Modernize Your SOC — Set Your Pathway into the future without Network Traffic Decryption

An integrated threat signal enables your SOC to move away from network traffic decryption while reliably detecting the most urgent threats.

Encryption is everywhere. Many vendors will lead you to believe that in order to detect attacks in encrypted protocols like HTTPS, you need to perform complicated deployments of performance-intensive SSL decryption. However, the Vectra AI Platform can reliably detect C2, exfiltration and other attack stages without the need for decryption. By leveraging industry-leading artificial intelligence/machine learning (AI/ML), the Vectra AI Platform is able to identify behaviors that attackers perform — even if the communication is encrypted. Unlike other solutions that need to match specific patterns that attacks can arbitrarily change, the Vectra AI platform is powered by Attack Signal Intelligence™, which delivers AI-driven detections that identify the underlying behaviors that must be performed to control an endpoint or exfiltrate data — providing robust detection even in encrypted environments.

Key challenges to consider

Decryption is limited to known threats: Once traffic is decrypted, it is often inspected with known patterns that attackers can easily modify to defeat traditional detection capabilities.

Decryption creates operational complexity: Decryption is operationally complex to perform, requires a great deal of resources and creates operational issues for deployment and compatibility.

Decryption can't be done on everything: Decryption is often not supported on certain types of network equipment like IoT and OT. Company policies may prevent SSL decryption on certain types of websites — and attackers can trick URL categorization engines to bypass SSL inspection.

Why the need for a purpose-built modern threat detection, investigation, & response (TDIR) solution:

- Delivers proven outcomes by leveraging models based on feedback from hundreds or even thousands of organizations to combat against known and unknown threats.
- Provides a holistic view in a single user interface that is ready to go right out of the box.
- A modern hybrid cloud TDIR solution provides the pivotal integrated signal for XDR across all domains including data center network, identity, public cloud and SaaS.

Key criteria to consider

Overcoming decryption challenges doesn't have to be overly complicated or create more work for security teams. Consider the following:

Focus on attack behaviors: Leverage technology that identifies attacker behaviors rather than specific patterns. Since behaviors can be detected within encrypted traffic, all attacks can be detected passively without any onerous requirements.

Collect network metadata: Identify transactions on the network like SSL certificates, negotiations and operations. These can be useful to compliment detections and power threat hunting and discovery use cases.

SaaS detection: Leverage SaaS detection technology to identify behaviors within popular SaaS platforms like M365 and Azure AD.

Keys to success:

Coverage: Reduce hybrid cloud attack latency by unifying and consolidating attack telemetry across the entire hybrid cloud attack surface including identity, public cloud, SaaS and data center networks.

Clarity: Integrated, real-time AI-driven attack signal to automate threat detection, triage and prioritization across your hybrid cloud domains. Shift from event-centric threat detection to entity-centric attack signal. Entity-centric attack signal provides higher-fidelity alerts on hosts and accounts under attack, removing the need to triage hundreds if not thousands of threat events per day. By leveraging a TDIR solution such as the Vectra AI Platform, your SOC team can truly differentiate between benign and malicious true positives, saving countless resources and time while also reducing analyst burnout.

Control: Arm SOC analysts by removing as much deployment complexity upfront to prevent further investigation and response latency in analysts' workflows and put all of the context and controls they need at their fingertips. In addition, leverage co-managed services to add more reinforcements to SOC teams when talent resources are scarce or have limited access to the expertise needed for threat hunting.

If you are tired of relying on legacy decryption methodologies that are overcomplicated and slow down your SOC team, then Vectra AI can help. The Vectra AI Platform provides the most reliable hybrid attack signal that does not depend on the ability to deploy complex and expensive traffic decryption techniques. The Vectra AI Platform delivers the most trusted integrated signal powering extended detection and response (XDR) by providing hybrid attack surface coverage across public cloud, identity, SaaS and data networks through real-time Attack Signal Intelligence that prioritizes entities under attack and integrated, automated, and co-managed response that stops attacks from becoming breaches without the hassle of decryption.

Learn more about the Vectra AI Platform

See the Vectra AI Platform in action

Explore the Vectra AI Platform

Schedule a personal demo of the Vectra AI Platform

About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in 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.

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