scala automatizzata. L'attendibilità presunta fallisce nei sistemi autonomi.
- **Imparare dai guasti anziché evitarli.** I guasti sono previsti e utilizzati deliberatamente come input. La diagnosi precoce, l'impatto limitato, il rapido recupero e l'apprendimento istituzionale definiscono le prestazioni della leadership. La velocità di ripristino, non la prevenzione, è la metrica che conta.

Nel 2026, la leadership è definita meno dalla pianificazione per la stabilità e più dalla progettazione per l'innovazione dirompente.

Le organizzazioni che saranno leader saranno quelle i cui dirigenti incorporano questi principi nelle decisioni quotidiane, trasformando la volatilità in apprendimento, la pressione in progresso e l'incertezza in vantaggio.

Le organizzazioni che saranno leader saranno quelle i cui dirigenti incorporano questi principi nelle decisioni quotidiane: **trasformando la volatilità in apprendimento, la pressione in progresso e l'incertezza in vantaggio.**



Informazioni su Cloudflare

INFORMAZIONI SU CLOUDFLARE

Una sola piattaforma. Una rete programmabile.

Oltre
330 città in più di 125 Paesi, inclusa la Cina continentale

↳ **con oltre 210 città**
che eseguono GPU per l'inferenza dell'IA in tutto il mondo

Circa 50 ms
da circa il 95% della popolazione mondiale connessa a Internet

Circa 13.000 reti
si connettono direttamente a Cloudflare, inclusi ISP, provider di servizi cloud e grandi aziende

477 Tb/s
di capacità della rete e in crescita

INFORMAZIONI SU CLOUDFLARE

Suite di sicurezza Cloudflare

Resilienza e difesa all'edge

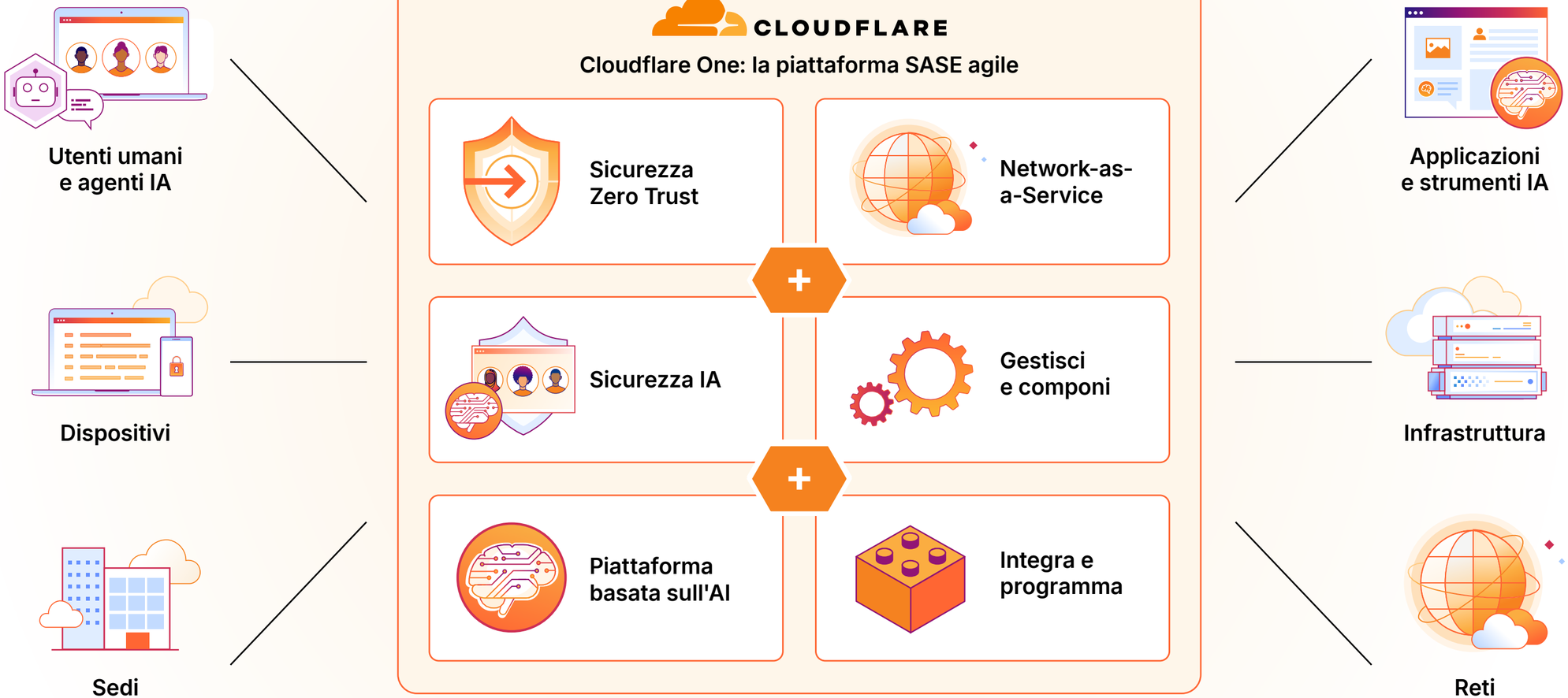
- Protezione delle app web e delle API: blocca gli attacchi, rileva le vulnerabilità e migliora la disponibilità
- Security Service Edge (SSE): applica la sicurezza Zero Trust su tutta la forza lavoro ibrida
- Mitigazione DDoS: resisti agli attacchi più grandi e avanzati con 477 Tb/s di capacità di rete

Integrazione sicura tra cloud e rete

- Secure Access Service Edge (SASE): connetti e proteggi la forza lavoro, gli agenti IA e l'infrastruttura
- Network-as-a-Service e multicloud: connetti, proteggi e accelera le tue reti aziendali senza i costi e la complessità dell'hardware legacy
- Interconnessione di rete: connetti direttamente le reti in locale e cloud alla rete di Cloudflare

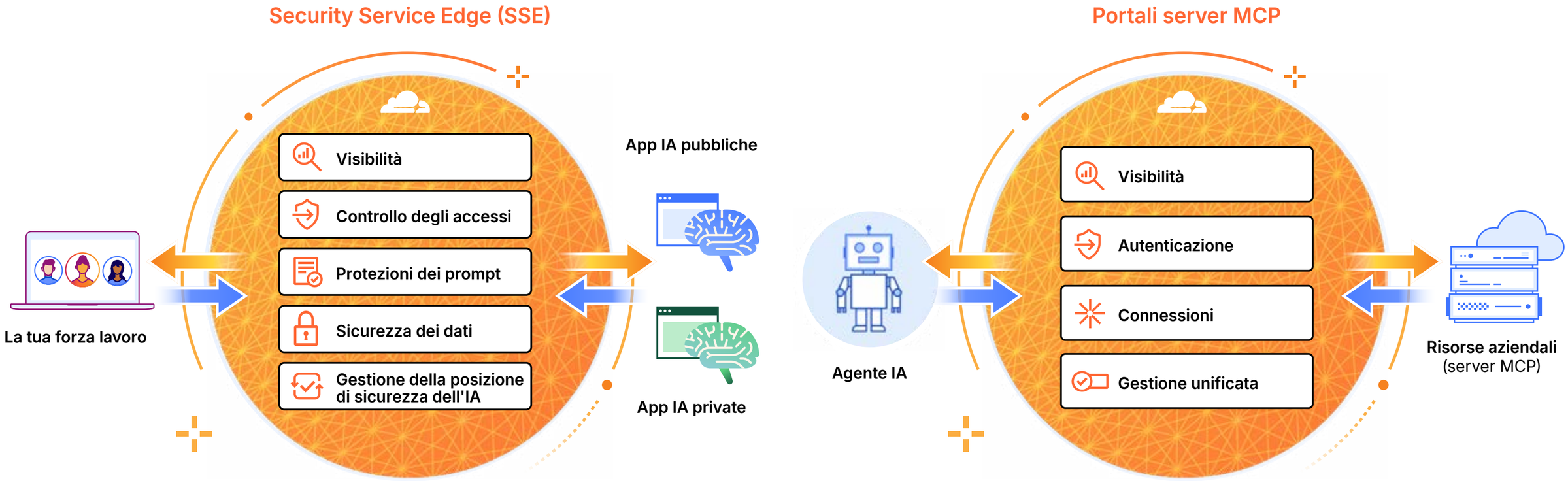
INFORMAZIONI SU CLOUDFLARE

Servizi Cloudflare One



INFORMAZIONI SU CLOUDFLARE

Proteggi l'uso della GenAI e governa gli agenti IA



INFORMAZIONI SU CLOUDFLARE

Servizi IA di Cloudflare nell'intero ciclo di vita

Crea IA
con la piattaforma per gli sviluppatori

Crea IA in ogni area geografica del mondo con un solo clic

Workers AI, Vectorize, AI Gateway

Crea un'infrastruttura IA, in modalità facile

Remote MCP Server, Agents SDK, AI Search, AI Gateway

Proteggi l'adozione dell'IA
con AI Security Suite

Utilizzo sicuro della GenAI da parte della forza lavoro

Piattaforma SASE (Cloudflare One)

Governa gli agenti IA

ZTNA di Cloudflare, inclusi i portali server MCP

Crea l'IA in modo sicuro

AI Gateway

Proteggi le app basate sull'IA

App Security, incluso Firewall for AI

Proteggi i contenuti
con servizi applicativi

Proteggi i contenuti originali online dai crawler IA

Bot Management, incluso AI Crawl Control

Piattaforma basata sull'IA su un'unica rete globale
Modelli di rilevamento delle minacce · Agente IA (Cloudy) · Modelli di prevenzione della perdita di dati

INFORMAZIONI SU CLOUDFLARE

Approfondimenti per il CxO moderno

Navigare nel panorama delle minacce odierne e nei rapidi cambiamenti tecnologici richiede più della semplice conoscenza operativa: necessita di lungimiranza strategica. "The Executive Lens" di Cloudflare è un hub di risorse dedicato curato specificamente per i leader della dirigenza.

Scopri approfondimenti guidati da esperti, framework fruibili e ricerche esclusive su argomenti aziendali critici come la resilienza informatica, la governance sicura dell'IA e la trasformazione digitale globale.

Esplora The Executive Lens oggi stesso.

Leggi di più

Risorse aggiuntive

Forrester Total Economic Impact

Affronta le minacce sofisticate e previeni quelle emergenti. Scopri come Cloudflare aiuta le aziende a utilizzare la sicurezza come vantaggio competitivo, resistendo a un panorama di minacce complesso con maggiore efficienza e prevedibilità.

Leggi di più

Security Signal

Scopri il segnale dal rumore e concentrati sulle tendenze più importanti della sicurezza informatica di oggi. Ogni episodio di Security Signal traduce le complessità della sicurezza informatica in intelligence fruibile per i dirigenti al timone.

Guarda ora

Report sulle minacce 2026 di Cloudflare

Comprendi il panorama delle minacce del 2026 definito da una nuova misurazione di efficacia (MOE, Measure of Effectiveness). Il report descrive in dettaglio i nuovi rischi derivanti dal preposizionamento sponsorizzato dagli stati, dal furto di token, dagli attacchi DDoS ipervolumetrici e altro ancora.

Leggi di più

theNET

Approfondimenti sull'innovazione della sicurezza informatica, sul panorama delle minacce e sul futuro di Internet, con prospettive dirigenziali su come risolvere le sfide organizzative con la tecnologia.

Leggi di più

the NET BY CLOUDFLARE

Contatti

	Globale	Nord e Sud America	EMEA	Asia Pacifico	Giappone
Leadership di mercato	 **Mark Anderson** President of Revenue markanderson@cloudflare.com	 **Rick Congdon** Geo Vice President, Nord e Sud America congdon@cloudflare.com	 **Tony Van den Berge** Geo Vice President, EMEA tonyberg@cloudflare.com	 **Goran Risticevic** Geo Vice President, APAC goran@cloudflare.com	 **Sayoko Matsumoto** Geo Vice President, Giappone sayoko@cloudflare.com
Field CXO Team	 **Ramy Houssaini** Chief Cyber Solutions Officer ramy@cloudflare.com	 **Khalid Kark** Field CIO, Nord e Sud America khalid@cloudflare.com	 **Christian Reilly** Field CIO, EMEA creilly@cloudflare.com	 **Volker Rath** Field CISO volker@cloudflare.com	 **Koichiro Otobe** Field CTO, Giappone koichiro@cloudflare.com

CLOUDFLARE

2026

Report Cloudflare Security Signals

Resilienza autonomica

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-8897.2026MAR19

Note

1. Jonathan Villa, "Hidden Risks of Shadow AI", Varonis, www.varonis.com/blog/shadow-ai. Consultato l'11 febbraio 2026.
2. IBM, "Cost of a Data Breach Report 2025", www.ibm.com/reports/data-breach. Consultato l'11 febbraio 2026.
3. MultiState, "Artificial Intelligence (AI) Legislation", www.multistate.ai/artificial-intelligence-ai-legislation. Consultato l'11 febbraio 2026.
4. Gartner, "Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up From Less Than 5% in 2025", 26 agosto 2025, www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025. Consultato l'11 febbraio 2026.
5. Cloudflare Radar, "Bot Traffic", radar.cloudflare.com/bots?dateRange=12w. Consultato l'11 febbraio 2026.
6. Cloudflare Radar, "Application Layer Security", radar.cloudflare.com/security/application-layer?dateRange=12w. Consultato l'11 febbraio 2026.
7. IBM, "Cost of a Data Breach Report 2025".
8. Lareina Yee, et al., "The AI Reckoning: How Boards Can Evolve", McKinsey & Company, 24 ottobre 2024, www.mckinsey.com/capabilities/mckinsey-technology/our-insights/the-ai-reckoning-how-boards-can-evolve. Consultato l'11 febbraio 2026.
9. IBM, "Cost of a Data Breach Report 2025".
10. ENISA, "SBOM Analysis - Towards an Implementation Guide". Dicembre 2025, www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf. Consultato l'11 febbraio 2026.
11. Verizon, "2025 Data Breach Investigations Report (DBIR)", www.verizon.com/business/resources/reports/dbir. Consultato l'11 febbraio 2026.
12. Cloudflare, "2026 Cloudflare App Innovation Report", 2026, www.cloudflare.com/resource/g/app-innovation-report/2026. Consultato l'11 febbraio 2026.
13. CrowdStrike, "2025 Global Threat Report", www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf. Consultato il 18 marzo 2026.
14. SANS Institute, "SANS 2025 CTI Survey: Cyber Threat Intelligence Survey", SOCRadar, maggio 2025, socradar.io/wp-content/uploads/2025/05/SANS-2025-CTI-Cyber_Threat_Intelligence_Survey-SOCRadar.pdf. Consultato l'11 febbraio 2026.
15. SANS Institute.
16. SANS Institute.
17. Mohammed Khalil, "Vulnerabilities Statistics 2025: Record CVEs, Zero-Days & Exploits", DeepStrike, 8 ottobre 2025, deepstrike.io/blog/vulnerability-statistics-2025. Consultato il 25 febbraio 2026.
18. VulnCheck, "VulnCheck State of Exploitation 2026", 21 gennaio 2026, www.vulncheck.com/blog/state-of-exploitation-2026. Consultato l'11 febbraio 2026.
19. Dati della rete globale Cloudflare.
20. Pegasystems, "Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research", 14 ottobre 2025, www.pega.com/about/news/press-releases/average-global-enterprise-wastes-more-370-million-every-year-through. Consultato l'11 febbraio 2026.
21. Protiviti, "Global Technology Executive Survey: Tech Debt a Major Burden", www.protiviti.com/us-en/global-technology-executive-survey-tech-debt-major-burden. Consultato l'11 febbraio 2026.
22. Cloudflare, "Report Cloudflare sull'innovazione delle app 2026".
23. Pegasystems, "Average Global Enterprise Wastes More Than $370 Million Every Year Through Technical Debt, Says Research".
24. Cloudflare, "Report Cloudflare sull'innovazione delle app 2026".
25. Cloudflare, "Report Cloudflare sull'innovazione delle app 2026".
26. Uptime Institute, "Uptime Annual Outage Analysis Report 2025", 6 maggio 2025, uptimeinstitute.com/about-ui/press-releases/uptime-announces-annual-outage-analysis-report-2025. Consultato l'11 febbraio 2026.
27. Nuno De la Torre, et al., "IT Resilience for the Digital Age", McKinsey & Company, 20 giugno 2023, www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/it-resilience-for-the-digital-age. Consultato l'11 febbraio 2026.
28. Ashwin Chaudhary, "Managing Cloud Misconfigurations Risks", Cloud Security Alliance, 14 agosto 2023, cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks. Consultato l'11 febbraio 2026.
29. IBM, "Cost of a Data Breach Report 2025".
30. IBM, "Cost of a Data Breach Report 2025".