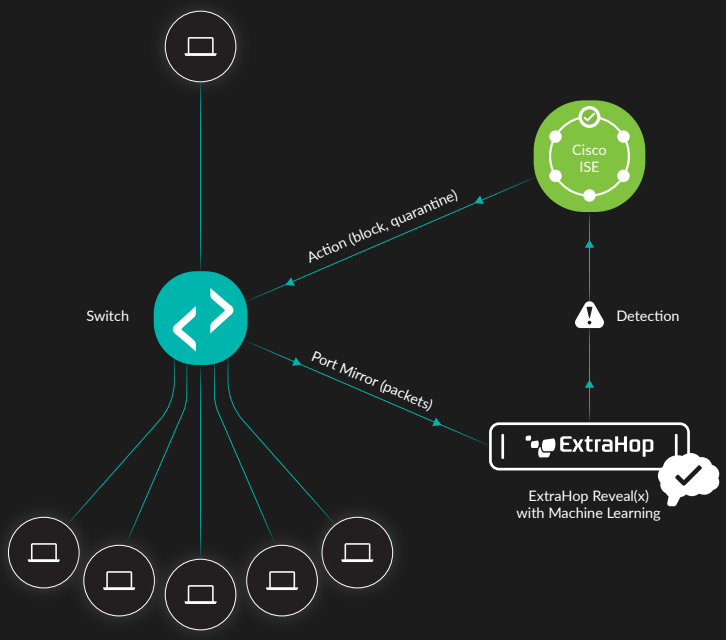
ExtraHop Reveal(x) + Cisco Identity Services Engine (ISE)



CISCO ISE

Automated containment through isolation and quarantine can be critical for minimizing the impact of attacks and suspicious behavior. Alignment of response with corporate policies, processes, and tools helps automation initiatives avoid mistakes, unnecessary risks, or side effects, especially network and system disruption.

ExtraHop® Reveal(x)™ analyzes all network interactions in real time and applies machine learning so that security and performance teams can quickly detect, investigate, and respond to threats. The Cisco® Identity Services Engine (ISE) is a network administration product that enables users to create and enforce security and access policies for endpoint devices connected to routers and switches. When combined with Cisco ISE, Reveal(x) proactively enforces security and access policies based on accurate machine learning-powered detections of threats, anomalies, and performance issues across the enterprise.

Rise Above the Noise Created by Low-Fidelity Data

A network access control product is only as good as the instructions it receives. If your Cisco ISE takes action based on surface-level insight from flow records, you're more vulnerable to threats or unintended consequences. According to Cisco, 70% of attacks in 2019 will hide behind encryption. Reveal(x) detects unusual and undesirable behavior using line-rate decryption of SSL and TLS 1.3 traffic as well as full Layer 2 - Layer 7 payload analysis of rich wire data. By seeing the complete transaction, including malicious activity operating within legitimately encrypted traffic, Reveal(x) can quickly identify an infected device or compromised connection, and then quarantine or block them with Cisco ISE.

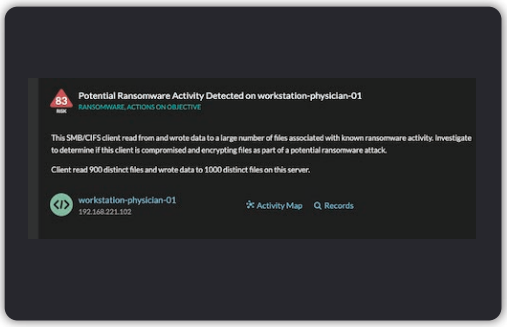
Context Breeds Confidence

Give your team the context it needs to respond with confidence. With so much happening in your enterprise, Reveal(x) network traffic analysis uses auto-discovery and auto-classification to continuously identify critical assets, and provides dynamic groups to support your priorities. Through this lens, Reveal(x) directs your attention to actionable, machine learning-driven detections of suspicious or anomalous behavior, previously unknown threats, and performance issues to your Cisco ISE for automated response. Your team can also drill down into transaction details and use guided investigation workflows to act quickly when human intelligence is needed, allowing you to direct resources to where they matter most.

Reveal(x) is network traffic analysis for the enterprise, built to keep up with all the network traffic your demanding business runs through Cisco equipment. Through a network tap or similar mirroring technology, it analyzes every packet that flows across your enterprise, at up to 100 Gbps. Reveal(x) integrates into your Cisco ISE and the Cisco Platform Exchange Grid (pxGrid) in a few simple steps to create a seamless security solution that improves hygiene, compliance, threat hunting, and more, all while reducing alert fatigue.

ExtraHop® Reveal(x)™ Integration with Cisco® ISE Use Cases

The Reveal(x) integration with the Cisco Identity Services Engine (ISE) slashes the time between discovering a breach and containing it by combining Reveal(x) detections with Cisco ISE's network access and policy enforcement capabilities, including examples like the below.



Ransomware detection in Reveal(x)

Use Case 1: Ransomware Activity

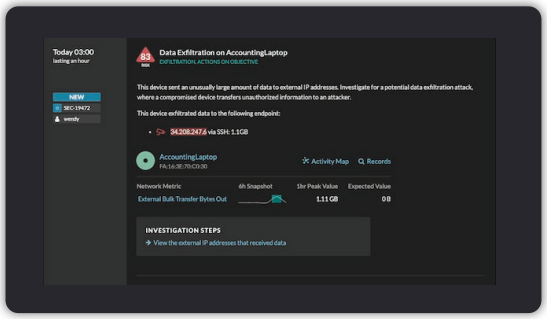
A client device infected by ransomware is using its permissions to access and encrypt files in network-attached storage. By automatically analyzing internal traffic to detect anomalous behaviors in real time, Reveal(x) uncovers this strong attack indicator and creates a trigger to request that your Cisco ISE block the device's network access. With the device isolated, your security team can investigate in Reveal(x) to see when and how the device was infected, identify which files were overwritten, determine if the ransomware spread to other devices, and create an alert that lets you know whenever Reveal(x) detects the extension in the future.

Use Case 2: SQL Injection Exploit

Reveal(x) detects activity from a host that is using encrypted traffic as cover so it can inject SQL commands into a database to trick it into sharing, deleting, or otherwise compromising critical data. Without line-rate decryption, all of the SQL injection's incriminating attributes would have remained hidden. With Reveal(x), those attributes are exposed in real time, and a trigger requests that your Cisco ISE blocks that host's access to the database.

Use Case 3: Data Exfiltration

While monitoring Layer 7 communications in real time, Reveal(x) detects a laptop sending an unusually large amount of data to an external IP address. Reveal(x) identifies the activity as indicative of a data exfiltration attempt, assigns a risk score, and accurately alerts your Cisco ISE to quarantine the device. With the device isolated, your security team can start a guided 1-click investigation to gather more information about the endpoint where the data was sent, in addition to drilling down by protocol and packets.



Data exfiltration detection in Reveal(x)

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com