VECTRA AI

EBOOK

Occhio ai tuoi gap di sicurezza

Come gli attaccanti attraversano il tuo ambiente

Di Lucie Cardiet · Cyberthreat Research Manager

Perché ho scritto questo libro

Lettera dell'autrice

Passo le mie giornate a osservare ciò che gli attaccanti fanno davvero, in ambienti che assomigliano al vostro.

Quello che constato sistematicamente è che i difensori non perdono per mancanza di investimenti. Perdono perché i loro investimenti restano in una zona di efficacia parziale. Il loro EDR funziona esattamente come previsto; l'attaccante opera sul piano dell'identità. Il loro SIEM ingerisce ogni log; e l'attacco è visibile solo nella correlazione tra log. Il loro IAM approva ogni login conforme alla policy; ma la persona dall'altra parte non è il dipendente di cui usano le credenziali.

Questa è la seconda edizione di ciò che ho scritto nel 2025. Le novità: due campagne aggiuntive (Volt Typhoon e AWS compromesso da agenti AI in otto minuti), i risultati misurati da IDC nel 2025 con Vectra AI, una sezione sulla pressione regolatoria che rende il rilevamento continuo una questione di compliance, e una self-assessment alla fine.

Lucie Cardiet

La rete ha superato la sua architettura di sicurezza.

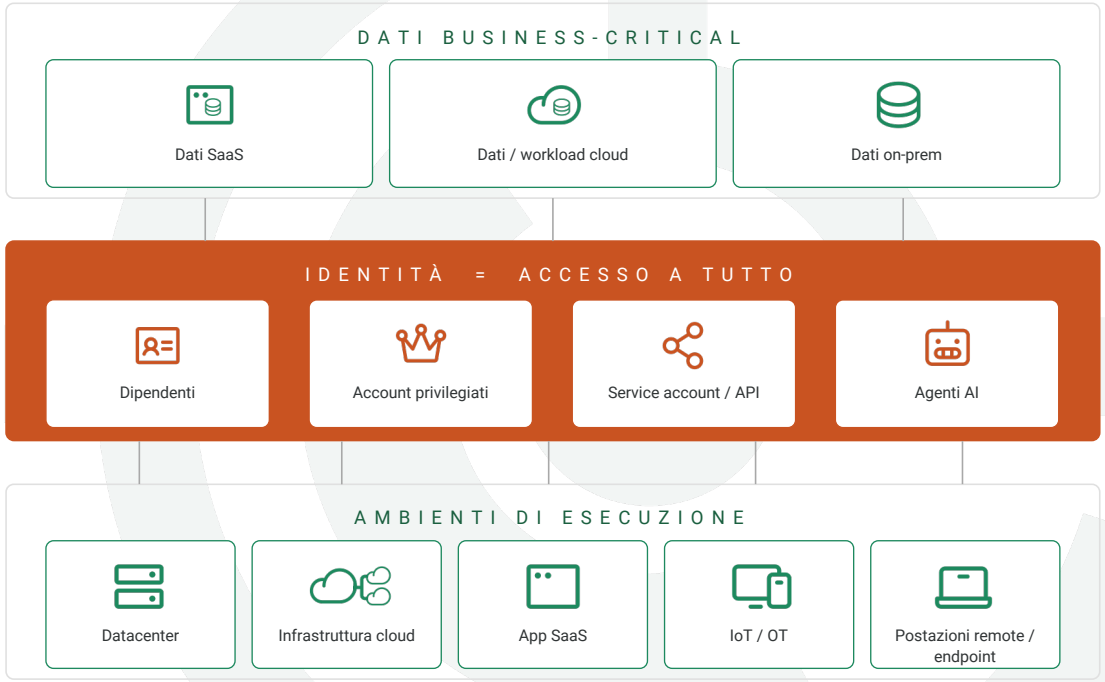
Oggi, l'azienda non vive più dietro un singolo perimetro

Gli ambienti aziendali si estendono su infrastruttura on-prem, più cloud pubblici, decine di app SaaS, identity provider, sistemi IoT e OT, servizi AI e gli agenti autonomi che operano sopra di essi. Questi domini non sono indipendenti, formano un unico sistema connesso.

- ✓ Il tuo EDR sorveglia gli endpoint.
- ✓ Il tuo IAM approva i login.
- ✓ Il tuo CSPM legge le configurazioni.
- ✓ Il tuo SIEM archivia i log.

Ognuno fa il suo lavoro.

Gli attaccanti, sempre più assistiti dall'AI, hanno passato gli ultimi tre anni a imparare a muoversi tra di essi, negli spazi che nessun tool è stato progettato per osservare.



La rete è evoluta. Anche gli attaccanti.

Il tuo stack è solido, ma è completo?

A prima vista, hai costruito uno stack di sicurezza solido.

- Hai investito nelle migliori tecnologie di sicurezza disponibili oggi.
- Hai una protezione degli endpoint su ogni dispositivo.
- Hai tool che monitorano la tua rete.
- I tuoi tool di cloud posture management scansionano correttamente le configurazioni.
- Hai rafforzato la gestione delle identità con IAM o PAM.

Eppure, gli attaccanti possono passare e lo fanno.

Non perché i tuoi tool siano rotti. Perché ogni tool è stato progettato per coprire il proprio dominio, e gli attaccanti ora operano tra di essi.

Gli attaccanti non rompono i tuoi tool. Li aggirano.

La realtà: gli attaccanti moderni non combattono il tuo stack. Lo evitano.

Abuso di identità
Le credenziali compromesse sono il vettore di accesso iniziale nel 22 % delle violazioni.[1] L'88 % degli attacchi web di base coinvolge credenziali rubate.[1]

Movimento laterale
Si muovono lateralmente senza generare alert. Il breakout time eCrime medio – il gap tra accesso iniziale e primo pivot laterale – è sceso a 29 minuti.[2]

Abuso di privilegi cloud
L'abuso di account validi rappresenta ora il 35 % degli incidenti cloud.[2]

Operare tra i tool
Si nascondono negli interstizi tra i tool, in spazi che nessun sistema è stato progettato per osservare.

Sfruttamento del rumore di alert
Operano sotto le tue soglie, sapendo che il SOC non può investigare tutto.

Velocità cross-domain
L'MFA blocca oltre il 99 % degli attacchi all'identità, ma gli avversari accedono sempre più via token rubati, app OAuth consentite, flussi device-code e proxy adversary-in-the-middle.[3]

Recon accelerata dall'AI
Gli attacchi condotti da avversari AI-enabled sono cresciuti dell'89 % anno su anno. Nel 2025, attaccanti hanno sfruttato tool GenAI legittimi in oltre 90 organizzazioni per generare comandi di credential theft.[2]

[1] Verizon DBIR 2025. [2] CrowdStrike 2026 Global Threat Report. [3] Microsoft Digital Defense Report 2025.

I tool best-in-class non equivalgono a copertura completa.

Ogni investimento riduce il rischio nella sua area, ma lascia gap di visibilità e rilevamento tra i tool. I numeri 2026 lo confermano:

- L'82 % dei rilevamenti d'intrusione nel 2025 era malware-free. Gli attaccanti hanno operato con credenziali valide, flussi d'identità trusted e integrazioni SaaS approvate.[1]
- Le violazioni che coinvolgono più ambienti costano 5,05 M$ in media, il 25 % in più rispetto alle breach solo on-prem.[2]
- Il breakout time medio è sceso a 29 minuti. Record osservato: 27 secondi.[1]

[1] CrowdStrike 2026 Global Threat Report. [2] IBM Cost of a Data Breach Report 2025.

Lo schema non è nuovo. È la nuova normalità.

Questo ebook serve a mappare questi gap, mostrarti dove si inserisce Vectra AI e come Vectra AI li chiude.

Indice

Panoramica della copertura

L'illustrazione del Security Gap, più tre campagne nominate che lo sfruttano.

L'illustrazione del Security Gap

Il tuo stack attuale: nessuna combinazione fornisce un rilevamento continuo sull'intera infrastruttura ibrida. Ogni tool si ferma a fasi chiave.

		Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Elusione delle difese	Accesso credenziali	Discovery	Movimento laterale	Raccolta	Command & Control	Esfiltrazione	Impatto
ENDPOINT	EDR	●	●	●	●	●	●	●	●	●	●	●	●
ENDPOINT	EPP	●	●	○	○	○	○	○	○	○	○	○	○
CLOUD	CASB	●	○	○	●	○	●	○	○	●	○	●	○
CLOUD	CNAPP	●	●	●	●	●	●	●	●	●	●	●	●
CLOUD	CSPM	○	○	○	●	○	●	○	○	○	○	○	○
CLOUD	CWPP	●	●	●	●	○	○	●	○	●	●	○	●
CLOUD	SASE	●	○	○	○	○	○	○	●	○	●	●	○
RETE	Email	●	○	○	○	○	○	○	○	○	○	○	○
RETE	Firewalls	●	○	○	○	○	○	●	○	○	●	●	○
RETE	IDPS	●	○	○	○	○	○	●	●	○	●	●	○
RETE	NAC	●	○	○	○	○	○	○	○	○	○	○	○
RETE	SSE	●	○	○	○	○	○	○	●	○	●	●	○
IDENTITÀ	IAM	●	○	○	●	○	○	○	○	○	○	○	○
IDENTITÀ	PAM	○	○	○	●	○	●	○	○	○	○	○	○
IDENTITÀ	UEBA	●	○	●	●	●	●	●	●	○	○	●	○
Vectra AI Platform		●	●	●	●	●	●	●	●	●	●	●	●

● Visibilità parziale ● Visibilità totale ○ Nessuna visibilità

Tre gap che ogni stack ha oggi.

Non gap di copertura. Gap di esecuzione. Controlli che esistono ma non rilevano.

1. Niente sembra fuori posto.

I tool dell'attaccante sono i tuoi tool. Remote desktop. PowerShell. Un binario firmato. Living-off-the-land binaries che i tuoi sysadmin usano alle 2 di notte. Ogni singola azione sembra normale.

2. L'autenticazione riesce.

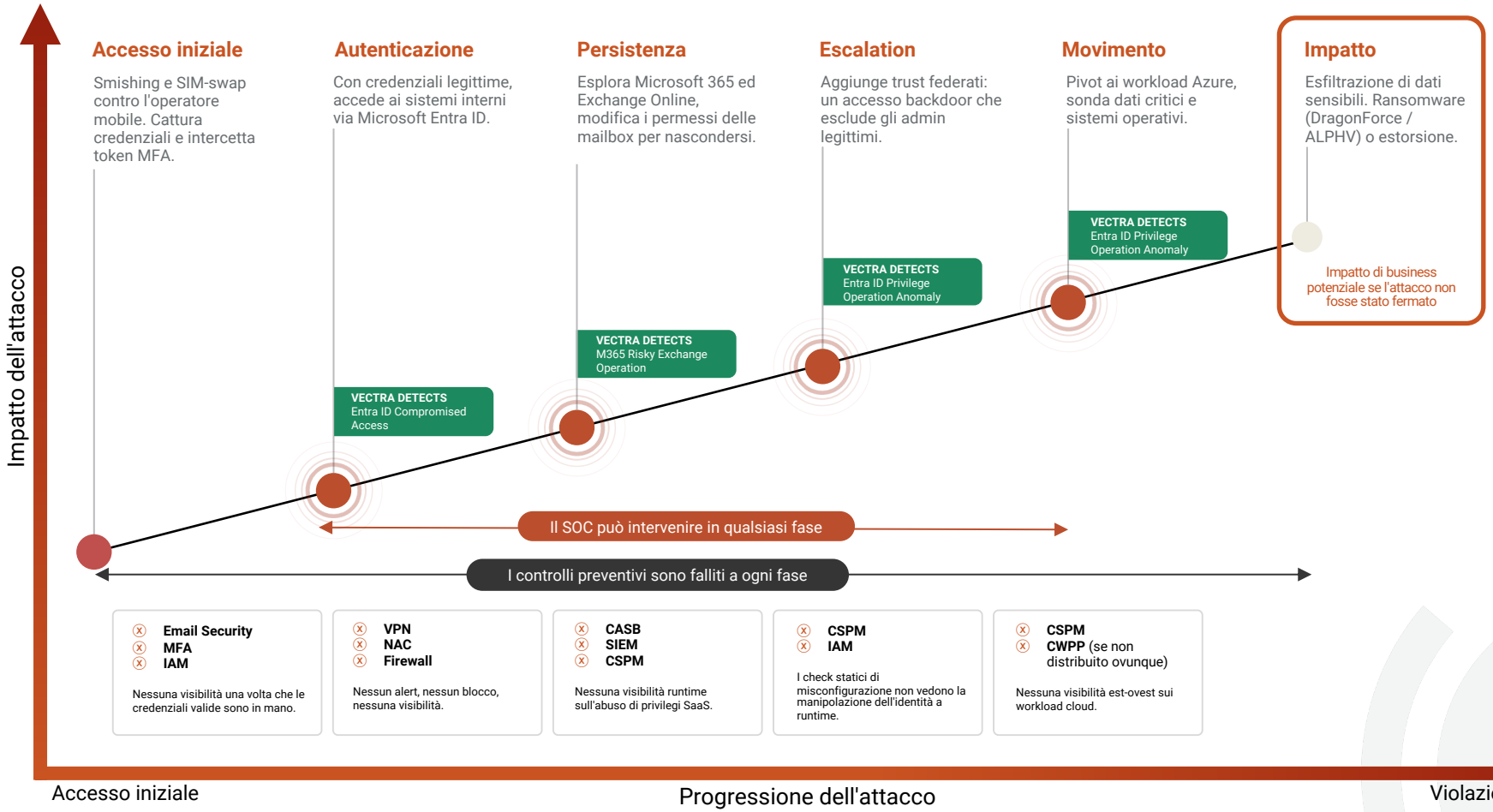
Credenziali valide, MFA approvato, il login è reale. Solo che non è la persona che pensi. Ogni controllo di autenticazione dice sì. La verità è che l'utente valido non è davvero l'utente.

3. Il movimento non è visibile.

Una volta dentro, il movimento laterale passa per integrazioni trusted: SaaS-to-SaaS, identità federata, token OAuth, service account. L'EDR non lo vede. Il CASB non lo vede. Il movimento è invisibile per architettura, non per furtività.

Scattered Spider: il playbook dell'helpdesk

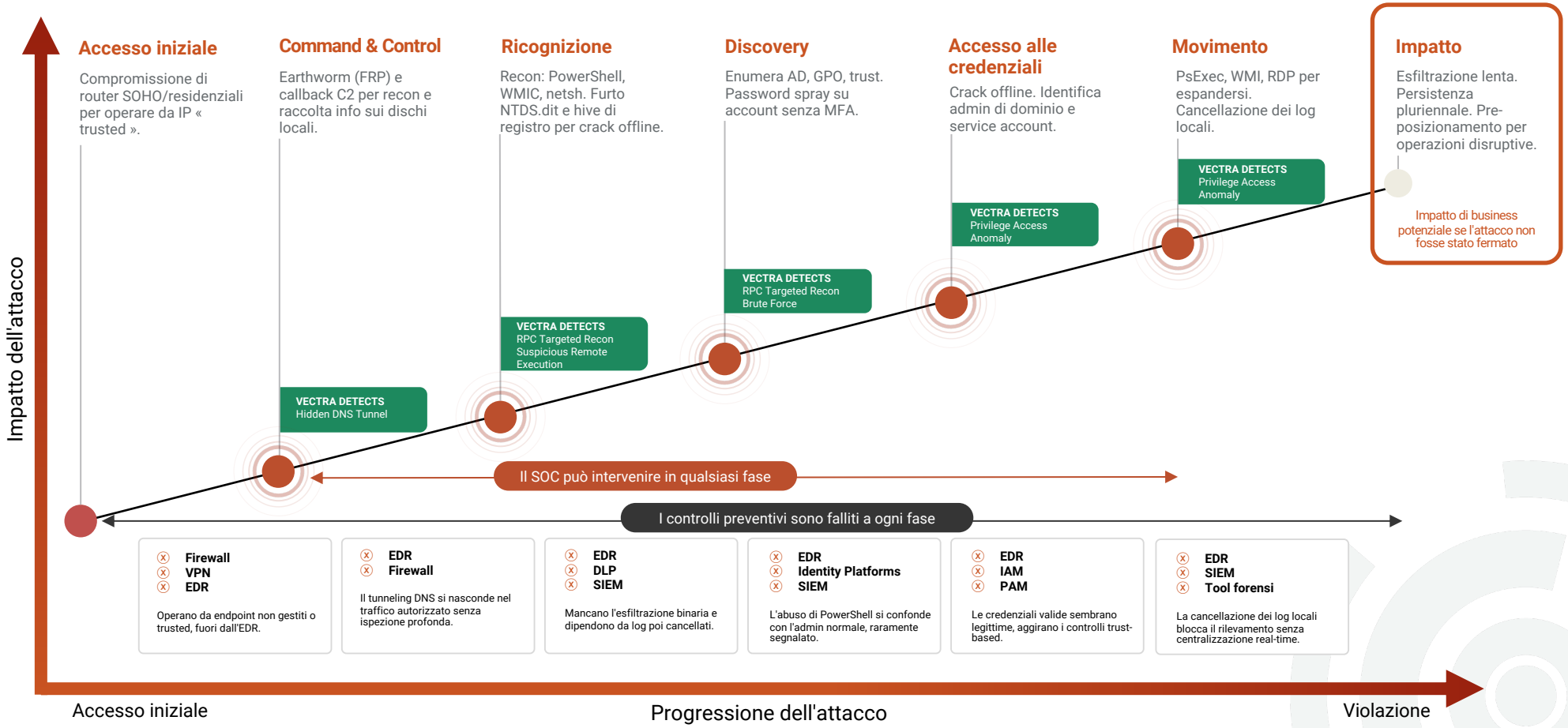
Scattered Spider (UNC3944) illustra perfettamente il motivo per cui le « credenziali valide » sono diventate un problema di rilevamento. Il gruppo non ha sfruttato vulnerabilità. Hanno chiamato l'helpdesk.



Fonti: reporting Mandiant UNC3944 (2023–2024); CISA Advisory AA23-320A sulle TTP di Scattered Spider.

Volt Typhoon: il playbook living-off-the-land

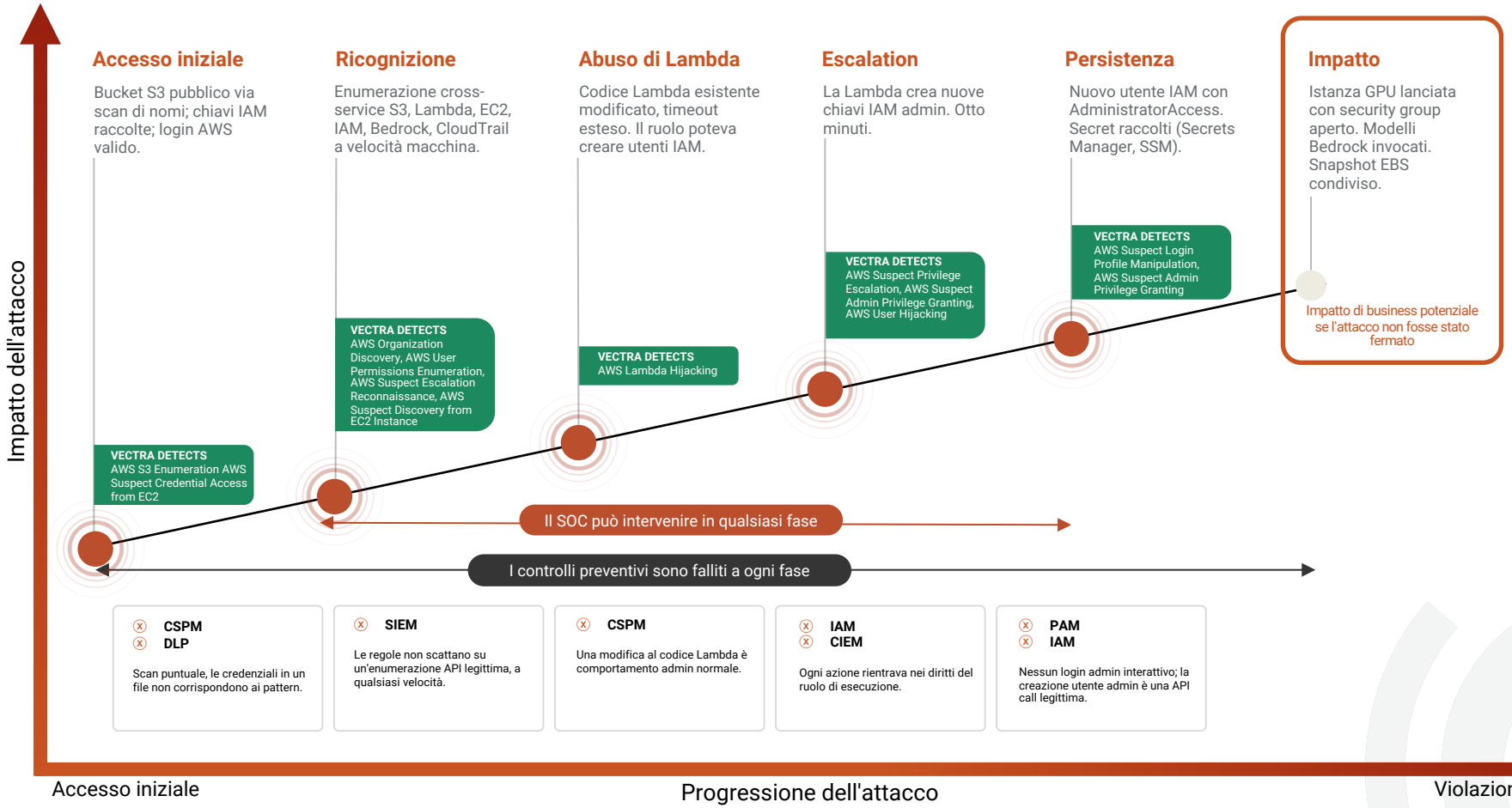
Volt Typhoon è la campagna attribuita alla RPC che ha mostrato ai difensori USA cosa significa davvero « living off the land ». L'advisory CISA/NSA/FBI di febbraio 2024 ha documentato operatori presenti dentro reti di infrastrutture critiche fino a cinque anni, usando solo tool Windows nativi, senza alcun malware da segnalare.



Fonti: advisory congiunto CISA/NSA/FBI AA24-038A (feb. 2024); Microsoft Threat Intelligence « Volt Typhoon targets US critical infrastructure with living-off-the-land techniques » (mag. 2023).

AWS compromesso da agenti AI in otto minuti.

Intrusione documentata da Sysdig (2025). Credenziali valide. Servizi AWS nativi. Recon a velocità macchina.



Fonti: blog di threat research Sysdig (2025); tecniche MITRE ATLAS di abuso di account validi e cloud service discovery.

Perché lo stack attuale ti lascia al buio.

Tre attaccanti diversi. Tre anni diversi. Tre punti d'ingresso diversi. Ogni attacco sembrava legittimo end-to-end dentro un singolo tool. Solo incrociando rete, piano dell'identità e piano di controllo cloud l'intento dell'attaccante diventa visibile.

Si tende a pensare che con investimenti in firewall, EDR, CASB, CSPM, IAM e SIEM, i gap siano chiusi. La realtà: questi tool non sono stati progettati per rilevare comportamenti d'attacco in ambienti ibridi, e i numeri lo dimostrano.

82 %

dei rilevamenti d'intrusione nel 2025 erano malware-free.

CrowdStrike 2026 Global Threat Report

32 %

in più di attacchi basati sull'identità nel primo semestre 2025.

Microsoft Digital Defense Report 2025

241 giorni

per identificare e contenere una violazione. 292 quando sono coinvolte credenziali rubate.

IBM Cost of a Data Breach Report 2025

Nelle sezioni che seguono, vediamo dove ogni parte dello stack non basta, e come Vectra AI chiude questi gap su rete, cloud, SaaS e identità.

VECTRA AI

OCCHIO AI TUOI GAPS

Sicurezza endpoint

Perché EDR ed EPP da soli non bastano.

EDR: profondo sull'host, ma non altrove.

L'Endpoint Detection and Response offre telemetria dettagliata dove è distribuito.

Accesso iniziale	Parziale
Esecuzione	Totale
Persistenza	Parziale
Escalation dei privilegi	Parziale
Elusione delle difese	Parziale
Accesso alle credenziali	Parziale
Discovery	Parziale
Movimento laterale	Parziale
Raccolta	Parziale
Command & Control	Parziale
Esfiltrazione	Parziale
Impatto	Totale

VISIBILITÀ: Parziale Totale Nessuna

L'EDR va oltre la prevenzione, con telemetria e analytics dettagliati su processi, modifiche al registry e attività locale. È potente dove è installato. La realtà 2025: l'82 % dei rilevamenti d'intrusione erano malware-free.[1] Gli attaccanti operano con credenziali valide in sessioni trusted, dove l'EDR non ha nulla da segnalare.

COME GLI ATTACCANTI AGGIRANO

- Evitano l'endpoint operando in console cloud o app SaaS.
- Sfruttano i gap di copertura. L'EDR vede solo gli host dove è installato.
- Si muovono via dispositivi non gestiti o BYOD senza agente.
- Usano credenziali valide per attività che all'EDR sembrano « normali ».

L'EDR non ha visibilità su attacchi cloud-nativi, abuso di identità o attività SaaS.

Tre delle quattro vulnerabilità più sfruttate nel 2024 erano zero-day in prodotti di sicurezza: Palo Alto, Ivanti, Fortinet.[2]

[1] CrowdStrike 2026 Global Threat Report. [2] Mandiant M-Trends 2025

EPP: blocca malware noti, cieco al resto.

Le Endpoint Protection Platform impediscono l'esecuzione di minacce note.

Accesso iniziale	●
Esecuzione	●
Persistenza	○
Escalation dei privilegi	○
Elusione delle difese	○
Accesso alle credenziali	○
Discovery	○
Movimento laterale	○
Raccolta	○
Command & Control	○
Esfiltrazione	○
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Le EPP usano firme, euristiche e sandboxing base. Le EPP moderne (NGAV) aggiungono rilevamento comportamentale e analisi fileless ML, ma restano endpoint-scoped e cieche al movimento cross-domain.

COME GLI ATTACCANTI AGGIRANO

- Malware fileless o staging accurato, sotto il radar comportamentale.
- Zero-day o binari inediti senza firma.
- PowerShell, WMI, RDP: indistinguibili dall'admin.

L'EPP non rileva in modo affidabile living-off-the-land o attacchi via credenziali.

Anche un EPP moderno resta endpoint-scoped. Cloud, identità, SaaS-to-SaaS sono invisibili by design.

Il gap della sicurezza endpoint e come Vectra AI lo chiude.

IL GAP ENDPOINT

EDR ed EPP sono fondamentali, ma coprono solo parte della kill chain.

Mancano:

- Identità con credenziali valide in M365 o Entra ID.
- Abuso di privilegi SaaS fuori dall'endpoint.
- Movimento laterale cloud, BYOD, identità federata.
- Recon ed esfiltrazione su canali cifrati o non-HTTP.

Anche sull'endpoint, l'EPP perde comportamenti sofisticati e l'EDR non sempre rileva l'abuso di account senza malware.

COSA AGGIUNGE VECTRA AI

- Identity Threat Detection per account compromessi che abusano di SaaS e cloud.
- SaaS Misuse Detection su M365, Exchange Online, Entra ID.
- Copertura ibrida: endpoint, cloud, rete, identità.
- Si integra con CrowdStrike, Microsoft Defender, SentinelOne e altre piattaforme EDR.

VECTRA AI

OCCHIO AI TUOI GAPS

Sicurezza del cloud

Il punto cieco del piano di controllo cloud.

CASB: blocca app non sanzionate, ignora gli abusi attivi.

Applica policy sul SaaS. Non vede gli attaccanti in sessioni valide.

Accesso iniziale	●
Esecuzione	○
Persistenza	○
Escalation dei privilegi	●
Elusione delle difese	○
Accesso alle credenziali	●
Discovery	○
Movimento laterale	○
Raccolta	●
Command & Control	○
Esfiltrazione	●
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

I CASB applicano policy via API o proxy inline. In modalità API (la più comune), vedono l'attività quasi in real-time con minuti di latenza. In ogni caso, i CASB operano sopra rete e identità, ciechi a ciò che fanno gli attaccanti dentro una sessione valida.

COME GLI ATTACCANTI AGGIRANO

- Usano credenziali valide per accedere al SaaS sanzionato (M365, Box, Salesforce).
- Sfruttano i permessi dall'interno (delega mailbox).
- Abusano del trust federato per loggarsi via SSO.

Il CASB non offre visibilità di rete.

Non sempre rileva abusi di privilegi live, manipolazione d'identità o comportamenti insider.

CSPM: trova misconfigurazioni, non comportamenti.

Identifica setting a rischio. Ottimo per prevenzione, non per rilevamento.

Accesso iniziale	○
Esecuzione	○
Persistenza	○
Escalation dei privilegi	●
Elusione delle difese	○
Accesso alle credenziali	●
Discovery	○
Movimento laterale	○
Raccolta	○
Command & Control	○
Esfiltrazione	○
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Il CSPM segnala bucket S3 aperti, porte SSH esposte, log disabilitati. È prevention-focused, scansiona condizioni che possono abilitare attacchi, non gli attacchi stessi.

COME GLI ATTACCANTI AGGIRANO

- Sfruttano una misconfigurazione prima che venga corretta.
- Usano token API o OAuth per escalare nei servizi cloud.
- Abusano di ruoli IAM over-privileged che il CSPM segnala ma non monitora real-time.

Il CSPM non offre visibilità di rete.

Non vede attività runtime, abuso di credenziali o movimento laterale. Segnala condizioni, non attacchi.

CWPP: protegge i workload, se distribuito ovunque.

VM, container, serverless, se gli agenti sono presenti.

Accesso iniziale	●
Esecuzione	●
Persistenza	●
Escalation dei privilegi	●
Elusione delle difese	○
Accesso alle credenziali	○
Discovery	●
Movimento laterale	○
Raccolta	●
Command & Control	●
Esfiltrazione	○
Impatto	●

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

I CWPP proteggono le istanze di compute con visibilità runtime sui workload cloud. La copertura dipende dal deployment.

COME GLI ATTACCANTI AGGIRANO

- Si muovono in workload non gestiti o regioni senza agente.
- Usano tool legittimi nel workload (PowerShell, bash) per evitare il rilevamento.
- Operano interamente in SaaS o identità, fuori dalla portata del CWPP.

I CWPP non offrono visibilità di rete.

Ciechi ad abusi SaaS e abuso di IAM cloud.

CNAPP: consolida, ignora il comportamento.

Combina CSPM, CWPP, sempre più CIEM e detection runtime.

Accesso iniziale	●
Esecuzione	●
Persistenza	●
Escalation dei privilegi	●
Elusione delle difese	●
Accesso alle credenziali	●
Discovery	●
Movimento laterale	●
Raccolta	●
Command & Control	●
Esfiltrazione	●
Impatto	●

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

I CNAPP moderni aggiungono detection runtime (CDR) oltre allo scan di posture. Ma il rilevamento runtime resta workload-scoped. Osserva ciò che accade su un workload, non i pivot su identità e rete tra workload.

COME GLI ATTACCANTI AGGIRANO

- Usano identità federata o manipolazione SaaS, non tracciate a fondo dal CNAPP.
- Operano tra workload, evitando il rilevamento se l'est-ovest non è ispezionato.
- Si muovono veloci, prima del prossimo scan di configurazione.

Il CNAPP migliora la visibilità, ma non basta.

Manca ancora il rilevamento di comportamenti d'attacco su rete, identità cloud e SaaS.

CIEM: gestisce diritti, non comportamenti al loro interno.

Categoria distinta dal 2023.

Accesso iniziale	○
Esecuzione	○
Persistenza	○
Escalation dei privilegi	●
Elusione delle difese	○
Accesso alle credenziali	●
Discovery	○
Movimento laterale	○
Raccolta	○
Command & Control	○
Esfiltrazione	○
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Il CIEM analizza i diritti d'identità cloud: chi può fare cosa in AWS, Azure, GCP. Segnala ruoli over-privileged, accessi dormienti, permessi eccessivi.

COME GLI ATTACCANTI AGGIRANO

- Usano diritti a basso rischio sfruttabili in escalation se concatenati.
- Agiscono entro confini approvati in modi che la baseline non ha mai modellato.
- Abusano di ruoli federati e trust cross-account. Il CIEM li mappa, ma non li monitora real-time.

Il CIEM segnala l'over-privilege. Non rileva l'abuso di privilegi legittimi.

Come CSPM e CNAPP, opera al livello di posture. I diritti sono statici; gli attacchi sono comportamenti dinamici dentro quei diritti.

SASE: controlla l'accesso, non ciò che accade dopo.

SWG + ZTNA + CASB + DLP, unificati.

Accesso iniziale	●
Esecuzione	
Persistenza	
Escalation dei privilegi	
Elusione delle difese	
Accesso alle credenziali	
Discovery	
Movimento laterale	●
Raccolta	
Command & Control	●
Esfiltrazione	●
Impatto	

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Il SASE controlla come gli utenti accedono alle app, non rileva ciò che fanno una volta dentro il cloud.

COME GLI ATTACCANTI AGGIRANO

- Si autenticano con credenziali rubate, aggirando i modelli trust.
- Abusano di feature SaaS legittime (regole mailbox, condivisioni) per persistere e rubare.
- Si muovono via percorsi cloud-native (chaining IAM, trust federato).

Il SASE vede i percorsi d'accesso, non i comportamenti d'attacco al loro interno.

Il gap della sicurezza cloud e come Vectra AI lo chiude.

IL GAP CLOUD

I tuoi tool cloud sono forti in prevenzione, deboli in rilevamento.

Mancano:

- Abuso di privilegi SaaS (delega mailbox in M365).
- Backdoor d'identità federata (manipolazione trust Entra ID).
- Traffico est-ovest cloud (tra VPC, container, account).
- Pattern API cross-account, chaining di ruoli IAM.
- Command-and-control cloud-nativo (token AWS STS, ruoli Entra ID).

L'abuso di account validi è stato il 35 % degli incidenti cloud nel 2025. Le intrusioni cloud-conscious sono cresciute del 37 % anno su anno, del 266 % tra gli attori statali.[1]

COSA AGGIUNGE VECTRA AI

- Detection real-time su M365, Entra ID, AWS, Azure, GCP, federazione.
- Vede ciò che la posture manca: chi fa cosa, ora.
- Correlazione comportamentale identità / rete / cloud.

[1] CrowdStrike 2026 Global Threat Report.

VECTRA AI

OCCHIO AI TUOI GAPS

Sicurezza di rete

Quando il traffico sembra normale, ma non lo è.

Email security: ferma lo spam, non l'ingegneria sociale.

Blocca il noto-malevolo. Manca la compromissione post-phishing.

Secure email gateway e filtri anti-phishing bloccano i messaggi noti come malevoli. Ma gli attaccanti usano phishing curato che li aggira.

COME GLI ATTACCANTI AGGIRANO

- Mandano phishing di credenziali via SMS, LinkedIn o email personali, aggirando i filtri aziendali.
- Usano lookalike domain o MFA fatigue per ottenere credenziali.
- Sfruttano la fiducia, non il malware. Nessun allegato o link viene segnalato.

L'email security non rileva la compromissione dopo un phishing riuscito.

È lì che vivono la maggior parte delle violazioni moderne.

Firewall: controllano il bordo, non l'interno.

Restringono al perimetro. Una volta passato un utente trusted, sono ciechi.

Accesso iniziale	●
Esecuzione	
Persistenza	
Escalation dei privilegi	
Elusione delle difese	
Accesso alle credenziali	
Discovery	●
Movimento laterale	
Raccolta	
Command & Control	●
Esfiltrazione	●
Impatto	

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

I firewall tradizionali filtrano per IP, porta, protocollo. I NGFW aggiungono ispezione applicativa e decryption TLS. Una volta passato un utente trusted con credenziali valide, il firewall ha fatto il suo lavoro.

COME GLI ATTACCANTI AGGIRANO

- Usano protocolli consentiti (HTTPS, DNS, RDP) per muoversi sotto traccia.
- Operano su canali cifrati, ispezionabili solo in parte.
- Sfruttano VPN o SSO per autenticarsi come utenti trusted.

I firewall non rilevano C2 nascosto in protocolli approvati, movimento laterale o accessi SaaS con credenziali valide.

IDPS: rileva firme, non furtività.

Il signature matching coglie pattern noti, non ciò che usano gli attaccanti sofisticati.

Accesso iniziale	●
Esecuzione	○
Persistenza	○
Escalation dei privilegi	○
Elusione delle difese	○
Accesso alle credenziali	○
Discovery	●
Movimento laterale	●
Raccolta	○
Command & Control	●
Esfiltrazione	●
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Gli Intrusion Detection and Prevention System cercano pattern noti. Gli attaccanti sofisticati raramente li usano.

COME GLI ATTACCANTI AGGIRANO

- Payload custom o cifrati che eludono le firme.
- Living-off-the-land: tool e porte legittime.
- Rallentano l'attività per stare sotto le soglie.

L'IDPS fallisce contro tecniche inedite e movimento est-ovest cifrato.

NAC: decide chi può connettersi, non cosa fa dopo.

Valida posture e identità al momento della connessione. Perde visibilità una volta dentro.

Accesso iniziale	●
Esecuzione	
Persistenza	
Escalation dei privilegi	
Elusione delle difese	
Accesso alle credenziali	
Discovery	
Movimento laterale	
Raccolta	
Command & Control	
Esfiltrazione	
Impatto	

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

Le soluzioni Network Access Control validano posture e identità prima di concedere l'accesso. Una volta connesso, il NAC perde visibilità.

COME GLI ATTACCANTI AGGIRANO

- Dirottano credenziali o dispositivi trusted senza far scattare il NAC.
- Si muovono tra sistemi trusted, fuori dal NAC.
- Sfruttano dispositivi non gestiti o BYOD che passano i check.

Il NAC non rileva movimento laterale, traffico sospetto o comportamenti post-autenticazione.

SSE: il perimetro moderno, con i vecchi gap.

Security Service Edge: SWG + ZTNA + CASB + FWaaS, cloud-delivered. Sostituto di firewall + VPN legacy.

Accesso iniziale	●
Esecuzione	○
Persistenza	○
Escalation dei privilegi	○
Elusione delle difese	○
Accesso alle credenziali	○
Discovery	○
Movimento laterale	◐
Raccolta	○
Command & Control	◐
Esfiltrazione	◐
Impatto	○

VISIBILITÀ: ◐ Parziale ● Totale ○ Nessuna

Il Security Service Edge consolida secure web gateway, zero-trust network access, CASB e firewall-as-a-service in una piattaforma cloud. L'SSE ha sostituito firewall + VPN in molte aziende ma eredita lo stesso punto cieco di ogni tool perimetrico.

COME GLI ATTACCANTI AGGIRANO

- Si autenticano con credenziali rubate.. ZTNA approva: la credenziale è valida.
- Operano in app sanzionate.. SWG vede la destinazione, non l'attività dentro.
- Pivot via percorsi cloud-native (chaining IAM, OAuth) fuori dal proxy SSE.
- Esfiltrano via SaaS-to-SaaS, invisibile all'SSE.

L'SSE sostituisce il firewall, non lo strato di detection mancante dietro.

Vale lo stesso argomento Vectra-chiude-il-gap, sia per ambienti SSE che firewall legacy.

Il gap della sicurezza di rete e come Vectra AI lo chiude.

IL GAP RETE

I tuoi tool di rete sono prevention-and-control, non detection.

Mancano:

- Movimento laterale tra workload e regioni, cloud e ibrido.
- Command-and-control su protocolli cifrati o trusted.
- Esfiltrazione travestita da traffico business.
- Anomalie est-ovest, accesso privilegiato, uso di credenziali.
- Comportamento post-autenticazione in sessioni SSE.

COSA AGGIUNGE VECTRA AI

- Analisi real-time: on-prem, cloud, SaaS.
- Rileva movimento laterale, escalation, esfiltrazione, (anche cifrato, via metadati).
- Si integra con SIEM e SOAR per alert ad alta fedeltà.
- Si integra nativamente con qualsiasi firewall che supporti l'ingestione di blocklist dinamiche esterne.

VECTRA AI

OCCHIO AI TUOI GAPS

Sicurezza delle identità

Quando i login validi diventano minacce invisibili.

IAM: blocca l'accesso non autorizzato, non quello abusato.

Controlla l'accesso, ma poi dà la fiducia per scontata.

Accesso iniziale	●
Esecuzione	
Persistenza	
Escalation dei privilegi	●
Elusione delle difese	
Accesso alle credenziali	
Discovery	
Movimento laterale	
Raccolta	
Command & Control	
Esfiltrazione	
Impatto	

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

I tool IAM controllano chi può loggarsi, da dove, con quali permessi. Gli IdP moderni aggiungono segnali risk-based (impossible travel, credenziali leaked, dispositivi non familiari) ma operano al momento dell'autenticazione. Una volta aperta una sessione, l'IAM presume fiducia. L'MFA blocca oltre il 99 % degli attacchi all'identità, eppure gli attacchi all'identità sono cresciuti del 32 % nel S1 2025[1]: token rubati, OAuth consentito, device-code, AiTM aggirano l'MFA.

COME GLI ATTACCANTI AGGIRANO

- Rubano credenziali o token di sessione, poi si loggano da utente legittimo.
- Si muovono con account over-permissioned o policy malconfigurate.
- Si autenticano via IdP trusted, federation e SSO inclusi.
- Cookie di sessione (es. ESTSAUTHPERSISTENT) che aggirano l'MFA.

L'IAM applica policy di login. Non sorveglia ciò che le identità fanno dopo.

Il 97 % degli attacchi all'identità sono attacchi via password[1]. L'MFA ferma quello. Niente nell'IAM ferma l'abuso post-autenticazione.

[1] Microsoft Digital Defense Report 2025:

PAM: protegge i privilegiati, se sai chi lo è.

Restringe l'accesso privilegiato. Ma all'attaccante non sempre serve.

Accesso iniziale	○
Esecuzione	○
Persistenza	○
Escalation dei privilegi	●
Elusione delle difese	○
Accesso alle credenziali	◐
Discovery	○
Movimento laterale	○
Raccolta	○
Command & Control	○
Esfiltrazione	○
Impatto	○

VISIBILITÀ: ◐ Parziale ● Totale ○ Nessuna

Le soluzioni PAM restringono come gli utenti accedono ai sistemi critici: vault password, registrazione sessioni, just-in-time. Ma agli attaccanti non sempre serve un account privilegiato per escalare.

COME GLI ATTACCANTI AGGIRANO

- Abusano di account non privilegiati per escalare via permessi SaaS (delega mailbox, scope OAuth).
- Sfruttano trust federato per accedere senza toccare account PAM-controlled.
- Usano shadow admin (ruoli con privilegi effettivi non flaggati come « privilegiati »).

Il PAM non rileva abusi d'identità fuori dai confini di privilegio predefiniti.

UEBA: calcola il rischio, ma non in tempo reale.

Sempre più una feature dentro SIEM/XDR che una categoria a sé.

Accesso iniziale	●
Esecuzione	○
Persistenza	●
Escalation dei privilegi	●
Elusione delle difese	●
Accesso alle credenziali	●
Discovery	●
Movimento laterale	●
Raccolta	○
Command & Control	○
Esfiltrazione	●
Impatto	○

VISIBILITÀ: ● Parziale ● Totale ○ Nessuna

L'UEBA costruisce profili di comportamento normale e assegna risk score quando gli utenti deviano. Dipende da dati completi e spesso reagisce troppo tardi. Gartner non mantiene più un Magic Quadrant UEBA distinto.

COME GLI ATTACCANTI AGGIRANO

- Imitano comportamento normale (stessa location, device, pattern).
- Agiscono lentamente o fuori orario, evitando picchi.
- Sfruttano log incompleti, impedendo all'UEBA la vista d'insieme.

L'UEBA ritarda la detection e non offre visibilità real-time sull'abuso d'identità.

Il gap della sicurezza identità e come Vectra AI lo chiude.

IL GAP IDENTITÀ

La maggior parte dei tool si concentra su access control o risk scoring, non sul comportamento d'attacco. L'ITDR è emerso per osservare ciò che l'IAM non vede.

Non vedono:

- Abuso di credenziali su SaaS e cloud.
- Escalation di privilegi in Entra ID o Exchange Online.
- Abuso di trust tra IdP.
- Movimento laterale identitario senza toccare l'endpoint.

COSA AGGIUNGE VECTRA AI

- AD, Entra ID, M365 / Exchange Online, Azure / AWS, ruoli IAM cloud, identità federata.
- Detection di abusi di privilegi SaaS (delega, OAuth).
- Detection di manipolazione federation (trust, role impersonation).
- Abuso di credenziali in ibrido, anche con MFA passato.

Pressione regolatoria: il rilevamento è la prova.

La compliance è continua, e la compliance continua richiede detection continuo.

Raccoglitori di policy e attestazioni annuali non bastano per una notifica d'incidente in 24 ore. Se lo stack non vede l'attacco, nessun framework di compliance risolve il problema.

NIS2

In vigore da ottobre 2024

Richiede misure tecniche adeguate per il rilevamento e la risposta agli incidenti. Notifica iniziale di incidente significativo entro 24 ore dalla conoscenza, rapporto intermedio entro 72 ore, rapporto finale entro un mese. L'articolo 21(2)(b) richiede esplicitamente capacità di gestione degli incidenti. Vigilanza ACN.

DORA

In vigore da gennaio 2025

Per le entità finanziarie: notifica iniziale entro 4 ore dalla classificazione (e al massimo 24 ore dopo il rilevamento) di un incidente ICT grave. Rapporto intermedio a 72 ore, rapporto finale a un mese. Vigilanza di Banca d'Italia e CONSOB.

PSNC

DPCM 81/2021

I soggetti inclusi nel Perimetro (TLC, energia, finanza, trasporti, sanità, ICT, spazio) devono notificare incidenti significativi al CSIRT Italia / ACN entro 1 ora o 6 ore secondo la categoria. Richiede detection continua e logging tracciabile.

La domanda di compliance è ora una domanda di detection.

Conclusione

Chiudi i gap prima che vengano sfruttati.

Non puoi difendere ciò che non vedi.

Gli attaccanti di oggi non si affidano al malware. I tuoi tool tradizionali non sono fatti per questo.

Gli attaccanti sfruttano credenziali, abusano di misconfigurazioni SaaS, manipolano la fiducia tra identità e si muovono nei workload cloud senza essere visti.

I tool tradizionali non vedono questa attività, non perché siano rotti, ma perché non sono progettati per farlo.

- L'EDR non vede l'abuso d'identità in M365.
- CASB e SASE non vedono il movimento laterale cloud.
- Il SIEM non può generare alert su minacce che gli strumenti a monte non rilevano.

Intanto il tuo SOC resta con troppi alert, poco contesto e nessuna vera visibilità sull'infrastruttura ibrida.

Come Vectra AI completa il tuo stack.

E cosa misurano i clienti che lo distribuiscono. IDC Business Value Study, 2025.

CAPACITÀ DI SICUREZZA	COSA MANCA	COSA AGGIUNGE VECTRA AI
Detection delle minacce endpoint	Cieco a rete e cloud	Detection real-time su tutto il traffico (agentless)
Detection delle minacce identità	Nessuna visibilità post-autenticazione	Rileva abuso di account validi ed escalation
Visibilità sulle minacce cloud	Cieco al comportamento ibrido	Rileva movimento cloud-native, ibrido, SASE, SaaS, IaaS
Detection del movimento laterale	Invisibile in ibrido	Detection real-time del movimento laterale
Riduzione del rumore	Alert fatigue	Chiarezza del segnale via AI, detection ad alta fedeltà

COSA OFFRE VECTRA, IN MODO MISURABILE — IDC 2025

391 %
ROI a 3 anni

6 mesi
di payback

3,4 M$
di beneficio annuo

40 %
di SOC più efficiente

60 %
tempo sugli alert

69,4 %
di violazioni in meno

99,9 %
di perdita di produttività evitata

Fonte: IDC Business Value Study of Vectra AI, aprile 2025

Vectra AI chiude i tuoi gap d'attacco.

Osservabilità. Segnale. Controllo. E risultati concreti, su clienti reali.

Osservabilità

Vectra AI analizza in continuo l'attività di rete per rivelare ogni identità, dispositivo e agente AI in tempo reale, così i team SecOps sanno sempre chi fa cosa nella loro rete.

Segnale

Correlando e contestualizzando l'attività in ambienti ibridi, Vectra AI aiuta i team a prioritizzare il rischio reale, investigare più veloce, fare hunting con sicurezza e fermare gli attacchi prima dell'impatto.

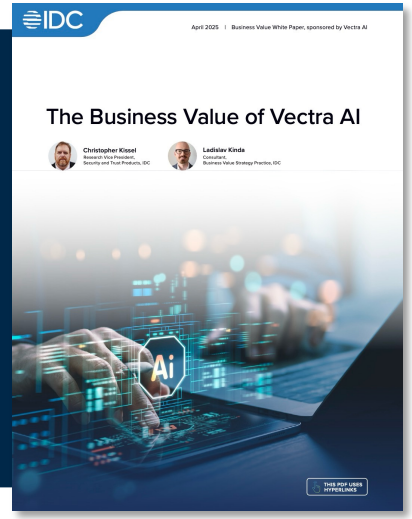
Controllo

Vectra AI mostra chi e cosa è sulla rete, quale attività segnala un attacco e dove l'esposizione cambia, per ridurre il rischio, guadagnare in efficienza e dimostrare compliance.

DA UN'INTERVISTA IDC · GRUPPO COSMETICO INTERNAZIONALE

« Prima di Vectra AI non ricevevamo alcun alert e scoprivamo l'accesso del Red Team solo dai loro report annuali, che mostravano costantemente domain admin e root. Il primo anno con Vectra abbiamo rilevato, espulso e completamente sconfitto il Red Team. Vectra è il mio tool di sicurezza numero uno. »

Lo stesso team SOC funziona con 7 full-time equivalent (FTE). Il loro benchmark dice che ne servirebbero 14.



Self-assessment: quali gap ti espongono ?

Leggi ogni affermazione. Spunta la casella se ti corrisponde. Le caselle spuntate sono i gap che porti.

GAP 1

Niente sembra fuori posto.

- [ ] Vediamo PowerShell, RDP e WMI nei nostri alert EDR, e quasi sempre presumiamo sia attività admin.
- [ ] Non abbiamo una baseline documentata di cosa significhi comportamento admin « normale » nel nostro ambiente.
- [ ] Quando l'EDR segnala un processo « potenzialmente indesiderato », a volte gli alert restano senza review oltre un giorno.
- [ ] Se un attaccante abusasse di binari firmati e facesse living-off-the-land per due settimane, non siamo sicuri di accorgercene.
- [ ] Le nostre regole di detection non distinguono in modo affidabile i task pianificati creati da un attaccante da quelli legittimi.

GAP 2

L'autenticazione riesce.

- [ ] L'MFA è applicato per gli utenti umani, ma siamo meno sicuri su service account e workload identity.
- [ ] Il nostro principale segnale di minaccia identità è il risk score dell'IdP (impossible travel, device non familiare).
- [ ] Non ingeriamo log audit M365, Entra ID o Okta in uno strato di detection oltre l'IdP.
- [ ] Se un token di sessione fosse rubato da un device personale infetto da infostealer e riusato, non abbiamo detection specifica.
- [ ] Quando una credenziale o un fattore MFA viene resettato, niente sorveglia automaticamente il comportamento dell'account per le 24 ore successive.

GAP 3

Il movimento non è visibile.

- [ ] La nostra detection di rete è solo nord-sud, non vediamo traffico est-ovest tra workload.
- [ ] Non rileviamo in modo affidabile movimento laterale SMB o RDP tra segmenti dove la copertura EDR è disomogenea.
- [ ] Le chiamate API del piano di controllo cloud (AWS STS, ruoli Entra ID) non alimentano la detection real-time.
- [ ] Non abbiamo detection per pivot OAuth tra piattaforme SaaS sanzionate.
- [ ] Quando citiamo il « dwell time » nei report SOC, il numero viene da ricostruzione post-incidente, non da misurazione continua.

Come leggere il punteggio: **0–3 spuntate** = copertura significativa. **4–7 spuntate** = il gap ti espone in modo misurabile. **8–11 spuntate** = via d'ingresso principale degli attaccanti. **12+ spuntate** = la detection è incompleta su tutta la progressione d'attacco.

Su Vectra AI

Vectra AI è lo strato di detection di rete e identità per gli attacchi che gli altri tool non sono fatti per vedere. Osserviamo il traffico est-ovest, i comportamenti sul piano dell'identità e l'attività sul piano di controllo cloud, per le tecniche che gli attaccanti usano quando « entrare con la forza » non è il punto d'ingresso, perché sempre più non lo è.

1.700 clienti. Dodici anni di ricerca AI/ML. 39 brevetti. Gartner NDR Leader 2025. Non sostituiamo l'EDR, il SIEM o l'IAM, osserviamo ciò che loro non vedono.

Per maggiori informazioni: www.vectra.ai.

VECTRA AI