

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

Federal agencies, suppliers, and commercial organizations seeking the highest levels of cybersecurity face mounting cybersecurity challenges due to a lack of visibility, accuracy, and resources. As digital transformation accelerates, the attack surface grows, driven by an increasing number of vulnerabilities and misconfigurations across the digital infrastructure.

But only a fraction of these vulnerabilities are actively exploited by threat actors, leading to alert fatigue and draining resources. This gap between volume and actual risk highlights a serious disconnect—defenders are being pulled in too many directions while attackers stay focused on what works.

Risk Operations Center (ROC)

A Risk Operations Center offers a solution by unifying:

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

into a single platform.

Compounding the issue is a fragmented security environment, with scarce security resources trying to reconcile multiple tools that create data silos, conflicting priorities, and enormous inefficiencies. This slows response times, raises costs, and weakens security. A Risk Operations Center (ROC) offers a solution by unifying asset inventories, risk signals, mission details, and threat intelligence into a single platform. The ROC transforms reactive, volume-based remediation into a multi-layered, risk-based defense, bringing enormous operational efficiencies to agencies by enabling them to focus on critical threats, optimize resources, and strengthen security posture and compliance.

Growing Exposures: Need for a Risk- Based Approach for Efficiency

Too Many Findings, Siloed Tools, Faster Attacks

The cybersecurity landscape has reached a critical inflection point. Agencies contend with an exponential growth in reported vulnerabilities—a 39% increase from 2023 to 2024—and an ever-expanding attack surface. Attackers are exploiting exposures faster than ever, yet security teams are trapped in a constant churn of monitoring the dashboards from disparate tools. This fragmented security environment creates data silos, conflicting priorities, and an overwhelming volume of alerts, making it impossible to gain a cohesive view of organizational risk.

This fragmentation leads to reactive, inefficient decision-making and delayed response times. Teams are stretched thin, remediating to the loudest alerts rather than the critical risks. Without a method to unify risk signals, evaluate, and prioritize them, remediation efforts become scattered and ineffective, and critical vulnerabilities are left unaddressed for far longer than necessary.

Fixing The Wrong Risks Without Prioritization

This fragmented ecosystem makes prioritization and mission context essential for effective risk management. Security teams face limited resources and overwhelming workloads, leaving them stretched thin and forced into reactive firefighting rather than focusing on the most critical threats. Without a unified platform, teams are forced to juggle fragmented data and make decisions without the context needed to quantify risks and align efforts with the agency's mission. A unified approach is key—one that prioritizes risks based on impact to the mission, enabling seamless remediation orchestration across teams, and providing actionable insights to reduce both risk and complexity.

The Efficiency Imperative: A Unified Risk Management Approach

Federal agencies, suppliers, and highly regulated organizations operate under unique constraints including strict budget cycles, compliance mandates, and mission-critical operations that demand a fundamentally different approach to cybersecurity 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. This approach recognizes that not all vulnerabilities pose the same risk. It integrates asset inventories and risk signals into a single, unified view, enriched with threat intelligence and mission context. By understanding the potential financial or mission impact of a vulnerability, agencies can prioritize remediation efforts, cut through the noise, and focus valuable resources on protecting what matters most. This ensures that security efforts are aligned with mission resilience and long-term success.

Key Statistics Highlighting the Challenge:

39%

YoY Increase Discovered

There are more than 300,000 reported CVEs, of which over 40,000 CVEs were discovered in 2024 alone, a 39% YoY increase

0.61%

Weaponized Exploit Code

Less than one percent (0.61%) of these newly published vulnerabilities have weaponized exploit code

>90%

Reduction in Cost / Effort

By focusing remediations on less than 4% of the exposures after risk-based prioritization

12 Days

Exploitation Opportunities

The average time to remediate (MTTR) CISA KEV vulnerabilities is 30.5 days, while attackers weaponize them in an average of just 18.5 days

18.5 Days Time to Weaponize

Exploitation Opportunities

12 Days

30.5 Days Mean Time to Remediate

The 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, but also strengthens security in critical government functions, safeguarding against evolving cyber threats, meeting compliance requirements, and ensuring public trust.

The Risk Operations Center (ROC)



Necessary Components of a ROC:

- **Unified Asset Inventory:** Comprehensive asset discovery is the foundation of any cyber risk management process. By identifying and cataloging all assets, agencies can ensure a unified view of their 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 agencies' threat landscape.
- **Threat Intelligence Enrichment:** The ROC enriches risk data using real-time threat intelligence to understand which vulnerabilities are being actively exploited, ensuring informed decision-making.
- **Mission Contextualization:** By quantifying risks in business and mission terms, the ROC enables agencies to assess the potential loss magnitude in financial value and align their decisions with mission objectives.
- **Risk Prioritization:** The ROC highlights the most critical risk combinations using custom risk scoring, helping teams focus their remediation efforts where they matter most.
- **Risk Response Orchestration:** Automated predefined workflows are triggered to mitigate or eliminate risks by patching, applying configurations, or isolating compromised assets.
- **Compliance and Executive Reporting:** Continuous compliance monitoring ensures audit readiness for regulatory standards like NIST 800-53, the Health Insurance Portability and Accountability Act (HIPAA), and PCI DSS 4.0. Selecting vendors with FedRAMP High Impact Authorization to Operate (ATO) ensures coverage of the 421 NIST SP 800-53 High baseline controls, compared to 325 controls at the Moderate level. Tailored executive reporting, especially for the latest compliance requirements, gives clear leadership insights into risk exposure and mitigation efforts.

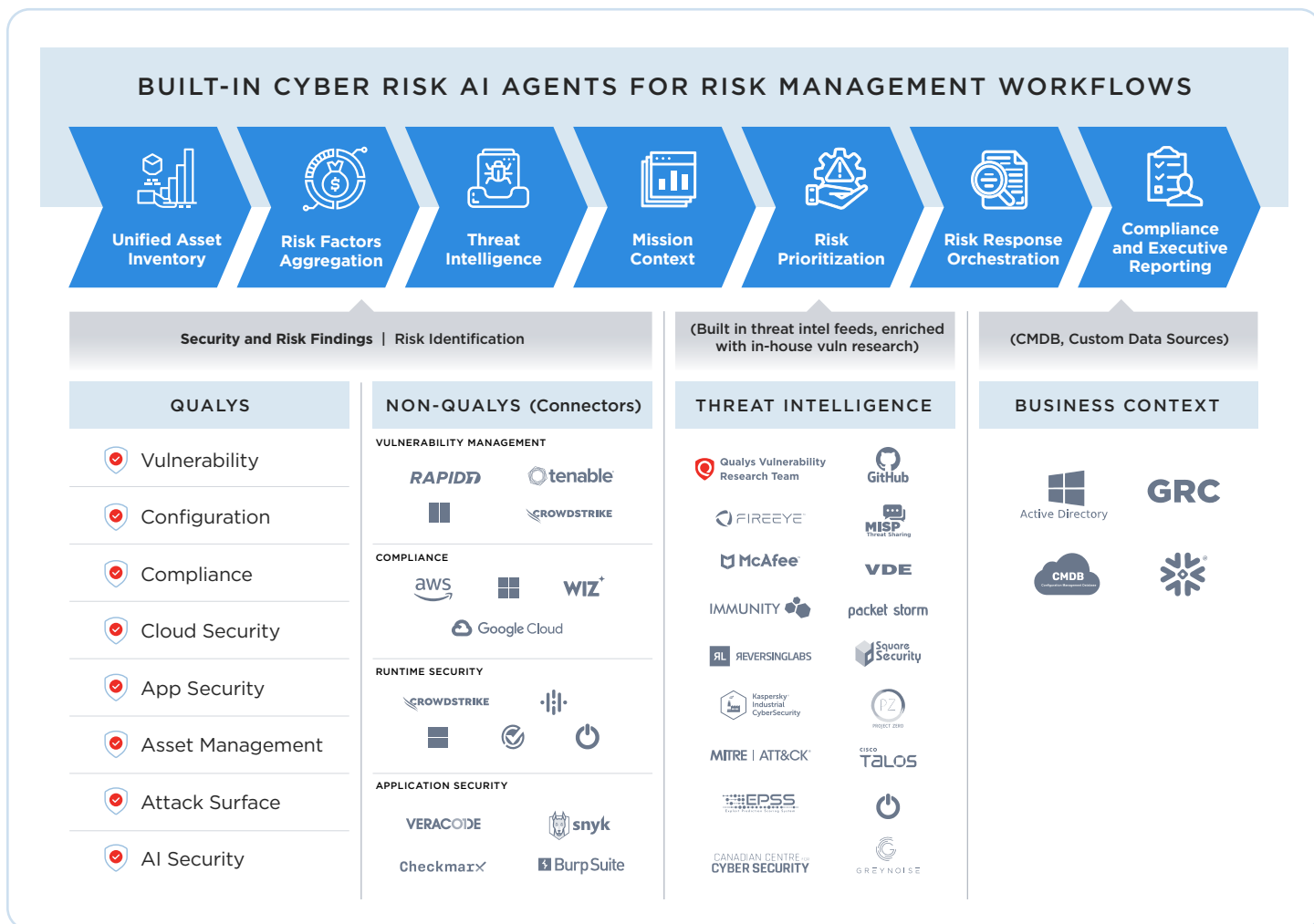
Operational Benefits for Federal Agencies

Implementing a ROC offers many benefits to help agencies, suppliers, and other firms achieve their mission objectives, including:

- **Operational Efficiency:** Cut through the noise and focus on the risks that really matter, while also 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 the MTTR, agencies deploying a ROC take away the opportunity of attackers to exploit.
- **Resource Optimization:** By moving to a proactive approach, the ROC reduces the strain on resources posed by reactive security measures, allowing the resources to focus on more strategic initiatives aligned to the agency's mission.

Qualys Enterprise TruRisk™ Management: The World's First AI-Native Solution Built for the ROC

Qualys Enterprise TruRisk Management (ETM) 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.



How Qualys ETM Capabilities Power the ROC

- **Unified Asset Inventory:** Qualys ETM offers complete visibility into your attack surface by consolidating data from its integrated asset inventory, including Qualys CyberSecurity Asset Management (CSAM), External Attack Surface Management (EASM), and third-party sources. This offers a real-time view of assets across your environment, from multiclouds to on-premises.
- **Risk Factor Aggregation:** Qualys ETM aggregates risk findings from diverse asset types, including virtual machines, Operational Technology/Internet of Things (OT/IoT) devices, cloud environments, codebases, and user identities. Agencies can leverage Qualys Vulnerability Management, Detection & Response (VMDB), Cloud Security Posture Management (CSPM), Web Application Scanning (WAS), Software Composition Analysis (SCA), and more to consolidate risk signals for a holistic risk perspective.
- **Threat Intelligence Enrichment:** Qualys ETM enhances an agency's aggregated risk data with over 25 real-time threat intelligence sources, including insights from Qualys Threat Protection's Live Threat Intelligence Feed, providing up-to-date risk assessments with the latest threat landscape.

CVE Prioritized with Threat Context

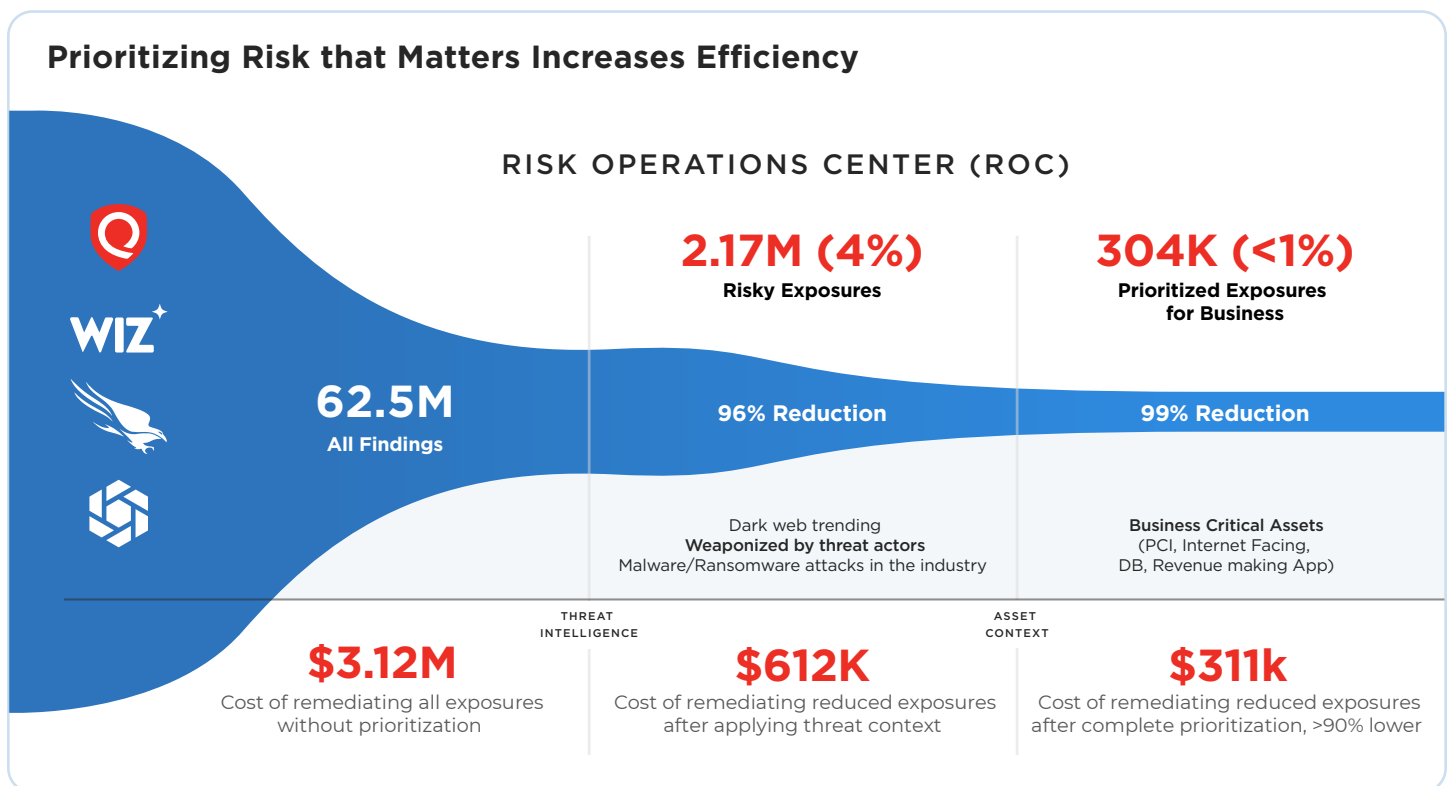


CVE Deprioritized with No Threat Context



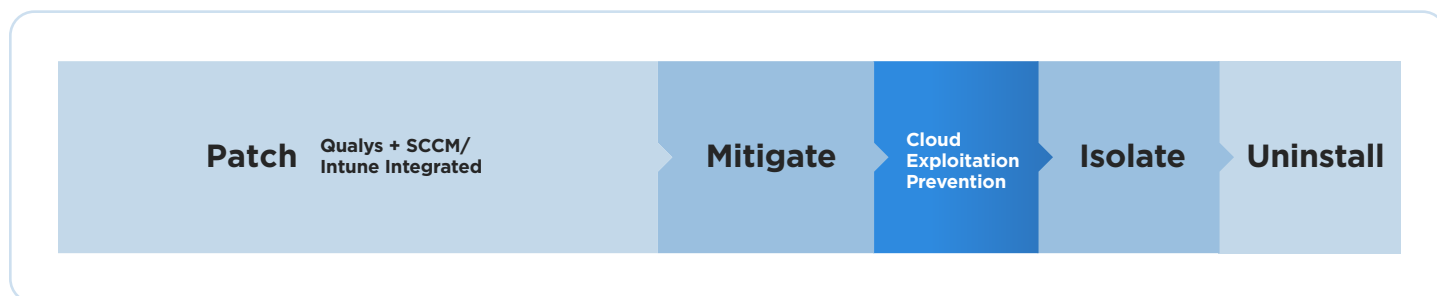
Examples of CVEs prioritized higher or lower based on threat context

- **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 business goals.
- **Risk Prioritization:** Qualys ETM prioritizes risks using the TruRisk™ Score, which factors in severity, exploitability, asset criticality, and business impact for a focused understanding of which risks pose the greatest threat to the agency.



Cutting through the noise with Qualys' risk prioritization funnel with asset, threat and business context.
The above example is based on real numbers from a large organization.

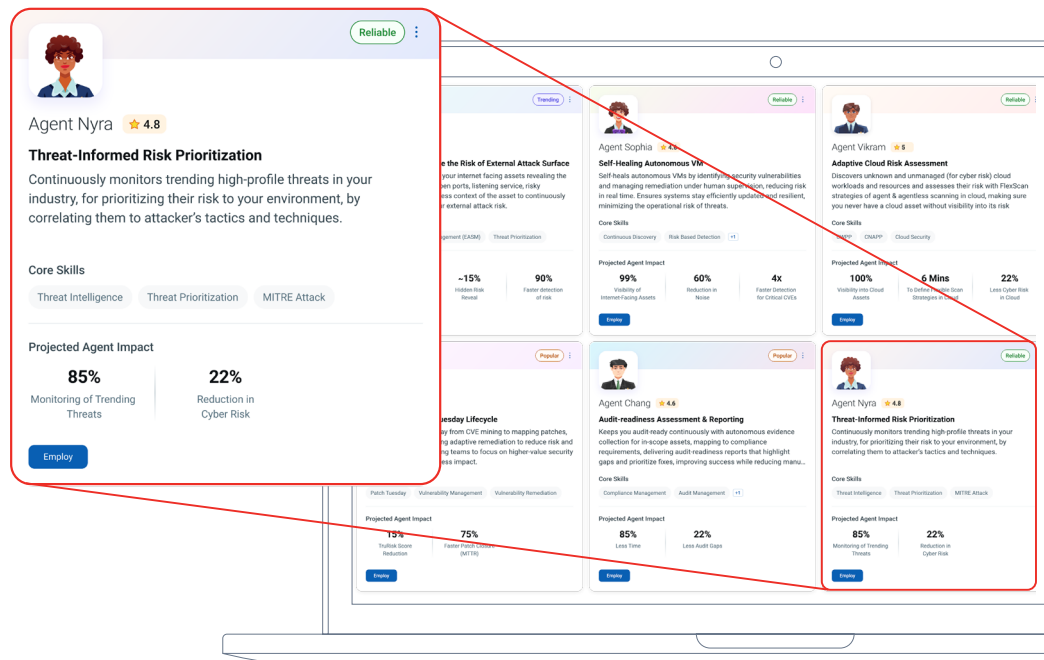
- **Risk Response Orchestration:** Qualys ETM automates precise risk response through TruRisk™ Eliminate's AI-driven workflows, enabling appropriate action based on flexible remediation options. Agencies can generate automated tickets and deliver real-time alerts. This eliminates risks efficiently, reducing manual effort and ensuring timely risk mitigation.
- **Compliance and Executive Reporting:** Qualys ETM ensures continuous compliance readiness with Qualys Policy Audit and File Integrity Monitoring by offering tailored executive reporting and detailed audit trails to meet regulatory standards such as NIST 800-53, NIST CSF 2.0, DISA STIGs, Binding Operational Directives (BODs), DoD Zero Trust, and other federal mandates and frameworks.



Qualys TruRisk Eliminate remediation options

Built-in Agentic AI for Autonomous Risk Management

Enhanced with Agentic AI for increased efficiency, Qualys ETM comes with a marketplace of pre-built Cyber Risk Agents that automate common risk management workflows. These specialized Cyber Risk Agents act as your skilled digital workforce and augment your security teams to accelerate risk mitigation. The platform also comes with 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.



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) to any of the broad platform capabilities, depending on the changing needs of the federal agency. As new binding directives (BODs) and Executive Orders (EOs) come up, the QLU model empowers agencies to easily transfer the licenses to unlock additional features of the platform, without needing to wait to acquire additional tools. This allows organizations to optimize the utilization of the platform while quickly adapting to evolving needs.

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 breaches could lead to severe or catastrophic consequences. FedRAMP High mandates around 421 NIST SP 800-53 controls, spanning comprehensive control families like Access Control, Contingency Planning, System & Communications Protection, and System & Information Integrity, significantly more rigorous than Moderate or Low baselines. As of late July 2025, the FedRAMP Marketplace lists 585 cloud service offerings (CSOs) with FedRAMP designations, but only 95 (about 16%) have attained High-level designation. This underscores both the elevated bar for High-impact systems and the growing demand from agencies for secure, highly resilient cloud offerings, especially as modernization, AI workloads, and risk classifications continue to evolve.

With this ATO, Qualys becomes 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.

The unified risk management platform from Qualys also helps meet compliance for multiple Operational Directives (BODs) such as BOD 23-01 and OMB M-24-04. CISA advises that any organization committed to improving cybersecurity maturity and reducing risks should consider implementing BOD 23-01 as it offers researched best practices to ensure compliance and mitigate breaches.

For organizations still operating using on-premises infrastructure, this also presents a perfect opportunity to move to the cloud, saving costs and bringing operational efficiencies. The FedRAMP High ATO Government Platform empowers organizations to leverage a highly secure unified platform for cyber risk management, reduce costs, and gain operational efficiency by not having to manage on-premises infrastructure, and benefit from the latest capabilities and threat intelligence inherent in a cloud solution.

Launching Your Risk Operations Center

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.

Qualys Enterprise TruRisk Management delivers the technology foundation necessary to implement this transformation immediately. With FedRAMP High Impact ATO, and a flexible licensing model, 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.



For more information about implementing a Risk Operations Center at your agency, [contact Qualys](#) or visit qualys.com.

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.