ExtraHop

# Strengthen Security Hygiene and Compliance

## Gain Clarity and Confidence in Complex Environments with Reveal(x)

### Enterprises cannot defend what they cannot see

Security hygiene is fundamental. But maintaining the health of your IT environment via cyber defense best practices isn't always easy when it spans on-premises and multiple clouds, serves a remote workforce, and relies on third parties. Add mergers and acquisitions and even basic hygiene can become infinitely more challenging. These factors can create vulnerabilities – from unidentified and unprotected assets to cloud misconfigurations and zero days like Log4Shell – that threat actors look to exploit.

### How to keep up with your ever-changing IT ecosystem

The Center for Internet Security provides a prioritized set of 18 safeguards, known as CIS Controls, to mitigate the most prevalent cyberattacks. These controls are trusted by security leaders in the private and public sectors, and map to major compliance frameworks (such as the NIST Cybersecurity Framework, NIST 800-53, and ISO 27000 series) and regulations (such as PCI DSS, HIPAA, NERC CIP, and FISMA).

### BENEFITS

- Maintain an up-to-date inventory of all networked assets automatically
- Audit vulnerabilities for faster remediation
- Know when threat actors scan for vulnerabilities
- Detect weak ciphers and expired certificates
- Improve efficiency of compliance reporting


### CIS Control #1: Inventory and control of enterprise assets

**The first CIS Control is critical. But for large, complex, dynamic enterprises, asset inventory and control can be extremely difficult. New assets may be installed but not yet securely configured. Unidentified assets may have weak security configurations. Unmanaged personal devices often join a network, then disappear. Cloud environments and virtual machines may be shut down or paused as quickly as they're spun up. If you're using manual approaches to address security hygiene issues, maintaining a current view of enterprise assets may be even more difficult.**

### Automatically maintain an up-to-date inventory of all networked assets

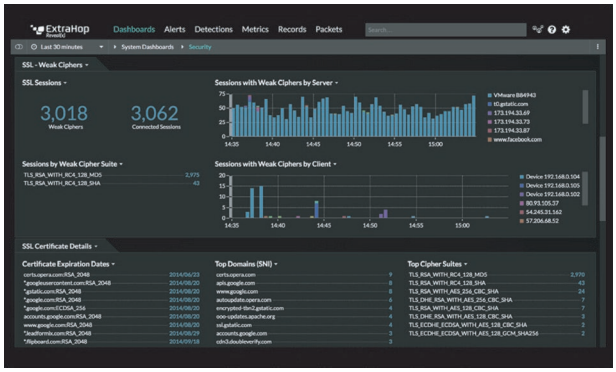
Reveal(x) automatically discovers and classifies all devices communicating on the network in real time. If a device unknown to network operations is acting as a DNS server, this needs to be tracked and investigated. Reveal(x) catalogs all activity for every device and extracts details such as manufacturer, operating system, and user accounts active on the system. Reveal(x) uses this information to detect suspicious behavior, and can also pass it a SIEM to track new or rogue devices or to a firewall to enforce access policies. Reveal(x) monitors network traffic passively and without agents, so there is no performance impact on users or networks, it cannot be detected or compromised by attackers, and is always up-to-date.

## Audit common vulnerabilities, vulnerable devices, and exploit attempts

Threat actors don't have to rely on zero-days. They'll use whatever works. The common vulnerabilities and exposures (CVEs) in CISA's Known Exploited Vulnerabilities Catalog are low hanging fruit. Reveal(x) has purpose-built detections for known network vulnerabilities and helps SecOps teams quickly discover devices that need to be patched. Reveal(x) can identify any suspect devices scanning for vulnerabilities and high-value targets, and alert users to potential exposure if a vulnerability is exploited.

## Detect weak ciphers and expired or expiring certificates

Cipher suites are cryptographic algorithms that determine how data is encrypted and authenticated. When they are weak, they are easier for threat actors to exploit. It is important to disable any weak cipher suites in use, such as DES, 3DES, MD5, and RC4.




SSL certificates help build trust between your customers and your business. They verify the identity of the website or website owner, encrypt the connection between the browser and website, and help ensure a secure experience when customers provide personal data. When a certificate expires, browsers can't verify the authenticity of a website, which may not comply with the latest security standards. Expired SSLs can lead to service outages that affect customer trust.

Proactive SecOps teams monitor when weak cipher suites are in use and when certificates are due to expire. Some solutions require manual upkeep, but Reveal(x) pulls this information in real time. Analysts can also discover which SSL certificates are self-signed and therefore more vulnerable to man-in-the-middle attacks, and which are wildcards and therefore putting all subdomains at greater risk of compromise.

## Improve efficiency of compliance reporting

ExtraHop can help you comply with several important regulations, including but not limited to:

- **Sarbanes-Oxley (SOX)** requires publicly traded companies to safeguard financial information, assure its integrity, protect it via internal security controls, and undergo annual audits.
- **New York Department of Financial Services (NYDFS) Cybersecurity Regulation** outlines requirements for implementing an effective cybersecurity program, including validating encryption controls and obtaining detailed, network-based audit trails.
- **Payment Card Industry Data Security Standard (PCI DSS)** optimizes security of credit, debit, and cash card transactions and protects cardholders against misuse of their personal information. ExtraHop can help you strengthen encryption and network segmentation, eliminate data leakage outside the cardholder data environment, and report on out-of-compliance transactions and devices.

### ABOUT EXTRAHOP NETWORKS

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The ExtraHop Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they can see more, know more, and stop more cyberattacks. Learn more at www.extrahop.com

info@extrahop.com
**www.extrahop.com**