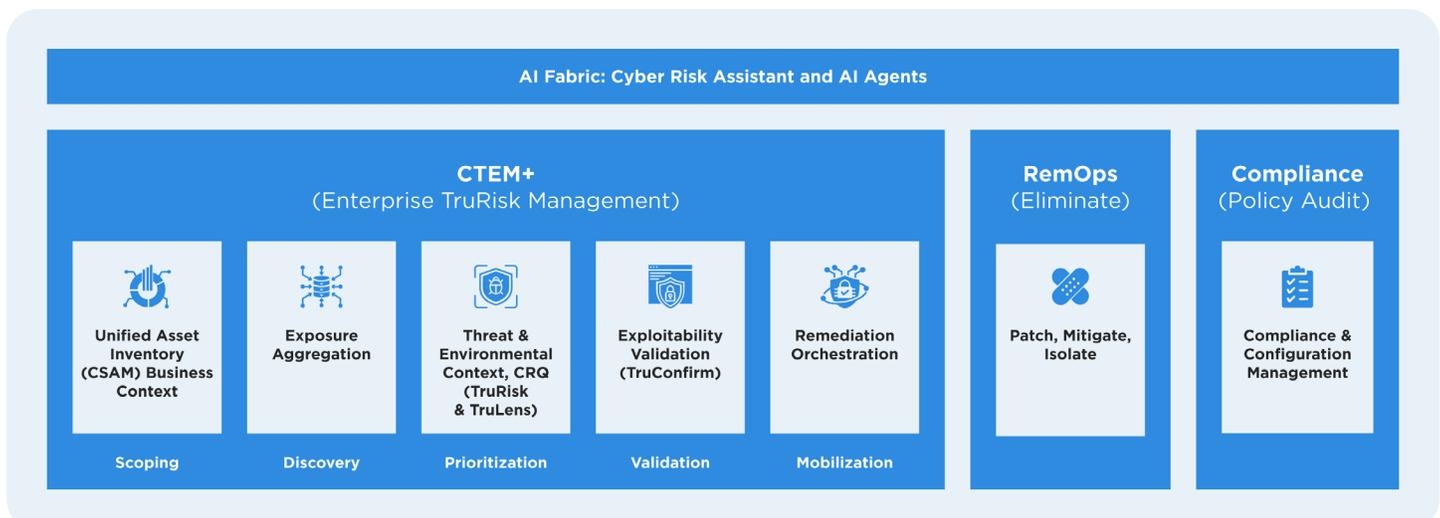# Operationalizing CTEM with Qualys ETM

In an era of constantly evolving attack surfaces and accelerated, AI-driven attackers, a robust framework that unifies disparate security tools is no longer optional—it is essential. Continuous Threat Exposure Management (CTEM) offers such a framework to quickly and accurately identify and remediate exposures with the biggest business impact.
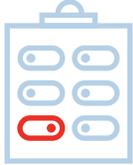
Qualys Enterprise TruRisk™ Management (ETM) delivers the unified platform required to streamline and operationalize a successful CTEM program. By seamlessly integrating asset management, risk prioritization, and response, ETM empowers organizations to master the five core pillars of the CTEM framework with a single solution.

For advanced organizations, ETM offers additional capabilities—including remediation operations, cyber risk quantification, and integrated compliance —to take their CTEM to the next level and establish a dedicated Risk Operations Center (ROC).

All of this is powered by natively integrated Agentic AI that transforms security teams from reactive responders to strategic orchestrators, truly bringing the CTEM to life.

AI Fabric: Cyber Risk Assistant and AI Agents

CTEM+
(Enterprise TruRisk Management)

Unified Asset Inventory (CSAM) Business Context	Exposure Aggregation	Threat & Environmental Context, CRQ (TruRisk & TruLens)	Exploitability Validation (TruConfirm)	Remediation Orchestration
Scoping	Discovery	Prioritization	Validation	Mobilization

RemOps
(Eliminate)

Patch, Mitigate, Isolate

Compliance
(Policy Audit)

Compliance & Configuration Management

1. Scoping: Defining the Attack Surface

ETM precisely scopes your organization's attack surface by consolidating data from all sources—on-premises, cloud, containers, identities, and applications—to provide complete visibility into known and unknown assets. By integrating data from CMDBs, third-party tools, and Qualys agents with business context, ETM focuses your CTEM program on the most critical risk.

> **ETM Feature:** CyberSecurity Asset Management (CSAM) provides a unified asset inventory that automatically links all organizational assets to their business entities with criticality and associated risks.

2. Discovery: Aggregating Exposures from Siloed Security Tools

ETM aggregates exposure data from disparate security tools, consolidating insights on vulnerabilities, misconfigurations, and identity risks into a single view. By identifying how attackers exploit combinations of these weaknesses—such as privilege escalation and lateral movement—ETM helps you pinpoint and neutralize toxic combinations before they lead to breaches.

> **ETM Feature:** ETM aggregates vulnerabilities, identities, misconfigurations, and policy gaps from across every risk surface – on-premises, cloud, and identity – to identify toxic combinations and critical exposures.

3. Prioritization: Focusing on What Matters

With Qualys TruRisk scoring, ETM moves beyond generic CVSS metrics to prioritize risks based on exposure data, threat intelligence, and business context. This approach cuts through the noise by quantifying cyber risk in terms of financial impact, significantly reducing alert fatigue while highlighting the most critical vulnerabilities based on business and industry context.

> **ETM Feature:** TruRisk scoring that combines vulnerability data, business criticality, and powerful threat intelligence with TruLens threat-based risk prioritization.

Qualys.

4. Validation: Confirming Exploitability

ETM ensures that remediation efforts focus on high-risk, exploitable vulnerabilities. By emulating attacker techniques in a safe manner, ETM validates which threats are genuinely exploitable in your unique environment.

> **ETM Feature:** TruConfirm for safe, real-world exploit validation that identifies and provides clear evidence of exploitability to accelerate remediation.

5. Mobilization: Orchestrating Risk Reduction

ETM streamlines remediation with tailored risk treatment plans and native remediation capabilities. Integration with ITSM platforms ensures the right teams are mobilized, equipped with clear, actionable steps to reduce risk effectively.

> **ETM Feature:** Eliminate for patch and patchless remediation that ensures aggressive threats are addressed efficiently and in alignment with strategic outcomes.
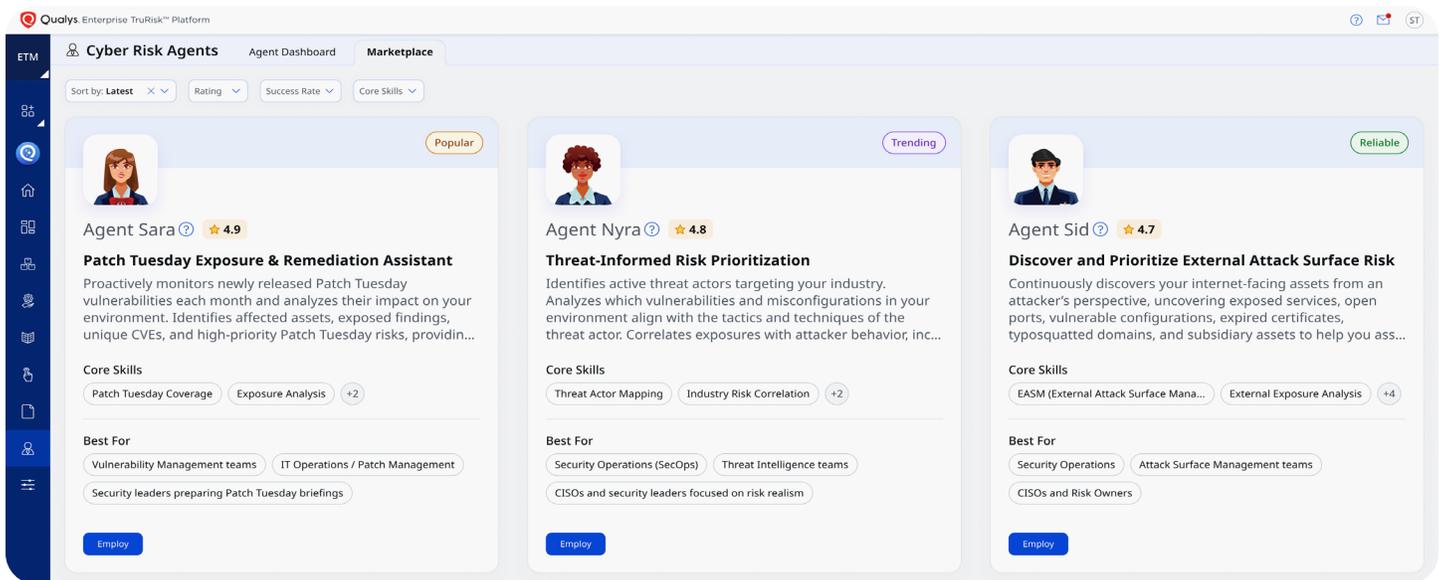
Powered by Agentic AI

Qualys ETM leverages the groundbreaking capabilities of Agentic AI to supercharge the entire Continuous Threat Exposure Management (CTEM) process. By deploying intelligent, context-aware agents, the platform delivers real-time guidance and support at every stage of the risk management workflows. From identifying high-priority risks to validating exploitability and orchestrating comprehensive remediation workflows, Agentic AI provides actionable insights and automated assistance. This ensures your organization can stay ahead of evolving threats while maximizing operational efficiency.

Elevate Your CTEM Program with Qualys ETM

Qualys ETM is engineered to power every stage of the CTEM framework, eliminating the complexity and expense of managing multiple security tools. It provides a single platform to unify processes, prioritize threats, and operationalize risk reduction. But ETM's capabilities extend beyond the standard CTEM lifecycle, integrating cyber risk quantification and compliance into a single, cohesive strategy. This holistic approach transforms your security posture, making Qualys ETM the definitive solution for building a robust and effective Risk Operations Center (ROC).

Try Qualys Enterprise TruRisk Management.

Get a Demo