VECTRA

Vectra Identity Threat Detection and Response: Comprehensive AI-powered defense against identity attacks

Arm your SOC analysts with AI-driven Attack Signal Intelligence™ to see and stop identity-based attacks in real time.

Traditional prevention and EDR tools fail to stop modern identity attacks. Proactive organizations must continuously monitor for identity attacks and respond before damage is done.

Why choose Vectra ITDR

Vectra ITDR (Identity Threat Detection and Response) works in tandem with prevention and EDR tools to defend against identity attacks. It is a capability on the Vectra AI platform to generate integrated identity attack signal to strengthen your XDR.

Vectra ITDR defends against attackers who abuse identities, including admin and service accounts, and target identity infrastructure. It effectively finds identity attacks spanning across Network Active Directory, Microsoft Entra ID (Azure AD) and cloud identities in real time. The Integrated visibility provides simplified investigations and automated, and customized response.

Why use Vectra ITDR to defend against identity attacks?

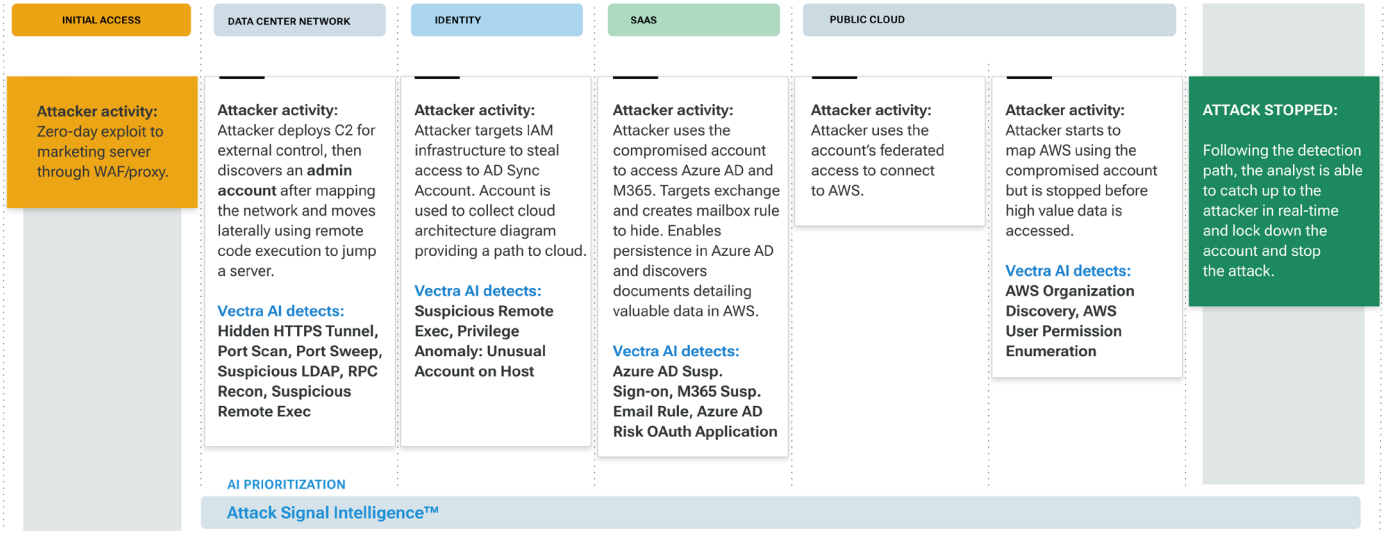
- **Finds Identity Attacks Faster:** Vectra ITDR finds attackers abusing identity across the hybrid attack surface and monitors attackers abusing Microsoft Entra ID (Azure AD), Active Directory, local, and cloud identities. Our solution correlates identity coverage with the broader network and cloud activity.
- **Protect Every Service Account:** Vectra ITDR removes the risk of service account sprawl with AI monitoring and finds service and admin accounts automatically when they are abused even if you don't know what and where they are.
- **Reduce Workload and Go Beyond UEBA Noise with AI:** Vectra ITDR understands privilege and delivers signal clarity that simple UEBA anomalies cannot. Our AI minimizes noise to highlight attacker behaviors, unlike simple UEBA and anomaly solutions which fail to detect attacks and overload analysts.

Vectra ITDR Use Cases

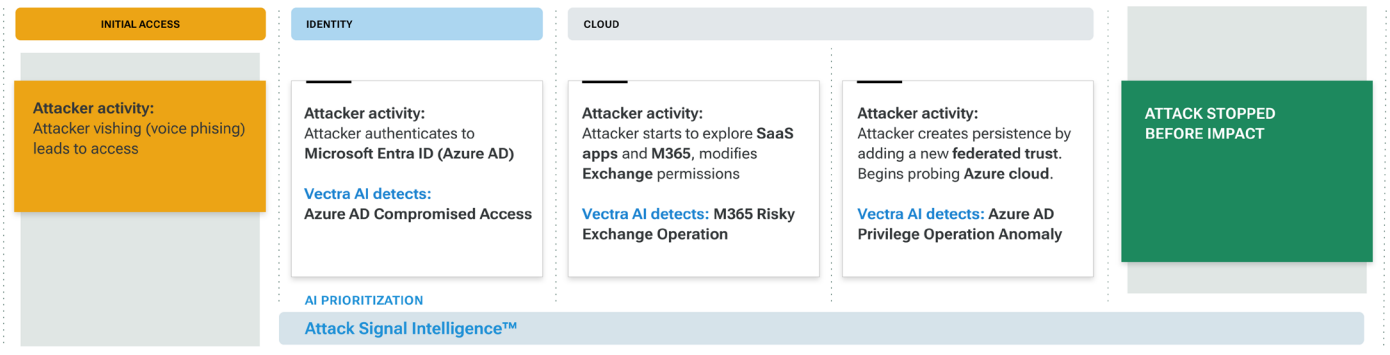
- **Stopping ransomware early:** Stops ransomware by detecting attackers before they have a chance to do damage.
- **Stopping phishing-driven compromises:** Discover and stop attackers accessing Microsoft Entra ID (Azure AD) and connected cloud apps.
- **Securing service account sprawl:** Automatically monitor all identities robustly, human and machine, and alert on service account abuse.
- **Defending privileged identities:** Stops privileged identities abuse by using patented AI to learn user privilege and understand what is malicious.
- **Defending identity infrastructure:** Coverage for attackers targeting credentials and identity stores using techniques like kerberoasting, DCSYC, and rouge LDAP queries
- **Stopping identity-based lateral movement:** Stop lateral movement by using behavior-based alerting over AD, Microsoft Entra ID (Azure AD), RDP, NTLM and more
- **Securing ZScaler connections:** Integrate with ZScaler to provide controlled access and continuous visibility on suspicious identities.
- **Monitoring for insider threats:** Stop insider threats by alerting on rogue network and cloud admins, and employee data theft from M365 applications.

Real attack examples demonstrating how Vectra ITDR correlated identity coverage with the organization's network and cloud activities and alerted about the attack fast, before the attacker could create damage

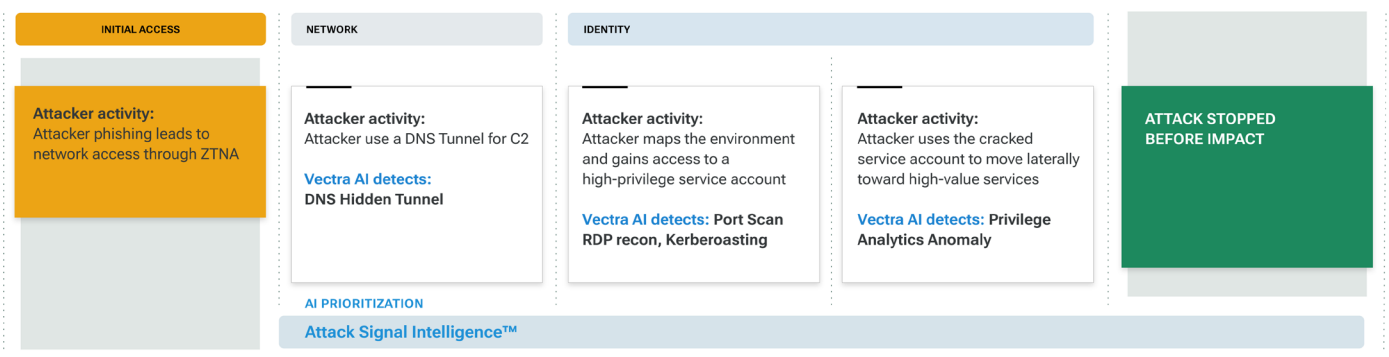
Network And Cloud Identity Threats



Cloud Identity Threats



Network Identity Threats



Vectra ITDR Value

Vectra ITDR protects your organization from business damage (e.g., data and operation loss, ransomware, reputational damage, etc.) when prevention fails, reduces analyst workload, and achieves a more resilient SOC.

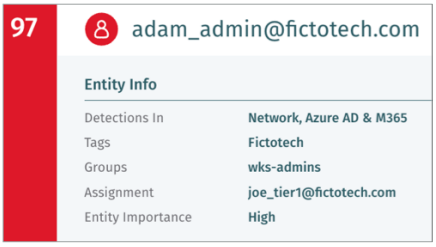
SOC Team: Strengthen your defense against identity attacks to protect against data loss, ransomware and reputation damage while reducing analyst workloads by 50% or more

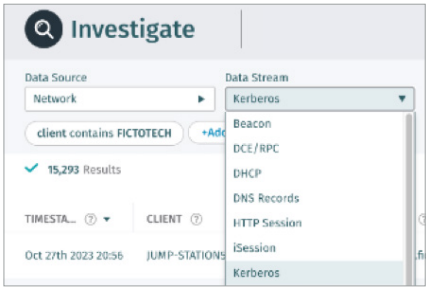
Security Engineers: Lighten the workload for engineers to build custom models with an out-of-the-box solution that requires minimal tuning.

IAM Team: Gain unrivaled visibility into how and where identities are being used to defend your infrastructure and support compliance.

Capabilities

- **Coverage:** Detects identity focused attackers in real time with patented Privilege Access Analytics detection capabilities that finds attacks that other tools miss.
- **Clarity:** Finds real attacks with less noise by automating the correlation and detection of attacker actions across network and cloud and automatically filtering benign activity.
- **Control:** Stops threats with simplified investigations and automated or customized response actions that stop attacks in minutes





Core Coverage Area

Vectra AI defends against identity attacks anywhere in your environment.

ITDR for Network

- Fully integrated and included with Vectra NDR
- Network Active Directory and local identity coverage, including encrypted activity
- Coverage for attackers targeting Domain Controllers and identity stores
- Alerting for Kerberoasting, rouge LDAP queries, RPC command abuse and more
- Patented privilege aware alerts for privileged and service account abuse
- Vectra AI enhanced and streamlined access to Network traffic and AD logs

ITDR for Microsoft Entra ID (Azure AD)

- Full standalone SaaS delivery deploys in 5 minutes
- Comprehensive coverage for attacker access, admin abuse and everything between
- Proven zero-day coverage for tenant backend attacks using privilege analytics
- Vectra AI enhanced and streamlined access to logs related to access and backed activity

CDR for M365

- Full standalone SaaS delivery deploys in 5 minutes
- Deep coverage for attackers abusing native tools and targeting data in Exchange, SharePoint, OneDrive, Teams, Power Automate and more.
- Vectra AI enhanced and streamlined access to logs related to Microsoft apps and data

CDR for AWS

- Full standalone SaaS delivery deploys in 5 minutes
- Comprehensive coverage for identity activity in AWS apps including EC2s, S3, IAM, RDS, AMI and more
- True AWS Identity tracking with Kingpin Technology that finds the true user behind a threat
- Vectra AI enhanced and streamlined access to CloudTrail logs

Vectra ITDR Features

- **AI-Prioritization:** correlates, scores, and ranks incidents by urgency level
- **AI-Triage:** triage benign behavior and reduce false positives
- **Attack Signal Intelligence™:** find identity attack signals inside the data along the entire attack lifecycle, from initial access to exfiltration or disruption
- **Privilege Access Analytics:** calculate the privilege of human and machine accounts, services, operations, and hosts, and alerts on privilege abuse
- **Enhanced Metadata:** augment identity data with additional context and intelligence, and enable easy search and investigation
- **Automated and Customized Response:** integrate with existing security tools and workflows, and enable direct response actions, such as revoking or disabling Microsoft Entra ID accounts

Vectra AI Platform Ecosystem

Integrated Attack Signal Intelligence no matter your pane of glass.

- **Cloud:** Microsoft Azure, Microsoft Entra ID, Microsoft 365, AWS, GCP
- **Endpoint:** Microsoft Defender for Endpoint, CrowdStrike, SentinelOne, VMWare Carbon Black, Cybereason, FireEye Endpoint Security
- **SIEM:** Microsoft Sentinel, Splunk, IBM, QRadar, Google Cloud Chronical, Elastic, Falcon LogScale
- **SOAR:** Palo Alto Networks Cortex XSOAR, ServiceNow SIR, Splunk, Swimlane
- **SASE:** Zscaler
- **ITSM:** ServiceNow
- **Firewalls:** Palo Alto Networks, Juniper, Fortinet, Check Point
- **Packet Brokers:** IXIA Keysight, Gigamon, cPacket networks

Vectra AI helps security teams with limited resources to stop identity attacks fast. Our ITDR solution defends against human and machine identity attacks across network and cloud. Our AI minimizes noise and alerts on attacker behaviors unlike simple UEBA and anomaly solutions which fail to detect attacks and overload analysts.

Schedule a Demo of Vectra ITDR

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by 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