ExtraHop

Accelerate Cybersecurity Mandate Compliance

FEDERAL AGENCIES are coming to grips with a host of new cybersecurity mandates. Complicated requirements, such as automated discovery and full packet retention, can be challenging to implement.

In the push to comply, federal agencies have quickly learned that procuring and deploying single point cybersecurity solutions to meet individual mandate requirements adds cost, complexity, and delays achieving full compliance of all the mandates.

In addition, NetOps teams and SecOps teams often request the acquisition of tools that are easily added to their current workflows but may create problems or add unintended blind spots in other parts of the entire hybrid environment. The question IT leaders must ask is, "Is a tool-centric strategy the best path to full compliance?"

To find an answer to the question, it is useful to focus on the essential factor in all cybersecurity strategies—visibility. To detect and defend against all cyber threats, you need 360-degree visibility and real-time situational intelligence across the entire hybrid environment.

No single point tool can provide that level of visibility. Only a cybersecurity strategy built on a unified platform can achieve it.

A platform-centric approach will enable agencies to unify their security efforts, establish a well-orchestrated cybersecurity posture, and deliver protection across users, servers, endpoints, and the entire hybrid network.

ExtraHop's Reveal(x) platform empowers federal agencies to accelerate and simplify complying with many of the critical cybersecurity mandate requirements. Reveal(x) matches the functionality of many legacy tools currently deployed by federal agencies, saving procurement and maintenance costs, and reducing the need to hire and train staff to monitor single point cybersecurity solutions.

SIMPLIFY COMPLIANCE WITH THE REVEAL(x) PLATFORM

When evaluating the applicability of any tool or platform to accelerate compliance with new cybersecurity mandates, it's helpful to determine how many of the specific requirements in all the current mandates the tool addresses.

ExtraHop's Reveal(x) directly addresses five of the key requirements with which agencies must comply.

Mandates	Requirements	ExtraHop Solutions
M-21-31 BOD 32-01 NIST 800-53	Automated Discovery	Reveal(x) is an NDR solution that automatically discovers and classifies all connected devices and feeds data from the various devices and protocols into one centralized interface with the capability to drill down to and store transaction-level details.
M-21-31 EO 14028 NIST 800-53	Passive Logging	A properly deployed Reveal(x) sensor can easily capture most required data formats, including but not limited to: • DHCP Lease Information • DNA Requests • Load Balancer URLs • Proxy Servers and Content Filter URLs • Authorization Access and Accounting (AAA) • Network Flow Logs • SMB and NFS File Access Records
M-21-31 EO 14028 NIST 800-53 BOD 23-01	Vulnerability Enumeration	ExtraHop provides deep insight into SSL/TLS versions, cipher types, and cipher sizes for all monitored network traffic.
M-21-31 NIST 800-53	Full Packet Retention	Reveal(x) can fully meet the requirement for 72 hours of full packet capture (PCP) and easily scale to longer retention periods as needed and offers a bring-your-own storage option if desired. Reveal(x) properly indexes packets allowing incident responders to quickly search for and access PCAPs as needed.

EXTRAHOP SENSORS deployed in data centers, clouds, and remote sites decrypt and analyze network traffic, using advanced analytics for behavioral analysis, real-time threat detection, and investigation performed in Reveal(x).

90-day lookback provides search capabilities for streamlined incident investigation. Reveal(x) also offers continuous packet capture (PCAP) for in-depth forensics and always-on incident response.

Built-in workflows enable your cyber protection teams to investigate alerts, respond quickly, and share vital information in a few clicks. Reveal(x) is easy to integrate and rapidly deployed.

Reveal(x) enables your agency to meet OMB M-21-31 event logging requirements for network device infrastructure, cloud environments, and application transactions categories.

Reveal(x) fulfills chain of custody and full packet data retention obligations with cost effective storage. Reveal(x) provides the scale and flexibility to achieve retention periods beyond 72 hours at a fraction of the cost of other retention methods.

Protect Your Environment and Your Investment

The value-add provided by Reveal(x) will persist as your infrastructure evolves protecting your investment. Built for enterprise scale Reveal(x) provides complete visibility even when traffic is encrypted. Reveal(x) finds threats in real time, while powerful investigations and forensics capabilities allow you to respond 87% faster.

Achieve Compliance Faster with Reveal(x)

Failure to fully implement the requirements of all the current mandates is not an option. Lives, money, and careers are at risk from an ever-expanding threat landscape. Reveal(x) is a foundational technology that becomes the facilitation platform for accelerating comprehensive mandate compliance.