VECTRA

EBOOK

Cuidado con tus gaps

Detección fragmentada, visibilidad incompleta

Por Lucie Cardiet · Cyberthreat Research Manager

Por qué escribí esto

Una nota de la autora

Paso mis días observando lo que los atacantes hacen realmente, no lo que los fabricantes dicen, no lo que decían los informes de amenazas del año pasado, no lo que la categoría de productos que todos usamos debería detectar. Lo que hacen realmente, esta semana, contra entornos como el tuyo.

Lo que veo de forma constante: los defensores no pierden por falta de inversión. Pierden porque las inversiones se quedan en una zona de eficacia parcial. Su EDR funciona exactamente como se diseñó; el atacante está en el plano de identidad. Su SIEM ingiere todos los logs; y el ataque solo es visible en la correlación entre logs. Su IAM aprueba cada login conforme a la política; pero la persona del otro lado no es el empleado cuyas credenciales utilizan.

Esta es la segunda edición de lo que escribí en 2025. Novedades: dos campañas adicionales (Volt Typhoon y AWS comprometido por agentes IA en ocho minutos), los resultados medidos por IDC en 2025 con Vectra AI, una sección sobre la presión regulatoria que convierte la detección continua en una cuestión de compliance, y un self-assessment al final.

Lucie Cardiet

La red ha superado a su arquitectura de seguridad.

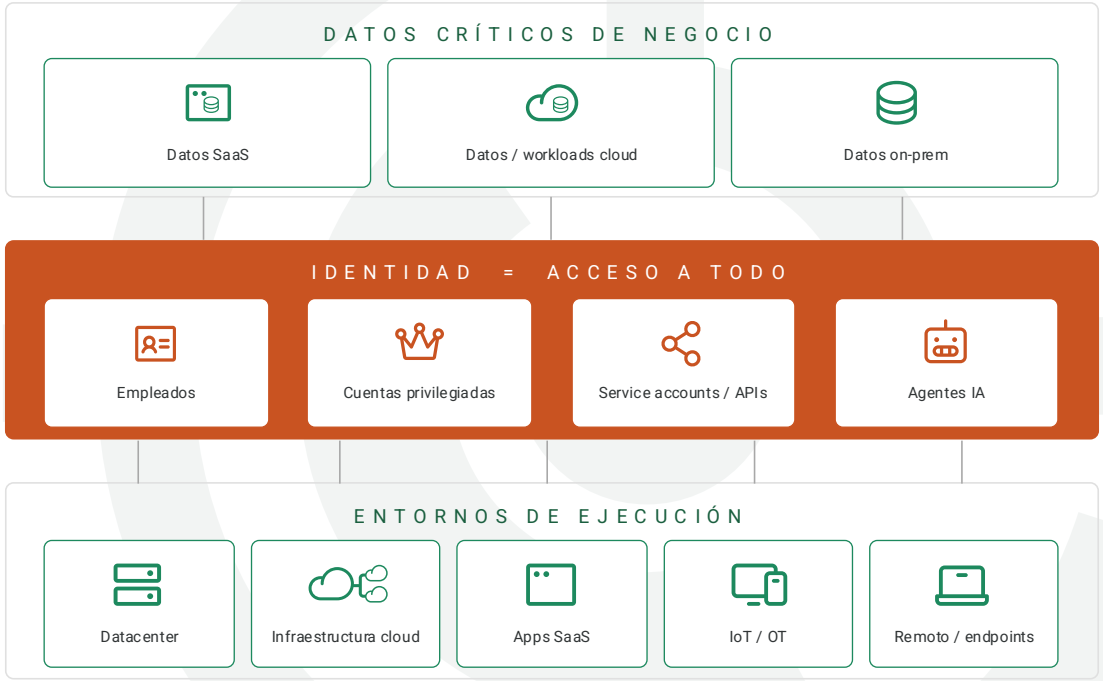
Hoy, las empresas ya no viven detrás de un único perímetro

Los entornos empresariales se extienden por on-prem, varias clouds públicas, decenas de apps SaaS, identity providers, sistemas IoT y OT, servicios de IA y los agentes autónomos sobre ellos. Estos dominios no son independientes, forman un único sistema conectado.

- ✓ Tu EDR vigila los endpoints.
- ✓ Tu IAM aprueba los logins.
- ✓ Tu CSPM lee las configuraciones.
- ✓ Tu SIEM almacena los logs.

Cada uno cumple su función.

Los atacantes, cada vez más asistidos por IA, han pasado los últimos tres años aprendiendo a moverse entre ellos, en los espacios que ningún tool fue diseñado para observar.



La red ha evolucionado. Los atacantes también.

Tu stack es sólido, ¿pero está completo?

A primera vista, has construido un stack de seguridad sólido.

- Has invertido en las mejores tecnologías de seguridad disponibles hoy.
- Tienes protección de endpoints en cada dispositivo.
- Tienes herramientas que monitorizan tu red.
- Tus tools de cloud posture management escanean correctamente las configuraciones.
- Has reforzado la gestión de identidades con IAM o PAM.

Y aun así, los atacantes pasan, y lo hacen.

No porque tus tools estén rotos. Porque cada tool fue diseñado para cubrir su dominio, y los atacantes ahora operan entre ellos.

Los atacantes no rompen tus tools. Los esquivan.

La realidad: los atacantes modernos no luchan contra tu stack. Lo evitan.

Abuso de identidad
Las credenciales comprometidas son el vector de acceso inicial en el 22 % de las breaches.[1] El 88 % de los ataques web básicos involucra credenciales robadas.[1]

Movimiento lateral
Se mueven lateralmente sin disparar alertas. El breakout time eCrime medio – el gap entre acceso inicial y primer pivote lateral – ha bajado a 29 minutos.[2]

Abuso de privilegios cloud
El abuso de cuentas válidas representa ya el 35 % de los incidentes cloud.[2]

Operar entre tools
Se esconden en los huecos entre tools, en espacios que ningún sistema fue diseñado para vigilar.

Explotación del ruido de alertas
Operan por debajo de tus umbrales, sabiendo que el SOC no puede investigarlo todo.

Velocidad cross-domain
MFA bloquea más del 99 % de los ataques de identidad, pero los adversarios entran cada vez más vía tokens robados, apps OAuth consentidas, flujos device-code y proxies adversary-in-the-middle.[3]

Reconocimiento acelerado por IA
Los ataques de adversarios con IA crecieron un 89 % interanual. En 2025, los atacantes explotaron tools GenAI legítimos en más de 90 organizaciones para generar comandos de robo de credenciales.[2]

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

Los mejores tools no equivalen a cobertura completa.

Cada inversión reduce el riesgo en su área, pero deja gaps de visibilidad y detección entre tools. Las cifras de 2026 lo confirman:

- El 82 % de las detecciones de intrusión en 2025 fueron malware-free. Los atacantes operaron con credenciales válidas, flujos de identidad de confianza e integraciones SaaS aprobadas.[1]
- Las breaches que abarcan varios entornos cuestan 5,05 M$ de media, un 25 % más que las breaches solo on-prem.[2]
- El breakout time medio ha bajado a 29 minutos. Récord observado: 27 segundos.[1]

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

El patrón no es nuevo. Es la nueva normalidad.

Este ebook está pensado para ayudarte a mapear estos gaps, mostrarte dónde encaja Vectra AI y cómo Vectra AI los cierra.

Índice

Visión general de la cobertura

La ilustración del Security Gap más tres campañas nombradas que lo explotan.

La ilustración del Security Gap

Tu stack actual: ninguna combinación ofrece detección continua sobre toda la infraestructura híbrida. Cada tool se queda corto en fases clave.

		Acceso inicial	Ejecución	Persistencia	Escalada de privilegios	Evasión de defensas	Acceso a credenciales	Descubrimiento	Movimiento lateral	Recolección	Command & Control	Exfiltración	Impacto
ENDPOINT	EDR	●	●	●	●	●	●	●	●	●	●	●	●
ENDPOINT	EPP	●	●	○	○	○	○	○	○	○	○	○	○
CLOUD	CASB	●	○	○	●	○	●	○	○	●	○	●	○
CLOUD	CNAPP	●	●	●	●	●	●	●	●	●	●	●	●
CLOUD	CSPM	○	○	○	●	○	●	○	○	○	○	○	○
CLOUD	CWPP	●	●	●	●	○	○	●	○	●	●	○	●
CLOUD	SASE	●	○	○	○	○	○	○	●	○	●	●	○
RED	Email	●	○	○	○	○	○	○	○	○	○	○	○
RED	Firewalls	●	○	○	○	○	○	●	○	○	●	●	○
RED	IDPS	●	○	○	○	○	○	●	●	○	●	●	○
RED	NAC	●	○	○	○	○	○	○	○	○	○	○	○
RED	SSE	●	○	○	○	○	○	○	●	○	●	●	○
IDENTIDAD	IAM	●	○	○	●	○	○	○	○	○	○	○	○
IDENTIDAD	PAM	○	○	○	●	○	●	○	○	○	○	○	○
IDENTIDAD	UEBA	●	○	●	●	●	●	●	●	○	○	●	○
Vectra AI Platform		●	●	●	●	●	●	●	●	●	●	●	●

● Visibilidad parcial ● Visibilidad total ○ Sin visibilidad

Tres gaps que tiene cualquier stack hoy.

No son gaps de cobertura. Son gaps de ejecución. Controles que existen pero no detectan.

1. Nada parece fuera de lugar.

Los tools del atacante son tus tools. Remote desktop. PowerShell. Un binario firmado. Living-off-the-land binaries que tus sysadmins usan a las 2 de la madrugada. Cada acción individual parece operación normal.

2. La autenticación tiene éxito.

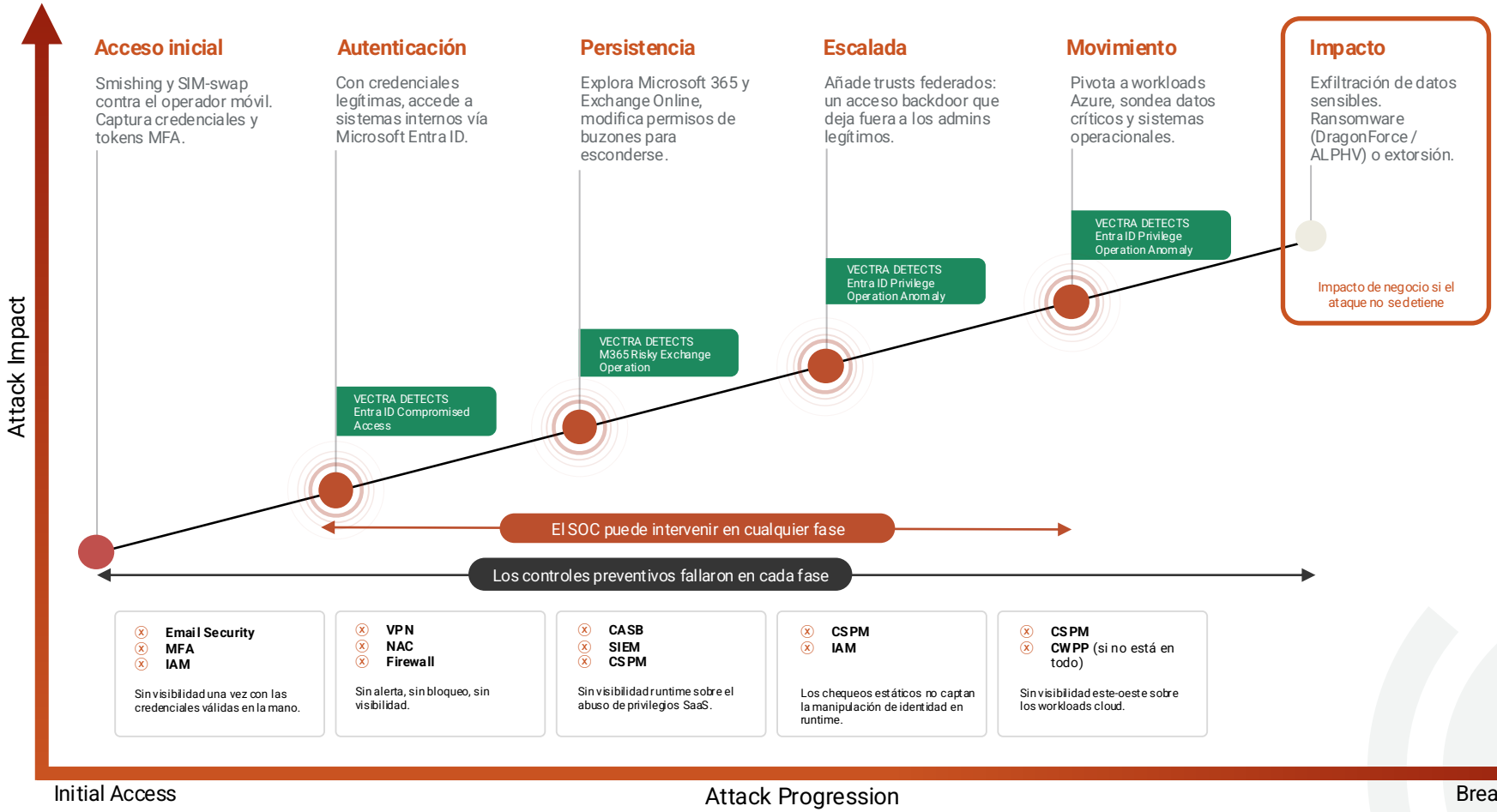
Credenciales válidas, MFA aprobado, el login es real. Solo que no es la persona que tú piensas. Cada chequeo de autenticación dice sí. La verdad: el usuario válido no es realmente el usuario.

3. El movimiento no es visible.

Una vez dentro, el movimiento lateral pasa por integraciones de confianza: SaaS-a-SaaS, identidad federada, tokens OAuth, service accounts. El EDR no lo ve. El CASB no lo ve. El movimiento es invisible por arquitectura, no por sigilo.

Scattered Spider: el playbook del helpdesk

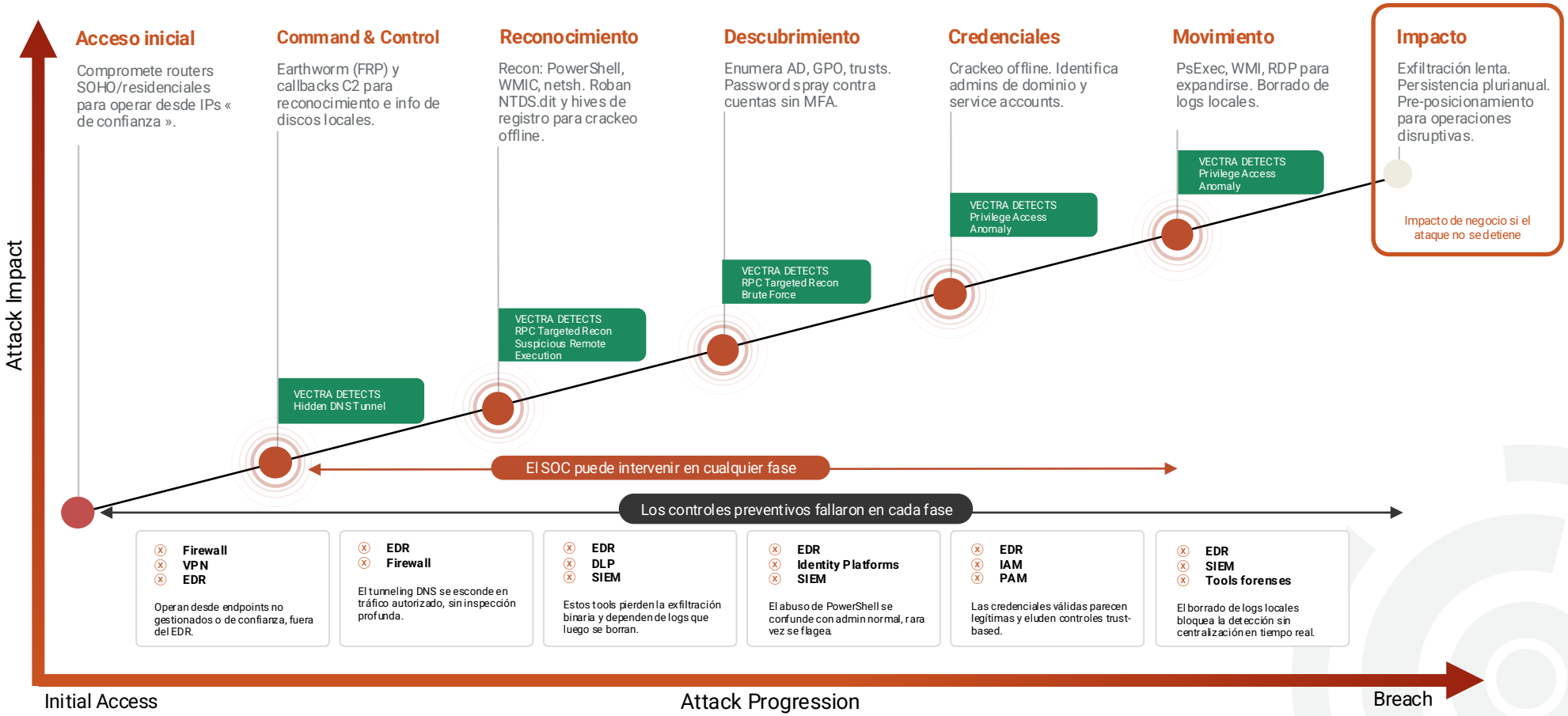
Scattered Spider (UNC3944) ilustra perfectamente la razón por la cual las « credenciales válidas » se han convertido en un problema de detección. El grupo no explotó vulnerabilidades. Llamó al helpdesk.



Fuentes: reporting Mandiant UNC3944 (2023–2024); CISA Advisory AA23-320A sobre TTPs de Scattered Spider.

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

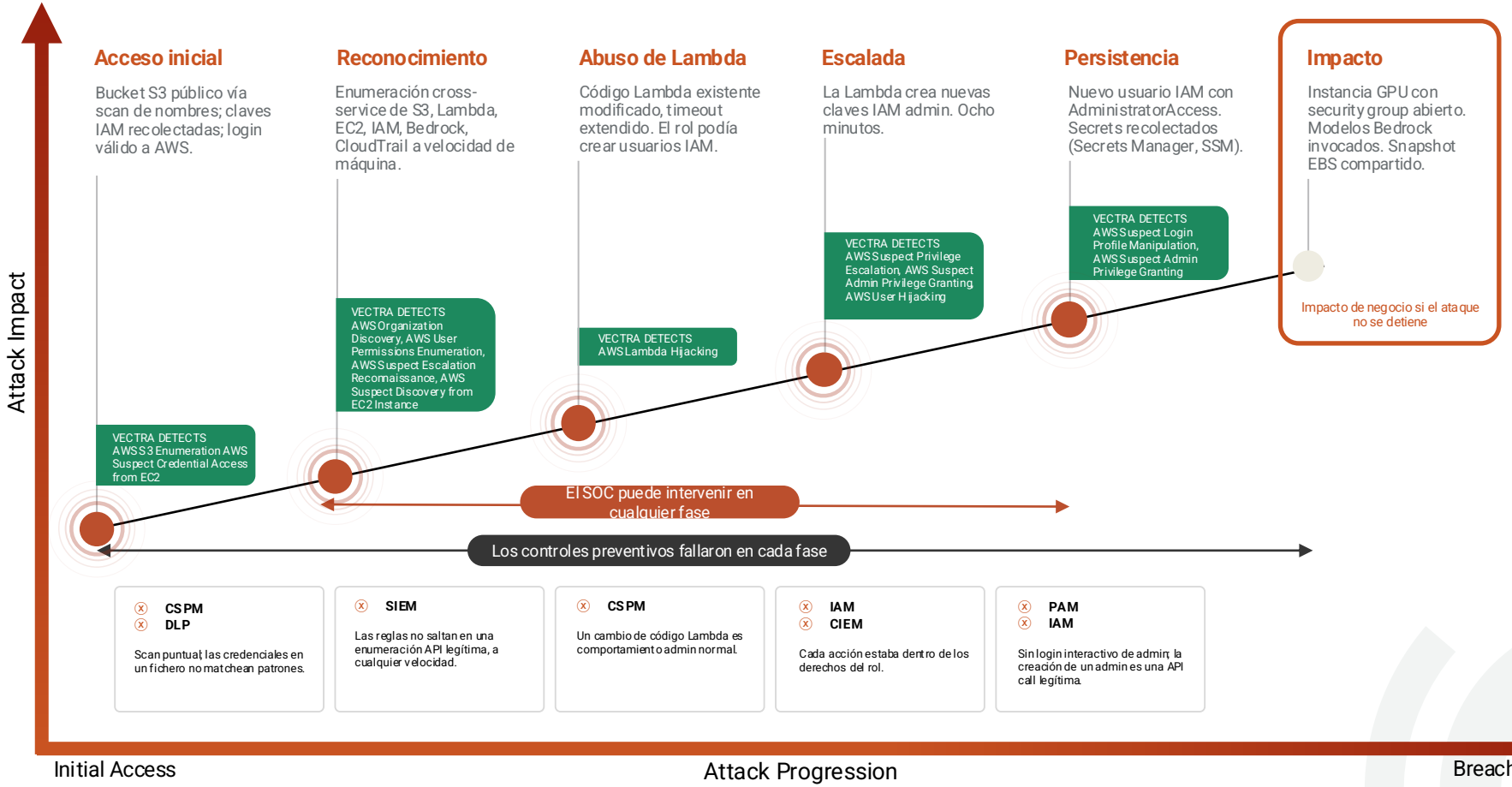
Volt Typhoon es la campaña atribuida a la RPC que enseñó a los defensores estadounidenses qué pinta tiene de verdad « living off the land ». El advisory CISA/NSA/FBI de febrero de 2024 documentó operadores dentro de redes de infraestructura crítica hasta cinco años, usando solo tools nativos de Windows, sin malware que detectar.



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

AWS comprometido por agentes IA en ocho minutos.

Intrusión documentada por Sysdig (2025). Credenciales válidas. Servicios AWS nativos. Recon a velocidad de máquina.



Fuentes: blog de threat research de Sysdig (2025); técnicas MITRE ATLAS de abuso de cuentas válidas y cloud service discovery.

Por qué tu stack actual te deja a ciegas.

Tres atacantes distintos. Tres años distintos. Tres puntos de entrada distintos. Cada ataque parecía legítimo de extremo a extremo en cualquier tool aislado. Solo cruzando red, plano de identidad y plano de control cloud aparece la intención del atacante.

Es fácil pensar que con firewalls, EDR, CASB, CSPM, IAM y SIEM los gaps están cerrados. La realidad: estos tools no fueron diseñados para detectar comportamiento de atacantes en entornos híbridos, y los datos lo demuestran.

82 %

de las detecciones de intrusión en 2025 fueron malware-free.

CrowdStrike 2026 Global Threat Report

32 %

más de ataques basados en identidad en el primer semestre de 2025.

Microsoft Digital Defense Report 2025

241 días

para identificar y contener una breach. 292 cuando hay credenciales robadas.

IBM Cost of a Data Breach Report 2025

En las secciones siguientes desglosamos exactamente dónde falla cada parte de tu stack, y mostramos cómo Vectra AI cierra estos gaps en red, cloud, SaaS e identidad.

VECTRA

Seguridad endpoint

Por qué EDR y EPP no bastan por sí solos.

EDR: profundo en el host, en ningún otro sitio.

Endpoint Detection and Response ofrece telemetría detallada donde está desplegado.

El EDR va más allá de la prevención con telemetría y analytics detallados sobre procesos, cambios de registry y actividad local. Es potente donde está instalado. Realidad 2025: el 82 % de las detecciones de intrusión fueron malware-free.[1] Los atacantes operan con credenciales válidas en sesiones de confianza, donde el EDR no tiene nada que flagear.

CÓMO LOS ATACANTES LO EVADEN

- Evitan el endpoint operando en consolas cloud o apps SaaS.
- Aprovechan los gaps de cobertura. El EDR solo ve hosts donde está instalado.
- Se mueven vía dispositivos no gestionados o BYOD sin agente.
- Usan credenciales válidas para actividad que al EDR le parece « normal ».

El EDR no ve ataques cloud-native, abuso de identidad ni actividad SaaS.

Tres de las cuatro vulnerabilidades más explotadas en 2024 fueron zero-days en productos de seguridad: Palo Alto, Ivanti, Fortinet.[2]

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

EPP: bloquea malware conocido, ciego al resto.

Las Endpoint Protection Platforms impiden la ejecución de amenazas conocidas.

Acceso inicial	●
Ejecución	●
Persistencia	
Escalada de privilegios	
Evasión de defensas	
Acceso a credenciales	
Descubrimiento	
Movimiento lateral	
Recolección	
Command & Control	
Exfiltración	
Impacto	

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

El EPP usa firmas, heurísticas y sandboxing básico. El EPP moderno (NGAV) añade detección comportamental y análisis fileless con ML, pero sigue siendo endpoint-scoped y ciego al movimiento cross-domain.

CÓMO LOS ATACANTES LO EVADEN

- Malware fileless o staging cuidado, bajo el radar comportamental.
- Zero-days o binarios nuevos sin firma.
- PowerShell, WMI, RDP: indistinguibles del admin.

El EPP no detecta living-off-the-land ni ataques por credenciales.

Incluso un EPP moderno es endpoint-scoped. Cloud, identidad, SaaS-a-SaaS son invisibles por diseño.

El gap de seguridad endpoint y cómo Vectra AI lo cierra.

EL GAP ENDPOINT

EDR y EPP son fundamentales, pero solo cubren parte de la kill chain.

No ven:

- Ataques de identidad con credenciales válidas en M365 o Entra ID.
- Abuso de privilegios SaaS fuera del endpoint.
- Movimiento lateral a workloads cloud, BYOD, identidad federada.
- Recon y exfiltración por canales cifrados o no-HTTP.

Incluso en endpoints, el EPP pierde comportamiento sofisticado y el EDR no siempre detecta abuso de cuentas sin malware.

QUÉ APORTA VECTRA AI

- Identity Threat Detection para cuentas comprometidas que abusan de SaaS y cloud.
- SaaS Misuse Detection en M365, Exchange Online, Entra ID.
- Cobertura híbrida: endpoint, cloud, red, identidad.
- Integra con CrowdStrike, Microsoft Defender, SentinelOne y otras plataformas EDR.

Seguridad cloud

El punto ciego del hybrid cloud.

CASB: bloquea apps no sancionadas, ignora abusos activos.

Aplica políticas sobre SaaS. No ve atacantes en sesiones válidas.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	●
Evasión de defensas	○
Acceso a credenciales	●
Descubrimiento	○
Movimiento lateral	○
Recolección	●
Command & Control	○
Exfiltración	●
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los CASB aplican políticas vía API o proxy inline. En modo API (lo habitual), ven la actividad cuasi-tiempo real con minutos de latencia. En cualquier caso, los CASB operan por encima de los planos de red e identidad, ciegos a lo que hacen los atacantes en una sesión válida.

CÓMO LOS ATACANTES LO EVADEN

- Usan credenciales válidas para acceder a SaaS sancionado (M365, Box, Salesforce).
- Aprovechan permisos desde dentro (delegación de buzones).
- Abusan del trust federado para entrar vía SSO.

El CASB no aporta visibilidad a nivel de red.

No siempre detecta abuso de privilegios en directo, manipulación de identidad ni comportamiento insider.

CSPM: encuentra misconfigs, no comportamiento.

Identifica ajustes de riesgo. Bueno para prevención, no para detección.

Acceso inicial	○
Ejecución	○
Persistencia	○
Escalada de privilegios	●
Evasión de defensas	○
Acceso a credenciales	●
Descubrimiento	○
Movimiento lateral	○
Recolección	○
Command & Control	○
Exfiltración	○
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

El CSPM señala buckets S3 abiertos, puertos SSH expuestos, logging desactivado. Es prevention-focused, escanea condiciones que pueden permitir ataques, no los ataques en sí.

CÓMO LOS ATACANTES LO EVADEN

- Aprovechan una misconfig antes de que se corrija.
- Usan tokens API u OAuth para escalar dentro de servicios cloud.
- Abusan de roles IAM sobre-privilegiados que el CSPM señala pero no monitoriza en tiempo real.

El CSPM no aporta visibilidad a nivel de red.

No ve actividad runtime, abuso de credenciales ni movimiento lateral. Señala condiciones, no ataques.

CWPP: protege workloads, si lo despliegas en todos.

VMs, contenedores, serverless, si los agentes están desplegados.

Acceso inicial	●
Ejecución	●
Persistencia	●
Escalada de privilegios	●
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	●
Movimiento lateral	○
Recolección	●
Command & Control	●
Exfiltración	○
Impacto	●

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los CWPP aseguran instancias de compute con visibilidad runtime sobre workloads cloud. La cobertura depende de la consistencia del despliegue.

CÓMO LOS ATACANTES LO EVADEN

- Se mueven a workloads no gestionados o regiones sin agente.
- Usan tools legítimos dentro del workload (PowerShell, bash) para evadir detección.
- Operan exclusivamente en SaaS o identidad, fuera del alcance del CWPP.

Los CWPP no aportan visibilidad a nivel de red.

Ciegos a abuso SaaS y abuso de IAM cloud.

CNAPP: consolida, sigue sin ver comportamiento.

Combina CSPM, CWPP, cada vez más CIEM y detección runtime.

Acceso inicial	●
Ejecución	●
Persistencia	●
Escalada de privilegios	●
Evasión de defensas	●
Acceso a credenciales	●
Descubrimiento	●
Movimiento lateral	●
Recolección	●
Command & Control	●
Exfiltración	●
Impacto	●

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los CNAPP modernos añaden detección runtime (CDR) además del scan de posture. Pero la detección runtime sigue siendo workload-scoped. Ve lo que pasa en un workload, no los pivotes de identidad y red entre workloads.

CÓMO LOS ATACANTES LO EVADEN

- Usan identidad federada o manipulación SaaS, que el CNAPP no rastrea en profundidad.
- Operan entre workloads, eludiendo la detección si no se inspecciona el este-oeste.
- Se mueven rápido, antes del próximo scan de configuración.

El CNAPP mejora la visibilidad, pero no lo suficiente.

Sigue faltando detección de comportamiento de atacantes en red, identidad cloud y SaaS.

CIEM: gestiona derechos, no el comportamiento dentro.

Categoría propia desde 2023.

Acceso inicial	○
Ejecución	○
Persistencia	○
Escalada de privilegios	●
Evasión de defensas	○
Acceso a credenciales	●
Descubrimiento	○
Movimiento lateral	○
Recolección	○
Command & Control	○
Exfiltración	○
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

El CIEM analiza derechos de identidad cloud: quién puede hacer qué en AWS, Azure, GCP. Señala roles sobre-privilegiados, accesos dormidos, permisos excesivos.

CÓMO LOS ATACANTES LO EVADEN

- Usan derechos clasificados como bajo riesgo pero útiles para escalar al encadenarlos.
- Actúan dentro de límites aprobados de formas que la baseline nunca modeló.
- Abusan de roles federados y trust cross-account. El CIEM los mapea, pero no los monitoriza en tiempo real.

El CIEM señala el sobre-privilegio. No detecta el abuso de privilegios legítimos.

Como CSPM y CNAPP, el CIEM opera a nivel posture. Los derechos son estáticos; los ataques son comportamiento dinámico dentro de esos derechos.

SASE: controla el acceso, no lo que pasa después.

SWG + ZTNA + CASB + DLP, unificados.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	○
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	○
Movimiento lateral	●
Recolección	○
Command & Control	●
Exfiltración	●
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

El SASE controla cómo los usuarios acceden a las apps, pero no detecta lo que hacen dentro del cloud una vez con el acceso concedido.

CÓMO LOS ATACANTES LO EVADEN

- Se autentican con credenciales robadas, esquivando los modelos de trust.
- Abusan de funcionalidades SaaS legítimas (reglas de buzón, sharing) para mantenerse y robar.
- Se mueven vía caminos cloud-native (chaining IAM, trust federado).

El SASE ve rutas de acceso, no el comportamiento de atacantes dentro.

El gap de seguridad cloud y cómo Vectra AI lo cierra.

EL GAP CLOUD

Tus tools cloud son fuertes en prevención, débiles en detección.

No ven:

- Abuso de privilegios SaaS (delegación de buzones en M365).
- Backdoors de identidad federada (manipulación de trust en Entra ID).
- Tráfico este-oeste cloud (entre VPCs, contenedores, cuentas).
- Patrones de API cross-account, chaining de roles IAM.
- Command-and-control cloud-native (tokens AWS STS, roles Entra ID).

El abuso de cuentas válidas fue el 35 % de los incidentes cloud en 2025. Las intrusiones cloud-conscious crecieron un 37 % interanual, 266 % entre actores estatales.[1]

QUÉ APORTA VECTRA AI

- Detección en tiempo real sobre M365, Entra ID, AWS, Azure, GCP, federación.
- Ve lo que tus tools de posture no ven: quién hace qué, ahora.
- Correlación comportamental entre identidad, red y cloud.

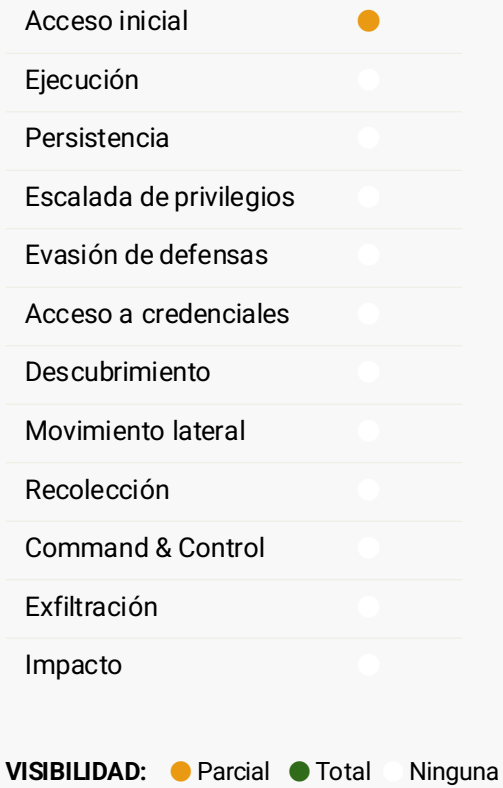
[1] CrowdStrike 2026 Global Threat Report.

Seguridad de red

Cuando el tráfico parece normal, pero no lo es.

Email security: frena el spam, no la ingeniería social.

Bloquea mensajes conocidos como malos. Pierde la compromisión tras un phishing exitoso.



Las pasarelas de correo seguras y los filtros anti-phishing bloquean los conocidos malos. Pero los atacantes usan phishing cuidado e ingeniería social que pasan los filtros.

CÓMO LOS ATACANTES LO EVADEN

- Mandan credential phishing por SMS, LinkedIn o correo personal, saltándose los filtros corporativos.
- Dominios lookalike o MFA fatigue para sacar credenciales.
- Aprovechan la confianza, no el malware. Ningún adjunto o link se flagea.

El email security no detecta la compromisión tras un phishing exitoso.

Y ahí es donde viven la mayoría de las breaches modernas.

Firewalls: controlan el borde, no el interior.

Los tradicionales y NGFW restringen en el perímetro; cuando un usuario de confianza pasa, son ciegos.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	○
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	●
Movimiento lateral	○
Recolección	○
Command & Control	●
Exfiltración	●
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los firewalls tradicionales filtran por IP, puerto, protocolo. Los NGFW añaden inspección a nivel de aplicación y descifrado TLS. En cualquier caso, una vez que un usuario de confianza pasa con credenciales válidas, el firewall ha hecho su trabajo.

CÓMO LOS ATACANTES LO EVADEN

- Usan protocolos permitidos (HTTPS, DNS, RDP) para moverse sin ser detectados.
- Operan sobre canales cifrados que el firewall solo inspecciona en parte.
- Aprovechan VPNs o SSO para autenticarse como usuarios de confianza.

Los firewalls no detectan C2 oculto en protocolos aprobados, movimiento lateral ni acceso SaaS con credenciales válidas.

IDPS: detecta firmas, no sigilo.

El matching de firmas captura patrones conocidos, no lo que usan los atacantes sofisticados.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	○
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	●
Movimiento lateral	●
Recolección	○
Command & Control	●
Exfiltración	●
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los Intrusion Detection and Prevention Systems buscan patrones de ataque conocidos. Los atacantes sofisticados rara vez los usan.

CÓMO LOS ATACANTES LO EVADEN

- Payloads personalizados o cifrados que esquivan firmas.
- Living-off-the-land: tools y puertos legítimos.
- Frenan la actividad para quedar bajo los umbrales.

El IDPS falla frente a técnicas novedosas y movimiento este-oeste cifrado.

NAC: decide quién conecta, no qué hace después.

Valida la posture del dispositivo y la identidad al conectar. Pierde visibilidad dentro.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	○
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	○
Movimiento lateral	○
Recolección	○
Command & Control	○
Exfiltración	○
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Las soluciones Network Access Control validan posture e identidad antes de conceder acceso. Una vez conectado el usuario, el NAC pierde visibilidad.

CÓMO LOS ATACANTES LO EVADEN

- Usan credenciales o dispositivos de confianza para entrar sin disparar el NAC.
- Se mueven entre sistemas de confianza, fuera del NAC.
- Aprovechan dispositivos no gestionados o BYOD que se cuelan en los chequeos de posture.

El NAC no detecta movimiento lateral, tráfico sospechoso ni comportamiento post-autenticación.

SSE: el perímetro moderno, con los mismos gaps.

Security Service Edge: SWG + ZTNA + CASB + FWaaS, entregado desde cloud. El sustituto del firewall + VPN.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	○
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	○
Movimiento lateral	◐
Recolección	○
Command & Control	◐
Exfiltración	◐
Impacto	○

VISIBILIDAD: ◐ Parcial ● Total ○ Ninguna

Security Service Edge consolida secure web gateway, zero-trust network access, CASB y firewall-as-a-service en una plataforma cloud. SSE ha sustituido al stack firewall + VPN en muchas empresas pero hereda el mismo punto ciego que cualquier tool perimetral.

CÓMO LOS ATACANTES LO EVADEN

- Se autentican con credenciales robadas.. ZTNA aprueba: la credencial es válida.
- Operan en apps sancionadas.. El SWG ve el destino, no la actividad dentro de la sesión.
- Pivotan vía caminos cloud-native (chaining IAM, OAuth) fuera del proxy SSE.
- Exfiltran vía SaaS-a-SaaS, invisible al SSE.

El SSE sustituye el firewall, no la capa de detección que falta detrás.

El mismo argumento Vectra-cierra-el-gap aplica a entornos SSE como a entornos con firewall legacy.

El gap de seguridad de red y cómo Vectra AI lo cierra.

EL GAP DE RED

Tus tools de red son prevención y control, no detección.

No ven:

- Movimiento lateral entre workloads y regiones, cloud e híbrido.
- Command-and-control sobre protocolos cifrados o de confianza.
- Exfiltración de datos disfrazada de tráfico de negocio.
- Anomalías comportamentales en tráfico este-oeste, acceso privilegiado y uso de credenciales.
- Comportamiento post-autenticación dentro de sesiones SSE.

QUÉ APORTA VECTRA AI

- Análisis en tiempo real: on-prem, cloud, SaaS.
- Detecta movimiento lateral, escalada y exfiltración, (también cifrado, vía metadatos).
- Integra con SIEM y SOAR para alertas de alta fidelidad.
- Integra con Splunk, Palo Alto, Juniper, Fortinet.

Seguridad de identidad

Cuando los logins válidos se vuelven amenazas invisibles.

IAM: impide el acceso no autorizado, no el abusado.

Pilar del Zero Trust. Asume confianza una vez que el usuario está dentro.

Acceso inicial	●
Ejecución	○
Persistencia	○
Escalada de privilegios	●
Evasión de defensas	○
Acceso a credenciales	○
Descubrimiento	○
Movimiento lateral	○
Recolección	○
Command & Control	○
Exfiltración	○
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

Los tools IAM controlan quién puede entrar, desde dónde y con qué permisos. Los IdP modernos añaden señales basadas en riesgo (viaje imposible, credenciales filtradas, dispositivos desconocidos) pero operan en el momento de la autenticación. Una vez abierta una sesión válida, el IAM asume confianza. MFA bloquea más del 99 % de los ataques de identidad, y sin embargo los ataques de identidad subieron un 32 % en el primer semestre de 2025[1] : tokens robados, OAuth consentido, device-code y AiTM esquivan MFA.

CÓMO LOS ATACANTES LO EVADEN

- Roban credenciales válidas o tokens de sesión y se loguean como usuario legítimo.
- Se mueven lateralmente con cuentas sobre-permisionadas o políticas mal configuradas.
- Se autentican vía IdP de confianza, federación y SSO incluidos.
- Apuntan a cookies de sesión (p. ej. ESTSAUTHPERSISTENT) que esquivan MFA.

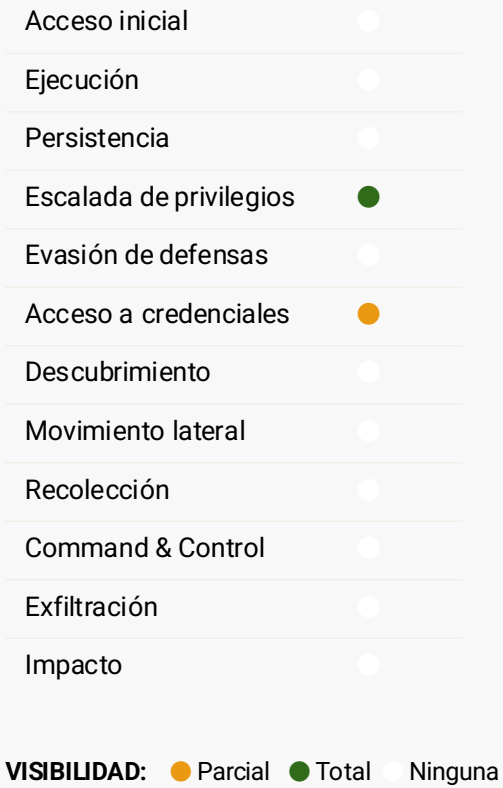
El IAM aplica políticas de login. No vigila lo que pasa después.

El 97 % de los ataques de identidad son ataques por contraseña[1]. MFA detiene el ataque por contraseña. Nada en IAM detiene el abuso post-autenticación.

[1] Microsoft Digital Defense Report 2025:

PAM: protege cuentas privilegiadas, si sabes cuáles son.

Restringe el acceso privilegiado. Pero el atacante no siempre lo necesita.



Las soluciones PAM restringen cómo los usuarios acceden a sistemas críticos: vaults de contraseñas, grabación de sesión, just-in-time. Pero a los atacantes no siempre les hace falta una cuenta privilegiada para escalar.

CÓMO LOS ATACANTES LO EVADEN

- Abusan de cuentas no privilegiadas para escalar vía permisos SaaS (delegación de buzones, scopes OAuth).
- Aprovechan trust federado para acceder sin tocar cuentas controladas por PAM.
- Usan shadow admins (roles con privilegios efectivos no marcados como « privilegiados »).

El PAM no detecta el abuso de identidad fuera de los límites de privilegio predefinidos.

UEBA: calcula riesgo, pero no en tiempo real.

Cada vez más una feature dentro de SIEM/XDR que una categoría aparte.

Acceso inicial	●
Ejecución	○
Persistencia	●
Escalada de privilegios	●
Evasión de defensas	●
Acceso a credenciales	●
Descubrimiento	●
Movimiento lateral	●
Recolección	○
Command & Control	○
Exfiltración	●
Impacto	○

VISIBILIDAD: ● Parcial ● Total ○ Ninguna

El UEBA construye perfiles de comportamiento normal y asigna risk scores cuando los usuarios se desvían. Depende de datos completos y suele tardar demasiado en reaccionar. Gartner ya no mantiene un Magic Quadrant UEBA aparte.

CÓMO LOS ATACANTES LO EVADEN

- Imitan comportamiento normal (mismo lugar, dispositivo, patrón de acceso).
- Actúan despacio o fuera de horario, evitando picos visibles.
- Aprovechan logs incompletos, impidiendo al UEBA ver el conjunto.

El UEBA retrasa la detección y no aporta visibilidad en tiempo real sobre el abuso de identidad.

El gap de seguridad de identidad y cómo Vectra AI lo cierra.

EL GAP DE IDENTIDAD

La mayoría de tools se centra en control de acceso o risk scoring, no en comportamiento de atacante. ITDR ha aparecido para ver lo que el IAM no ve.

No ven:

- Abuso de credenciales en SaaS y cloud.
- Escalada de privilegios en Entra ID o Exchange Online.
- Abuso de relaciones de trust entre IdP.
- Movimiento lateral basado en identidad sin tocar el endpoint.

QUÉ APORTA VECTRA AI

- AD, Entra ID, M365 / Exchange Online, Azure / AWS, roles IAM cloud, identidad federada.
- Detección de abuso de privilegios SaaS (delegación, OAuth).
- Detección de manipulación de federación (trust, role impersonation).
- Abuso de credenciales en híbrido, incluso con MFA superado.

Presión regulatoria: la detección es la prueba.

La compliance es continua, y la compliance continua exige detección continua.

Carpetas de políticas y atestaciones anuales no bastan para una notificación de incidente en 24 horas. Si tu stack no ve el ataque, ningún marco de compliance arregla el problema.

NIS2 (UE)

En vigor desde octubre de 2024

Exige medidas técnicas adecuadas para detección y respuesta. Obliga a notificar incidentes significativos en 24 horas. Artículo 21(2)(b): capacidad explícita de gestión de incidentes.

DORA (UE financiero)

En vigor desde enero de 2025

El capítulo II exige resiliencia operativa. Las ventanas de notificación de incidentes TIC son cortas. Se espera prueba continua de que la detección funciona, no una auditoría puntual.

SEC Cyber Disclosure

En vigor desde diciembre de 2023

Las cotizadas deben divulgar incidentes ciber materiales en cuatro días hábiles tras determinar la materialidad. Exige entender qué hicieron los atacantes (es decir, detección que ve el comportamiento).

La pregunta de la compliance es ahora una pregunta de detección.

Conclusión

Cierra el gap antes de que lo exploten.

No puedes defender lo que no ves.

Los atacantes de hoy no se apoyan en malware. Tus tools tradicionales no se diseñaron para esto.

Los atacantes explotan credenciales, abusan de misconfigs SaaS, manipulan la confianza de identidad y se mueven por workloads cloud sin ser vistos.

Los tools tradicionales no ven esta actividad, no porque estén rotos, sino porque no se diseñaron para esto.

- El EDR no ve el abuso de identidad en M365.
- CASB y SASE no ven el movimiento lateral cloud.
- El SIEM no puede alertar sobre lo que los tools de aguas arriba no ven.

Mientras tanto, tu SOC se queda con demasiadas alertas, poco contexto y ninguna visibilidad real sobre la infraestructura híbrida.

Cómo Vectra AI completa tu stack.

Y lo que miden los clientes que lo despliegan. IDC Business Value Study, 2025.

CAPACIDAD DE SEGURIDAD	QUÉ FALTA	QUÉ APORTA VECTRA AI
Detección de amenazas endpoint	Ciega a red y cloud	Detección en tiempo real sobre todo el tráfico (sin agente)
Detección de amenazas de identidad	Sin visibilidad post-autenticación	Detecta abuso de cuentas válidas y escalada
Visibilidad de amenazas cloud	Ciega al comportamiento híbrido	Detecta movimiento cloud-native, híbrido, SASE, SaaS, IaaS
Detección de movimiento lateral	Invisible en híbrido	Detección en tiempo real del movimiento lateral
Reducción de ruido	Fatiga de alertas	Claridad de señal con IA, detecciones de alta fidelidad

LO QUE VECTRA APORTA, MEDIBLE — IDC 2025

391 %
ROI a 3 años

6 meses
de payback

3,4 M$
de beneficio anual

40 %
de SOC más eficiente

60 %
menos tiempo en alertas

69,4 %
menos breaches

99,9 %
pérdida de productividad evitada

Fuente: IDC Business Value Study of Vectra AI, abril 2025

Vectra AI cierra tus gaps de ataque.

Observabilidad. Señal. Control. Y resultados reales de clientes reales.

Observabilidad

Vectra AI analiza la actividad de red de forma continua para revelar cada identidad, dispositivo y agente IA en tiempo real, así los equipos SecOps siempre saben quién hace qué en su red.

Señal

Correlacionando y contextualizando la actividad en entornos híbridos, Vectra AI ayuda a los equipos a priorizar el riesgo real, investigar más rápido, hacer threat hunting con seguridad y detener ataques antes del impacto.

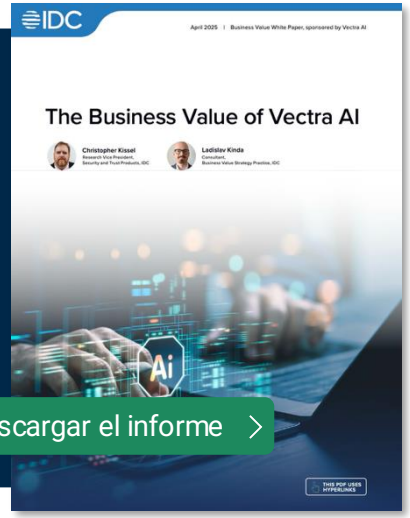
Control

Vectra AI muestra quién y qué hay en tu red, qué actividad indica un ataque y dónde cambia la exposición, para que reduzcas riesgo, ganes en eficiencia y demuestres compliance.

DE UNA ENTREVISTA IDC · GRUPO COSMÉTICO GLOBAL

« Antes de Vectra AI no recibíamos alertas y nos enterábamos del acceso del Red Team solo por sus informes anuales, que mostraban siempre acceso domain admin y root. El primer año con Vectra detectamos, expulsamos y derrotamos completamente al Red Team. Vectra es mi tool de seguridad número uno. »

El mismo equipo SOC funciona con 7 equivalentes a tiempo completo (FTEs). Su benchmark dice que necesitan 14.



Descargar el informe

Self-assessment: ¿qué gaps te exponen?

Lee cada afirmación. Marca la casilla si te suena. Las casillas marcadas son los gaps que cargas.

GAP 1

Nada parece fuera de lugar.

- [ ] Vemos PowerShell, RDP y WMI en nuestras alertas EDR, y la mayoría del tiempo asumimos que es actividad admin.
- [ ] No tenemos una baseline documentada de cómo se ve el comportamiento admin « normal » en nuestro entorno.
- [ ] Cuando el EDR flagea un proceso « potencialmente no deseado », las alertas a veces quedan sin revisar más de un día.
- [ ] Si un atacante abusara de binarios firmados e hiciera living-off-the-land dos semanas, no estamos seguros de detectarlo.
- [ ] Nuestras reglas de detección no distinguen de forma fiable las scheduled tasks creadas por un atacante de las legítimas.

GAP 2

La autenticación tiene éxito.

- [ ] MFA está aplicado a usuarios humanos, pero estamos menos seguros de service accounts y workload identities.
- [ ] Nuestra señal principal de amenaza de identidad es el risk score del IdP (viaje imposible, dispositivo desconocido).
- [ ] No ingestamos audit logs de M365, Entra ID u Okta en una capa de detección más allá del IdP.
- [ ] Si robaran un session token de un dispositivo personal con infostealer y lo reutilizaran, no tenemos detección específica.
- [ ] Cuando se resetea una credencial o factor MFA, nada vigila automáticamente el comportamiento de la cuenta las siguientes 24 horas.

GAP 3

El movimiento no es visible.

- [ ] Nuestra detección de red es solo norte-sur, no vemos tráfico este-oeste entre workloads.
- [ ] No detectamos de forma fiable movimiento lateral SMB o RDP entre segmentos donde la cobertura EDR es desigual.
- [ ] Las API calls del plano de control cloud (AWS STS assume-role, cambios de roles Entra ID) no alimentan la detección en tiempo real.
- [ ] No tenemos detección para pivotes de apps OAuth entre plataformas SaaS sancionadas.
- [ ] Cuando citamos « dwell time » en informes SOC, la cifra viene de reconstrucción post-incidente, no de medición continua.

Cómo leer tu puntuación: 0–3 marcadas = cobertura significativa. 4–7 marcadas = el gap te expone de forma medible. 8–11 marcadas = ruta principal de los atacantes hacia tu entorno. 12+ marcadas = la detección es incompleta en toda la progresión del ataque.

Sobre Vectra AI

La plataforma Vectra AI protege a las empresas modernas al detectar y detener ataques a través de red, identidad y cloud como una única superficie de ataque unificada. Combina la gestión de la exposición a amenazas, la detección y respuesta impulsadas por IA, y la mejora de la postura de seguridad para reducir el riesgo antes de que comiencen los ataques y detener las amenazas en curso. Los equipos de seguridad obtienen una señal clara, una respuesta más rápida y mejoras medibles en la resiliencia.

Más información en www.vectra.ai.

VECTRA