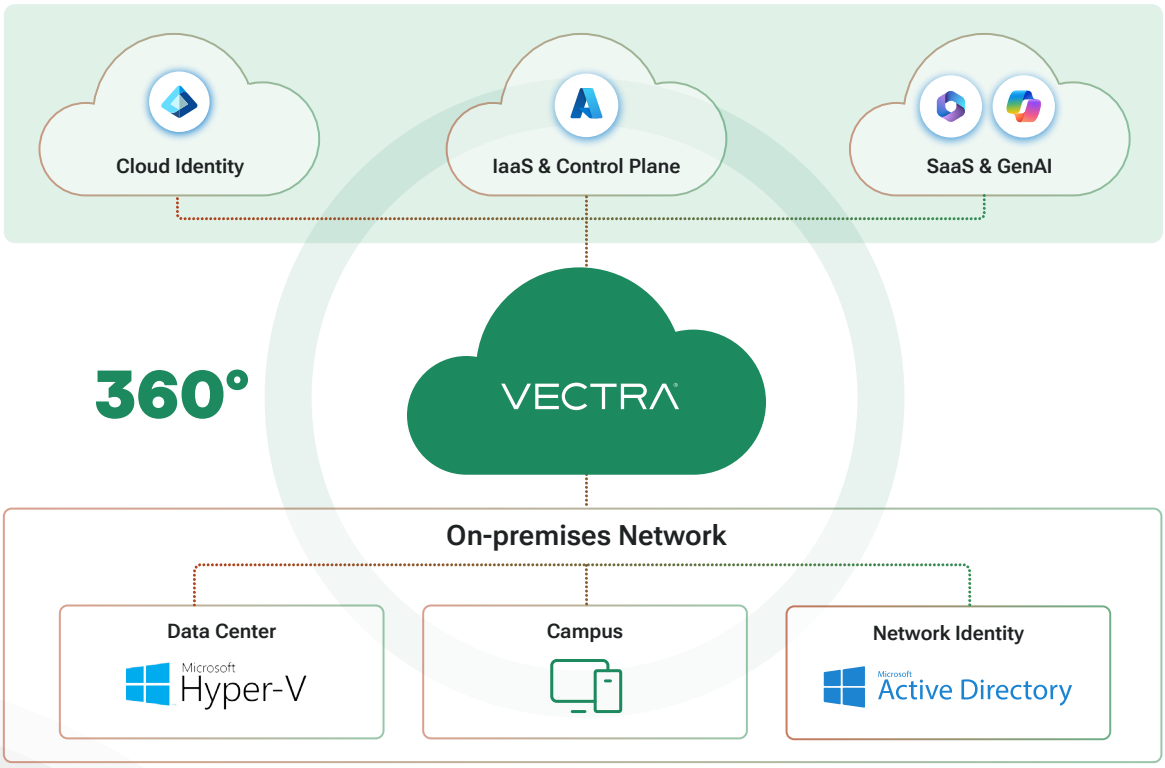
VECTRA

Vectra AI Shield for Microsoft

Comprehensive threat protection across Entra ID, Microsoft 365, Copilot for M365, and Azure Cloud in the Vectra AI Platform

Your Microsoft environment spans multiple domains—so do today's attackers. They log in stealthily, move laterally undetected, and quickly exfiltrate data within Microsoft SaaS and cloud environments. Vectra AI Shield for Microsoft delivers unified protection across Entra ID, Microsoft 365, Copilot for M365, and Azure Cloud, correlating detections of network-based attacks to empower security teams to stop threats before they become breaches. This datasheet details Vectra AI Shield for Microsoft's detection coverage, key capabilities, use cases, architecture, and administration features.



Key Differentiators

- **Native Tool Reinforcement.** Over 100 AI detections for Microsoft environments across all stages of an attack
  - Example detections not available with native tools: Azure Policy Hijacking, Azure AD Scripting Engine Usage, Azure AD Privilege Operation Anomaly, Azure AD Suspicious OAuth Application, M365 Disabling of Security Tools, M365 Risky Exchange Operation
- **Monitor the abuse of human and machine identities** (service principals, cloud principals, and machine, application, and instance credentials)
- **Real-time detection of living-off-the-land and zero-day attack techniques**, covering every stage of the kill-chain.
- **Privilege Access Analytics (PAA)**. Our patented graph-based AI algorithm monitors interactions between accounts, services and hosts to detect attacker abuse of privileges.
- **Cloud Identity attribution**. Attribute detections and activities to human or machine account names — not alphanumeric Object IDs — helping analysts instantly identify affected accounts, while avoiding manual effort and tool pivots for deeper investigations.

Vectra AI Shield for Microsoft Use Cases

Security Team Pain Points	How Vectra AI Shield for Microsoft Helps
Stop Cloud Data Breaches, Ransomware, and Data Exfiltration	Spots ransomware, data exfiltration attempts, and breaches in their earliest stages—before damage is done. By monitoring for abnormal file modifications, suspicious automations, and high-risk data movements across Azure and Microsoft 365 (including Exchange, OneDrive, SharePoint, Storage accounts, and Key Vault), Vectra AI provides deep, real-time visibility and alerting that fills detection gaps left by native tools.
Stop Phishing-Driven Compromises, Identity Compromise and Account Takeover	Finds attackers accessing and abusing cloud credentials (human and machine) before damage is done
Stop Cloud-Based Lateral Movement and Privilege Escalation	Monitors suspicious privilege changes, unusual admin assignments, and account role modifications across Entra ID, Azure, Copilot, and M365. AI-powered privilege access analytics provide early warning of attackers trying to escalate access or move laterally across cloud and hybrid environments
Monitoring for Insider Threats	Detects rogue cloud admin activities and employee data theft using M365 apps, enabling security teams to investigate abnormal data access, improper file sharing, and suspicious device connections. Integrates context from identity, cloud, and network layers for fast, cross-domain investigations.
Secure Copilot for M365 Deployments	Monitors for abuse of Copilot access, unauthorized sensitive data queries, and anomalous behavior patterns linked to generative AI, minimizing the risk of attackers using AI tools to fast-track sensitive information discovery.
Fortify Against Hybrid Attacks	Surfaces malicious behaviors tied to hybrid Azure workloads (Automation Accounts, ARC servers)
Shield Against Cryptomining and Destruction of Resources	Identifies cryptomining attempts (e.g., malicious resource creation, unusual extensions) and destruction tactics (like mass resource deletion), protecting business-critical assets before attackers can exploit them.
Securing Governance and Compliance Services	Provides robust visibility into Azure policy assignments, admin privilege changes, and compliance-related modifications—critical for catching governance gaps, policy misconfigurations, and potential compliance violations in real time.

Vectra AI Shield for Microsoft Coverage

Microsoft Azure Cloud: Detect Azure control plane attacks, providing hybrid visibility into critical infrastructure, control plane and resources, such as policies, App Service, automation accounts, and more.

Microsoft M365: Detect living-off-the-land attacks across Microsoft 365, including Teams, Exchange, OneDrive, eDiscovery, Power Automate, and SharePoint, ensuring full threat monitoring of critical business data.

Microsoft Copilot for 365: Detect attackers using Microsoft's Gen AI to accelerate data discovery and steal high-value information.

Microsoft Entra ID: Detect initial access to Microsoft Entra ID credentials and track attackers' next move, including cloud privilege abuse, new device registrations, and backdoor creation.

For more coverage details, please see Understand Vectra AI Detections

Vectra AI Shield for Microsoft Provides:

Vectra AI Behavioral Detections Across Entra ID, Microsoft 365, Copilot for M365, Azure Cloud

AI-driven detections to identify indicators of attack (IoA) aligned to the MITRE ATT&CK cyber kill chain and MITRE D3FEND countermeasures.

- Vectra AI's Attack Signal Intelligence detects attacker behavior across network, cloud, identity, and SaaS.
- Uses AI to spot indicators of attack like account compromise, privilege escalation, lateral movement, and data exfiltration.
- Enables early detection of insider threats, ransomware, and SaaS abuse.

Vectra AI Agents

A core innovation, **Vectra AI Agents** are purpose-built, intelligent microservices that automate manual tasks associated with threat defense. Key agents include:

- **AI Triage Agent** – Automatically investigate and triage benign behaviors using context and history to reduce false positives.
- **AI Stitching Agent** – Correlates discrete signals across users, hosts, and services spanning network, identity and cloud to create complete attack narratives.
- **AI Prioritization Agent** – Scores and ranks entities under attack based on risk level to elevate critical incidents and reduce analyst workload.

These agents automatically distill thousands of potential threat events into actionable entity-based alerts in the single digits, cutting alert noise by up to 99% and increasing SOC efficiency by up to 40%.

Vectra AI Investigations

Vectra AI Investigations provides analysts with a unified, intuitive interface to accelerate threat resolution. Key capabilities include:

- **Attack Graphs** – Understand complete attack campaigns across network, identity and cloud with an interactive, entity-centric visualization of an attack path.
- **Attack Summaries** – Automatically shows AI-generated summaries of attack campaigns and provides recommended next steps.
- **Metadata** – Tap into enriched metadata from over 25 sources and 300+ fields spanning network, identity and cloud, with up to 30 days of historical visibility.
- **Natural Language Search** - Use natural language to search enriched Vectra AI metadata to quickly gain insights on without needing to know query languages.

Vectra AI Investigations brings together AI-powered insights, enriched context, and intuitive workflows in a single interface—empowering security analysts to understand, prioritize, and respond to complex attacks 50% faster and with greater confidence than ever before.

Vectra AI Response

Vectra AI delivers a full spectrum of response capabilities that empower organizations to stop threats with speed and precision.

- **Native Response Workflows** – The Vectra AI Platform includes built-in response features through the unified Respond UX interface, allowing analysts to isolate hosts, suspend accounts, tag risky assets, and initiate forensic actions directly from a prioritized detection view.
- **Automated Response with AI Agents** – Vectra's AI Agents drive automated playbooks that take action on high-confidence detections—such as auto-suspending compromised accounts in Microsoft 365 or isolating endpoints via EDR integrations.
- **Integrated Ecosystem Response** – Vectra AI integrates natively with leading security tools including CrowdStrike, Microsoft Sentinel, Cortex XSOAR, Splunk, Zscaler, and AWS Security Hub. These integrations allow customers to trigger SOAR workflows, enrich SIEM alerts, or orchestrate broader containment actions across their security stack.
- **Managed Response via Vectra MDR** – For organizations seeking expert support or 24/7 threat coverage, Vectra MDR offers managed detection, investigation, and response services delivered by in-house Vectra analysts.

Together, these capabilities deliver true Coverage, Clarity, and Control—not only in detecting threats, but in resolving them decisively, whether via automation, orchestration, or expert-guided human response.

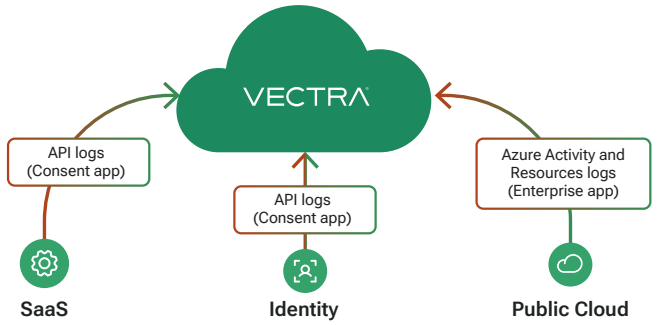
Architecture & Administration

Licensing

- Unified protection across Entra ID, M365, Copilot for M365 and Azure
- Pricing for Entra ID, M365, Copilot for M365 and Azure Cloud coverage is based on # of Entra ID identities
- Predictable, affordable and simple pricing
- Additional incentives are available for migrating to Vectra AI Respond UX

Deployment

- Agentless. Deploy in minutes. Full SaaS Deployment.
- Flexibility. Integrate with your processes and tools (EDR, SIEM, SOAR, ITSM) seamlessly.
- Scalability. Grow with your organization - increase the number of monitored identities and extend data retention for investigations at any time.
- Managed Services Support. Leverage our MDR team to assist with 24/7 monitoring or to supplement your threat hunting, detection, investigation, and response program.



Integrations

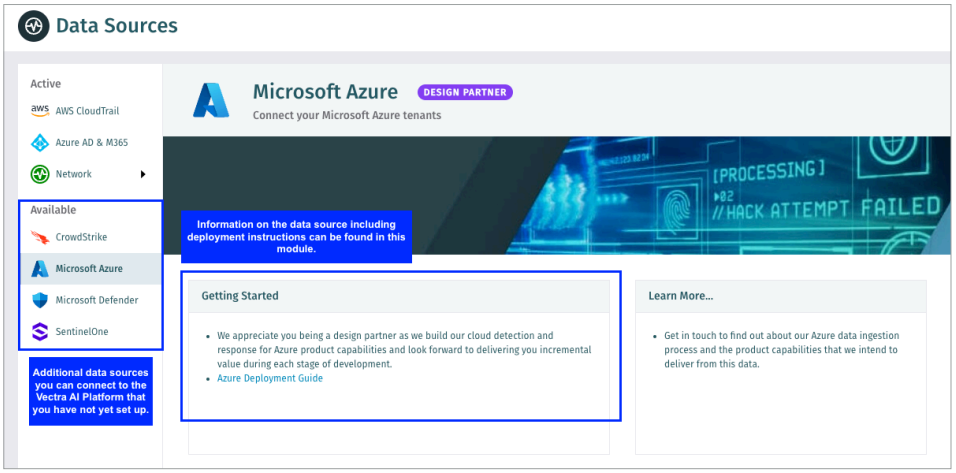
3rd Party Signal	Investigative Workflow	Incident Response
Bring 3rd party data, rules, threat intel, or detections into the Vectra AI Platform. Integrations: • AWS • Zscaler • Microsoft Azure • Microsoft 365 • Azure AD, Entra ID • VMWare Carbon Black • CrowdStrike Falcon Insight • Cybereason • FireEye Endpoint Security • Microsoft Defender for Endpoint • SentinelOne • Gigamon • IXIA Keysight • Endace • cPacket Networks • VMWare Virtualization • VM • Nutanix • Hyper-V	Send Vectra AI Platform detections, signal, metadata, or telemetry to your SIEM platform. Integrations: • Elastic • Google Cloud Chronical • Fortinet SIEM • IBM Qradar • Microsoft Sentinel • Splunk • CrowdStrike NG-SIEM	Send Vectra AI Platform detections, signal, metadata, or telemetry to your incident response platform. Integrations: • Fortinet Firewall • Juniper • Palo Alto Networks • Check Point • ServiceNow ITSM • Nozomi Networks • Superna • Fortinet NAC • Palo Alto Networks Cortex XSOAR • ServiceNow SIR • Swimlane • Splunk SOAR

Management

Flexible, customizable based on your environment, maturity, and risk tolerance.

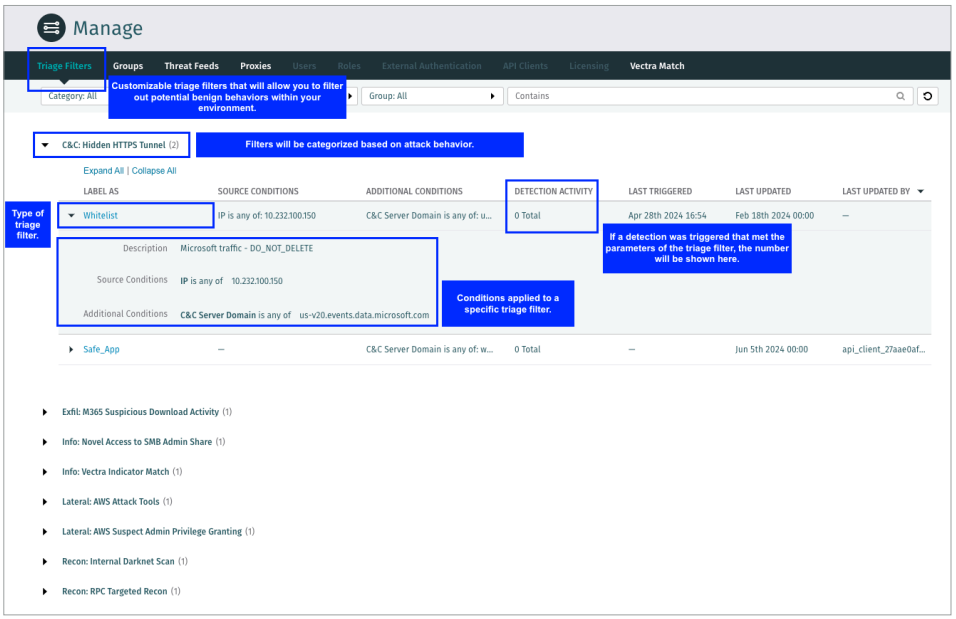
Data Sources

Track the available data sources you may choose to ingest into the Vectra AI Platform.



Triage Filters

Customize rules for benign behaviors within your environment that may trigger a detection, keeping the noise minimal on the Respond module.

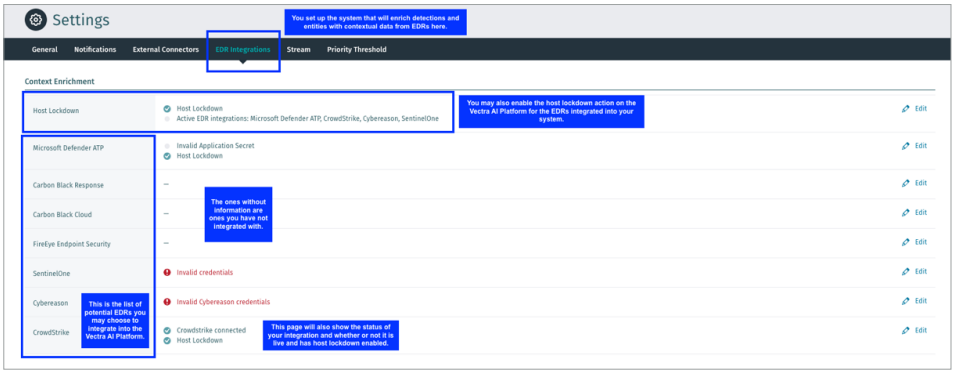


Priority Threshold

Customize the urgency score threshold for high, medium, and low prioritized entities.

EDR Integrations

Enable host lockdown and monitor status of your EDR integrations.



Vectra AI Industry Validation

Gartner:

- A leader in 2025 Gartner® Magic Quadrant for Network Detection and Response (NDR)

GigaOm:

- A leader and outperformer in Network Detection and Response (NDR)
- A leader and outperformer in Identity Threat Detection and Response (ITDR)

According to IDC, Vectra AI helps customers achieve these business value:

- 52% more potential threats identified
- 40% more efficient SOC teams
- 51% less time spent monitoring and triaging alerts
- 60% less time spent assessing and prioritizing alerts

Visit our website | **Schedule A Demo**

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.

VECTRA

For more information please contact us: Email: info@vectra.ai | vectra.ai