tenable | Solution Overview

Tenable for Federal Civilian Agencies

Exposure management for federal agencies

Proactively securing the mission in a complex, high stakes environment

Federal agencies face mounting cybersecurity challenges that threaten to undermine mission execution and public trust. Decades-old systems, fragmented infrastructures, and expanding digital footprints have created a complex and dynamic attack surface, one that adversaries are increasingly exploiting.

Meanwhile, evolving mandates and modernization efforts are raising the bar for visibility, accountability, and resilience across federal networks. The National Cybersecurity Strategy and OMB's Federal Cloud Strategy further emphasize proactive risk management, modernization, and measurable progress.

Recent cyber incidents have shown that reactive defenses are no longer enough. Federal agencies need proactive, continuous security that identifies and mitigates risk across their entire infrastructure before they can impact mission critical operations. And that's where exposure management comes in.

Breaking down silos to strengthen security

Federal environments often rely on a patchwork of tools, one for vulnerability management, another for cloud security, another for OT or identity, each managed by different teams with limited visibility into the broader enterprise.

This siloed approach slows response times and creates operational inefficiencies that can leave exploitable gaps across interconnected systems. As IDC's 2025 MarketScape Report notes, "Security teams need to investigate solutions that unify exposures because each exposure does not exist in a vacuum. Exposures may be chained together for initial access or lateral movement."

Attackers don't respect silos, and neither should cybersecurity strategies. Exposure management unifies disparate tools, data and teams into a single, continuous risk picture. By assessing the accessibility, exploitability and criticality of all assets, resources and identities agencies can systematically reduce risk where it matters most.

What is Exposure Management?

Exposure Management is a strategic approach to proactive security designed to improve cybersecurity and risk management outcomes. Exposure management programs continuously identify, prioritize and close an agency"s most urgent cyber exposures - those toxic combinations of preventable risks, including vulnerabilities, misconfigurations and excessive permissions, that if exploited could lead to significant operational disruption or other material impacts.

Rather than reacting to threats after they occur, exposure management empowers agencies to measure, communicate and reduce cyber risk as part of their ongoing mission assurance strategy, directly aligning with federal goals and mandates.data from the start.

Trusted partner to federal agencies

Tenable is a proven partner for federal agencies, combining decades of cybersecurity expertise with a portfolio of FedRAMP-authorized solutions that meet the most stringent government standards. By delivering unified exposure management, proactive risk prioritization, and measurable security outcomes, Tenable empowers agencies to reduce vulnerabilities, secure critical systems, and maintain mission readiness. With Tenable, federal leaders can trust that their cyber defenses are not only resilient but also aligned to the evolving threat landscape and mission objectives.

Exposure Management with Tenable

Tenable One is a FedRAMP authorized exposure management platform that gives federal agencies the insight they need to improve security outcomes, simplify operations, reduce costs and accelerate strategic initiatives like Zero Trust and broader IT modernization. With Tenable One agencies get the following benefits:

Unified visibility across attack surfaces

Gain a continuous, enterprise-wide view of all assets and vulnerabilities across IT, cloud, OT/IoT, web apps and identity systems. This allows agencies to consolidate risk data and insight into a single platform to eliminate blind sports and align visibility with the CDM programs core objectives.

Risk-based prioritization

Not all vulnerabilities pose the same level of risk to mission outcomes. Tenable One combines asset criticality, business impact and potential attack paths, with threat intelligence from Tenable Research to help agencies identify and prioritize the exposures that matter most, enabling more efficient resource allocation and faster risk reduction.

Accelerated Zero Trust maturity

Tenable One directly supports the implementation of the CISA Zero Trust Maturity Model by correlating asset and identify data to enforce principals like least privilege, continuous validation and segmentation. Agencies can pinpoint which vulnerable assets are externally accessible or have elevated domain privileges- critical insight for containing limiting lateral movement and enforcing access controls.

Tool consolidation and cost efficiency

As agencies balance modernization with fiscal responsibility, Tenable One helps consolidate security tools under one unified platform. This reduces complexity and costs and streamlines processes while delivering consistent visibility, reporting and control, key to meeting OMB's IT modernization and efficiency directives.

Operational efficiency and automation

By automating asset discovery, risk prioritization and remediation workflows, Tenable One enables agencies to act fast, even with limited resources. When high profile vulnerabilities emerge, agencies can instantly identify affected assets, prioritize those posing mission risk and initiate guided response actions, all in a single platform with centralized visibility and reporting.

Accountability and measurable progress

Transparency and measurement are central to federal mandates. Tenable One provides metrics that align with FISMA and OMB risk reporting, allowing agencies to track exposure remediation and compliance posture over time. Interactive dashboards and consolidated reports make it easy to demonstrate outcomes to leadership, auditors and oversight bodies.

AI-Driven innovation

Agencies are rapidly adopting AI to drive mission outcomes, but AI itself is becoming an attack surface. Tenable's AI-powered capabilities not only help agencies prioritize threats faster but also discover, monitor, and secure AI assets alongside traditional systems. This forward-looking approach ensures agencies stay ahead of adversaries.

Awards and industry recognition

Tenable has consistently been recognized as a leader in cybersecurity innovation and effectiveness, reflecting our commitment to helping federal agencies stay ahead of evolving threats. Recent accolades include:

- Tenable One was named a leader in the Forrester Wave: Unified Vulnerability Management (UVM), Q3 2025 report
- The IDC Markescape: Worldwide Exposure Management 2025 Vendor Assessment ranked Tenable One as a leader
- IDC has ranked Tenable #1 for the seventh consecutive year in their Device Vulnerability and Exposure Management Market Shares, 2024 report
- Tenable was the only vendor recognized as a Customer's Choice in the 2025 Gartner Peer Insights report for vulnerability assessment

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.