

Activate a Risk Operations Center to Comply with CISA BOD 26-04

Risk-Based Remediation Is Now a Federal Mandate, on a 72-Hour Clock

Blanket Patching Is No Longer a Defensible Strategy

On June 10, 2026, CISA issued Binding Operational Directive 26-04, formally moving federal civilian agencies away from patch-everything programs toward risk-based vulnerability management. The directive responds directly to frontier AI models now capable of discovering and weaponizing software vulnerabilities at speeds that compress exploitation timelines from weeks to hours.

Agencies need visibility at the speed of disclosure, not the next scheduled scan. Under this directive, agencies must remediate the highest-risk exposures within a 72-hours: internet-facing, KEV-listed, fully automatable vulnerabilities that can grant full system control. Before any patch is applied, they must also complete forensic triage to confirm attackers have not already established persistence on the system.

Why Traditional Models Fall Short

Vulnerability disclosures have nearly doubled in three years, climbing from roughly 26,000 in 2022 to almost 50,000 in 2025, and early 2026 data shows the pace accelerating. No team can scale headcount as fast as disclosures multiply, which has mathematically broken the patch-everything model. The gap between average and median time-to-close

is not statistical noise. It is the compounding cost of assets that manual processes cannot reach at speed, what we call the Manual Tax. The Manual Tax begins before remediation, when teams must wait for scan cycles to determine whether a newly disclosed vulnerability affects their environment.

The Whack-a-Mole Trap

Of 48,172 CVEs disclosed in 2025, just 357 (0.74%) were weaponized and added to CISA KEV, and most were neutralized by compensating controls. Teams still burn finite cycles on the wrong vulnerabilities, closing visible tickets fast enough to look defensible while the long tail of forgotten servers, deferred patches, and shadow IT stays exploitable for months. BOD 26-04 retires activity metrics like patch counts for a higher standard: defensible, auditable, evidence-based risk reduction.

only **0.74%**
weaponized
CVEs in 2025

What BOD 26-04 Changes for Federal and State Agencies

BOD 26-04 retires blanket, CVSS-driven patching and supersedes BOD 22-01 and 19-02. Agencies must now prioritize by evidence of risk and defer the rest. Remediation urgency is set by four attributes of a vulnerability:

Asset Exposure Is the asset publicly or internet exposed?	KEV Status Is the CVE on CISA's Known Exploited Vulnerabilities catalog?	Exploit Automation Can an adversary fully automate every step of exploitation?	Technical Impact Does exploitation give partial or total control of the asset?
---	--	--	--

Dynamic Remediation Timelines More attributes met means a shorter deadline. Timelines change as exposure or KEV status changes. All 4 Attributes: ≤ 3 days + forensic triage 3 Attributes: ≤ 3 days, highest urgency tier Exposed / KEV Mix: ≤ 14 days (normal outer Limit) Low-risk / internal: Deferrable to next system upgrade	Compliance Clock Now: Update VM policy and stand up ongoing KEV remediation. 60 days: Update processes and procedures. 180 days: Meet the directive's remediation timelines.
--	---

The Path Forward

Meeting BOD 26-04 takes more than faster and selective patching. It takes an operating model that continuously answers one question: what risk matters most right now, and how quickly can we reduce it? A Risk Operations Center (ROC) unifies AI-speed detection, hyper-prioritization, and zero-day remediation into a single closed loop that continuously proves risk reduction.

The ROC Maps Directly to the Core Requirements of BOD 26-04

Qualys delivers a unified, AI-powered platform to power the ROC, eliminating tool sprawl so security and IT operate as one. The Qualys Government Platform is FedRAMP High authorized, with 400+ inherited technical controls to streamline FISMA, OMB, and Zero Trust reporting, and it moves agencies beyond compliance to sustainable, mission-aligned cybersecurity.

BOD Requirement	ROC Capability
Risk-based prioritization	Context-driven, exploitability-aware triage
Focus on KEV and active threats	Integrated threat intelligence and validation components
Continuous assessment	Real-time detection and monitoring
Demonstrable risk reduction	Verified remediation and validation loops
Operational efficiency	Automation and workflow integration

AI-Speed Detection Detect exposures at the speed of disclosure.	Hyper-Prioritization Cut the noise. Prove exploitability from network to endpoint.	Zero-Day Remediation Remediate at machine speed, with operational control.
Qualys Platform	Qualys ETM	Qualys TruRisk Eliminate
<ul style="list-style-type: none"> • InstaScan identifies affected assets within minutes of a new advisory using existing inventory, telemetry, and threat intelligence. • High-confidence findings are validated using existing Qualys agents, scanners, sensors, and imported third-party telemetry. • Six Sigma detection accuracy across endpoint, cloud, container, and OT. • Faster, confidence-scored exposure signals feed TruRisk and downstream remediation workflows. • Digital certificate and CIS configuration assessment built in. 	<ul style="list-style-type: none"> • TruRisk and TruLens layer threat, business, and environmental context into ranked exposure queues. • TruConfirm validates vulnerabilities across both network-exposed and endpoint-local attack surfaces. • KEV-aligned, mission-weighted prioritization of every exposure. • Agent Val automates high-risk CVE validation, prioritizes confirmed exposures, and revalidates remediation to prove closure. • Theoretical risk filtered down to validated, reachable risk. 	<ul style="list-style-type: none"> • AI-powered Patch Reliability Scores assess patch stability and evolve with new evidence. • Agent Sara organizes remediation into waves: Easy Fixes, Connectivity-Sensitive, Operational Risk, and Beyond Patching. • Patchless options including mitigate, customize, uninstall, fix, and isolate reduce exposure when a reliable patch is unavailable. • Continuous revalidation proves every attack path is closed. • Forensic-aware workflow aligned to BOD 26-04 triage requirements.
#1 coverage for CVEs, KEV	99% noise reduction	#1 Patch Management Vendor (GigaOm)

Qualys ETM: Powering the Federal ROC

885 Critical
TruRisk™
Score



Security & Risk Findings Risk Identification				Built-in Threat Intel Feeds, Enriched With In-House Vuln Research				CMDB, Custom Data Sources	
Qualys		Non-Qualys		Threat Intelligence				Business Context	
✓ Vulnerability	✓ App Security	Vulnerability Management							
✓ Configuration	✓ Asset Management	Compliance							
✓ Compliance	✓ Attack Surface	Runtime Security							
✓ Cloud Security	✓ AI Security	Application Security							
Measure Quantify Cyber Risk in Business Terms				Communicate Executive Reporting & Ticketing				Eliminate Patch Mitigate & Track	



Ready to Meet BOD 26-04?

Operationalize continuous, auditable risk reduction. See how Qualys powers a Risk Operations Center for your agency.



Get a Briefing

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and 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. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit qualys.com