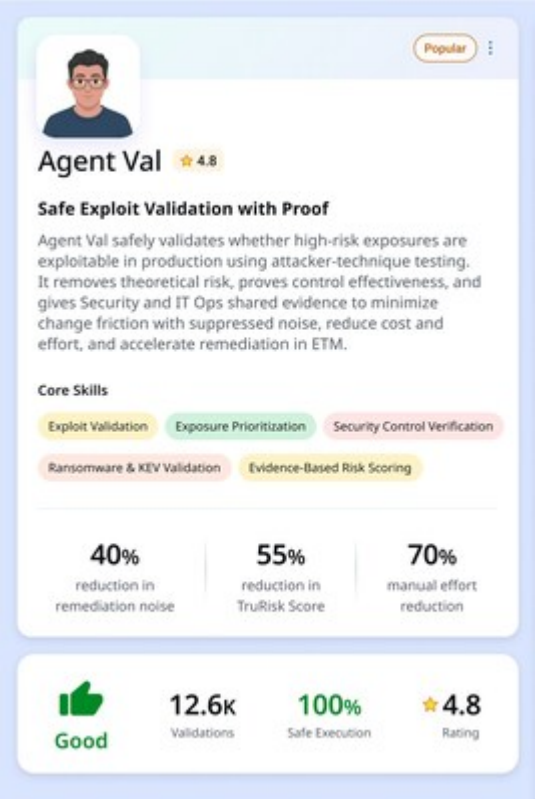
Qualys Debuts Industry's First AI Agent for Safe Exploit Validation and Autonomous Remediation

March 23, 2026

Agent Val exploits, mitigates and revalidates exposures against compensating controls continuously, dramatically reducing the average window of exposure

FOSTER CITY, Calif., March 23, 2026 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a leading provider of cloud-based IT, security and compliance solutions, today launched Agent Val within Enterprise TruRisk Management (ETM) to bring safe, agent-led exploit validation and autonomous risk remediation to the Risk Operations Center (ROC). Agent Val represents a fundamental shift in vulnerability and exposure management from assumption-driven prioritization to evidence-based execution, accelerating response, reducing wasted effort, and delivering measurable reductions to cyber risk.



Research shows that known exploited vulnerability volume has grown 6.5 times in the past four years, while the percentage of critical vulnerabilities still open at Day 7 has increased — proof that manual remediation has hit a hard ceiling. To make matters worse, the time to exploit has now shrunk to minus one day, meaning attackers are exploiting them before patches exist. For CISOs, the challenge is closing the gap between vulnerabilities that look severe on paper and those truly exploitable in production environments, so teams are not wasting valuable time remediating low-impact issues and missing other dangerous exposures. Organizations need proof of exploitability, not assumptions, to move faster and reduce risk with confidence.

"Exposure management efforts often focus on counts, trends, and heat maps that describe risk but don't consistently drive action," said Melinda Marks, practice director for cybersecurity at Omdia. "The next step in maturity is extending attack path analysis through actual exploit validation, turning potential exposure into operational certainty. Validation is critical to risk reduction, and offensive validation remains a significant gap across the market. Capabilities like what Agent Val offers can help teams prioritize real attack paths, move faster, and focus effort where it delivers measurable impact."

Agent Val, powered by TruConfirm, serves as the agentic AI orchestration layer within ETM. It coordinates and identifies high-risk exposures, validates exploitability in production using business context and asset criticality, and feeds confirmed results directly into ETM to drive prioritized remediation and measurable risk reduction with minimal manual effort, shifting security teams from chasing volume to reducing verified risk.

"In an era of infinite vulnerabilities and finite engineering cycles, the primary challenge is no longer discovery—it is the strategic allocation of remediation capital," said Florian Bielak, CISO, BitMEX. "Agent Val with TruConfirm will enable us to further shift away from a reactive posture based on theoretical CVSS scores to a disciplined, evidence-based model. By validating actual attack paths at scale, we'll have a way to effectively eliminate the noise tax, ensuring our lean teams are engineering against real-world risk rather than chasing statistical outliers."

Agent Val enables organizations to:

- **Validate real exploitability –** Agent Val analyzes exposure signals across assets and determines what should be validated first based on attacker relevance, business context, and exposure. Then, it uses TruConfirm to safely test exploitability in the live environment, providing evidence-based confirmation of whether an exploit path is open, blocked by controls, or unreachable. The result is a 90%+ reduction in remediation noise, so security teams can stop chasing findings that cannot be exploited.

- **Mitigate confirmed risks** – Once risk is confirmed, ETM prioritizes that exposure to the top of the remediation queue and extends response beyond patching deployment with mitigation controls and isolation, where patching is not feasible. This enables targeted mitigation to reduce exposure quickly, resulting in 70% faster time-to-remediate on confirmed exploitable findings and allowing engineering teams to prioritize exposures that matter.

- **Prove Risk Reduction** —After mitigation, Agent Val runs validation again using TruConfirm to verify that the exploit path is closed, controls are working and risk has been reduced. With over 1,600 CVEs covered, Agent Val provides unmatched coverage with no new sensor footprint required. Teams now have proven exploitability evidence captured for board reporting to show measurable risk reduction.

"Having a vulnerability does not equal risk," said Sumedh Thakar, president and CEO of Qualys. "What matters is whether an attacker can successfully reach and execute an exploit path in your environment. As exploit timelines shrink and adversaries use AI to move faster, the industry can't keep running on assumptions. Agent Val in ETM moves the Risk Operations Center (ROC) from 'we think' to 'we know' to 'it's been taken care of' with minimal manual effort, giving the power of AI back into the hands of defenders to drive measurable risk reduction at scale."

Availability
Agent Val, powered by TruConfirm, is included as part of Qualys ETM and is now generally available. Sign up at https://www.qualys.com/demo/enterprise-trurisk-management to be among the first to experience Agent Val within Qualys ETM.

Additional Resources

- Read our blog post, *"Meet Agent Val: Closing the Validation Gap in Exposure Management at Machine Speed with Agentic AI"*
- Sign up for a free trial of Qualys ETM at https://www.qualys.com/demo/enterprise-trurisk-management
- Watch the video here
- Follow Qualys on LinkedIn, Instagram and X

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a leading provider of 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.

The Qualys Enterprise TruRisk Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Oracle Cloud Infrastructure, Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit http://www.qualys.com.

Media Contact:
Rachel Yap Winship
Qualys
Media@Qualys.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-debuts-industrys-first-ai-agent-for-safe-exploit-validation-and-autonomous-remediation-302721708.html

SOURCE Qualys, Inc.