EBOOK

Mind Your Attack Gaps

Across Identity, Network, Cloud, and Endpoint Security

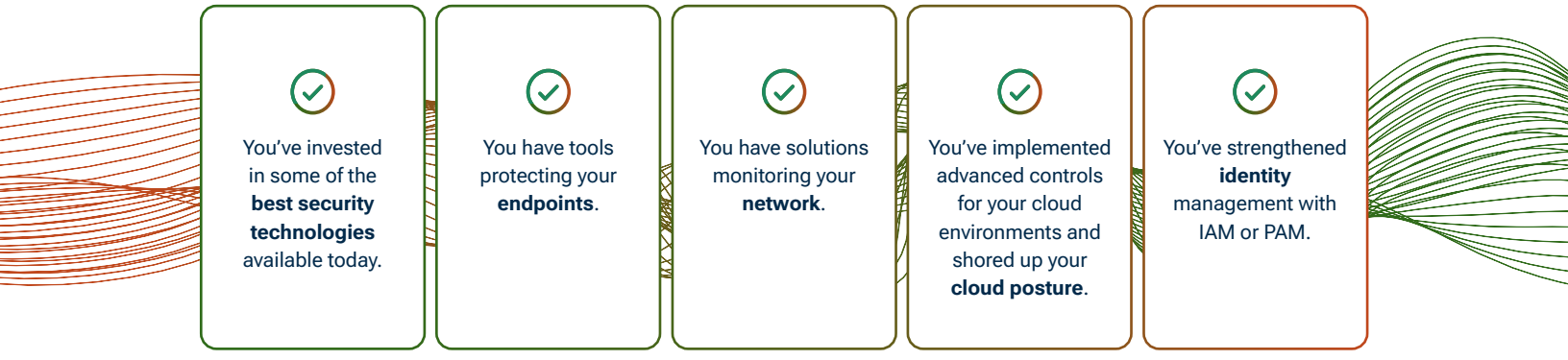
VECTRA®

Today's enterprise networks are no longer confined to a single perimeter.

They span on-prem infrastructure, public cloud environments, SaaS applications, and identity providers—interconnected, always-on, and constantly evolving.

But as the network has evolved, so have the attackers.

Your Stack Is Strong—But Is It Complete?



You've invested in some of the **best security technologies** available today.

You have tools protecting your **endpoints**.

You have solutions monitoring your **network**.

You've implemented advanced controls for your cloud environments and shored up your **cloud posture**.

You've strengthened **identity** management with IAM or PAM.

By all appearances, you've built a strong **security stack**.

And yet, modern attackers can and are still getting through.

The reality is that attackers **aren't breaking your tools and controls—they're bypassing them.**

They're leveraging **stolen identities** to log in undetected.

They're **moving laterally across your network** without triggering alerts.

They're **abusing cloud privileges** you've already granted.

They're hiding in the **gaps between your tools**—knowing that most security solutions operate in silos, each focusing on a specific domain.

They're buried in your **alert noise**, knowing your analysts won't have time to investigate every anomaly.

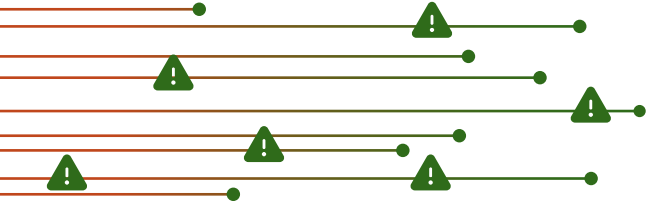
They're moving **fast across domains**, from endpoint to cloud to identity, faster than your tools can correlate.

They're already using your **GenAI tools** to understand your environment, automate reconnaissance, and speed-up decision-making.

Best-in-class tools don't equal complete coverage.

While your investments reduce risk in their respective areas, they leave gaps in visibility and detection between your tools. No wonder 40% of successful breaches were attacks that involved multiple domains*.

* IBM 2024 Cost of a Data Breach



Gaps that attackers exploit.

This ebook is designed to help you map those gaps—and show you where Vectra AI fits and how **Vectra AI closes your gaps.**

Table of Contents

Coverage Overview

VISIBILITY: Partial Full None

Security Gap illustration

		Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
ENDPOINT	**EDR**	●	●	●	●	●	●	●	●	○	●	○	●
ENDPOINT	**EPP**	●	●	○	○	○	○	○	○	○	○	○	○
CLOUD	**CASB**	●	○	○	●	○	●	○	○	●	○	●	○
CLOUD	**CNAPP**	●	●	●	●	●	●	●	●	●	●	●	●
CLOUD	**CSPM**	●	○	○	●	○	●	○	○	○	○	○	○
CLOUD	**CWPP**	●	●	●	●	○	○	○	○	○	●	○	●
CLOUD	**SASE**	●	○	○	○	○	○	○	●	○	●	●	○
NETWORK	**Email Security**	●	○	○	○	○	○	○	○	○	○	○	○
NETWORK	**Firewalls**	●	○	○	○	○	○	●	●	○	●	●	○
NETWORK	**IDPS**	●	○	○	○	○	○	●	○	○	●	●	○
NETWORK	**NAC**	●	○	○	○	○	○	○	○	○	○	○	○
IDENTITY	**IAM**	●	○	○	●	○	○	○	○	○	○	○	○
IDENTITY	**PAM**	○	○	○	●	○	●	○	○	○	○	○	○
IDENTITY	**UEBA**	●	○	○	●	○	●	●	●	○	○	●	○

You've already invested in the standard stack—firewalls, EDR, CASB, and more. But as this matrix makes clear, no combination of these tools provides continuous detection across your entire hybrid infrastructure. Each solution stops short at key stages—leaving dangerous blind spots in cloud control planes, SaaS identities, and east-west network traffic.

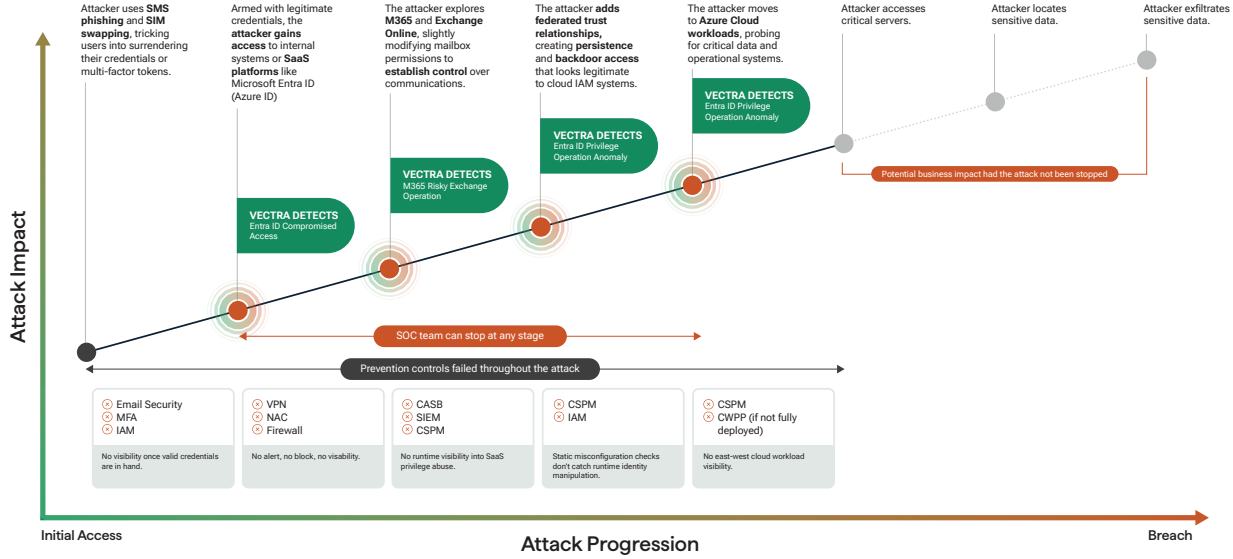
This is your Security Gap.

It's the space attackers exploit to bypass your defenses, escalate privileges, and exfiltrate data—unseen by your existing tools.

Anatomy of a Modern Hybrid Attack

Scattered Spider is one of the most notorious adversaries targeting hybrid environments—using a combination of social engineering, identity abuse, and cloud exploitation to achieve their objectives. Let's walk through a real-world scenario inspired by their tactics to illustrate how traditional security stacks fail—and where Vectra AI fills the gap.

Scattered Spider exploited hybrid visibility gaps that your current stack was never designed to cover. Vectra AI closes these gaps by providing unified detection across network, cloud, SaaS, and identity—enabling your SOC to detect and stop attackers before breach impact.



Why Your Existing Stack Leaves You Blind: Breaking Down the Gaps

It's easy to assume that with your investment in firewalls, EDR, CASB, and CSPM, you've closed the gaps. But the truth is, these tools weren't designed to detect attacker behavior across hybrid environments. They leave blind spots in four critical areas—the same areas that sophisticated attackers like Scattered Spider exploit every day.

In this section, we'll break down exactly where each part of your stack falls short and show you how **Vectra AI closes these gaps across Network, Cloud, SaaS, and Identity.**

Endpoint Security

The Endpoint Visibility Illusion: Why EDR and EPP Are Not Enough

Endpoints are the **most targeted part of your infrastructure**—they're where users interact with cloud apps, where credentials live, and where malware often begins. You've likely deployed **Endpoint Detection and Response (EDR)** and **Endpoint Protection Platforms (EPP)** to cover this surface. That's a strong start—but if you think that's enough to stop modern attackers, think again.

EDR and EPP provide **great visibility into what happens on the device**—but attackers are no longer limited to devices. They exploit **identity, cloud workloads, SaaS platforms, and east-west movement**, where your endpoint agents don't reach.

EDR – Deep on the Host, But Nowhere Else

Endpoint Detection and Response goes further, offering **detailed telemetry and analytics** for processes, registry changes, and local activity. It's powerful—when and where it's deployed.

HOW ATTACKERS BYPASS EDR:

Avoid the endpoint entirely by operating in **cloud consoles or SaaS apps**. (e.g., mailbox rule abuse, identity federation manipulation)

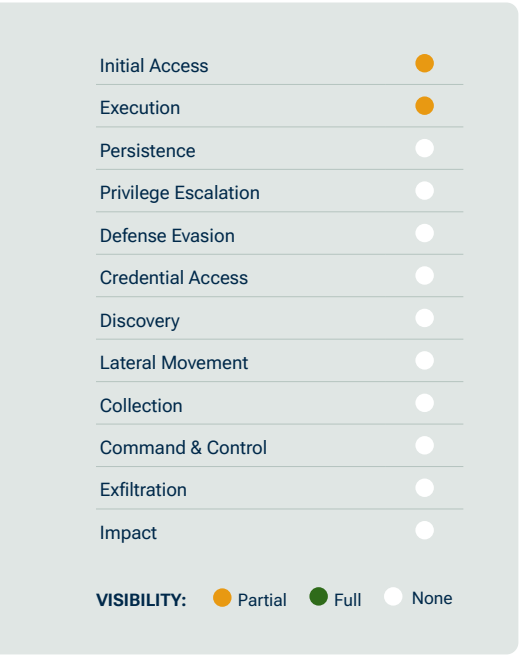
Exploit coverage gaps—EDR only sees hosts where it's installed.

Move through unmanaged or bring-your-own (BYOD) devices that don't run an agent.

Use valid credentials to perform malicious activity that appears "normal" to EDR.

EDR has no visibility into cloud-native attacks, identity abuse, or SaaS activity.

EPP – Blocks Known Malware, Blind to Everything Else



Endpoint Protection Platforms are built to **prevent execution** of known threats—primarily through **signatures, heuristics,** and **basic sandboxing.**

HOW ATTACKERS BYPASS EPP:

Use fileless malware that never touches disk.

Exploit zero-days or newly crafted binaries that don't match existing signatures.

Operate through legitimate tools (PowerShell, WMI, RDP) that EPP can't flag.

EPP can't detect living-off-the-land tactics or credential-based attacks.

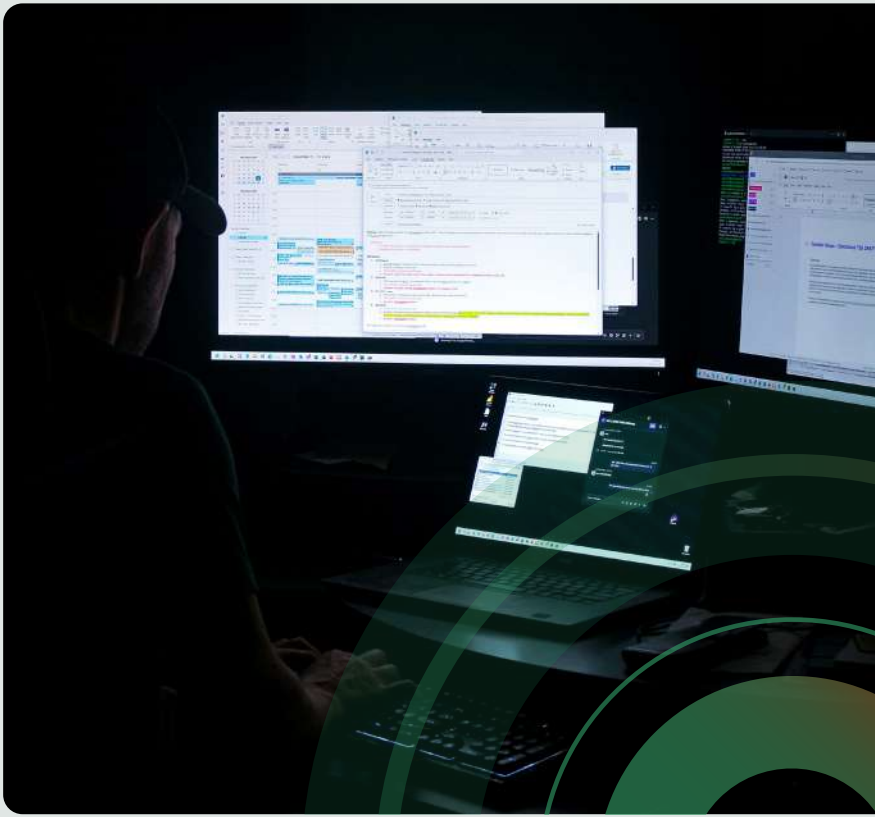
The Endpoint Security Gap

EDR and EPP are **foundational**, but they only cover part of the kill chain—**what happens on the endpoint itself**.

THEY MISS:

1. **Identity-based attacks** that use valid credentials in Microsoft 365 or Entra ID.
2. **SaaS privilege abuse** that doesn't touch the endpoint (e.g., mailbox delegation, OAuth abuse).
3. **Lateral movement across cloud workloads**, unmanaged devices, or federated identity systems.
4. **Network-based reconnaissance and exfiltration**, especially over encrypted or non-HTTP channels.

Even on endpoints, **EPP often misses sophisticated behaviors**, and **EDR doesn't always detect account misuse** if no malware is involved.



How Vectra AI Fills the Endpoint Gap

Vectra AI doesn't replace EDR—it **completes** it by adding **behavioral detection across everything EDR can't see**:

- **Identity Threat Detection** for compromised accounts abusing SaaS and cloud services.
- **SaaS Misuse Detection** in Microsoft 365, Exchange Online, and Entra ID—**even when no malware is involved**.
- **Hybrid Coverage** that extends from endpoints to cloud, network, and identity—**so attackers can't hide between your tools**.
- Vectra AI integrates with: Crowdstrike, Microsoft Defender, SentinelOne, VMware, and more.

Cloud Security

The Cloud Control Plane Blind Spot: Why Cloud Security Tools Still Leave You Exposed

Cloud security tools promise complete protection for your expanding attack surface—but the reality is, most were built for **compliance, configuration, and policy enforcement**, not for **detecting attacker behavior in real time**.

If you're relying on CASB, CSPM, CWPP, CNAPP, or SASE to protect your cloud, **you're missing the threats that live between controls**—especially those using **valid credentials, federated trust, or SaaS privilege abuse**.

CASB – Blocks Unsanctioned Apps, But Misses Active Abuse

Cloud Access Security Brokers (CASBs) are designed to enforce policies across SaaS platforms—monitoring for **unsanctioned apps, DLP violations**, or **compliance gaps**. But they rely on APIs and **can't see what attackers are doing in real time**.

HOW ATTACKERS BYPASS CASB:

Use valid credentials to access sanctioned SaaS apps like M365, Box, or Salesforce.

Exploit permissions from inside the environment (e.g., delegate access to mailboxes).

Abuse federated identity trust to log in through trusted SSO pathways.

CASB provides **no network-layer visibility** and **doesn't always detect live privilege abuse,** identity manipulation, or insider-style behaviors.

CSPM – Finds Misconfigurations, Not Malicious Behavior

Cloud Security Posture Management (CSPM) identifies **risky settings** in your cloud environment—like open S3 buckets, exposed SSH ports, or disabled logging. It's great for **prevention**, not **detection**.

HOW ATTACKERS BYPASS CSPM:

Exploit a misconfiguration before it's remediated.

Use API tokens or OAuth access to escalate inside cloud services.

Abuse over-privileged IAM roles that CSPM may flag but not monitor in real time.

CSPM provides **no network-layer visibility** and **doesn't see runtime activity,** credential misuse, or lateral movement.

CWPP – Protects Workloads, If You Deploy It Everywhere

Cloud Workload Protection Platforms (CWPPs) secure compute instances—VMs, containers, and serverless workloads—**if** agents are deployed. They offer visibility into **runtime behavior** on cloud workloads, but their coverage depends on deployment consistency.

HOW ATTACKERS BYPASS CWPP:

Move into unmanaged workloads or regions where agents aren't installed.

Use legitimate tools within a workload (PowerShell, bash scripts) to avoid detection.

Operate entirely in SaaS or identity layers, where CWPP has no reach.

CWPPs provide **no network-layer visibility** and are blind to **SaaS abuse** and **cloud IAM misuse.**

CNAPP – Consolidates Controls, Still Misses Behavior

Cloud-Native Application Protection Platforms (CNAPPs) combine CSPM and CWPP features—offering **config scanning + workload visibility.** But CNAPPs still focus more on **security posture** than on **real-time attacker detection.**

HOW ATTACKERS BYPASS CNAPP:

Use federated identity or SaaS manipulation, which CNAPP doesn't track deeply.

Operate between workloads, avoiding detection if east-west traffic isn't inspected.

Move quickly before configuration scans run again.

CNAPP improves visibility but still **lacks attacker behavior detection in network, cloud identity, and SaaS layers.**

SASE – Controls Access, But Not What Happens After

Secure Access Service Edge (SASE) combines **SWG, ZTNA, CASB, and DLP** into a unified platform. It controls **how users access apps**, but doesn't detect **what those users do inside the cloud once access is granted**.

HOW ATTACKERS BYPASS SASE:

Authenticate using stolen credentials, bypassing trust models and access rules.

Abuse legitimate SaaS features (e.g., mailbox rules, data sharing) to maintain access and steal data.

Move laterally via cloud-native connections (e.g., IAM role chaining, federated trust).

SASE sees access paths—not the attacker behaviors hidden within them.

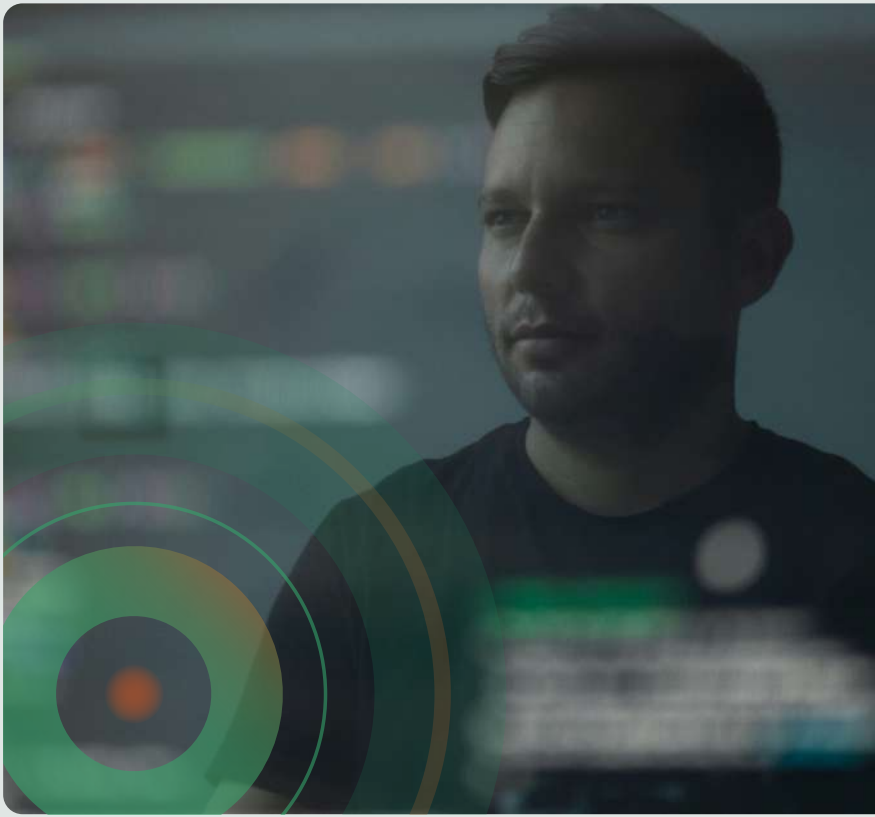
The Cloud Security Gap

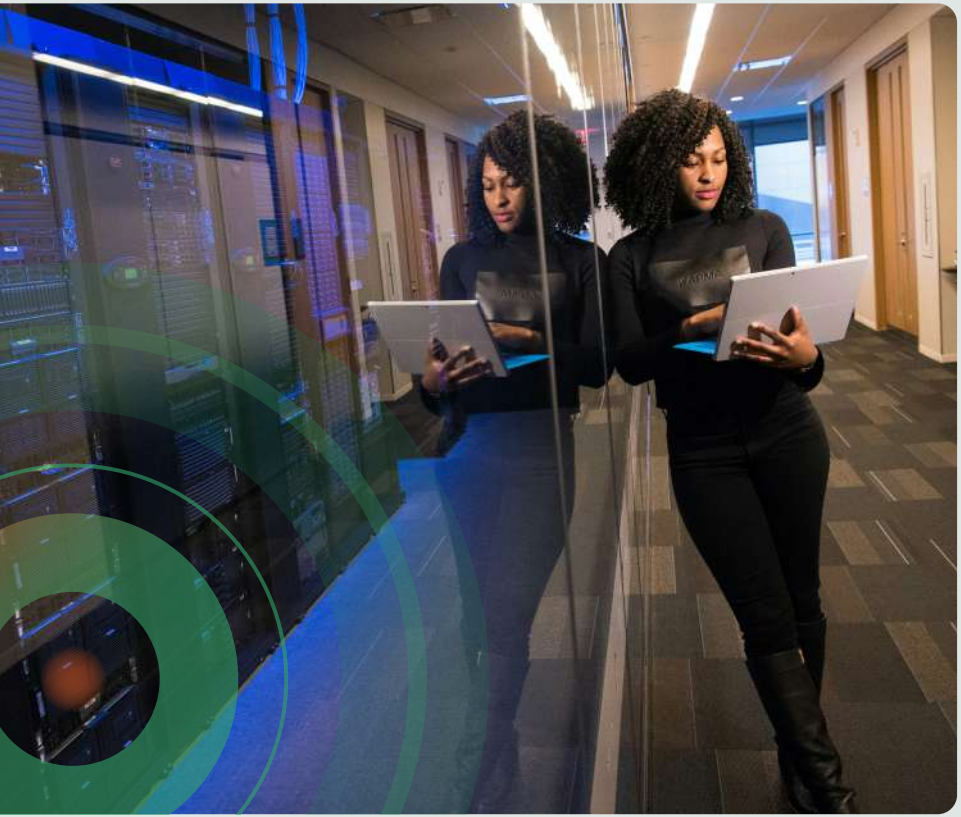
Your cloud security tools are **strong on prevention, weak on detection.**

They help enforce policy, scan configurations, and limit exposure—**but they don't see attackers** once inside.

THEY MISS:

1. **SaaS privilege abuse** (e.g., mailbox delegation in M365).
2. **Federated identity backdoors** (e.g., Entra ID trust manipulation).
3. **East-west traffic inside cloud** (e.g., lateral movement between workloads).
4. **Cloud-native command and control** (e.g., abuse of AWS STS tokens or Azure AD roles).





How Vectra AI Fills the Cloud Security Gap

Vectra AI provides real-time detection of attacker behavior in cloud, SaaS, and identity systems—across:

- Microsoft 365
- Microsoft Entra ID (Azure AD)
- AWS, Azure, Google Cloud workloads
- Hybrid and federated identity infrastructure

It sees **what your posture tools miss**:

Who is doing what, right now, and whether it's normal.

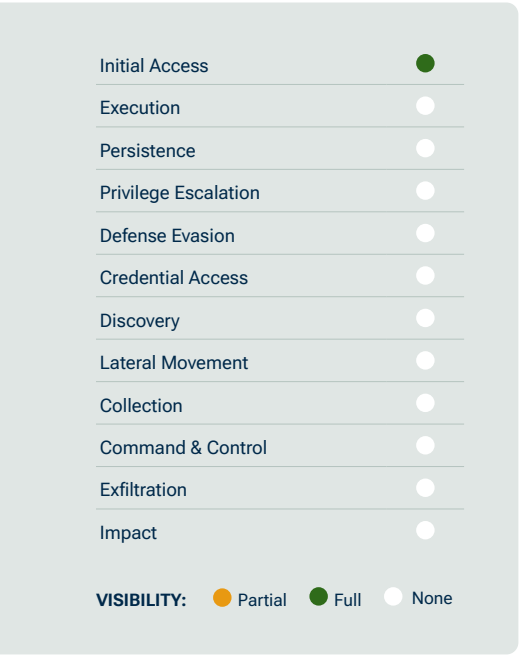
Network Security

The Network Blind Spot: When Traffic Looks Normal but Isn't

You've likely built your network defenses around **Email Security, Firewalls, NAC,** and **IDPS**. These tools are all critical—but they were **designed to control and respond to known threats**, not to detect **the unknown, the stealthy, or the credentialed attacker moving inside your network**.

In today's hybrid environments, attackers bypass your network stack by simply **blending in with trusted users, protocols, and encrypted traffic**—leaving your SOC blind until damage is already done.

Email Security – Stops Spam, Not Social Engineering



Email is often the **first entry point**. Tools like secure email gateways and phishing filters block **known bad messages** and attachments. But attackers now rely on **well-crafted phishing and social engineering** that evades traditional detection.

HOW ATTACKERS BYPASS EMAIL SECURITY:

Send credential phishing via SMS, LinkedIn, or personal email— completely bypassing the corporate email filter.

Use lookalike domains or MFA fatigue to trick users into surrendering credentials.

Exploit trust, not malware—so no attachment or link is flagged.

Email security tools can't detect account compromise that occurs after a successful phish.

Firewalls – Control the Edge, Not What Happens Inside

Firewalls restrict traffic based on **IP, port, protocol, and policy**. They're your gatekeepers—but once access is granted, they go blind.

HOW ATTACKERS BYPASS FIREWALLS:

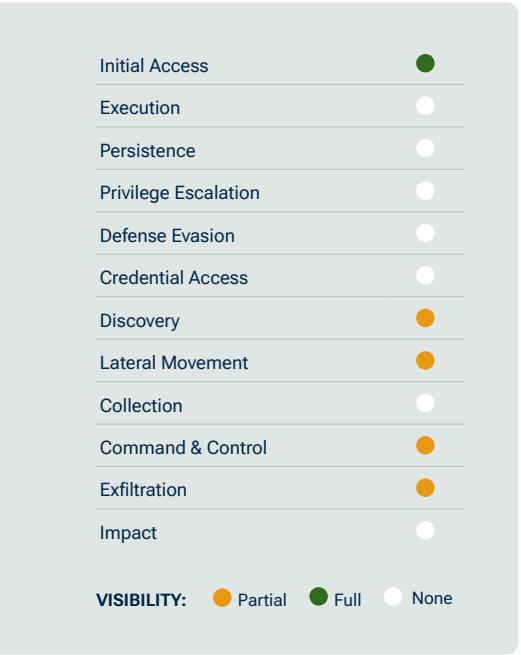
Use allowed protocols like HTTPS, DNS, or RDP to move undetected.

Operate over encrypted channels that firewalls can't inspect.

Leverage VPNs or SSO to authenticate like trusted users.

Firewalls can't detect C2 traffic, lateral movement, or SaaS access that uses valid credentials.

IDPS – Detects Signatures, Not Stealth



Intrusion Detection and Prevention Systems look for **known attack patterns**—but sophisticated attackers rarely use them.

HOW ATTACKERS BYPASS IDPS:

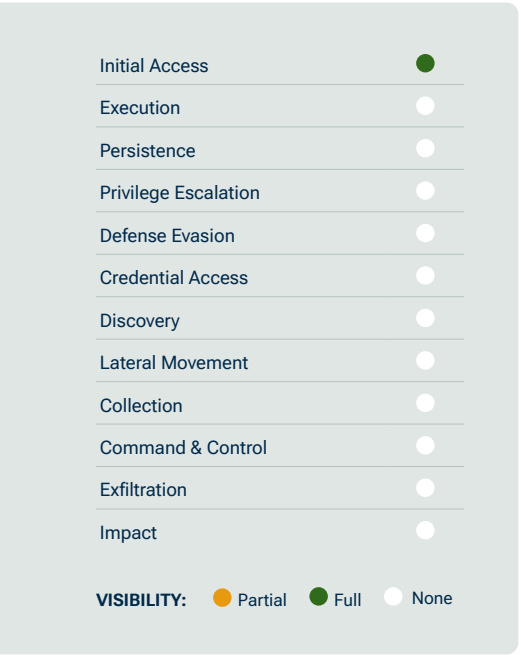
Use custom or encrypted payloads that evade signature matching.

Live off the land, using legitimate tools and ports.

Throttle activity to fly under detection thresholds.

IDPS fails against novel techniques and encrypted east-west movement.

NAC – Decides Who Can Connect, Not What They Do After



Network Access Control solutions validate **device posture and identity** before granting access. But once a user is connected, **NAC loses visibility**.

HOW ATTACKERS BYPASS NAC:

Hijack trusted credentials or devices to gain access without triggering NAC controls.

Move between trusted systems, which NAC doesn't monitor.

Exploit unmanaged or BYOD devices that slip through posture checks.

NAC doesn't detect lateral movement, suspicious traffic, or post-authentication behavior.

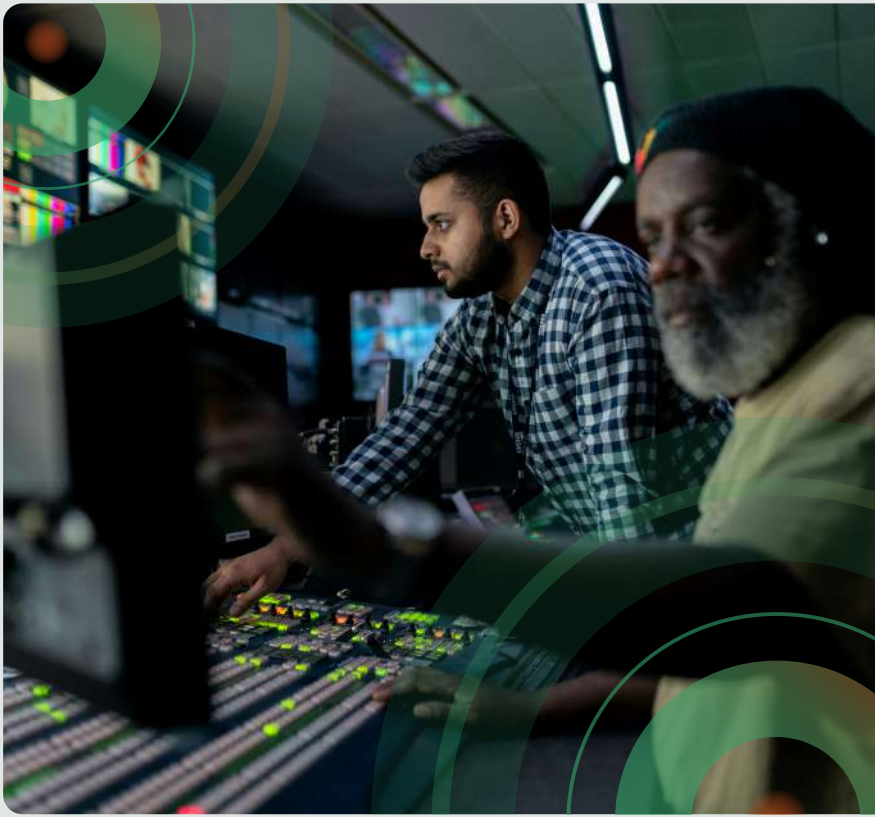
The Network Security Gap

Your current network tools focus on **prevention and control**—not detection.

THEY MISS:

1. **Lateral movement between workloads and regions** in cloud and hybrid networks.
2. **Command-and-control (C2) over encrypted or trusted protocols.**
3. **Data exfiltration disguised as business traffic.**
4. **Behavioral anomalies** in east-west movement, privileged access, and credential use.

Even SIEM and SOAR are only as good as the alerts they receive—and today's attackers ensure those alerts never come.



How Vectra AI Fills the Network Security Gap

Vectra AI delivers **Network Detection and Response (NDR)** designed for **modern hybrid infrastructure**:

- **Analyzes traffic from on-prem, cloud, and SaaS** environments in real time.
- **Detects attacker behaviors** like lateral movement, privilege escalation, and data exfiltration—even when hidden in encrypted traffic.
- Integrates with SIEM and SOAR to provide high-fidelity alerts your SOC can act on immediately.
- Vectra AI integrates with: Splunk, PaloAlto, Juniper, Fortinet, and more.

Identity Security

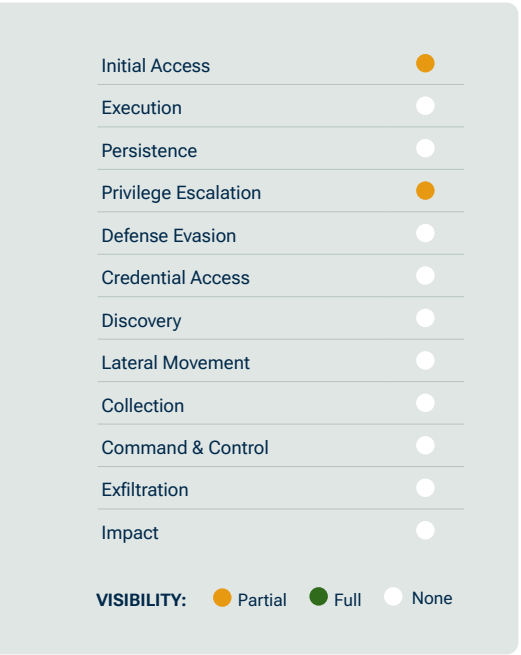
The Identity Blind Spot: When Valid Logins Become Invisible Threats

Modern attacks rarely rely on malware alone. Today's adversaries **don't need to exploit vulnerabilities**—they exploit **people**.

By stealing credentials, abusing identity federation, or operating through legitimate access paths, they **bypass your controls undetected**.

You've likely invested in **IAM, PAM, and maybe UEBA,** but these tools are focused on **prevention, policy, and risk scoring—not real-time detection of attacker behavior** across hybrid environments.

IAM – Prevents Unauthorized Access, Not Abused Access



Identity and Access Management (IAM) tools are foundational to Zero Trust. They control **who can log in, from where, and with what permissions.** But once a user is in, **IAM assumes trust.**

HOW ATTACKERS BYPASS IAM:

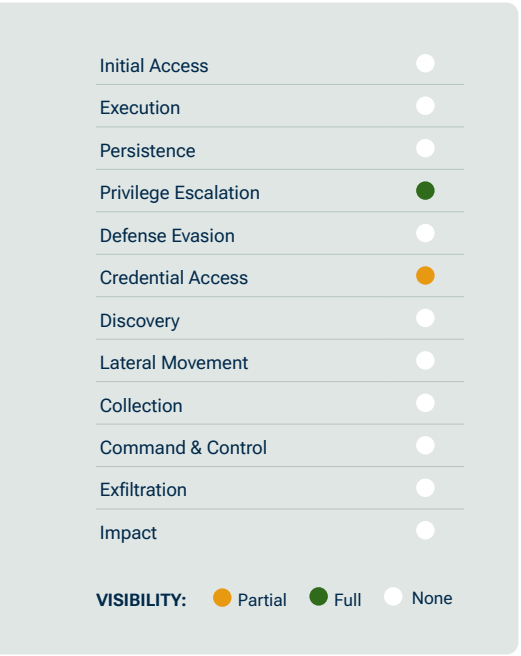
Steal valid credentials or session tokens, then log in as a legitimate user.

Move laterally using over-permissioned accounts or misconfigured access policies.

Authenticate through trusted identity providers, including federated logins and SSO.

IAM doesn't detect abuse of credentials—it only enforces login policies.

PAM – Protects Privileged Accounts, If You Know Who's Privileged



Privileged Access Management (PAM) solutions restrict how users access critical systems—often through **password vaults, session recording, or just-in-time access.** But attackers don't always need a privileged account to escalate.

HOW ATTACKERS BYPASS PAM:

Abuse non-privileged accounts to escalate using SaaS platform permissions (e.g., mailbox delegation, OAuth scopes).

Exploit federated identity trust relationships to gain access without touching PAM-controlled accounts.

Use shadow admins—roles with effective privileges but not flagged as "privileged."

PAM can't detect identity abuse that doesn't match predefined privilege boundaries.

UEBA – Scores Risk, But Can't See in Real Time

User and Entity Behavior Analytics (UEBA) platforms build profiles of normal behavior and assign risk scores when users deviate from them. Useful in theory—but they depend on **complete data,** and often **take too long to respond.**

HOW ATTACKERS BYPASS UBEA:

Mimic normal user behavior (e.g., same location, device, or access pattern).

Act slowly or during off-hours, avoiding noticeable spikes.

Exploit incomplete log sources, preventing UEBA from ever seeing the full picture.

UEBA delays detection and can't provide real-time visibility into identity misuse.

The Identity Security Gap

Identity is the **common thread in every modern breach**, yet most tools focus on **access control** or **risk scoring**—not **attacker behavior**.

THEY CAN'T SEE:

1. Credential abuse across SaaS platforms and cloud services.
2. Privilege escalation in Microsoft Entra ID or Exchange Online.
3. Trust relationship abuse between identity providers.
4. Identity-based lateral movement that doesn't touch the endpoint.

How Vectra AI Fills the Identity Security Gap

Vectra AI provides **real-time detection of identity misuse** by analyzing how human and non-human identities behave across:

- Active Directory
- Microsoft Entra ID (Azure AD)
- Microsoft 365 / Exchange Online
- Azure and AWS Cloud
- Cloud IAM roles and federated identities

Unlike policy-driven or log-delayed tools, Vectra detects:

- **SaaS privilege abuse** (mailbox delegation, OAuth abuse)
- **Federation manipulation** (new trust relationships or role impersonation)
- **Credential misuse** across hybrid infrastructure—**even when MFA was passed**

Conclusion

Close the Gap Before It's Exploited

You've invested in the best-of-breed security stack—firewalls, EDR, CASB, IAM, and more.

Each tool plays a role. But together, they still leave gaps—in the cloud, across SaaS apps, and between identity and network layers.

These are the blind spots attackers rely on to move freely, stay hidden, and cause damage.

You Can't Defend What You Can't See

Today's attackers don't rely on malware. They **leverage credentials, exploit SaaS misconfigurations, manipulate identity trust, and move across cloud workloads unseen.**

Traditional tools don't see this activity—not because they're broken, but because **they weren't designed to**.

- **EDR doesn't see identity abuse in Microsoft 365.**
- **CASB and SASE don't detect lateral movement in cloud workloads.**
- **SIEM can't alert on threats that upstream tools don't detect.**

Meanwhile, your SOC is left with **too many alerts, not enough context,** and **no real visibility** across hybrid infrastructure.

How Vectra AI Completes Your Stack

SECURITY CAPABILITY	WHAT'S MISSING	VECTRA AI ADDS
Endpoint Threat Detection	Blind to network & cloud	Real-time detection across all traffic (agentless)
Identity Threat Detection	No visibility post-authentication	Detects misuse of valid accounts & privilege escalation
Cloud Threat Visibility	Blind to attacker behavior and hybrid environments	Detects cloud-native, hybrid cloud, SASE, SaaS, & IaaS attacker movement
Lateral Movement Detection	Unseen across hybrid environments	Real-time detection of lateral movement
Noise Reduction & Prioritization	Alert fatigue, too much noise	AI-driven signal clarity with high-fidelity detections

Vectra AI Closes the Security Gap

Vectra AI is the missing layer—an AI-driven platform purpose-built to detect and respond to attacker behavior across your hybrid environment:

Coverage across on-prem networks, cloud workloads, SaaS platforms, and identity systems.

Clarity through behavioral detection, context-rich alerts, and prioritized investigations.

Control via integrations with SIEM, SOAR, and your existing tools to accelerate response and reduce dwell time.

Whether attackers are operating inside Microsoft Entra ID, accessing M365 via OAuth, pivoting through Azure workloads, or exfiltrating data over encrypted channels—**Vectra AI sees it, understands it, and alerts your team in real time.**

Why Vectra AI Is Critical Now

1 Close Identity-Based Gaps

Detect attackers leveraging valid accounts to move laterally, escalate privileges, and access sensitive data undetected by IAM, PAM or UEBA.

2 Complete Cloud and SaaS Coverage

Expose threats that Cloud Security tools can't see—such as credential abuse, privilege misuse, and lateral movement across hybrid, multi-cloud and SaaS environments.

3 Go Beyond Signature and Rule-Based Detection

Detect real attacker behavior in real time, not just anomalies or known IOCs—eliminating noise from UEBA, SIEM, and SOAR while surfacing high-priority incidents.

4 Correlate Signals Across Your Entire Environment

Bridge data silos across EDR, SIEM, and SOAR, delivering attack signal clarity to help your SOC focus on what matters most.

Ready to see what your stack is missing?

Watch the self-guided demo

Play Video

Learn how Vectra AI can integrate with your current environment

Learn More

Contact us to request a offensive security assessment

Contact Us

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. When modern cyber attackers bypass existing controls, evade detection and gain access to customers' data center, campus, remote work, identity, cloud, and IoT/OT environments, the Vectra AI Platform sees their every move, connects the dots in real-time, and stops them from becoming breaches. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't.
For more information, visit www.vectra.ai. version: 062625