



## Qualys Enterprise TruRisk Platform Now Accelerates Federal Agency's Zero-Trust Journey with Automated Compliance for OMB M-24-04 and CISA BOD 23-01

May 21, 2024

New update uniquely brings External Attack Surface Monitoring (EASM), risk-based vulnerability management and patch management into a single unified FedRAMP-authorized platform

WASHINGTON, May 21, 2024 /PRNewswire/ -- [Qualys, Inc.](https://www.qualys.com) (NASDAQ: QLYS), a leading provider of disruptive cloud-based IT, security and compliance solutions today announced it is expanding its focus on the government sector by enhancing and operationalizing the capabilities of the Qualys Enterprise TruRisk Platform. This expansion aims to accelerate support for federal zero-trust strategies through automated asset visibility and attack surface risk management as defined by OMB M-24-04, CISA BOD 23-01 and the broader FISMA guidelines.



As defined in EO 14028, federal agencies must show progress in their zero-trust implementation (OMB M-22-09). To further help operationalize zero trust, the OMB released FY24 FISMA Guidance (M-24-04) to focus on the visibility and security of the entire attack surface, specifically on monitoring and real-time reporting on vulnerabilities and threats.

While agencies recognize the value of zero trust, they need to take fundamental steps to progress. Insights from the Qualys Threat Research Unit show that better management of the external attack surfaces is needed as, on average, 31 percent of the assets are unknown to enterprises and agencies, while 45 percent of the assets do not have accurate criticality defined and fail to classify high-value assets (HVA).<sup>\*</sup> This aligns with the OMB M-24-01 directive emphasizing the importance of understanding the attack surface. Further, Qualys analysis shows the mean time to remediate CISA catalog vulnerabilities is over 30 days, while attackers exploit vulnerabilities within an average of five days. This discrepancy underscores the need for agencies to continuously discover their known and unknown attack surfaces, perform effective risk assessments, and prioritize remediation efforts to comply with CISA BOD 23-01.

The Qualys Enterprise TruRisk Platform's integrated solutions, CyberSecurity Asset Management, Vulnerability Management, Detection and Response (VMDR) and Patch Management, now seamlessly help federal agencies fast-track the implementation of zero-trust strategies with continuous compliance and posture visibility into M24-04 and FISMA's broader risk assessment and remediation requirements. With the Qualys platform, agencies get visibility and reporting for all their high-value assets, physically and virtually connected devices, including OT and IoT devices and their applications.

The Qualys Enterprise TruRisk Platform, with its unified view, allows agencies to:

- **Clearly understand the assets and attack surface in compliance with OMB M-24-04:** Qualys allows agencies to discover and inventory both the known and unknown internal and external attack surface of IT, IoT, cloud, and mobile assets across hybrid environments, along with software and applications, including open-source packages, while also identifying high-value assets.
- **Address FISMA patching requirements per CISA BOD 23-01:** In addition to discovering high-value assets, detecting, and assessing vulnerabilities and prioritizing risks according to the CISA catalog, Qualys allows patching from within the same integrated solution to minimize the risk of exploitation of federal assets.
- **Showcase and fast-track measurable progress to zero-trust implementation:** Qualys helps agencies identify and manage the entire attack surface along with integrated detection, prioritization, and remediation of vulnerability risks,

allowing agencies to easily implement FISMA's foundational guidance.

"The administration's push for modernization with zero-trust principles shifts the focus from compliance to visibility of cyber assets and risk management," said Sumedh Thakar, president and CEO of Qualys. "Qualys is committed to helping the public sector as it works to ensure a more secure environment through enhancing and operationalizing the capabilities of our Enterprise TruRisk Platform. This includes fast tracking the federal zero-trust journey by leveraging Qualys solutions to identify and secure high-value assets and automating risk management."

#### **Qualys Public Sector Cyber Risk Conference**

Qualys is hosting its first [Public Sector Cyber Risk Conference](#) in Washington, D.C. today. The conference will emphasize a comprehensive security approach across federal agencies, with a specific focus on High-Value Assets (HVAs), Internet of Things (IoT)/Operational Technology (OT) devices and other internet-connected assets. Notable conference speakers include Paul Selby, chief information security officer at the Department of Energy (DOE), Bailey Bickley, Chief DIB Defense, Cybersecurity Collaboration Center at the National Security Agency (NSA), and Paul Blahusch, chief information security officer at the Department of Labor (DOL), amongst other esteemed public sector luminaries.

#### **Availability**

The enhanced and operationalized Enterprise TruRisk Platform supporting the federal zero-trust journey is immediately available. To learn more, visit [qualys.com/forms/federal-zero-trust](https://qualys.com/forms/federal-zero-trust) or attend our webinar, "Jumpstarting FISMA (M-24-04) Requirements with the Qualys Enterprise TruRisk Platform" at [qualys.com/federal-zero-trust-webinar](https://qualys.com/federal-zero-trust-webinar).

#### **Additional Resources**

- Read our blog post, "[Meeting FISMA \(M-24-04\) Requirements with a Unified Attack Surface Management Strategy](#)"
- Learn more about the [Qualys Enterprise TruRisk Platform for federal agencies](#)
- Follow Qualys on [LinkedIn](#) and [X](#)

#### **About Qualys**

[Qualys, Inc.](#) (NASDAQ: [QLYS](#)) is a leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Enterprise TruRisk Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Oracle Cloud Infrastructure, Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit <http://www.qualys.com>

\* Based on Qualys Threat Research Unit (TRU) analysis of anonymized customer data

*Qualys, Qualys VMDR®, Qualys TruRisk and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.*

#### **Media Contact:**

Rachel Yap Winship  
Qualys  
[Media@Qualys.com](mailto:Media@Qualys.com)

 View original content to download multimedia: <https://www.prnewswire.com/news-releases/qualys-enterprise-trurisk-platform-now-accelerates-federal-agencys-zero-trust-journey-with-automated-compliance-for-omb-m-24-04-and-cisa-bod-23-01-302150845.html>

SOURCE Qualys, Inc.