Qualys

WHITE PAPER

BUSINESS

Qualys TruConfirm: The End of Vulnerability Guesswork

QUALYS TRUCONFIRM: THE END OF VULNERABILITY GUESSWORK

Every day, security teams are asked to do the impossible.

Vulnerability scanners generate thousands—sometimes millions—of "critical" findings. Executives want clear answers. Auditors demand defensible evidence. And while teams sift through dashboards and debate priorities, attackers are already exploiting the small subset of vulnerabilities that actually work.

The reality is stark: fewer than one percent of vulnerabilities labeled critical are ever exploited in the wild. Yet traditional scanners treat them all as equally urgent, overwhelming teams with noise and obscuring the exposures that truly matter.

The consequence is predictable. Highly skilled security engineers spend their time chasing theoretical risk instead of eliminating proven attack paths. Remediation backlogs grow. Confidence erodes. And breaches still happen—at an average cost of $4.88 million.

Now consider a different question: **What if you could know—definitively—which vulnerabilities attackers can actually exploit in your environment, right now?**

Introducing TruConfirm:

Qualys TruConfirm redefines exposure management by replacing assumption with evidence. Instead of inferring risk from software versions or static severity scores, TruConfirm validates whether a vulnerability can actually be exploited in a live production environment.

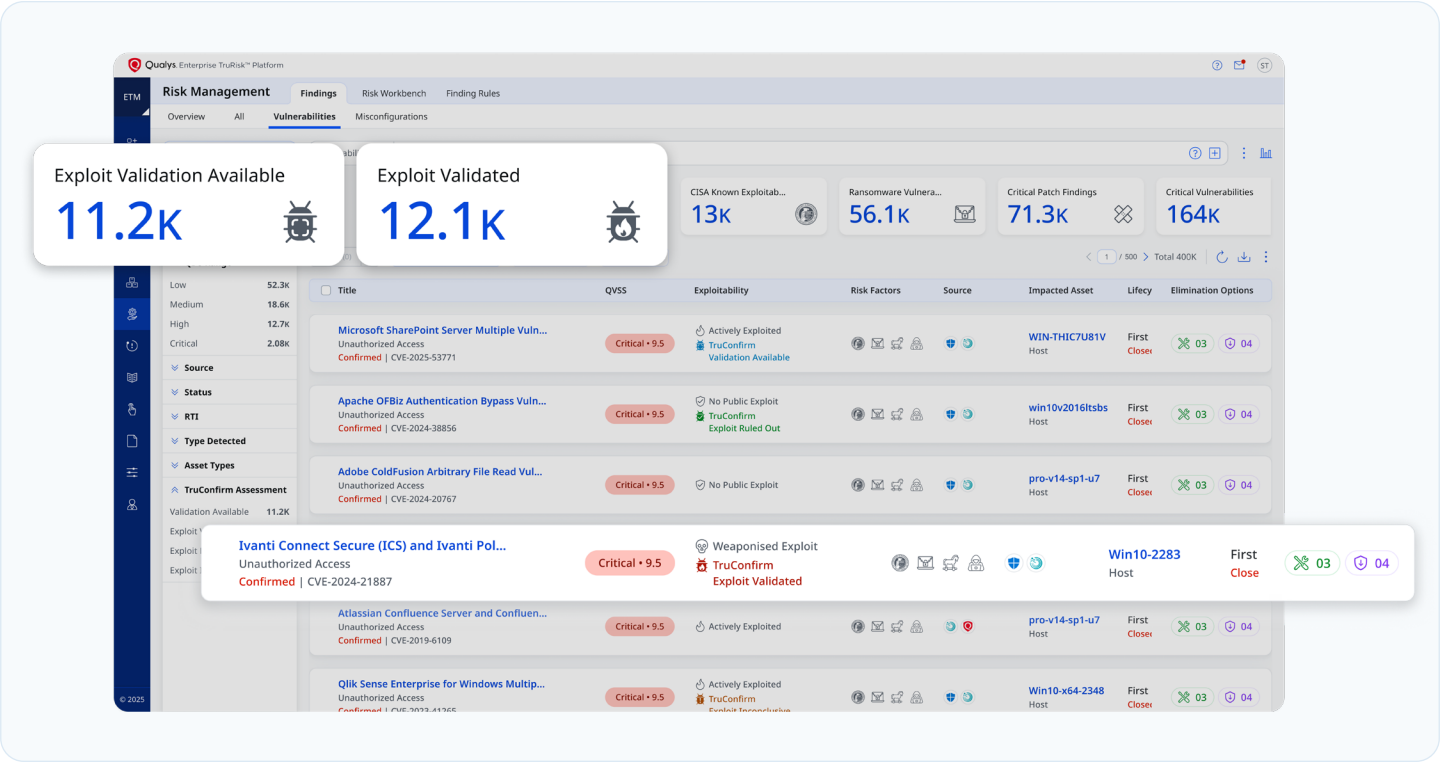
Traditional scanners ask a narrow question:

"Is this version potentially vulnerable?"

TruConfirm answers the question that matters:

Can an attacker exploit this vulnerability in my environment-right now?

That distinction is not incremental. It is foundational. By shifting exposure management from probabilistic inference to deterministic proof, TruConfirm changes how risk is prioritized, debated, and ultimately eliminated.



TruConfirm eliminates both failure modes by validating exploitability directly — replacing assumption with proof.

Why Version-Based Detection Fails

Most traditional vulnerability scanners operate on a simple - and fundamentally flawed - assumption: if a software version matches a known CVE, it represents exploitable risk.

That assumption breaks down in real-world environments. Version-based detection ignores the conditions that actually determine whether an attacker can succeed:

Reachability	
The vulnerable code exists	**Does the vulnerable code path ever execute?**
Exposure	
The service is running	**Is the service actively running and accessible?**
Control Effectiveness	
The vulnerability is exploitable	**Are existing defenses—such as WAFs, firewalls, or IPS—blocking the attack vector?**

Without answers to these questions, severity becomes speculative.

This gap produces two persistent and costly failure modes:

False Positives: Teams spend weeks patching libraries that are never loaded, unreachable, or already mitigated by compensating controls.

Missed Threats: High-impact blind vulnerabilities—such as blind SSRF or asynchronous RCE—are overlooked because they produce no visible scanner output, even as attackers exploit them silently.

TruConfirm eliminates both failure modes by validating exploitability directly — replacing assumption with proof.

The TruConfirm Difference: See What Attackers See

TruConfirm does not speculate about risk—it validates it. It applies the same execution paths and techniques used by ethical hackers and red teams, but re-engineered for safe, automated operation at enterprise scale. Instead of relying on inference, TruConfirm establishes certainty through three deterministic validation methods.

Three Pillars of Certainty

01 Direct Response Validation

Traditional scanners infer risk based on whether a software version might be vulnerable. TruConfirm goes further by validating execution directly. It delivers a safe, non-destructive payload and evaluates the system's actual response.

If the command executes, the evidence is explicit and observable. There is no interpretation, no version matching, and no ambiguity—only auditable proof that the vulnerable code path is reachable and exploitable.

02 Cryptographic Verification

For code injection scenarios, TruConfirm relies on mathematical certainty rather than fragile string matching. The validation payload instructs the target system to compute a cryptographic hash derived from a unique seed. That hash can only be produced if the injected code executes successfully.

This eliminates spoofing, reflection artifacts, and false positives. The result is deterministic proof of execution—not a heuristic guess.

03 Out-of-Band Detection (Silent Verifier)

Blind vulnerabilities pose some of the highest risk precisely because they produce no visible response. TruConfirm addresses this class of exposure through its Silent Verifier architecture.

If an attacker can coerce a system to initiate an outbound connection to their infrastructure, TruConfirm proves exploitability by inducing that same controlled callback to the Qualys TruConfirm secure cloud. No callback means the exploit path is not viable. A callback received is irrefutable evidence that execution occurred and egress controls permitted it.

Built for Production. Engineered for Trust.

The most common objection to active exploit validation is simple and justified: **production systems cannot be put at risk.**

TruConfirm was designed to remove that concern entirely. From the outset, it was engineered for live environments—where stability, performance, and data integrity are non-negotiable. Every validation method, payload, and execution path is constrained by safety-first controls that prioritize verification without disruption.

The result is exploit validation that delivers certainty without introducing operational risk—making proof possible where traditional tools force teams to rely on assumption.

Five Safety Principles

TruConfirm's exploit validation is governed by five non-negotiable safety principles, each designed to ensure proof without disruption in live production environments.

01 Pre-Query Verification

TruConfirm verifies the presence of the target service and vulnerable condition before any payload is sent. Validation is precise and intentional—never indiscriminate, never "spray and pray."

02 Benign Payloads Only

Where attackers deploy destructive commands, TruConfirm substitutes benign verification actions. Payloads request a harmless operation—such as a controlled network callback like "hello" —that proves the exploit path exists without causing impact.

03 Zero Footprint

No agents are installed. No files are written or modified. No configurations are changed. Every interaction is ephemeral, leaving no residual artifacts once validation is complete.

04 Non-Blocking Operations

All validation runs asynchronously. Primary application threads remain unaffected, users experience no latency, and production systems continue to operate normally throughout testing.

05 Privacy by Design

Exploit validation relies on cryptographic hashes rather than customer data. Even in the unlikely event of log inspection, no sensitive application logic, content, or proprietary information is exposed or retained.

Every TruConfirm payload is authored, vetted, and stress-tested by the **Qualys Threat Research Unit (TRU)** in isolated sandbox environments prior to release. Each validation technique is evaluated not only for effectiveness, but for safety, repeatability, and zero-impact execution in production systems. The outcome is exploit validation that delivers enterprise-grade certainty—without introducing enterprise-grade risk.

The Business Impact: From Backlog to Action

TruConfirm changes the economics of vulnerability management by replacing manual effort and debate with evidence-driven execution. The result is a measurable shift from managing volume to eliminating real risk.

Laser focus on the vulnerabilities attackers can actually exploit

Automated validation replaces manual triage

Risk-based remediation prioritized by proven exploitability actually exploit

Operational Impact: Before vs. After TruConfirm

Area	Before TruConfirm	After TruConfirm
Alert Volume	Thousands of “critical” findings with no clear signal	Focused list of vulnerabilities proven exploitable
Validation Effort	Weeks spent on manual validation and re-validation	Automated exploit validation replaces manual triage
Prioritization	Driven by CVSS, version matches, and scanner scores	Driven by verified exploitability and attacker paths
Security–Ops Alignment	Ongoing debate over severity and urgency	Evidence-based alignment and faster decision-making
Remediation Focus	Broad patching of theoretical risk	Precision remediation of confirmed threats
Compliance Evidence	Assumptions and inferred severity	Auditable proof of exploitability and control effectiveness
MTTR	Slow, inconsistent, and backlog-driven	Faster MTTR on threats that materially reduce risk

Confidence to act with evidence that satisfies security, operations, and compliance

Faster MTTR on the threats that matter most

Dynamic Risk Scoring

TruRisk™ scores adjust dynamically based on TruConfirm validation outcomes. When exploitability is confirmed, scores are immediately elevated, ensuring prioritization reflects **actual exposure**, not theoretical severity.

Score Escalation Over Time

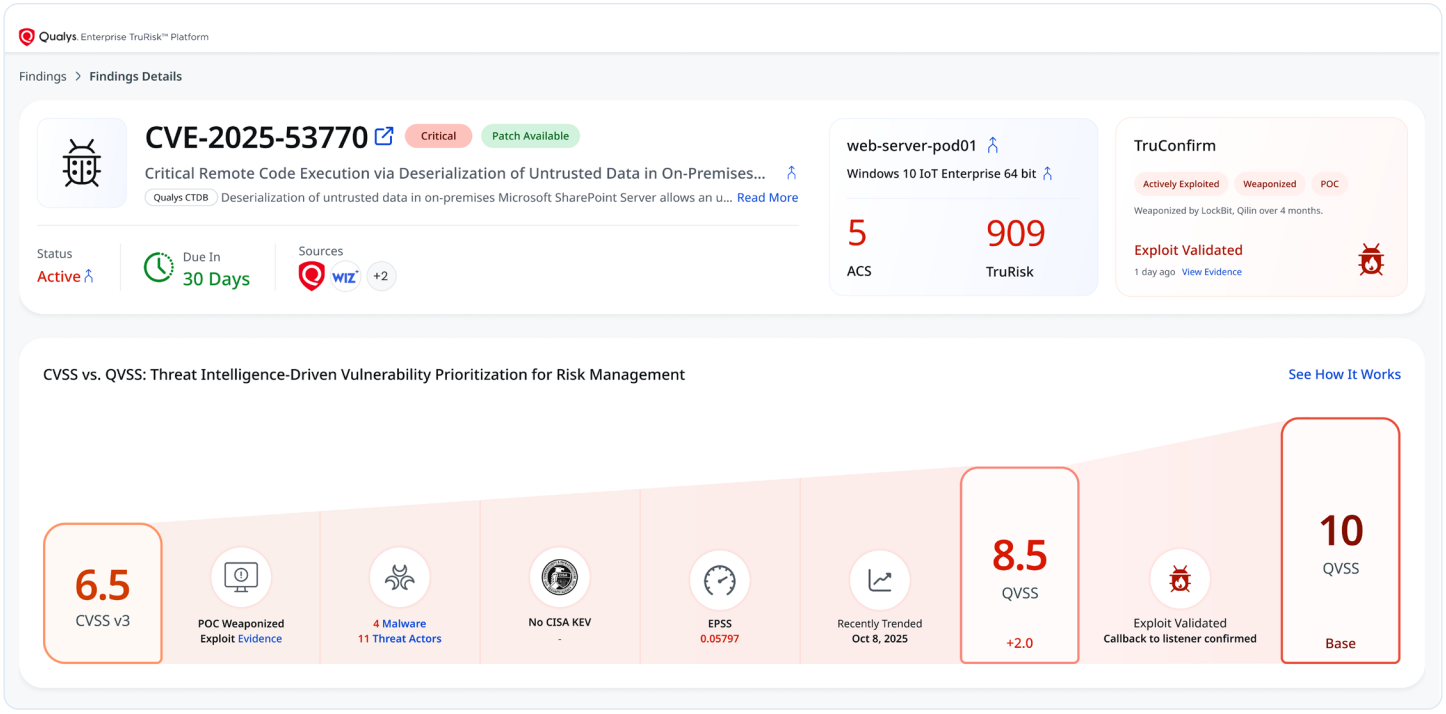
Validated exploits do not remain static. If a confirmed exposure is left unremediated, TruRisk applies an age-based escalation factor. As dwell time increases, so does risk, driving urgency until remediation occurs and the exposure is eliminated.

Continuous Threat Intelligence Integration

Underlying vulnerability scores are continuously refreshed using live threat intelligence, including EPSS updates, CISA KEV additions, dark-web activity, and newly emerging proof-of-concept exploits. TruConfirm-driven scoring always references the **current base score**, not the score at initial detection ensuring prioritization reflects the latest attacker reality.

Impact

Validated threats surface immediately. Unresolved exposures escalate predictably. Prioritization remains continuously aligned to real-world exploitability until risk is reduced.



Comprehensive Coverage Across Your Attack Surface

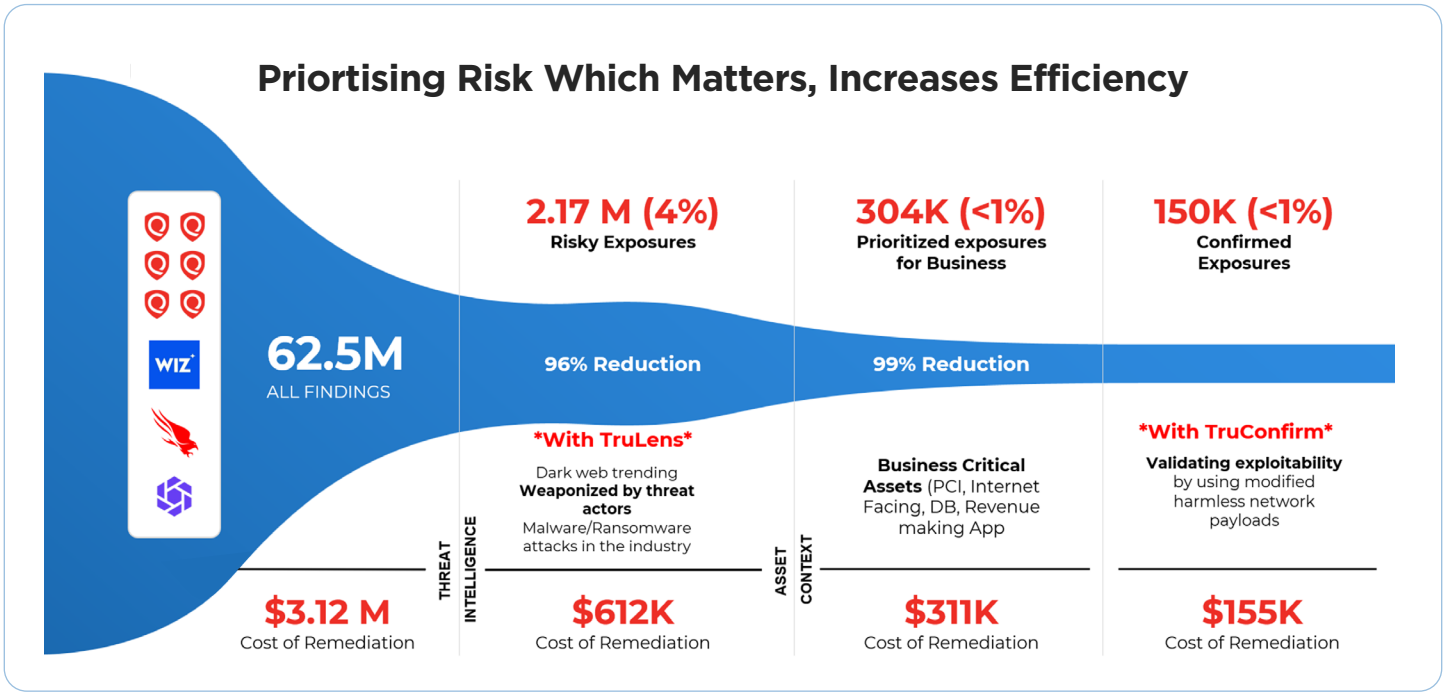
TruConfirm validates exploitability across **1,600+ CVEs**, with coverage deliberately aligned to the technologies and attack paths most frequently exploited in enterprise environments, not simply those that are easiest to scan.

This balance reflects real attacker behavior. Legacy vulnerabilities continue to serve as reliable entry points, and focusing exclusively on new disclosures leaves known, weaponized exposures unvalidated.

Coverage is continuously expanded by the **Qualys Threat Research Unit**, which prioritizes new validations as exploits are weaponized and high-risk CVEs emerge. Updates emphasize current-year disclosures when active exploitation is observed in the wild, ensuring validation keeps pace with how attackers actually operate.

The validation library spans both **recent and persistent threats:**

- **60%** of validated CVEs originate from **2020–2025**
- **40%** address **pre-2020 vulnerabilities** that remain actively exploited in the wild



Modern Exposure Management with Qualys ETM

TruConfirm is a core capability within **Qualys Enterprise TruRisk Management (ETM)**, the platform designed to turn fragmented security signals into decisive risk reduction. Rather than adding another layer of detection, TruConfirm embeds exploit validation directly into ETM's prioritization and response workflows, grounding exposure management in evidence.

TruConfirm
provides detection of

1,600+ CVEs

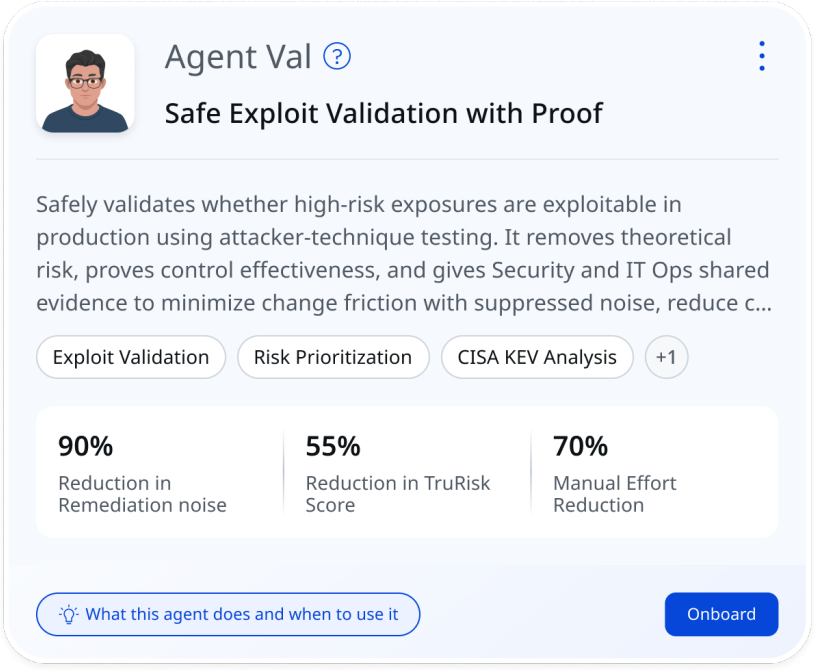
for enterprise

With TruConfirm integrated into Qualys ETM, organizations achieve:

1. **Attacker-Context Clarity:** Clear visibility into which exposures represent real, reachable attack paths
2. **Precision Remediation:** Resources focused exclusively on vulnerabilities that are proven exploitable
3. **Accelerated Risk Reduction:** Faster movement from detection to elimination, without debate or delay
4. **Board-Ready Evidence:** Reporting based on validated risk posture—not inferred severity or theoretical exposure

Agent Val for Autonomous Exploit Validation for Risk Operations

Agent Val is the decisioning and orchestration engine behind TruConfirm in Qualys ETM. Agent Val is the agentic AI-driven cyber risk agent that turns exploit validation into a continuous, closed-loop process: prioritize, validate, remediate, and revalidate. It continuously selects which exposures to test first using TruRisk, threat context, asset exposure profile, business criticality, CISA KEV alignment, and exploit availability.



Once prioritized, Agent Val invokes TruConfirm to safely verify real exploitability in production using modified benign payloads and the right verification method for the target assets and CVE, including direct response validation, cryptographic verification, or out-of-band callback detection.

When exploitability is confirmed, the result feeds back into ETM to elevate risk, drive the next best action, and support targeted patching, mitigation, or compensating controls.

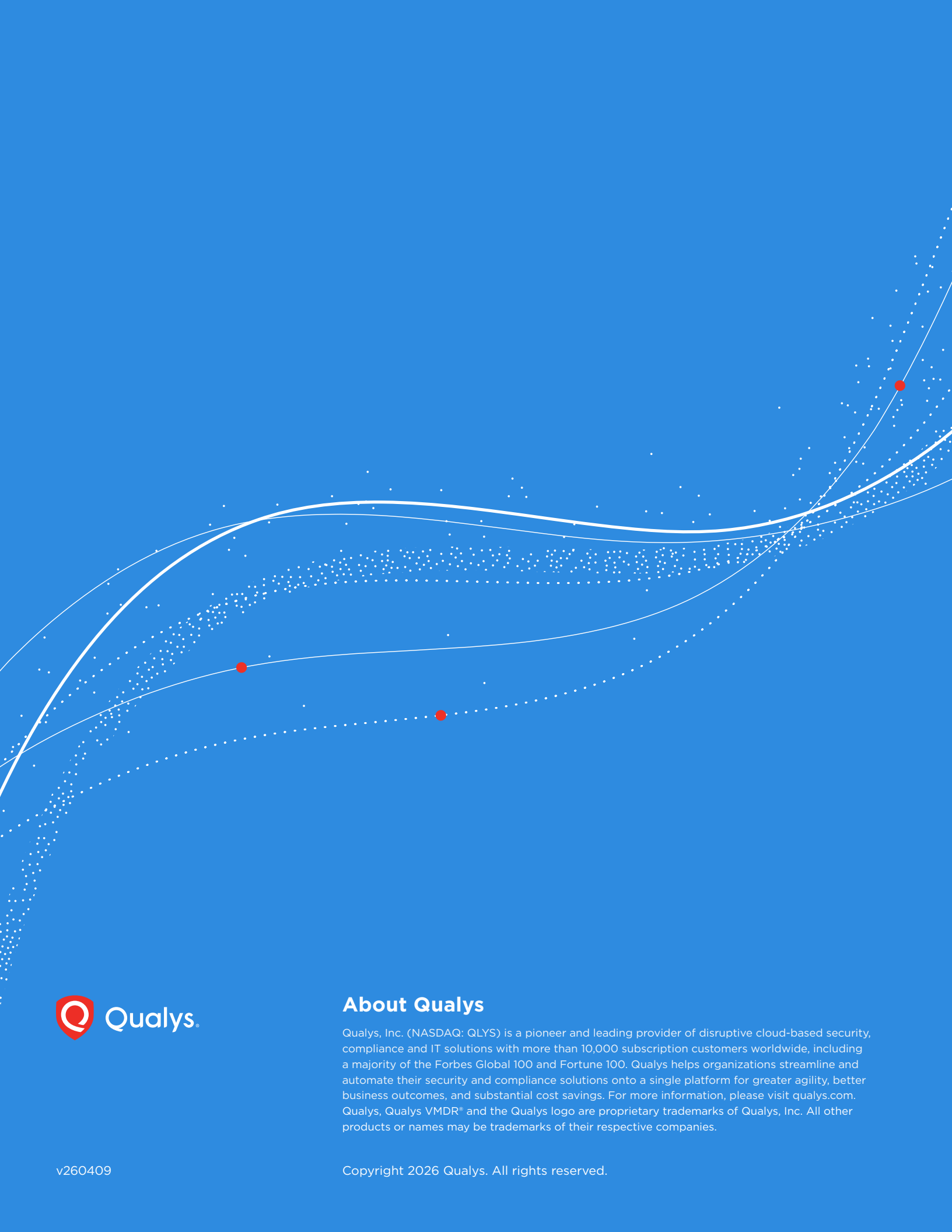
After remediation, Agent Val reruns validation against the same exploit path to confirm the exposure is actually closed, replacing assumption-based prioritization with evidence-backed risk reduction.

The Future of Exposure Management Is Proof

For too long, the security industry has operated on assumption—assumptions about what is vulnerable, what is exploitable, and what truly matters. That model no longer holds in an environment where attackers weaponize vulnerabilities faster than patch cycles can respond.

TruConfirm ends the guessing game. It replaces probability with certainty and transforms exposure management from an exercise in volume into a discipline of proof.

In a world where every remediation decision carries cost, risk, and operational impact, certainty becomes the most valuable control. TruConfirm delivers that certainty - showing, definitively, where your organization is exposed and where it is not.



Qualys.

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. For more information, please visit qualys.com. 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.

v260409