VECTRA

Vectra AI Platform

The days of the network being narrowly defined as on-premises data centers and campuses are long over. Today, the network is highly complex, interconnected and spans across data centers, campuses, remote locations and workers, clouds, identities, and IoT/OT.

Modern networks, modern attacks.

Modern attackers don't think multiple attack surfaces, they think one-giant network attack surface where they can :

- Expose gaps, exploit vulnerabilities, bypass controls, steal credentials.
- Establish command and control (C2), conduct recon, move laterally.
- Escalate privileges, establish C2, pivot to cloud and/or OT systems.
- Access critical systems and data, disrupt, extort, exfiltrate.
- Use GenAI and abusing copilots to be more efficient and effective.

The Vectra AI Platform protects modern networks from modern attacks with attack coverage, signal clarity, and intelligent control.

- Attack coverage reduces exposure to modern attacks.
- Signal clarity removes detection latency and workload.
- Intelligent control maximizes existing talent and tech.

Attack Coverage reduces exposure

We see what modern attackers see – one giant networked attack surface. We have you covered with AI Detections that expose attackers' every move across network, identity, cloud. Unlike anomaly-based tools that use AI to detect what is different, our AI is behavior-based detecting ever-evolving and emerging attacker methods spanning:

- Account Compromise
- Privilege Escalation
- Command & Control
- Lateral Movement
- Reconnaissance
- Data Exfiltration

Network	Identity	Cloud
Shore up defenses with AI for Network and close intrusion and endpoint detection gaps. Vectra AI Detections for Network surface attackers in your infrastructure moving laterally both east-west and north-south across data centers, campuses, remote work, cloud and OT environments.	Strengthen defenses with AI for Identity and know when attackers compromise accounts, abuse privilege. Vectra AI Detections for Identity surface attackers compromising and escalating privileges for both human and machine accounts across Active Directory, Microsoft Entra ID, Microsoft 365, AWS and Azure.	Fortify defenses with AI for Cloud and detect attacker behaviors other tools can't. Vectra AI Detections for Cloud surface multi-cloud attacks spanning your AWS, Microsoft Azure, Microsoft 365, and Microsoft Copilot for M365 environments.

Network

Key Differentiators:

- Detection without decryption: Unlike other tools that introduce operational burden, latency, and risk by needing to decrypt to detect, we see through encryption to detect threats.
- Advanced C2 Coverage: AI Detections for the most advanced attacker methods of establishing command and control (C2) early in the cyber kill chain.
- Signature and threat intel ingestion: Ingest signatures and threat intel feeds to make your attack signal stronger, and threat hunting and investigations faster.

Identity

Active Directory: Detect credential attacks involving zero-day techniques and privileged credential abuse for lateral movement, including Kerberoasting, brute force, and protocol abuse of RDP, SSH, NTLM, LDAP, DCERPC, SMB, and more.

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.

Microsoft 365: Detect living-off-the-land attacks across Microsoft 365, including Teams, Exchange, OneDrive, eDiscovery, Power Automate, SharePoint, and more.

Microsoft Azure: Detect Azure cloud identity attacks with visibility into critical infrastructure and resources, such as policies, App Service, automation accounts, and more.

AWS: Detect AWS cloud identity attacks with visibility into S3, EC2, Lambdas and more.

Key Differentiators:

- Privilege Access Analytics (PAA). Our patented graph-based AI algorithm monitors interactions between accounts, services and hosts to detect attacker abuse of privileges.
- Host-ID Attribution. We attribute detections to hosts, devices, and accounts — human and machine — saving a ton of manual work and tool pivoting for analysts.
- Native Tool Reinforcement. Real-time detection of living-off-the-land and zero-day attack techniques, covering every stage of the attack.

Cloud

AWS: Detect attacks threatening control plane and resources, such as S3, EC2, Lambdas and more.

Microsoft Azure: Detect Azure 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.

GCP: Detect GCP cloud network attacks, leveraging packets to close GCP network visibility gaps.

Key Differentiators:

- Multi-cloud coverage. AI detections across all stages of an attack for AWS, Microsoft Azure, Microsoft 365, and Microsoft Copilot for M365.
- Native Tool Reinforcement. Over 100 AI detections for Microsoft environments and over 40 AI detections for AWS.
- Entity Attribution. Our cloud attribution technology leverages AI/ML to analyze over a dozen artifacts to confidently attribute attacks to a specific entity.

Signal Clarity removes latency and workload

We find modern attackers inside your network so you can stop them — while removing 99% of alert noise and reducing manual effort by up to 50%.

Vectra AI Assistants connect the dots across network, identity, and cloud, reducing alert noise and benign false positives.

- AI Triage automatically distinguishes true from false, malicious from benign.
- AI Stitching automatically connects the dots across detected events and domains in real-time.
- AI Prioritization automatically scores, ranks, and alerts what's most critical and urgent based on attack velocity technique breadth, and entity importance.

Vectra AI-enabled Threat Hunting reduces analyst workload, accelerating investigations and threat hunting.

- 25 enhanced network, identity, and cloud metadata types with over 250+ fields, enriched with host, account privilege, and security context.
- Instant Investigations provide zero-query access to relevant data automatically aggregated and organized.
- Advanced investigations enable custom filters and queries of network, identity and cloud metadata.
- Attack Graphs enable visualization of attack progression across network, identity, and cloud domains over time.

AI enabled Response provides flexible, surgical response actions to stop attacks before they become breaches.

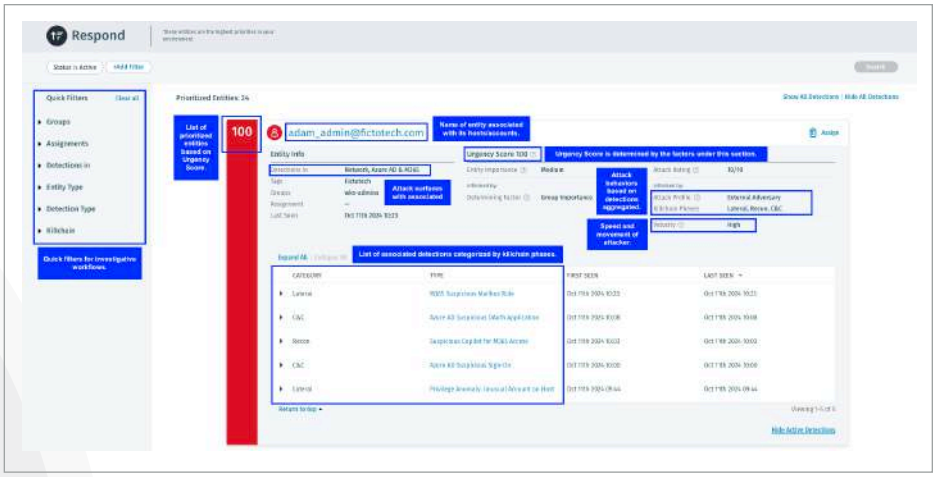
- Isolate compromised hosts with EDR integrations.
- Disable compromised human or machine accounts in Active Directory, Entra ID, and AWS.
- Revoke attacker access with MFA re-prompt.
- Block attacker communication at the firewall.
- Integrate with existing processes, controls and playbooks with the Vectra Automated Response framework.
- Partner with Vectra AI managed services to remediate and respond 24x7.

Intelligent Control maximizes talent and tech

We put you in control with the Vectra AI Respond User Experience (RUX) to discover, hunt, detect, investigate, and respond – preventing attacks from becoming breaches while improving analyst efficiency and effectiveness.

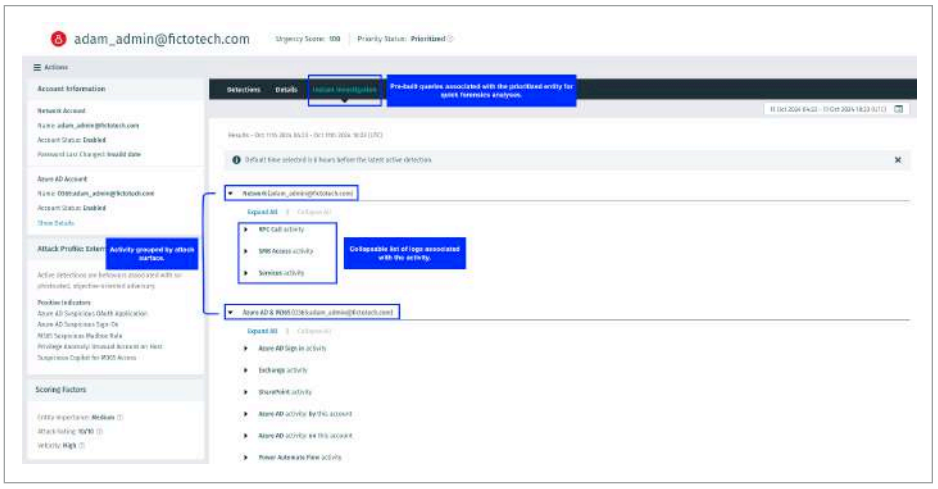
Detect

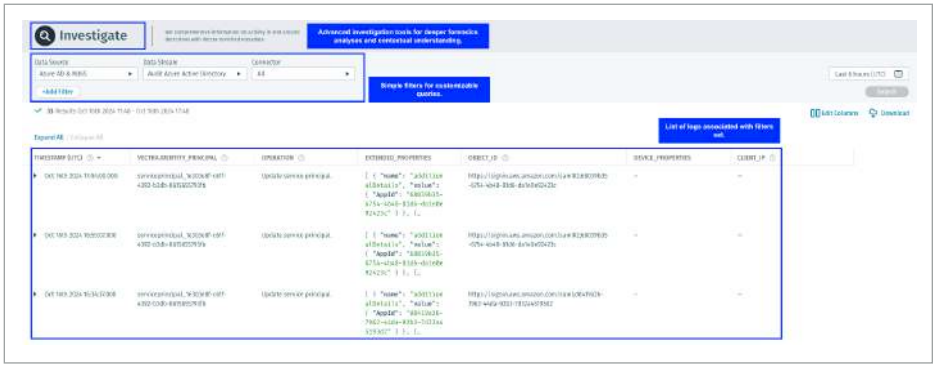
See threats ranked by urgency score in a single, unified view.



Investigate

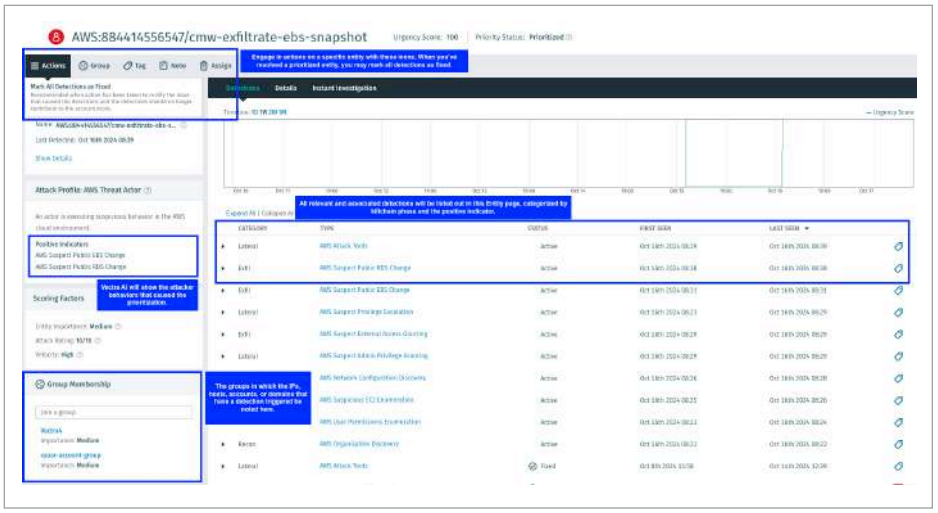
Deep dive into detections with Instant and Advanced Investigations.

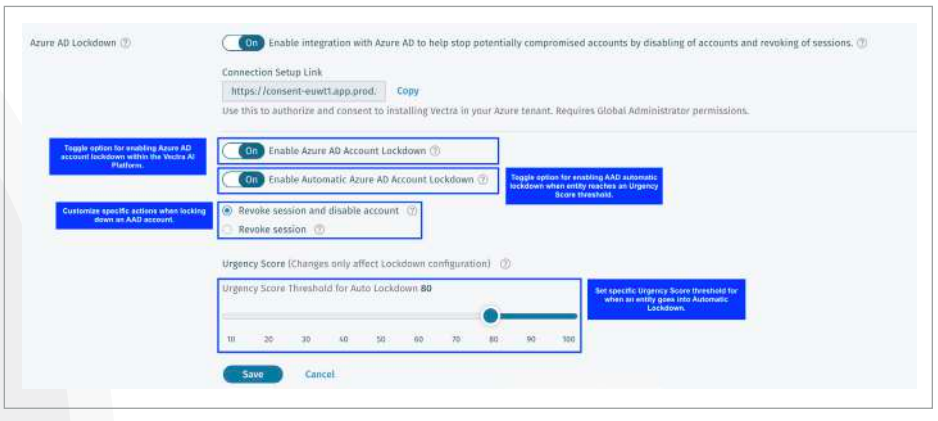




Respond

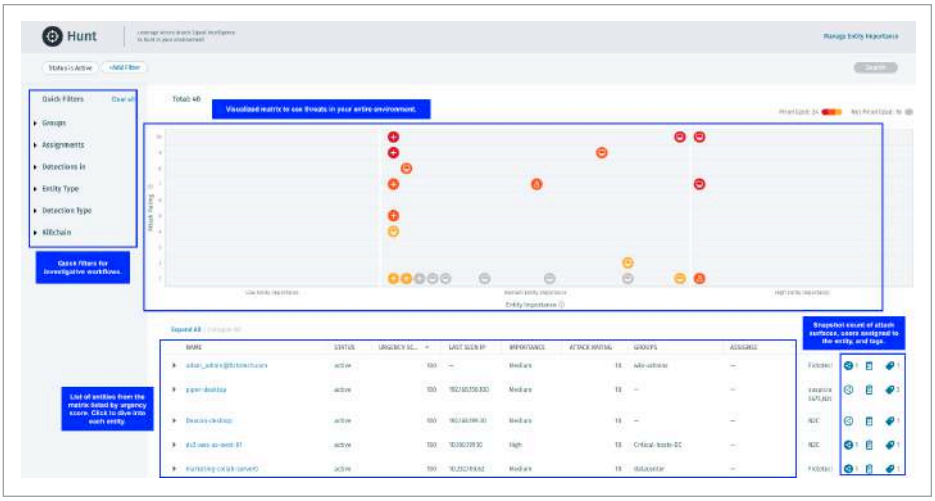
Stop attacks with native, integrated, and managed response capabilities.





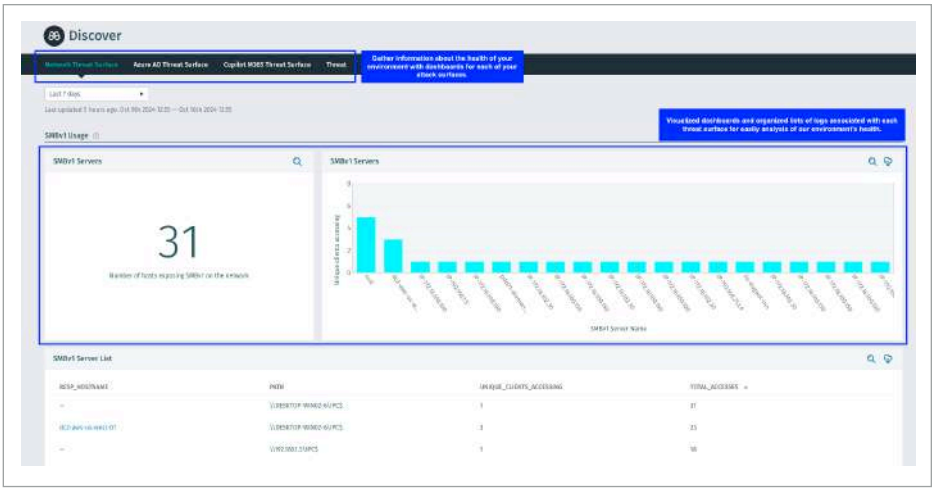
Hunt

Hunt down unusual behaviors in your environment with a visualized matrix.



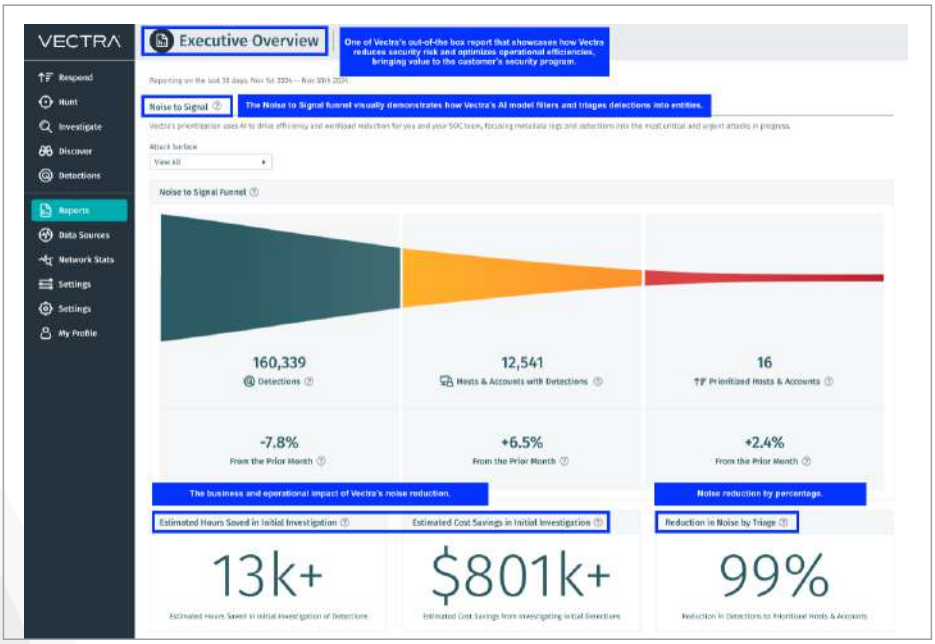
Discover

Monitor all your network, cloud, SaaS, and identity threat services in dynamic dashboards.



Reporting

Curated and customizable reports catered to your security leader or SOC manager, demonstrating risk reduction and operational efficiency.



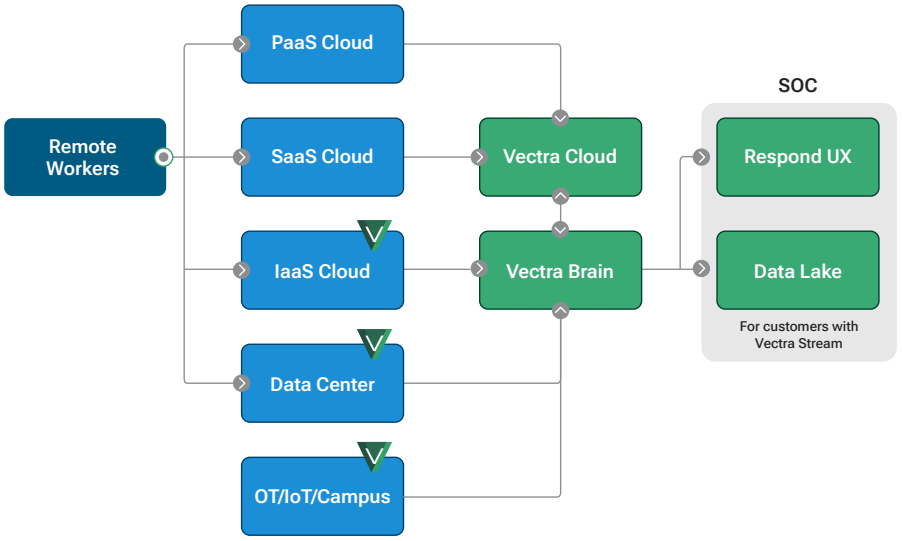
Architecture and Administration

Deployment

Deploy agentless as on-premises, SaaS, or hybrid and get actionable attack signal in days to hours across the network, and hours to minutes for identity and cloud.

Simplified deployment steps:

1. Vectra Respond UX is instance created.
2. Welcome email is sent, and admin configures roles, users and any non-network data sources.
3. Vectra Brain appliance deployed and connected to Vectra Respond UX instance.
4. Vectra Sensors are paired to the Vectra Brain and network traffic are directed to Sensors.

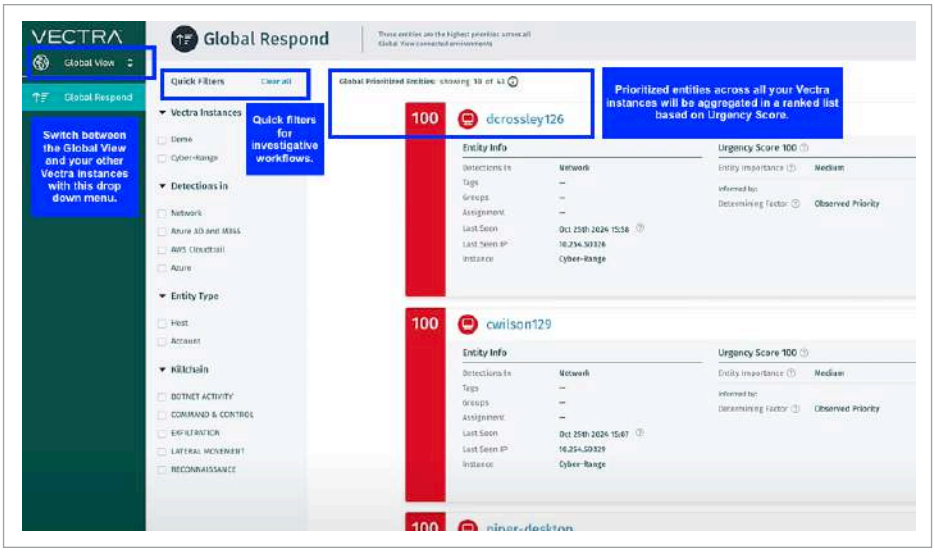


Management

The Vectra AI Platform allows you to customize your experience and how your detections are interpreted based on your organization's needs.

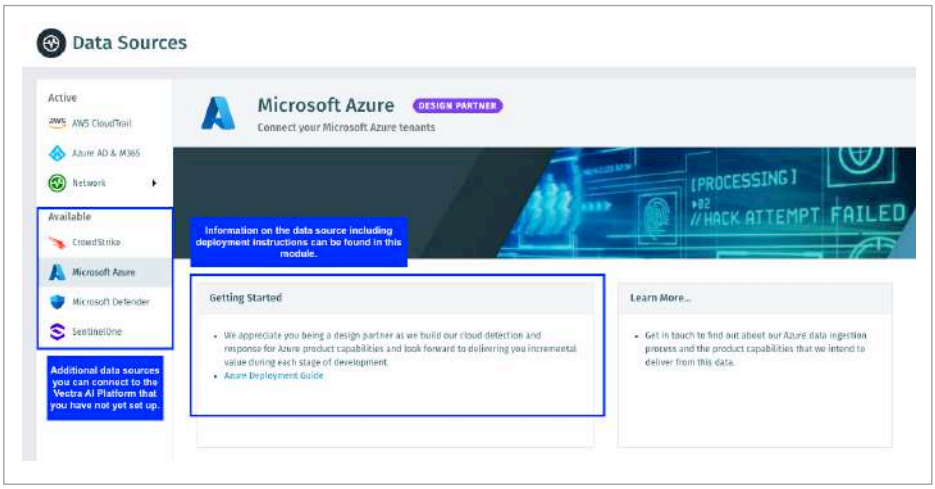
Global View

Enable Global SOC teams to oversee multiple regions or subsidiaries in multiple Vectra AI instances.



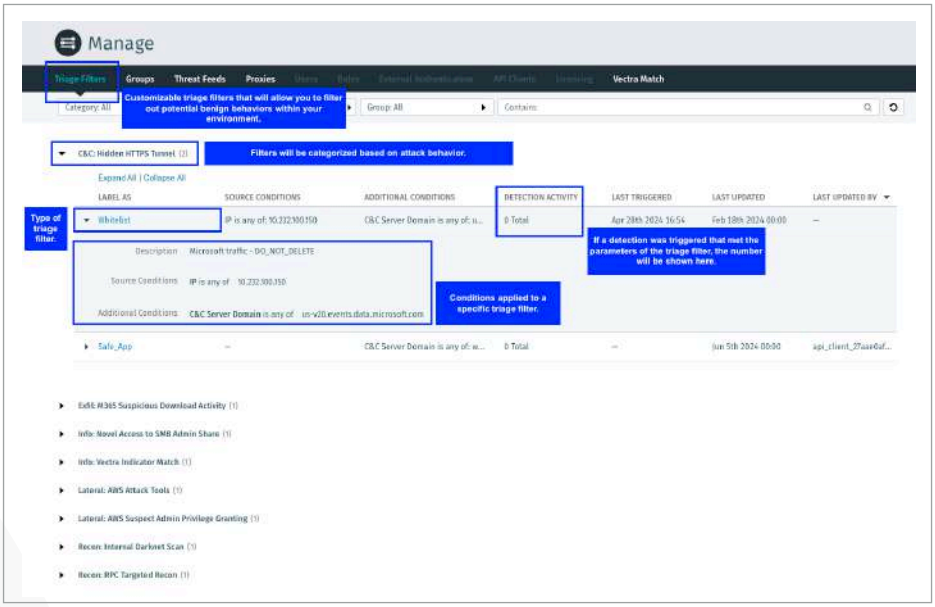
Data Sources

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



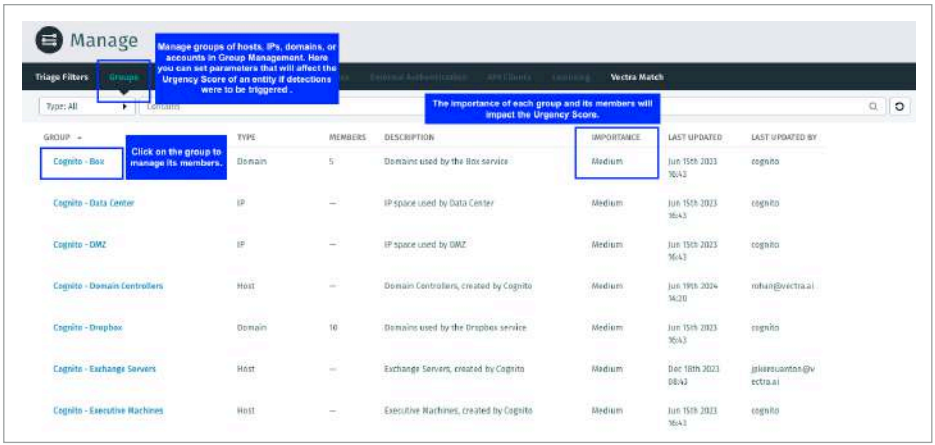
Triage Filters

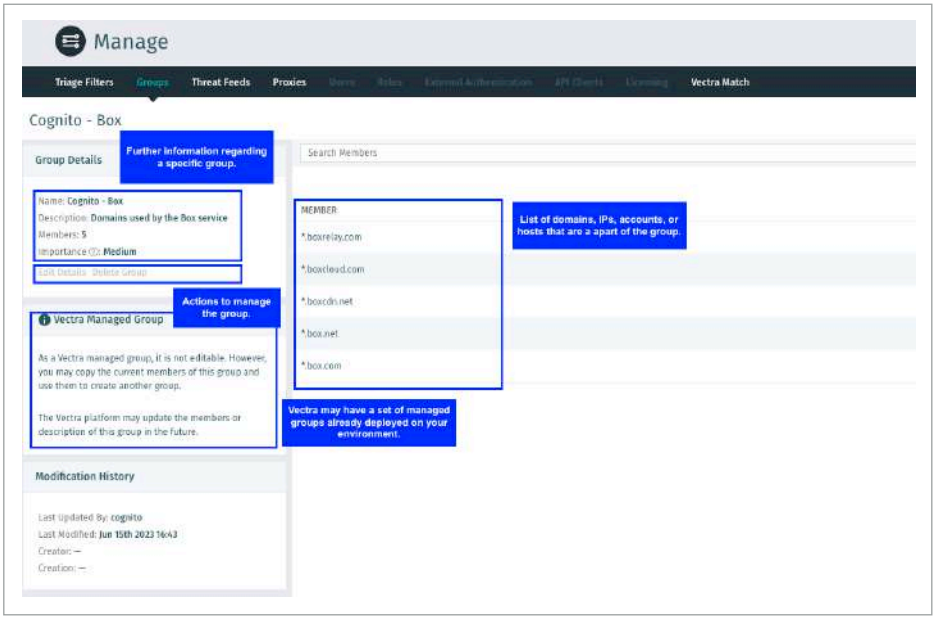
Customize rules for benign behaviors within your environment that may trigger a detection, keeping the noise minimal on the Respond module.



Group Management

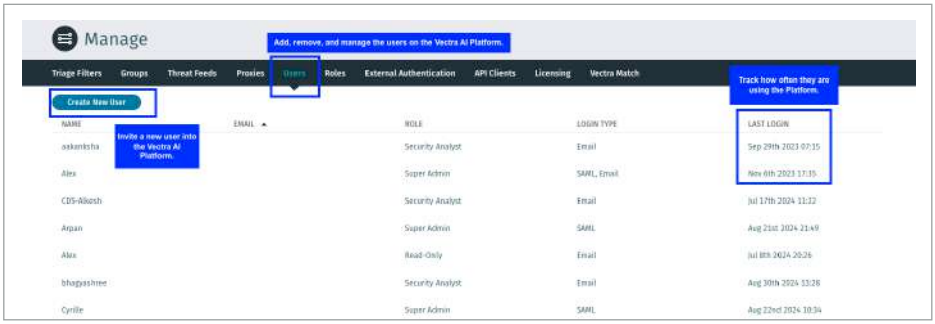
Group hosts, IPs, domains, and accounts within your environment and set their importance, ensuring accurate prioritization if a detection were to be triggered.

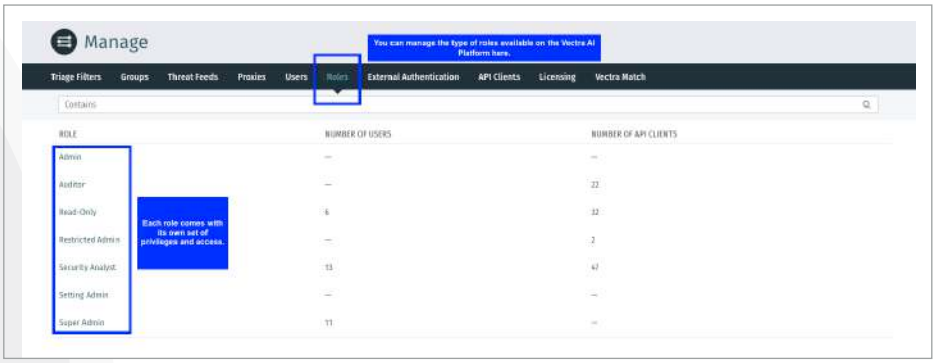




Users and Roles

Manage your team and their roles within the Vectra AI Platform.





Priority Threshold

Customize the urgency score threshold for High, Medium, and Low prioritized entities.

EDR Integrations

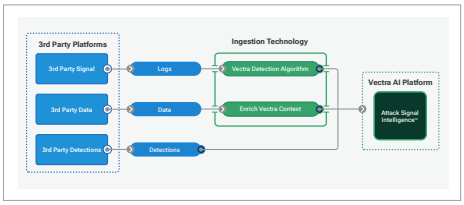
Enable host lockdown and monitor status of your EDR integrations.

Integrations

Maximize the value of your existing tools, and streamline your existing processes.

3rd Party Signal

Bring 3rd party data, rules, threat intel, or detections into the Vectra AI Platform.

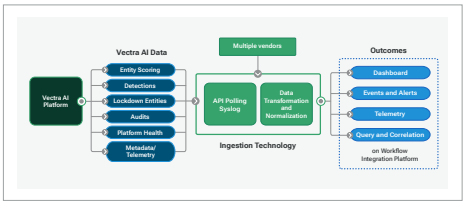


Integrations:

- 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

Investigative Workflow

Send Vectra AI Platform detections, signal, metadata, or telemetry to your SIEM platform.

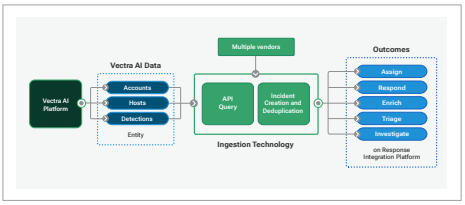


Integrations:

- Elastic
- Google Cloud Chronical
- Fortinet SIEM
- IBM Qradar
- Microsoft Sentinel
- Splunk
- CrowdStrike NG-SIEM

Incident Management and Response

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

Visit our website

Get started

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that stops attacks others can't. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

VECTRA

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