VECTRA
SECURITY THAT THINKS.®

SOLUTION BRIEF

Stop the Next Ransomware Attack

Ransomware continues to evolve as threat actors now implement components and features that make it more difficult for victims to recover their data. Today's attacks are driven by invasive human activity where attackers gain access to high-privilege accounts and then move laterally to search for, steal and encrypt your most sensitive data.

Detecting attacker activity early is the only proven way to stop ransomware. However, cybersecurity has relied on understanding the known threats, where detection and response methodologies use signatures, anomalies and rules to see and stop attacks. This approach is broken. As enterprises shift to hybrid and multi-cloud environments, embrace digital identities, digital supply chains, and ecosystems — security, risk and compliance leaders are faced with more.

- More attack surface to cover.
- More evasive and sophisticated attackers.
- More tools and more data sets to analyze.
- More signatures, anomalies, rules to maintain.
- More alert noise, triage, false positives.
- More analyst fatigue, burnout, turnover.

Despite more tools, data, signatures, policies, rules, alerts and people — the core problem remains the same:

"We don't know where we are compromised – *right now*."

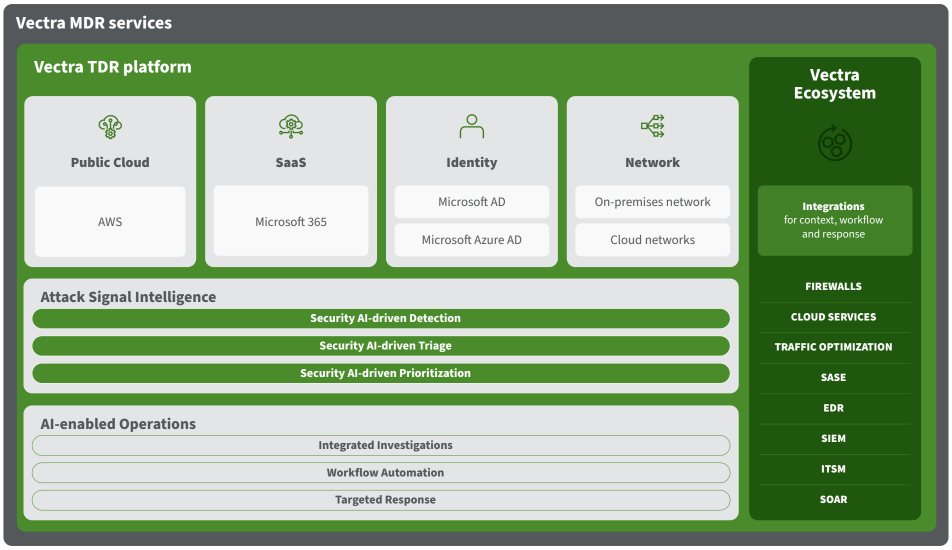
Ransomware actor intetions:

- Locate and exploit vulnerabilities
- Gain unguarded access to your business
- Infiltrate and progress laterally inside your systems
- Get unknown access and control of your data
- Steal valuable and critical data

Vectra Threat Detection and Response platform erases ransomware

Today's single biggest security risk to organizations is the unknown threat. Expanding attack surfaces require better coverage and evasive attackers can only be detected by understanding their behavior, while analysts can't afford to be burdened with more work and noise from security tools.

Vectra Threat Detection and Response platform provides complete threat coverage and signal clarity that puts your defenders in control against emerging, evasive and sophisticated cyber attackers. This includes stopping motivated ransomware attackers who move fast once they've gained access to your environment regardless of how they get in. To stop them, the Vectra TDR platform empowers analysts with:



Attack Coverage

Erase unknown threats across four of five attack surfaces — public cloud, SaaS, identity and networks.

Signal Clarity

Harnesses Security AI-driven Attack Signal Intelligence™ to automatically detect triage and prioritize unknown threats.

Intelligent Control

Arm human intelligence to hunt, investigate and respond to unknown threats.

Get ahead and stay ahead of today's ransomware attacks

The Vectra TDR platform harnesses Vectra's Security AI-driven Attack Signal Intelligence — a risk-based approach to cyberattacks reducing manual tasks, alert noise and analyst burnout. Attack Signal Intelligence empowers security analysts with AI-driven detection, triage and prioritization to find and stop attackers who target and attempt to progress across your environment long before patching is available. Your team can investigate and respond to public cloud, SaaS, identity and network attacks before they become breaches.

AI-Driven Detections that think like an attacker

- Behavior-based models accurately detect attacker TTPs.
- Correlated detections of attacker TTPs across domains.
- Comprehensive visibility of the complete attack narrative.

AI-Driven Triage so you know what is malicious

- Continuous analysis of all active detections for commonalities.
- Intuitive by design to distinguish malicious vs. benign activity.
- Automated to expose the malicious and log the benign.

AI-Driven Prioritization so you know what is urgent

- Real-time threat analysis for severity and impact.
- Unified view of prioritized threats by severity and impact.
- Contextual alerting accelerates investigation and response.

Integrated Investigations

Intuitive user interface puts answers at analysts' fingertips, attributing threats to compromised accounts and users.

Ecosystem Integrations

Integrate existing tech for correlation and context and to automate analyst workflows and response controls.

Managed Services

Managed detection, response and training services provide the skills and 24/7/365 reinforcements defenders need.

Turn the tables on ransomware attacks

With the Vectra Threat Detection and Response (TDR) platform and services, your organization is more resilient to ransomware attacks with early detection of attacks, protection against data loss, downtime, reputation damage and ransom payments:

- Up and running with actionable detections in days if not hours.
- Future-proof your data breach defense as your attack surface expands.
- Reinforcements at the ready with Vectra MDR services.

Your processes and workflows are more efficient:

- Reduce SIEM costs and detection rule creation and maintenance.
- Automate analysts' manual tasks and time to investigate and respond.
- Optimize existing investments in EDR, SOAR and ITSM.

Your security analysts are more effective:

- Reduce analyst burnout with accurate detection of malicious true positives.
- Increase analyst throughput by accelerating investigation and response.
- Builds analyst expertise and skills hunting and defending against advanced attacks.

Unlike other approaches that center on simple anomaly detection and require human tuning and maintenance, the Vectra platform exposes the complete narrative of an attack without human intervention. By harnessing Attack Signal Intelligence, security teams are empowered to erase the unknown, turn the tables on attackers and make the world a safer and fairer place.

Learn more about the Vectra platform

About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enable security operations teams to prioritize, investigate and respond to cyber attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyberattacks.

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