

SECOND EDITION · ALIGNED TO FY2026 FEDERAL CYBER DIRECTIVES

Delivering Efficiency in Cyber Risk Management for Federal Agencies with a Risk Operations Center

Executive Summary

Risk Operations Center

A ROC delivers efficiency by unifying:

- **Asset inventories**
- **Risk signals**
- **Mission details**
- **Threat intelligence**

...into a single platform.

What's New in this Edition

- FY2026 CISA BOD and Emergency Directive landscape
- Current Executive Order requirements
- Department of War CSRMC, Cyber Strategy, and CIO direction
- Qualys ETM agentic AI and Q-FLEX licensing
- FedRAMP High Impact ATO and FedRAMP 20x

Federal agencies now face a widening gap between the volume of exposures they can see and the less than 1% that attackers actually weaponize. The mean time to remediate sits at 43 days while adversaries move from discovery to exploit in hours. Weaponization of Frontier AI like Mythos has only accelerated the problem. The attack surface keeps expanding across cloud, container, OT, identity, and AI workloads, and large organizations now run dozens of security tools to watch it. More tools have not closed the gap. They have fragmented it.

Policy has responded by putting exposure management on a clock. BOD 26-04 replaced severity-based patching with risk-based criteria. BOD 23-01 sets 7-day discovery and 72-hour reporting. Emergency Directives against actively exploited edge products compress response to days. EO 14409, issued in June 2026, directs the establishment of an AI cybersecurity clearinghouse to coordinate vulnerability scanning, validation, remediation prioritization, and patch distribution, and tasks CISA with expanding agency access to AI-enabled defensive tools — a signal that federal cyber defense is expected to operate at machine speed. Alongside these, existing Executive Orders push secure software attestation, post-quantum readiness, and machine-readable evidence, while the Department of War's CSRMC shifts authorization from periodic paperwork to continuous proof. Every one of these mandates asks the same three questions: what do we operate, what is wrong with it, and which of those problems is being exploited right now.

An agency running dozens of un-integrated tools cannot answer those questions inside a 72-hour window. A Risk Operations Center (ROC) can, because asset inventory, risk signals, threat intelligence, mission context, and remediation workflow all draw on one data model. Rather than pushing every finding into the patch queue, the ROC surfaces the validated, reachable exposures — those confirmed exploitable on assets that matter to the mission — so agencies direct scarce remediation effort at the riskiest exposures first. Agentic AI compounds that advantage: agents absorb the repetitive scoping, correlation, validation, and ticketing that consume analyst hours during a directive response, driving down both the cost and the time to remediate by an order of magnitude while humans retain decision authority over what gets fixed, mitigated, or accepted.

Qualys Enterprise TruRisk Management is purpose-built for this model, delivered on a FedRAMP High authorized government platform with 400+ inherited controls and Q-FLEX licensing that lets agencies unlock new capability against a new mandate without waiting on an acquisition cycle. This paper maps the current directive landscape to ROC capabilities and lays out a path to standing one up.

Growing Exposures: The Case for Risk-Based Efficiency

Too Many Findings, Siloed Tools, Faster Attacks

The cybersecurity landscape has reached a critical inflection point. Over the last four years, the volume of critical vulnerabilities has surged by [650%](#), while the mean time to exploit has collapsed to [-7 days](#) in 2026. Attackers exploit exposures faster than ever, yet security teams remain trapped monitoring dashboards from disparate tools. This fragmented environment creates data silos, conflicting priorities, and an overwhelming volume of alerts, making a cohesive view of organizational risk impossible.

Tool sprawl compounds the problem. Large enterprises now manage an average of [76 security tools](#), and federal agencies face the same pressure: reactive adoption of point products for each emerging threat and each new mandate, layered on vendor-driven expansion of un-integrated stacks. Teams remediate the loudest alerts rather than the most critical risks, and genuinely dangerous vulnerabilities stay open far longer than necessary.

The Gap Is Widening, Not Closing

Successive editions of the Verizon Data Breach Investigations Report have tracked exploitation of known vulnerabilities growing as an initial access vector, with edge and perimeter devices a particular focus. Over the same period the median time organizations take to fully remediate those exposures has not kept pace, and the remediation within the categories attackers favor most has deteriorated.

Fixing the Wrong Risks Without Prioritization

This fragmented ecosystem makes prioritization and mission context essential. Security teams face limited resources and overwhelming workloads, leaving them forced into reactive firefighting rather than focusing on the most critical threats. Without a unified platform, teams juggle fragmented data and make decisions without the context needed to quantify risk and align effort with the agency's mission. A [2024 Government Accountability Office report](#) note that fewer than half of federal agencies achieve effective cybersecurity ratings annually.

Growing Exposures: The Case for Risk-Based Efficiency

The Efficiency Imperative: A Unified Risk Management Approach

Federal agencies, suppliers, and highly regulated organizations operate under unique constraints — strict budget cycles, compliance mandates, and mission-critical operations — that demand a fundamentally different approach to cyber risk management. Traditional risk management programs fail because they treat all threats as equal and lack the context needed for true prioritization.

The solution requires a paradigm shift to a unified, risk-based model that recognizes that not all vulnerabilities pose the same risk. It integrates asset inventories and risk signals into a single view, enriched with threat intelligence and mission context, so agencies can prioritize remediation by mission impact, cut through the noise, and focus scarce resources on protecting what matters most.



6X

Post-Mythos CVE count in July 2026 Microsoft Patch Tuesday



0.74%

Weaponized CVEs out of the 48K published in 2025.



43 days

MTTR to resolve a vulnerability, while attackers weaponize in hours



Adversary cycle

Hours

discover → weaponize → exploit



Legacy defender cycle

Weeks to months — scan windows, manual triage, approvals, quarterly cycles

The time gap between the two is the exposure window.

The Federal Mandate Landscape

Sorted by directive type (Binding Operational Directives first, then Executive Orders / OMB memos), latest first within each group.

Federal cyber policy has shifted from periodic self-assessment toward continuous, evidence-backed operations on fixed clocks. Binding Operational Directives set recurring discovery and reporting intervals. Emergency Directives, issued when a widely deployed edge product comes under active exploitation, have repeatedly required agencies to inventory affected devices, apply mitigations, and report status within days — occasionally within hours.

That tempo is a direct response to the widening exploitation window, and it is the real test of an agency's architecture. An agency running dozens of un-integrated tools cannot reliably answer "which assets do we own, which are affected, and what is their current state" inside a 72-hour window. A Risk Operations Center can, because the inventory, the risk signal, the threat context, and the remediation workflow all draw on one data model. Sorted by directive type (Binding Operational Directives first, then Executive Orders / OMB memos), latest first within each group.

Binding Operational Directives & Emergency Directives

Directive/Authority	Core Requirement	ROC Capability That Delivers It
BOD 26-04 CISA, June 10, 2026	Supersedes BOD 19-02 and BOD 22-01. Requires agencies to prioritize vulnerability remediation using four risk criteria: asset exposure, KEV status, exploit automation, and post-exploitation technical impact. Vulnerabilities meeting all four criteria require remediation and forensic triage within 3 calendar days. Other risk combinations follow 14- or 60-day remediation timelines, while the lowest-risk vulnerabilities may be deferred to the next scheduled system upgrade.	A risk-based prioritization engine continuously evaluates asset exposure, KEV status, exploit automation, and technical impact, then enforces workflows for the 3-day critical tier and applicable 14- and 60-day remediation timelines.
BOD 25-01 CISA, Dec 2024	Apply CISA's SCuBA secure configuration baselines to Microsoft 365 tenants and maintain continuous assessment of configuration drift.	Configuration and compliance scanning with continuous drift detection and audit-ready evidence for cloud productivity tenants.
BOD 23-02 CISA, Jun 2023	Remove internet-exposed networked management interfaces from the public internet, or protect them by zero trust controls, within 14 days of identification.	External attack surface management continuously identifies exposed interfaces and shadow IT; policy audit confirms the corrected state.
BOD 23-01 CISA, Oct 2022	Asset discovery every 7 days, vulnerability enumeration every 14 days, and results reported to CISA's CDM Federal Dashboard within 72 hours.	Unified asset inventory across IT, cloud, OT/IoT, containers, web apps, and external attack surface, with continuous enumeration and automated reporting.
Emergency Directives e.g., ED 25-03, ED 26-03	Rapid inventory of a specific affected product, mitigation or disconnection, and status reporting on compressed timelines measured in days.	Software and hardware inventory queried in minutes rather than weeks; agentic workflows scope affected assets and open remediation tickets automatically.

Executive Orders & OMB Memoranda Directives

Directive/Authority	Core Requirement	ROC Capability That Delivers It
EO 14409 The White House, June 2, 2026	Promoting Advanced Artificial Intelligence Innovation and Security. Directs Treasury, in consultation with the National Cyber Director, NSA, and CISA, to establish an AI cybersecurity clearinghouse within 30 days to coordinate vulnerability scanning, validation, remediation prioritization, and patch distribution with industry and critical-infrastructure partners. Directs CISA to issue BODs and guidance that accelerate civilian federal cyber defense and expand access to AI-enabled defensive tools. It also establishes a classified benchmarking process for identifying covered frontier models, with a separate voluntary developer-engagement framework. The order creates no mandatory AI licensing, pre-clearance, or permitting requirements.	AI-enabled detection and exploitability validation align with the clearinghouse's intended workflows for coordinated vulnerability discovery, validation, remediation prioritization, and patch distribution. Automated remediation orchestration can operationalize relevant vulnerability and patch intelligence as authorized sources and integrations become available.
EO 14144 & EO 14306 The White House, Jan 2025 / Jun 2025	Strengthen secure software development practices and attestation, advance post-quantum cryptographic readiness, secure federal AI use, and move toward machine-readable policy.	Cryptographic and software inventory, AI workload security, and machine-consumable compliance evidence rather than document-based attestation.
EO 14028 The White House, May 2021	Modernize federal cybersecurity, adopt zero trust, improve software supply chain security, and standardize incident response.	Continuous visibility and software composition analysis feed both zero trust enforcement and supply chain assurance.
OMB M-22-09, M-24-04, M-25-04 OMB	Federal zero trust architecture strategy and annual FISMA reporting guidance, including metrics on asset management and vulnerability remediation timeliness.	Compliance and executive reporting produce the underlying metrics continuously, with detailed audit trails.

The Federal Risk Operations Center: Transforming Risk Management

Introducing the Risk Operations Center (ROC)

A ROC provides continuous, risk-based visibility across the entire attack surface — from discovery through remediation — while ensuring compliance with regulatory and organizational requirements. It redefines cyber risk management by shifting from a reactive, siloed approach to a proactive, integrated framework. This approach not only improves operational efficiency, it strengthens security in critical government functions: safeguarding against evolving threats, meeting compliance requirements on the clocks those requirements now set, and sustaining public trust.

The Federal Risk Operations Center (ROC)



Necessary Components of a Federal ROC

Unified Asset Inventory Comprehensive asset discovery is the foundation of any cyber risk management process. By identifying and cataloging all assets, agencies ensure a unified view of risk posture across the attack surface.

Risk Factor Aggregation Risks from multiple environments — cloud, applications, on-premises infrastructure — are consolidated into a centralized platform, creating a complete picture of the threat landscape.

Threat Intelligence Enrichment

The ROC enriches risk data with real-time threat intelligence to understand which vulnerabilities are being actively exploited, ensuring informed decision-making.

Mission Contextualization

By quantifying risk in business and mission terms, the ROC enables agencies to assess potential loss magnitude in financial value and align decisions with mission objectives.

Operational Benefits for Federal Agencies

Operational Efficiency

Cut through the noise and focus on the risks that really matter, while consolidating point tools into a unified risk management platform in the cloud with FedRAMP High ATO to reduce technology and operational costs.

Improved Security Posture

By addressing the truly risky vulnerabilities and cutting down MTTR, agencies deploying a ROC take away the opportunity attackers depend on.

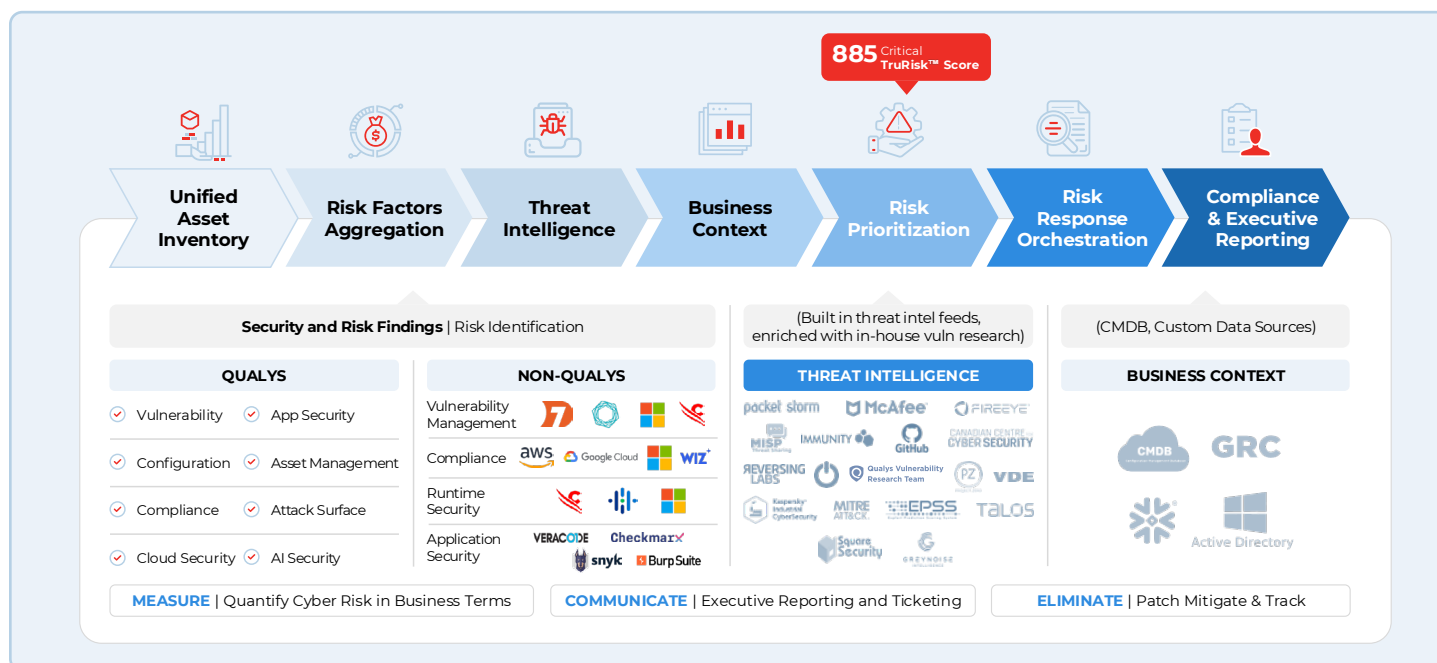
Resource Optimization

Moving to a proactive approach reduces the strain reactive security places on staff, freeing resources for strategic initiatives aligned to the agency's mission.

Qualys Enterprise TruRisk™ Management

Qualys Enterprise TruRisk Management (ETM): The World's First AI-Native Solution Built for the ROC, represents the culmination of decades of risk management innovation. As the industry's first comprehensive platform purpose-built for the ROC, ETM transforms complex risk data into actionable intelligence that drives measurable security improvements — and produces the continuous evidence that current federal directives increasingly demand.

How Qualys ETM Capabilities Power the ROC Directives



Unified Asset Inventory

Unified Asset Inventory Qualys ETM offers complete visibility into the attack surface by consolidating data from its integrated asset inventory, including Qualys Cyber Security Asset Management (CSAM), External Attack Surface Management (EASM), and third-party sources. This provides a real-time view of assets across the environment, from multi-cloud to on-premises — the capability that makes BOD 23-01-style discovery and reporting intervals achievable without manual reconciliation.

Risk Factor Aggregation Qualys ETM aggregates risk findings from diverse asset types, including virtual machines, Operational Technology and Internet of Things (OT/IoT) devices, cloud environments, codebases, and user identities. Agencies can leverage Qualys Vulnerability Management, Detection and Response (VMDR), Cloud Security Posture Management (CSPM), Web Application Scanning (WAS), Software Composition Analysis (SCA), and more to consolidate risk signals into a holistic perspective.

Threat Intelligence Enrichment Qualys ETM enhances aggregated risk data with over 25 real-time threat intelligence sources, including insights from Qualys Threat Protection's Live Threat Intelligence Feed, providing an up-to-date risk assessment against the current threat landscape. When an Emergency Directive lands, the affected product is already correlated to the assets that run it.

Together, these three capabilities answer the question every current federal directive ultimately asks: what do we operate, what is wrong with it, and which of those problems is being exploited right now?

Prioritizing the Risk That Matters

Severity scores alone do not tell an agency what to fix first. A vulnerability with a moderate CVSS rating that is actively exploited by named threat actors on an internet-facing mission system is a materially larger problem than a critical-rated flaw with no exploit code, no malware association, and no observed activity. Threat context inverts the queue.

Mission Contextualization By adding business context, Qualys ETM enables agencies to quantify cyber risk in terms of monetary and mission impact. Agencies can use ETM Asset Tags and Business Entities to evaluate loss attributes and Value at Risk (VAR), ensuring risk management is aligned with mission goals rather than raw finding counts.

Risk Prioritization Qualys ETM brings together exposure data from Qualys and third-party sources to turn theoretical severity into actionable risk. TruRisk and TruLens add threat intelligence and business context, while TruConfirm safely validates exploitability across network and endpoint attack paths. Agent Val continuously identifies high-risk CVEs, directs validation to affected assets, automatically prioritizes confirmed exposures, orchestrates remediation, and revalidates each exploit path to prove closure.

CVE Prioritized with Threat Context

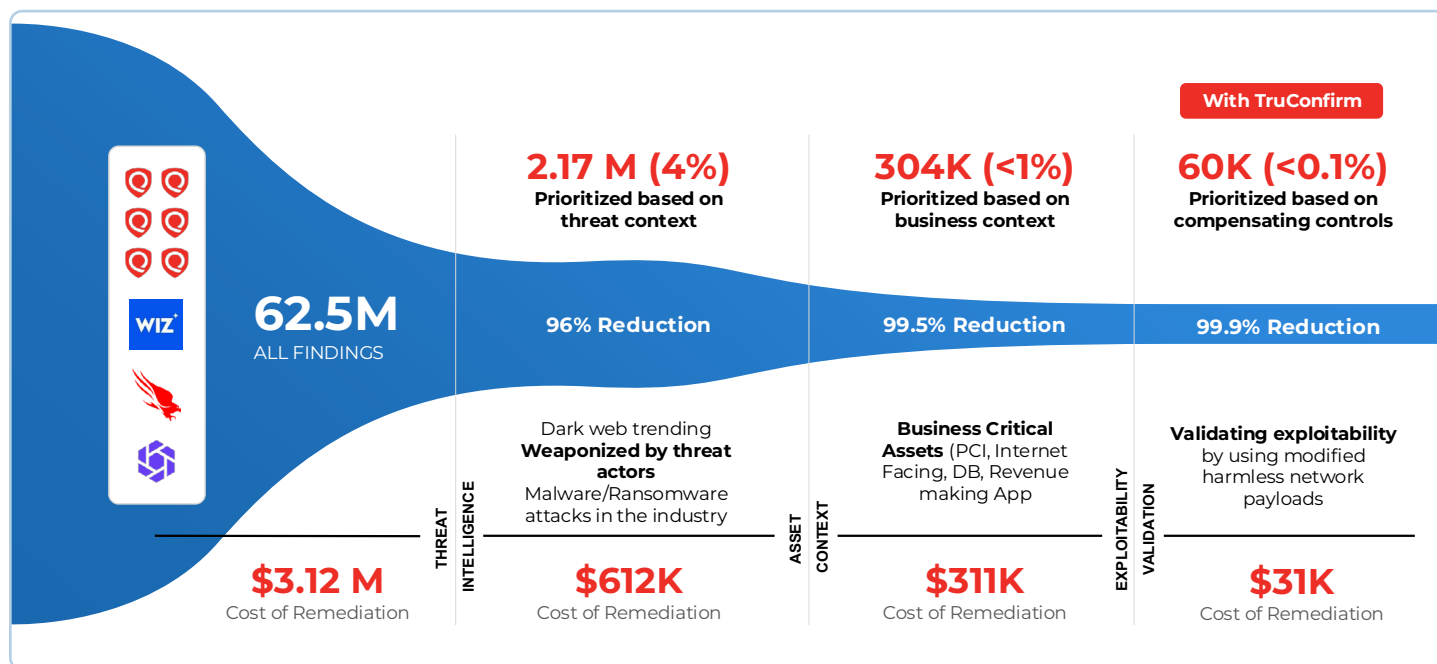


CVE Deprioritized with No Threat Context



Examples of CVEs prioritized higher or lower based on threat context

Detection to Prioritization to Hyper-Prioritization



Note - Representative data from a large Enterprise Customer

From Prioritization to Response

Cutting through the noise with the Qualys risk prioritization funnel, using assets, threats, and business context. The example above uses real numbers from a large organization.

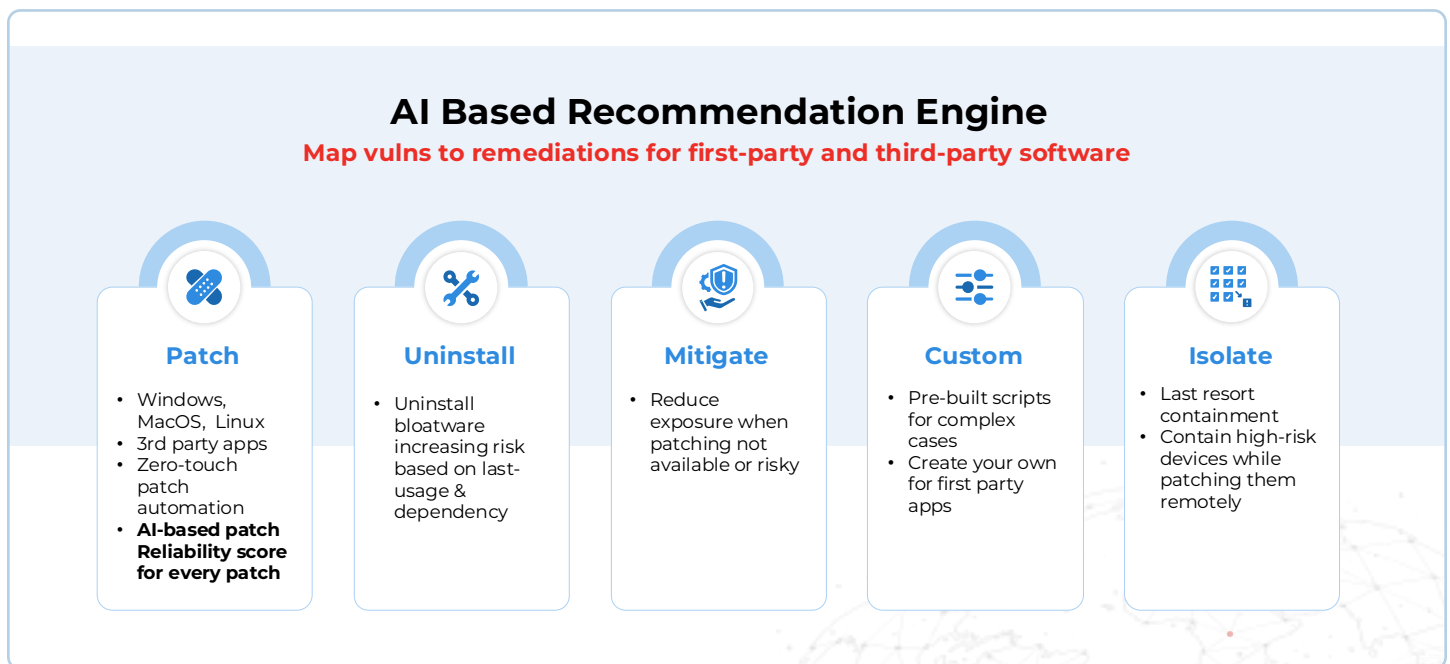
Risk Response Orchestration Qualys ETM automates precise risk response through TruRisk™ Eliminate's AI-driven workflows, enabling appropriate action based on flexible remediation options. Agencies can generate automated tickets and deliver real-time alerts, eliminating risk efficiently, reducing manual effort, and ensuring timely mitigation. Where a patch is not immediately available or cannot be applied to a mission system inside a maintenance window, mitigation, isolation, and uninstall provide directive-compliant alternatives with a recorded justification.

Compliance and Executive Reporting Qualys ETM ensures continuous compliance readiness with Qualys Policy Audit and File Integrity Monitoring, offering tailored executive reporting and detailed audit trails to meet standards such as NIST SP 800-53, NIST CSF 2.0, DISA STIGs, CISA Binding Operational Directives, DoW Zero Trust, and other federal mandates. Because the evidence is generated continuously rather than assembled for an audit, the same data serves the agency's FISMA metrics, its directive status reporting, and its authorization package.

Compliance and Executive Reporting

Qualys ETM ensures continuous compliance readiness with Qualys Policy Audit and File Integrity Monitoring, offering tailored executive reporting and detailed audit trails to meet standards such as NIST SP 800-53, NIST CSF 2.0, DISA STIGs, CISA Binding Operational Directives, DoW Zero Trust, and other federal mandates. Because the evidence is generated continuously rather than assembled for an audit, the same data serves the agency's FISMA metrics, its directive status reporting, and its authorization package.

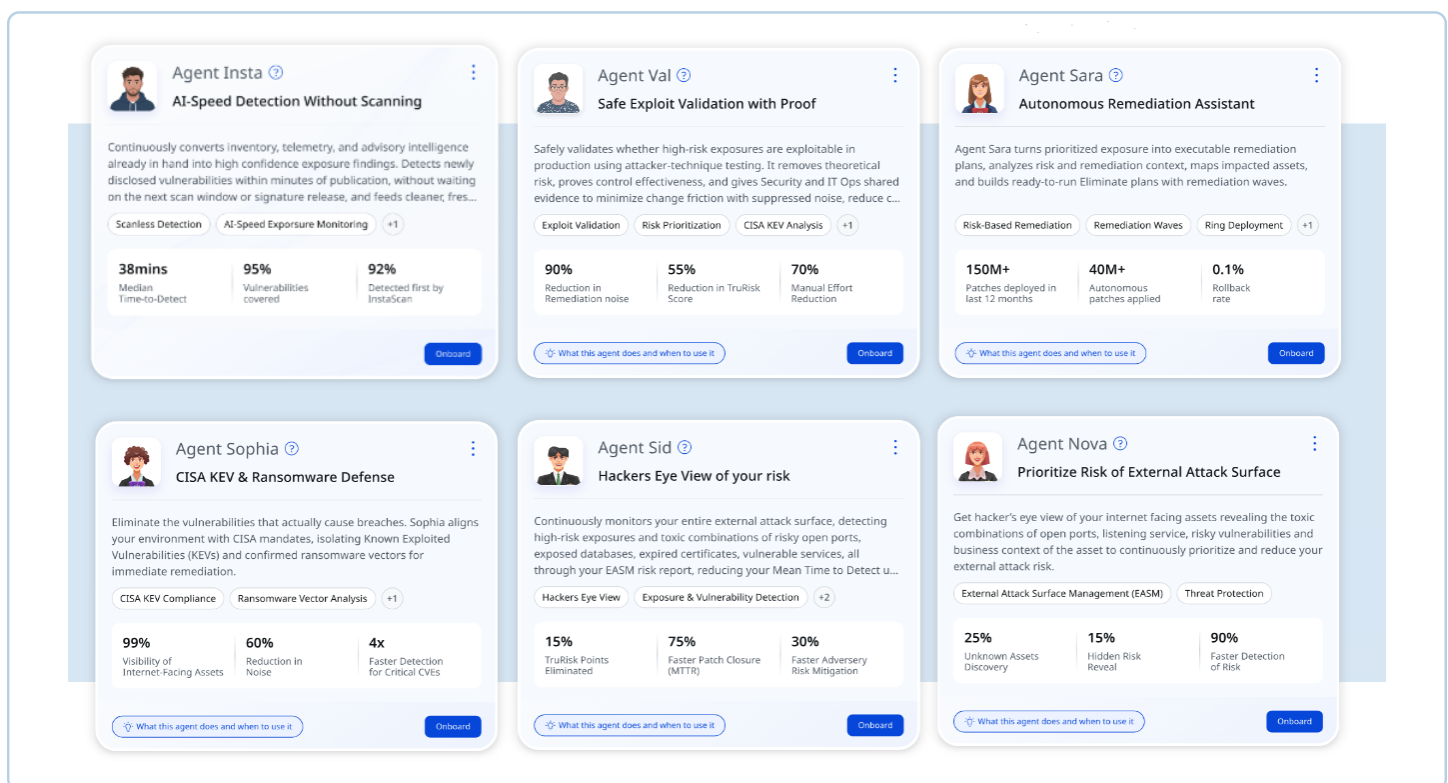
TruRisk Eliminate: Remediate with Six-Sigma Accuracy



Qualys TruRisk Eliminate remediation options

Built-in Agentic AI for Autonomous Risk Management

Enhanced with agentic AI for increased efficiency, Qualys ETM includes a marketplace of pre-built Cyber Risk Agents that automate common risk management workflows. These specialized agents act as a skilled digital workforce, augmenting security teams to accelerate risk mitigation. The platform also includes a Cyber Risk Assistant — an intuitive, prompt-based interface — that further empowers teams to translate complex exposure data into clear, context-driven actions with autonomous execution. For federal teams, the practical value is throughput. Agents handle the repetitive scoping, correlation, and ticketing work that consumes analyst hours during a directive response, while humans retain decision authority over what gets remediated, mitigated, or accepted. Every agent action is recorded, which matters when the resulting evidence has to survive an audit.



Flexible Licensing for Efficiency and Cost Optimization

Qualys provides a flexible licensing model called Q-FLEX that allows organizations to apply and transfer Qualys Units (QLUs) across the breadth of platform capabilities as agency needs change. As new Binding Operational Directives and Executive Orders are issued, the QLU model lets agencies transfer licenses to unlock additional platform features immediately, without waiting on a new acquisition cycle to procure another tool. That elasticity is a direct answer to the tempo problem described earlier in this paper. When a directive arrives with a two-week clock, the binding constraint is rarely analytical capability — it is procurement. **Q-FLEX** removes that constraint, allowing organizations to optimize platform utilization while adapting quickly to evolving requirements.

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

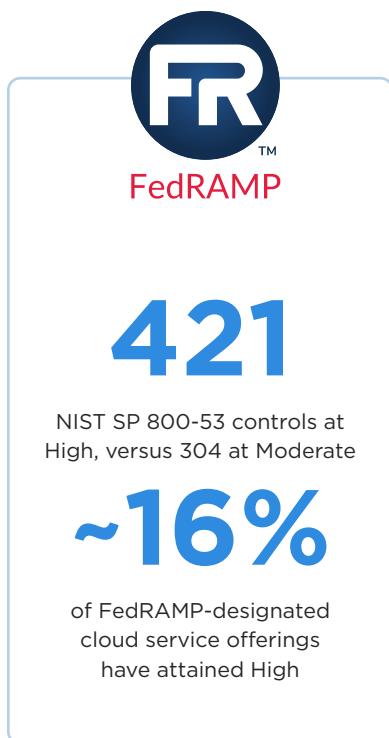
Qualys delivers a unified, AI-powered platform to power the ROC, eliminating tool sprawl so security and IT operate as one. The Qualys Government Platform is FedRAMP High authorized, with 400+ inherited technical controls to streamline FISMA, OMB, and Zero Trust reporting, and it moves agencies beyond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

Binding Operational Directives & Emergency Directives

BOD Requirement	ROC Capability
Risk-based prioritization	Context-driven, exploitability-aware triage
Focus on KEV and active threats	Integrated threat intelligence and validation
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 VMDR + ETM <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 #1 coverage for CVEs, KEV	Qualys ETM <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 99% noise reduction	Qualys TruRisk Eliminate™ <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 Patch Management Vendor (GigaOm)

FedRAMP High Impact ATO



Achieving FedRAMP High ATO remains one of the most formidable milestones in cloud service compliance. It is critical because systems at this level handle extremely sensitive federal data, where a breach could lead to severe or catastrophic consequences.

FedRAMP High mandates around 421 NIST SP 800-53 controls spanning comprehensive control families including, Access Control, Contingency Planning, System and Communications Protection, and System and Information Integrity — significantly more rigorous than the Moderate or Low baselines.

As of late July 2025, the FedRAMP Marketplace listed 585 cloud service offerings with FedRAMP designations, but only 95 — roughly 16% — had attained High-level designation. That underscores both the elevated bar for High-impact systems and the growing agency demand for secure, highly resilient cloud offerings, especially as modernization, AI workloads, and risk classifications continue to evolve.

With this ATO, Qualys is one of the few cybersecurity platforms offering a full-spectrum security solution — asset inventory, vulnerability management, patch management, compliance, EDR, policy enforcement, container security, web application security, and more — at the FedRAMP High Impact ATO level.

Meeting Directive Obligations on the Platform Itself

The unified risk management platform from Qualys also helps agencies meet obligations under multiple Binding Operational Directives, including BOD 23-01 and OMB guidance such as M-24-04. CISA advises that any organization committed to improving cybersecurity maturity and reducing risk should consider implementing BOD 23-01 practices, as it reflects researched best practice for eliminating blind spots and mitigating breaches — advice that applies equally to state, local, and commercial organizations not formally bound by it.

FedRAMP 20x and the Move to Automated Evidence

FedRAMP's ongoing modernization effort is pushing authorization toward automated, continuously validated, machine-readable evidence rather than periodic document packages. This is the same direction of travel as CSRMC on the defense side and the machine-readable policy themes in recent Executive Orders. Agencies that adopt a ROC now are building the evidence pipeline these programs will assume, rather than retrofitting it later.

A Path Off On-Premises Infrastructure

For organizations still operating on-premises security infrastructure, this presents an opportunity to move to the cloud, saving cost and gaining operational efficiency. The FedRAMP High ATO government platform lets organizations leverage a highly secure unified platform for cyber risk management, reduce cost, avoid the overhead of managing on-premises infrastructure, and benefit from the latest capabilities and threat intelligence inherent in a cloud solution.

Conclusion: Launching Your Risk Operations Center

A 90 - DAY LAUNCH PATH

Days 1-30

Establish truth

Deploy unified asset inventory across IT, cloud, OT/IoT, containers, and external attack surface. Reconcile against the CMDB and retire duplicate discovery tooling.

Days 31-60

Add context

Aggregate risk signals from Qualys and third-party sources, enrich with threat intelligence, and apply asset tags and business entities to encode mission criticality.

Days 61-90

Automate response

Stand up orchestration workflows for patch, mitigate, isolate, and uninstall; enable Cyber Risk Agents for repetitive scoping; publish continuous directive and FISMA reporting.

The cybersecurity challenges federal agencies and their suppliers encounter demand innovative approaches that balance security effectiveness with operational efficiency. The Risk Operations Center framework provides a methodology for transforming risk management from a resource-intensive burden into a strategic capability — one that answers directive questions in hours rather than weeks.

Qualys Enterprise TruRisk Management delivers the technology foundation necessary to implement this transformation immediately. With FedRAMP High Impact ATO and a flexible licensing model that allows agencies to leverage the broader platform, Qualys enables agencies to launch their ROC with confidence and achieve measurable efficiency and security improvements.

Transform your agency's cybersecurity posture today. Launch your Risk Operations Center with Qualys Enterprise TruRisk Management and join the growing number of federal agencies achieving operational excellence through risk-based security.

Related Qualys Research

[How Federal Agencies Can Activate a Risk Operations Center \(ROC\) to Meet CISA BOD 26-04](#)

[Why Every Enterprise Needs a Risk Operations Center \(ROC\)](#)



For more information about implementing a Risk Operations Center at your agency, **contact Qualys** or visit **qualys.com**.

About Qualys

Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers, managed service providers, and consulting organizations. The company is also a founding member of the Cloud Security Alliance (CSA).