Qualys

WHITEPAPER

Transforming Modern Cybersecurity

How the Risk Operations Center (ROC) Redefines Risk Management with Qualys Enterprise TruRisk™ Management (ETM)

Table of Contents

Executive Summary

In today's digital age, the complexities and uncertainties surrounding enterprise risk management have reached unprecedented levels. The traditional approaches to managing these risks—often reactive, siloed, and narrowly focused—are no longer adequate to protect organizations from the multifaceted threats they face.

The Risk Operations Center (ROC) emerges as a pivotal response to these challenges, redefining how enterprises approach risk management with a holistic, integrated practice that spans across all domains of risk, unlike traditional fragmented approach. At the heart of the ROC's effectiveness is the platform that transforms this theoretical concept into a practical, operational reality.

This whitepaper explores how Qualys Enterprise TruRisk Management (ETM), world's first cloud-based Risk Operations Center, represents a fundamental shift in how enterprises approach risk management and examines the key challenges of fragmented risk management. As the digital landscape continues to evolve, the future of cybersecurity risk management lies in the strategic integration of people, processes, and technology that transcend traditional, reactive approaches.

Introduction

"**A problem well defined is a problem half solved.**" – *Charles Kettering*

In today's modern enterprises, risk management has evolved into a critical discipline—one that must account for an ever-expanding array of uncertainties. Organizations are swamped with risks originating from multiple sources—cyber threats, operational disruptions, and financial losses. The challenge becomes worse by the siloed tools, leaving security teams struggling to determine which threats are most critical to the business. IT and development teams are overwhelmed with alerts, while security teams are often paralyzed by not knowing where to begin. This fragmented approach leaves organizations vulnerable, as critical risks can slip through the cracks, with potentially devastating impacts on the business. Yet, the common thread remains—risk is fundamentally about managing uncertainty and loss.

In cybersecurity, this uncertainty is particularly acute as the concept of risk is often reduced to a checklist of vulnerabilities or compliance requirements. But risk, in its truest form, is far more complex. Cyber risks are not just potential vulnerabilities; they represent plausible future losses that could disrupt or derail the business. These risks are no longer confined to IT departments or security operations centers (SoCs); they permeate every aspect of an organization's operations, influencing decisions from the boardroom to the data center.

This is where traditional risk management, which often involves siloed functions operating independently, falls short. It focuses on the immediate, the tangible—patching a vulnerability, meeting a regulatory compliance requirement—without fully accounting for the broader implications.

With interconnected threats and business processes, organizations require a new practice—one that integrates risk management across all domains, providing a cohesive strategy to navigate this uncertainty. This is where the Risk Operations Center (ROC) emerges as a pivotal practice, redefining how enterprises approach risk.

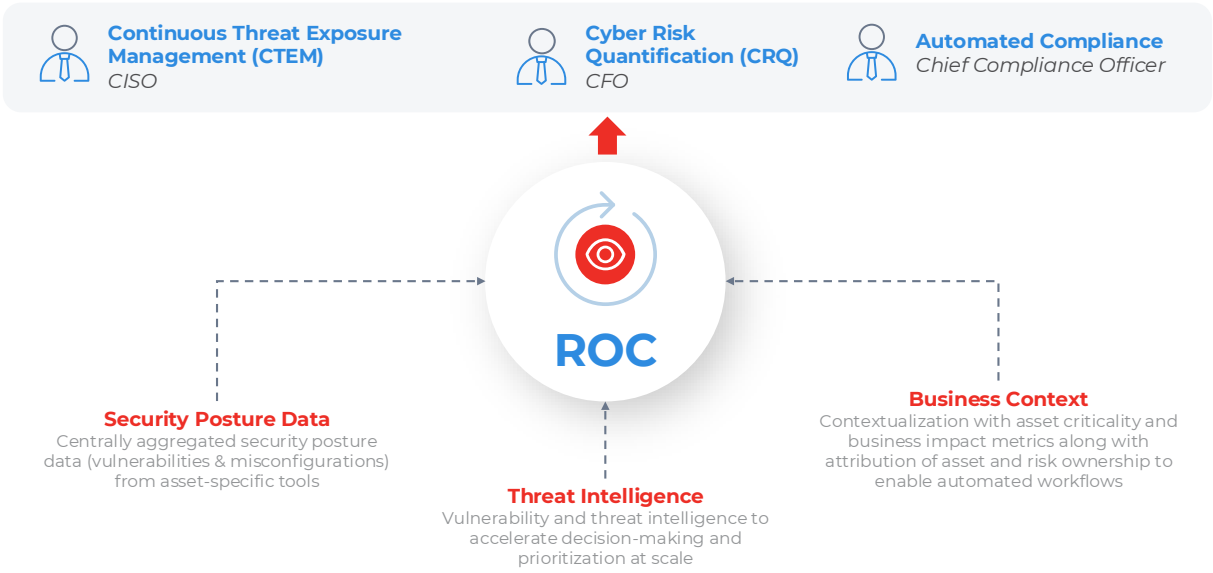
Introducing the Risk Operations Center

The Evolution of Risk Management

The Risk Operations Center (ROC) represents a fundamental shift from reactive, isolated risk management to a proactive, integrated practice that monitors and responds to changes in the enterprise's risk surface in real-time. Just like a SOC aggregates the indicators of compromise from various cyber security tools to orchestrate a unified incident response, the ROC serves as a cross-functional, data-integrated hub that continuously monitors and responds to changes across the organization's risk surface in real time with coordinated actions that align risk management with business context.

To solve the problem of fragmented risk management, where data from various tools remain isolated and unanalyzed, the ROC integrates all vulnerability data into a central hub on a unified platform. This data is normalized, deduplicated, and enriched, creating a single source of truth. Without this centralized integration and financial risk quantification, the investment in cybersecurity tools is fundamentally flawed. This is why the ROC is indispensable—it transforms cybersecurity from a collection of disjointed efforts into a coherent strategy that speaks the unified language of risk.

Foundations of a Risk Operations Center (ROC)



Breaking Down Operational Silos

Traditional models often confine risk management to isolated functions—security in the domain of the CISO, financial risk under the CFO, and operational risk somewhere in between. These silos create gaps, where critical information is either lost or misaligned.

The ROC dismantles these operational silos by establishing a central hub for risk management, where information flows freely across departments and decisions are made with a holistic view of the organization's risk posture. It's about promoting collaboration among the CISO, CTO, CCO, CFO, and other key stakeholders to ensure that risk management strategies are aligned with overall business objectives. It's about managing large residual risks, defining budgets for risk mitigation, and coordinating actions across different lines of defense.

Continuous Oversight and Adaptation

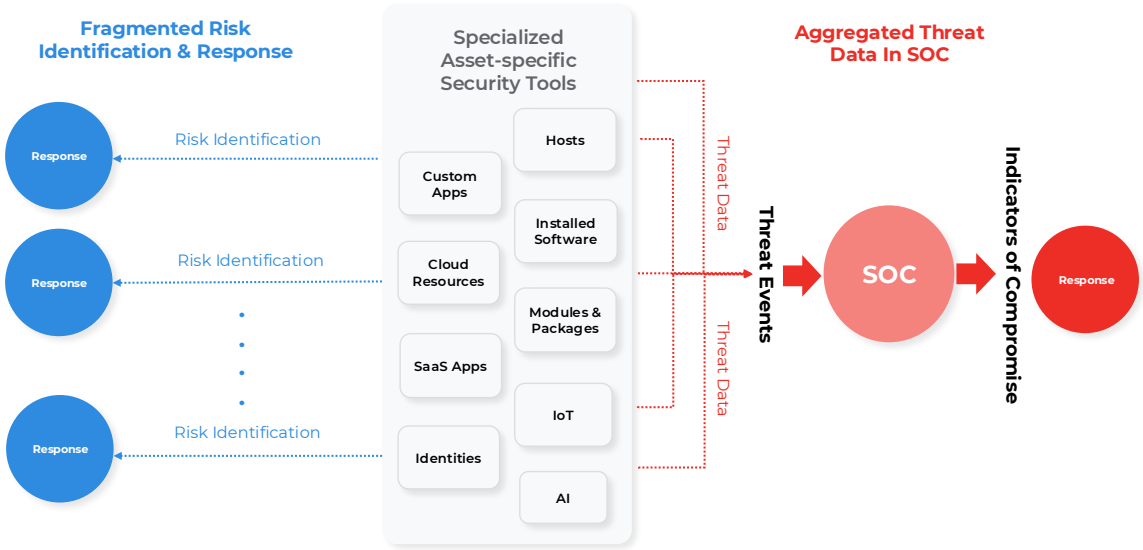
At the heart of the ROC is the idea that risk is not static—it's an ever-evolving challenge that requires continuous oversight and adaptation. The ROC aggregates, normalizes, and prioritizes risk data in real time, enabling organizations to anticipate and address risks before they materialize into full-blown material impact.

The Enterprise Challenge: Fragmented Risk Management and Lack of Unified Data Fabric

Disconnected Risk Management Functions

In large enterprises, risk management often resembles a disjointed puzzle—pieces scattered across various departments, business units, and regions, each focusing on its own slice of the risk spectrum. Security teams manage cyber threats, compliance officers ensure regulatory adherence, and operational units tackle day-to-day risks. Meanwhile, the CFO is left to grapple with financial exposures, often without a precise understanding of how much additional investment is required to mitigate or transfer that risk through insurance.

This lack of process and platform integration to handle cybersecurity risk presents a critical challenge, with the organization losing the ability to see the full picture. The first line of defense, typically the operational units, is separated from the second line of defense—risk management—and the third line of defense, which includes audit and compliance. This structure can lead to inefficiencies, with each function operating within its own isolated domain, using its own set of tools, data sources, policies, and priorities.



The CFO's Dilemma

The Chief Risk Officer, for example, might have a risk register, but without a cohesive process to quantify, track, and treat these risks across different domains, materially impacting risks can slip through the cracks. The result is often duplicated efforts, missed opportunities for mitigation, and, ultimately, an incomplete risk management strategy that leaves the enterprise exposed.

For the CFO, this fragmentation creates a particularly problematic dilemma. Charged with managing the financial aspects of risk—securing cybersecurity insurance, allocating captive budgets for risk mitigation, and other forms of financial risk transfer—the CFO's decisions are often made in a vacuum. Without integrated input from cybersecurity and operational risk teams, the CFO may end up purchasing insurance that doesn't align with the actual risk exposure of the enterprise. Furthermore, without integrated risk insights, CFOs are often forced to approve or deny budgets based on a vague sense of moral obligation, rather than with the confidence that their investments are safeguarding business objectives. This disconnect between the CFO and cybersecurity can leave the organization vulnerable to financial loss in the event of a breach.

Consider the case of an enterprise where the CFO and the General Counsel were unaware of the full extent of their data risk—such as vast amounts of Personally Identifiable Information (PII) stored in unsecured cloud environments. This lack of visibility led to the purchase of inadequate insurance coverage. When breaches occurred, the organization was forced to scramble for additional coverage, exposing the disconnect between financial risk management and cybersecurity realities.

The Need for a Unified Data Fabric

The challenge goes beyond fragmented roles—without a unified data fabric for shared visibility, compliance and security efforts can also become misaligned with the actual risk landscape. A Risk Operations Center addresses this by creating a control plane where centralized data integration empowers governance and

compliance teams to align their efforts with the organization's true risk profile. Simultaneously, security teams can deploy focused, strategic measures that address the most significant risks. By bridging these gaps, the ROC ensures that all teams are working together to meet operational objectives.

These scenarios highlight the critical need for a Risk Operations Center (ROC)—a centralized hub where financial, operational, and cybersecurity risks converge, enabling informed decisions aligned with the enterprise's true risk profile. This approach improves budgeting and insurance strategies, boosting both capital and operational efficiency, and enhancing the overall resilience of the enterprise.

The Unavoidable Jobs-to-be-Done to Operationalize RoC

24/7 Risk Monitoring and Response

In enterprise risk management, certain jobs are the backbone of any effective risk management strategy, and they must be executed with accuracy and efficiency. The Risk Operations Center (ROC) is designed to ensure that these critical jobs are done right.

Just as a Security Operations Center (SOC) provides continuous surveillance over security incidents caused by malicious threats, the ROC must maintain constant vigilance over the organization's risk landscape. Continuous monitoring of exploitable vulnerabilities that could lead to material impact is essential because risks don't adhere to business hours. The ROC's mandate is to provide around-the-clock oversight, ensuring that emerging risks are identified and addressed, remediated, and mitigated in real-time with robust risk and operational impact analysis capabilities.

Risk Aggregation and Normalization

One of the most significant challenges in risk management is the sheer volume and diversity of data. Risk information comes from multiple sources—vulnerability assessments, configuration scans, threat intelligence feeds, and more. The ROC platform must aggregate this data, normalize it, prioritize it, and present it in a unified format, turning this complex web of data into actionable intelligence.

Cross-Functional Coordination

The ROC is the hub where cross-functional efforts converge. It facilitates collaboration between different teams and lines of defense—security, IT, finance, compliance—ensuring that risk is managed in a holistic, integrated way, breaking down silos, and ensuring that everyone is working toward the same goals.

Informed Budgeting

The ROC plays a critical role in providing detailed insights into the financial implications of risks and maximizing the return on investment in risk management efforts. With a clear understanding of the potential impact of different risks, the ROC can guide budgeting decisions, ensuring that investments in risk mitigation are both adequate and aligned with the organization's overall risk appetite.

Risk Communication and Reporting

In the past, risk communication was often reactive. The RoC changes this dynamic by establishing a proactive communication strategy, ensuring senior leadership is continuously informed with real-time, actionable insights to make decisions. The ROC must ensure that risk communication is not only accurate but also tailored to the needs of different stakeholders, from the boardroom to the front lines.

Qualys Enterprise TruRisk Management (ETM) - the world's first Risk Operations Center (ROC)

Qualys introduces Enterprise TruRisk Management (ETM) —the world's first Risk Operations Center (ROC) in the cloud – a platform transforms the ROC from a theoretical concept into a practical, operational reality. By unifying and simplifying the complexity of risk data, ETM, as a cloud-based Risk Operations Center, monitors and mitigates risks in real-time, ensuring that organizations can proactively manage risks before they manifest into full-blown crises.

Addressing Data Complexity

At its core, Qualys ETM addresses one of the most pressing challenges in risk management—the overwhelming volume and complexity of data. As infrastructures increasingly move to the cloud, enterprises no longer deal solely with known vulnerabilities in commercial software; they now face the complexities of custom-built applications, integrated with a vast array of open-source software and cloud services. This shift necessitates a move towards 'shifting left'—integrating security earlier in the development process by embedding it into developers' and platform engineers' toolchains, such as CI/CD tools, SAST, DAST, SCA, and IAST.

Integrating Cyber Risk Quantification (CRQ) and Continuous Threat Exposure Management (CTEM)

Risk telemetry flows in from every corner—vulnerability scans, configuration assessments, threat intelligence, asset inventories—each providing a piece of the puzzle. The challenge lies in piecing these together into a coherent picture that can drive actionable insights. Qualys ETM tackles this challenge by ingesting data at a petabyte scale, normalizing and correlating it across full-stack and hybrid environments. Moreover, the importance of Cyber Risk Quantification (CRQ) and Continuous Threat Exposure Management (CTEM) cannot be overstated in this context, representing the economics of modern risk management. CRQ quantifies cyber risk into financial terms, transforming it from a technical issue into a concrete business challenge, highlighting operational costs and capital allocation. Integrating CRQ models with CTEM enables informed resource allocation to mitigate risks cost-effectively. Qualys ETM is crucial in this process, as it provides the necessary infrastructure to track, predict, and manage cybersecurity risks with a focus on operational efficiency and return on investment.

Enhancing Operational Efficiency Through Automation

Operational efficiency is further enhanced through ETM's automation capabilities, replacing slow, manual processes with rules-based and AI-enabled risk elimination workflows. This allows the ROC to focus on strategic decision-making rather than getting bogged down by day-to-day operations. In a typical siloed setup, multiple modularized tools often perform overlapping functions without sharing data. By centralizing the security functions, Qualys ETM eliminates redundancies, reduces operational costs, and ensures that resources are allocated where they are needed most.

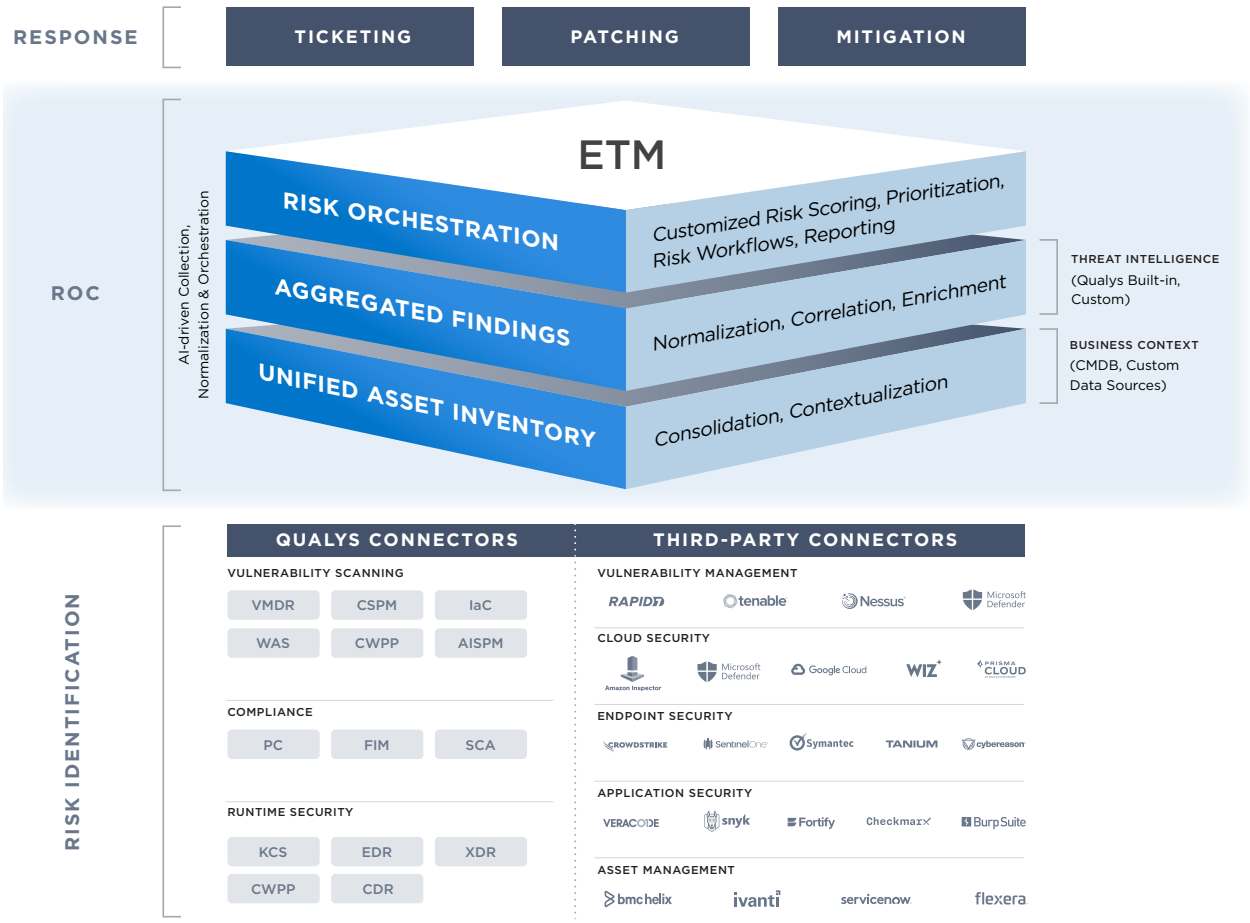
Decoupling Security Posture Management

However, operational efficiency is only part of the equation. The real power of Qualys ETM lies in decoupling security posture management with risk telemetry integration from a wide range of sources—including vulnerability, configuration, threat, and asset management. This centralized visibility layer enables sophisticated orchestration and a unified strategy for assessing and improving security posture across different asset types. Informed budgeting is a prime example of this strategic insight in action.

Qualys ETM – Key Capabilities as a Risk Operations Center

a. Full-Stack Asset Discovery

Qualys ETM delivers a holistic solution that encompasses the entire spectrum of cybersecurity risk management: ETM integrates robust asset discovery capabilities that span across IT environments, cloud-native assets, and operational technology (OT). This ensures continuous monitoring and evaluation of every component in the organization's digital footprint, providing a comprehensive inventory of all assets.



b. Data Aggregation and Correlation

Qualys ETM aggregates and orchestrates data from diverse sources, including internal tools like Qualys VMDR, CSAM, and WAS, as well as third-party tools like Wiz, Tenable, Rapid7, MS Defender, and more than 25 external threat intelligence feeds such as Talos, McAfee, and MITRE ATT&CK. This creates a unified view of the organization's threat landscape.

c. Advanced Risk Analysis and Prioritization

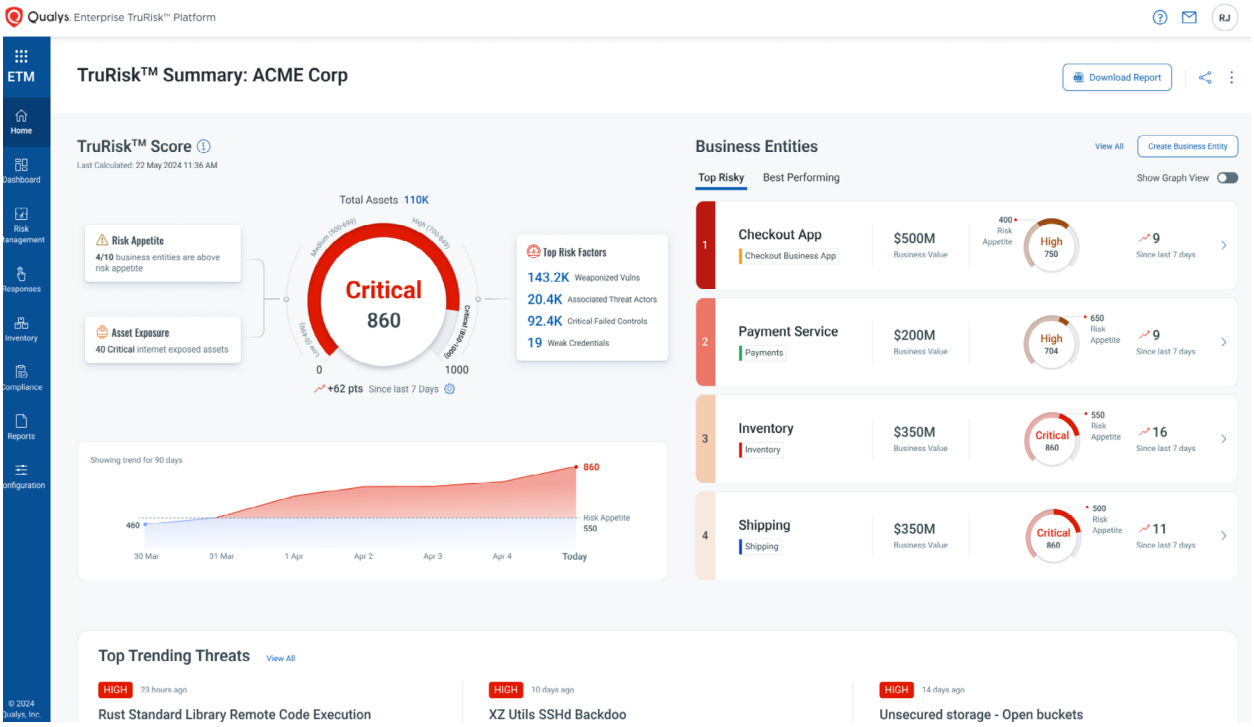
By correlating this aggregated data, ETM delivers real-time, actionable insights into vulnerabilities and their financial impact on the organization. This enables precise prioritization of the most critical risks, ensuring that attention is focused where it's needed most.

i. Cyber Risk Quantification

Utilizing advanced algorithms, ETM quantifies cyber risk by assigning financial values to potential security threats. This approach transforms risk management into a data-driven process, allowing organizations to understand the financial implications of each threat and make decisions that are aligned with business priorities.

ii. Contextual Prioritization

One of ETM's core strengths is its ability to prioritize findings effectively. By incorporating context such as asset criticality, business impact, and the broader threat landscape, ETM identifies and highlights the risks that truly matter to the organization. This contextual intelligence distinguishes ETM from traditional tools, which may struggle to sift through and prioritize vast amounts of data efficiently.



d. Risk Reduction Plans

Risk reduction plans of Qualys ETM strategically configure automated remediation actions to lower the TruRisk™ score across an organization, by prioritizing vulnerabilities, ensuring that the most critical risks are mitigated first, reducing the organization's overall risk exposure, and demonstrating a direct return on investment in cybersecurity measures.

e. Scalable Cybersecurity Risk Management

Built on a petabyte-scale platform, ETM is engineered to handle massive volumes of data without sacrificing performance. This scalability ensures that as an organization grows and its digital ecosystem becomes more complex, ETM remains a robust and responsive tool for managing cybersecurity risks.

f. Automated Remediation Response

ETM is designed to actively manage and eliminate risk through advanced strategies such as threat hunting, vulnerability management, and automated patching via Qualys Patch Management and TruRisk Eliminate. TruRisk Eliminate goes beyond conventional patching, offering innovative "patchless" remediation options, including targeted isolation and configuration changes, which are particularly effective for addressing nearly 100% of CISA Known Exploited Vulnerabilities (KEVs) and ransomware threats. By seamlessly integrating with tools like Jira, Microsoft Teams, and ServiceNow, ETM ensures tight coordination across departments, aligning risk mitigation efforts with operational workflows.

Transforming the Future of Cybersecurity Risk Management

The future of cybersecurity risk management lies in the strategic integration of tools, processes, and insights that transcend traditional, reactive approaches. Qualys Enterprise TruRisk Management (ETM) as a Risk Operations Center (ROC), represents this evolution—moving beyond fragmented efforts to create a unified, proactive, and business-aligned risk management framework.

Organizations embracing this new practice will not only protect their business against materially impactful risk scenarios but also position themselves as resilient. The RoC will become the essential component of a well-run, resilient enterprise that is able to fulfil its obligations towards its stakeholders, shareholders, and customers.

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**