EXTRAHOP

Security Hardening and Compliance with ExtraHop

Every certificate, every cipher suite, every protocol—used by every device

SOLUTION BRIEF

Establish Comprehensive Visibility | **Auto-Detect Every Device on the Network** | **Audit Weak Cipher Suites in Real Time** | **Detect Expired and Expiring Certificates**

Effective security hardening requires proactive preparation to minimize the enterprise's attack surface and harden its defenses.

The enterprise will need best-of-breed tools in these three categories to achieve the level of real-time visibility that is necessary for world-class security hygiene and compliance.

Auto-Discover Every Cipher Suite, Certificate, and Protocol Version in Real Time

Of the Center for Internet Security (CIS) controls for cybersecurity best practices, the very first one is that every organization should "utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory." ExtraHop RevealX™ is the best way to meet this goal. RevealX automatically detects and classifies all devices communicating across the network by reconstructing every conversation and parsing over 90 enterprise protocols, spotting and tracking outdated protocols, expired certificates, and weak cipher suites. This is a foundational capability for security operations, and RevealX provides it faster, with greater fidelity, than any other NDR product.

Detect Weak Ciphers in Use on the Network in Real Time

Using strong encryption on their internal networks is a must for any company whose data is valuable or regulated. If you handle PCI or HIPAA-regulated data, encrypting is literally required, but everyone should be protecting sensitive data with strong encryption. Since RevealX sees all communications on the network, and parses application-layer (L7) transactions, it can immediately detect when weak cipher suites are in use on the network. Older ciphers like SSLv3, anything using MD5 hashes, and older RSA versions are not sufficient, but they're still in use by many legacy systems, creating serious vulnerabilities for some businesses.

Auto-Discovery and Monitoring Should Encompass the Entire Enterprise Infrastructure.

Perimeter Monitoring

Traditional north-south controls will generate logs and NetFlow, for L2-L4 visibility, letting you know about communications between services and devices and the ports and protocols used. Additional monitoring at the DMZ can provide visibility to application traffic and content leaving the enterprise.

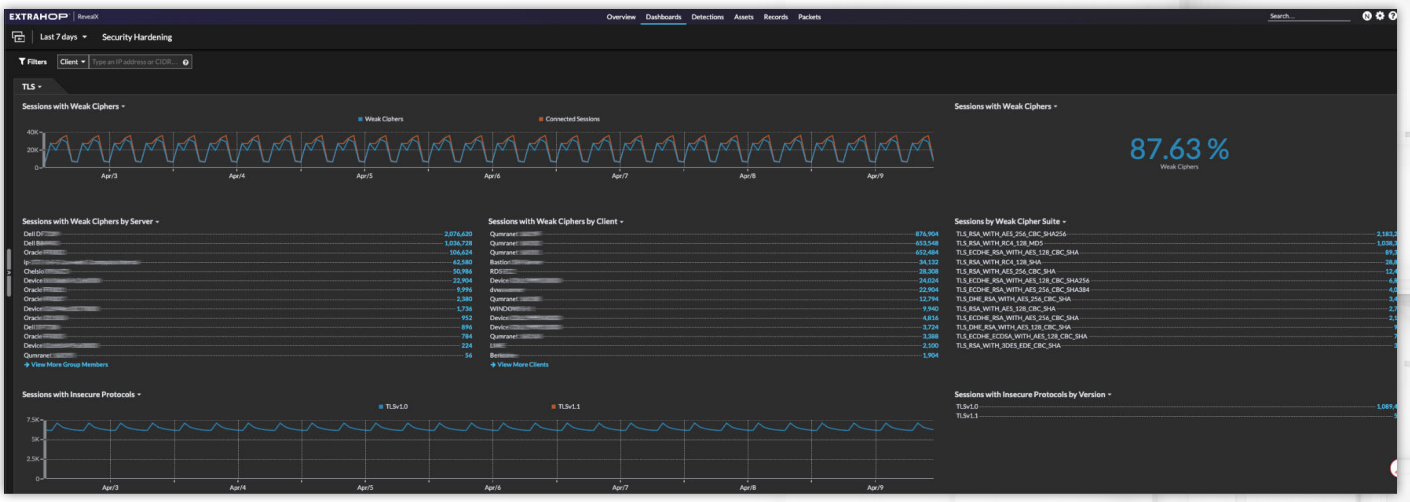
Endpoint Monitoring

Agent-based monitoring can generate logs and insights about what happens within a device, and the user, software, and system activities over time.

Network Traffic

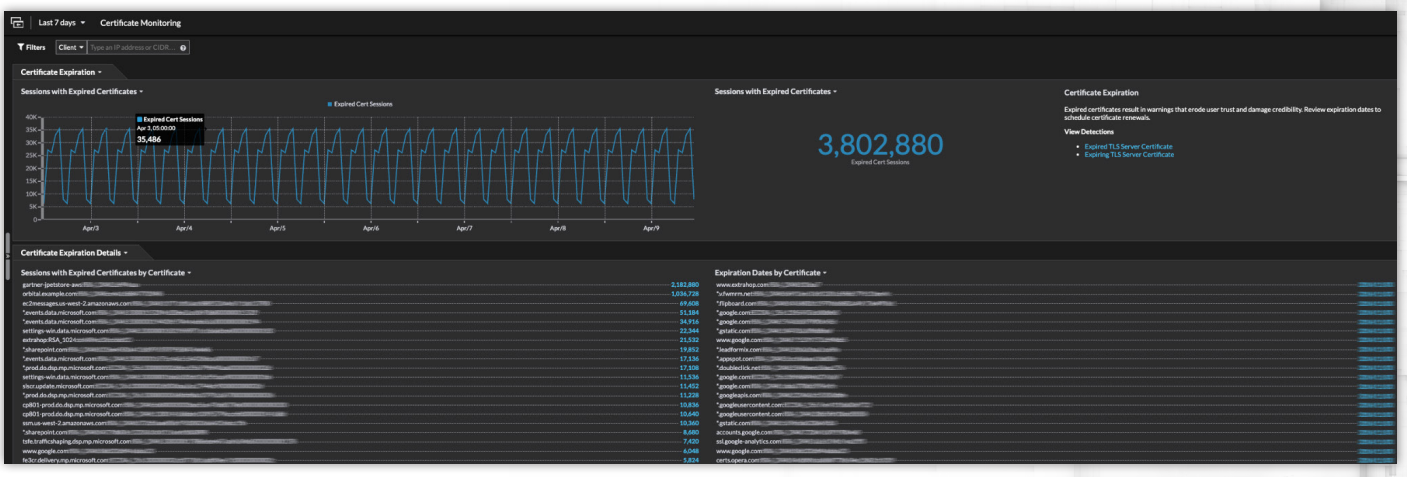
Internal east-west traffic is the least instrumented today, yet it represents a high proportion of enterprise traffic and creates dark space where attackers and insider threats thrive. ExtraHop RevealX offers a solution.

RevealX provides a real-time view into all weak cipher suites in use and can warn SecOps teams when new instances pop up, enabling a level of visibility and control not available from any other audit mechanism.



Detect Expired and Expiring Certificates

Maintaining current SSL certificates is another vital practice for businesses hoping to protect sensitive data. A certificate expiring can set off a chain of events that knocks production applications offline and impacts the bottom line quickly. RevealX can warn SecOps teams when certificates are about to expire (and when they've already expired), to prevent application outages or ongoing security degradation. ExtraHop not only shows you all expired certificates but tracks all sessions using expired certs using pre-built dashboards, so you can prioritize effectively.



Make Compliance Easier to Track and Easier to Improve

By leveraging the **Certificate Monitoring** and **Security Hardening** dashboards, organizations can effortlessly track and bolster their alignment with rigorous standards like **PCI DSS** and **HIPAA**. Unlike traditional tools that rely on static snapshots, ExtraHop utilizes **real, observed wire data to surface weak cipher suites and outdated protocols**. Instead of staring at a flat list of vulnerabilities, you can see exactly how many active sessions are currently using an insecure protocol or a legacy certificate. This granular visibility allows you to **prioritize remediation efforts based on actual usage**, ensuring you tackle the highest-risk exposures first to rapidly improve your security posture and reduce organizational risk.

ExtraHop is an out-of-band, passive solution, meaning that it sees all communications inside the network and conducts analytics in real time without impacting network performance. Hackers can't tamper with it or avoid being seen by it since every sophisticated attack, by necessity, must communicate across the network. RevealX sees these communications and can decrypt them if necessary, parsing TLS 1.3 in real time, even with perfect forward secrecy enabled. RevealX lets SecOps see into the dark spaces that other solutions simply can't uncover.

Launch our live and interactive demo

Take a look at our Security Hardening Dashboard and Certificate Monitoring Dashboard in our online demo.

extrahop.com/demo

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com