

Agent-led, safe exploit validation for the entire attack surface. Built into Qualys Enterprise TruRisk™ Management (ETM).

Organizations don't have the time, budget, or people to fix everything. Pretending otherwise is how risk programs stall. Security teams drown in "critical" findings, yet far fewer are exploitable in your environment, with your controls in place. So, the real question is: Which risks can actually be exploited right now, and which are already mitigated? Version-based detection, static severity scores, and dashboards built on assumptions cannot answer that. BAS tools add deployment friction and simulate attacks outside real production context. And because teams can't safely prove exploitability or control effectiveness in production, findings stay open, debates drag on, and exposure windows widen.

Qualys TruConfirm

TruConfirm is a native capability inside Qualys Enterprise TruRisk Management (ETM) that shifts exposure management from theoretical risk to evidence-based, validated execution, powered by Agent Val. TruConfirm safely validates whether high-risk exposures are actually exploitable in your production environment, against your deployed controls, across the network and hosts using attacker techniques with production-safe payloads. This combines outside-in validation from the network with inside-out validation from hosts to provide coverage for the entire attack surface. It confirms what is reachable, what is blocked, and what can truly be weaponized, then feeds deterministic proof directly into ETM to drive action. Instead of chasing 10,000 "critical" findings, teams can narrow exposure to a few hundred confirmed risks in minutes, at scale, without disrupting uptime. Limited remediation effort goes where it measurably reduces risk.

False positives suppressed

Suppress false positives by proving which "critical" findings are unreachable or blocked by controls, so teams stop chasing risk that cannot be exploited.

Confirmed exploitable assets

Safely validate real attack paths in production to identify assets that are truly exploitable and require action, not theoretical severity.

Faster remediation with proof

Turn validation into action with proof-backed remediation that cuts CAB friction, aligns IT and security, and measurably lowers TruRisk.



Agent Val ★ 4.8

Safe Exploit Validation with Proof

Agent Val safely validates whether high-risk exposures are exploitable in production using attacker-technique testing. It removes theoretical risk, proves control effectiveness, and gives Security and IT Ops shared evidence to minimize change friction with suppressed noise, reduce cost and effort, and accelerate remediation in ETM.

Core Skills

- Exploit Validation
- Exposure Prioritization
- Security Control Verification
- Ransomware & KEV Validation
- Evidence-Based Risk Scoring

Popular

Continuous validation with Agent Val

Operationalize TruConfirm at scale by autonomously selecting high-risk exposures, safely validating exploits on live assets, and delivering evidence-backed remediation inside ETM with minimal manual effort.

Multi-modal exploit validation

Confirms real exploitability using direct response execution, cryptographic proof-of-execution, and out-of-band callbacks, validating reachable attacker paths via external and internal scanners for remote exploits and cloud agents for local privilege escalation and kernel attacks.

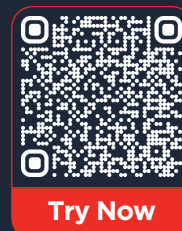
Safety-first production guardrails

Built for live environments with benign payloads, pre-validation checks, zero-footprint execution, and asynchronous verification. No outages. No data exposure.

Coverage for attacker reality

Continuously expands validation across weaponized CVEs and real-world techniques, outside-in and inside-out, to cover the full attack surface and focus on what attackers actually exploit, not just what scanners label critical.

Run Qualys ETM with TruConfirm on your top revenue-critical assets and get an evidence-backed list of what's actually exploitable.



Try Now