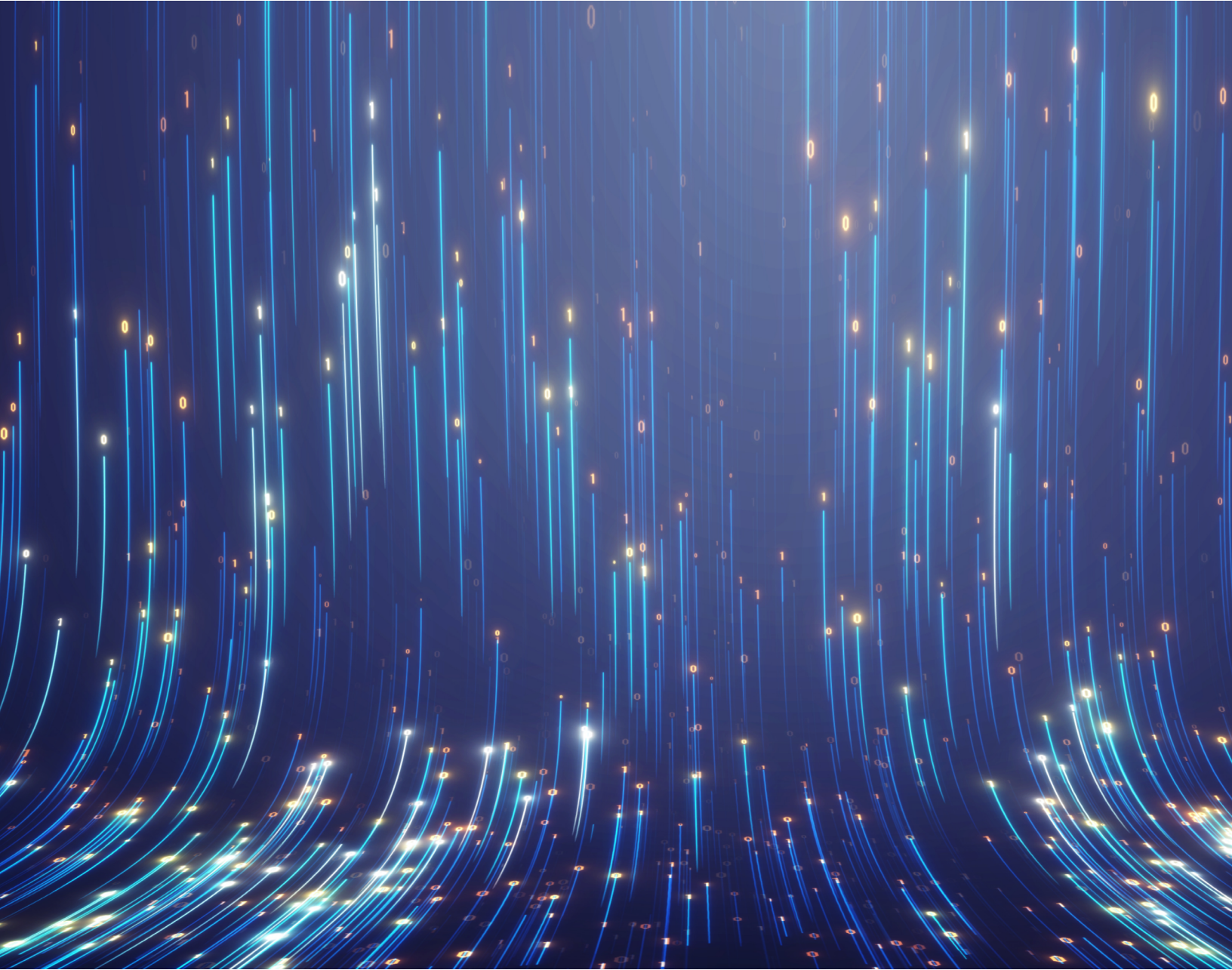




Qualys InstaScan

Scanless Vulnerability Detection at the Speed of Disclosure

Table of Contents

Executive Summary	2
The Cadence Gap: Why the Detection Clock Broke	3
Why Scan-Driven Detection Cannot Close the Gap	4
Introducing InstaScan: Detection Without a Scan	5
How Agent Insta Works	6
Detect, Confirm, Validate: Why a Scanless Finding Holds Up	9
What InstaScan Delivers	10
Closing the Loop: InstaScan in the ETM Platform	12
Availability and Next Steps	13
Conclusion	13



Executive Summary

The economics of vulnerability management have inverted. For nearly two decades, the gap between a vulnerability disclosure and the emergence of a working exploit gave defenders time to scan, assess the findings, and apply patches before an exposure could become a breach. Frontier AI has closed that window. Adversaries now weaponize newly disclosed advisories in hours, while most enterprise detection programs still wait on the next scheduled scan, signature build, or agent re-evaluation to learn they are exposed.

Qualys InstaScan, powered by Agent Insta, closes that gap. Built into the Enterprise TruRisk Management (ETM) platform, InstaScan is a continuous, scanless vulnerability detection capability that operates 24x7. It uses the software inventory, telemetry, and threat intelligence Qualys already collects from Qualys sensors and third-party sources to identify high-confidence exposures within an hour of disclosure, typically in minutes. No new scan. No agent action. No waiting for a signature build.

At a Glance

- **Coverage where the volume is.** Across its supported technologies, InstaScan detects more than 90% of exposures without a scan job running, technologies that commonly account for 60–70% of vulnerability volume in a typical enterprise.
- **A closed loop, natively.** InstaScan detects within the hour of disclosure; Qualys sensors and third-party telemetry independently confirm; TruConfirm and Agent Val validate exploitability; TruRisk Eliminate remediates; Agent Val proves the fix. No third-party stitching required.
- **Built on data already collected.** InstaScan runs entirely on inventory Qualys and its connectors already hold — no new scans, no agent redeployment, no IT coordination windows.
- **Speed you can act on.** Every finding is confidence-scored before it reaches TruRisk, so faster detection does not arrive as more noise.
- **Available now** within the Qualys ETM platform.



The Cadence Gap: Why the Detection Clock Broke

Every vulnerability management program runs on a silent clock. The countdown starts when a CVE is disclosed and ends when an attacker has a working exploit. Historically, that interval was long enough to absorb a scheduled scan and a patch cycle. It no longer is. Between vulnerability disclosure and the next scheduled scan, attackers can already have a working exploit. For many teams, that exposure remains invisible until the next scan runs.

The numbers make the compression concrete:

- **A record 48,177 CVEs were published in 2025, on pace toward roughly 59,000 in 2026.**
- **The median time from disclosure to a first working exploit fell from 56 days in 2024 to 23 days in 2025. At the fast end of that distribution, it is now measured in hours.**
- **AI-assisted attackers have weaponized new advisories in as little as 4 to 12 hours. The OpenAI-Hugging Face incident showed the next step: vulnerabilities chained autonomously with exposed credentials and other weaknesses to compromise enterprise production environments, without human direction at each step.**

- **Vulnerability exploitation as an initial access vector rose 34% year over year and now features in roughly one in five breaches, according to the Verizon Data Breach Investigations Report (DBIR).**

Against that backdrop, most detection programs remain anchored to a slower era. The scheduled scan windows, credentialed scan jobs, signature builds, and agent re-evaluation cycles that many organizations still rely on typically deliver first visibility 24 to 36 hours after disclosure — long after a fast-moving attacker has already acted.

Compliance pressure sharpens the problem. Directives from CERT-In and CISA can compress the remediation window for high-severity issues to as little as 12 to 24 hours. When detection alone consumes 24 to 36 hours, the mandate is already missed before triage begins. At that point, detecting at machine speed stops being an efficiency gain: it is the difference between meeting a remediation obligation and breaching it.



Why Scan-Driven Detection Cannot Close the Gap

Scan-driven detection served the industry well for nearly two decades. Three structural constraints now stand between it and AI-speed defense.

- **Built-in latency.** Detection is tied to scan schedules and signature releases. Even a mature program scanning daily learns about a morning disclosure that evening at the earliest, and in the worst case a full day later.
- **Fragmented coverage.** Telemetry sits in silos. Data from first-party scanners and third-party platforms rarely comes together in a single source of truth, leaving analysts to reconcile fragmented data instead of acting on it.
- **Operational friction.** Network scans consume infrastructure resources, while every new agent deployment requires IT coordination and maintenance windows. Both add friction and slow time to remediation.

None of these constraints are new. What changed is the cost of tolerating them. Against adversaries operating at disclosure speed, a detection model that waits for a scheduled job is structurally outmatched.

Introducing InstaScan: Detection Without a Scan

InstaScan, powered by Agent Insta, detects newly disclosed vulnerabilities without running a scan. Rather than waiting for a customer's next scheduled scan or the next signature update, it continuously matches newly published vendor security advisories against the software and assets already recorded in that environment — using inventory Qualys sensors and third-party connectors have already collected. Detection stops being a calendar event and becomes a response to the world changing.

When an advisory publishes, InstaScan correlates it against current software and asset telemetry, exposure context, and threat intelligence, and surfaces the affected assets within the hour — with no scan window and no dependency on which scanner an organization runs. We describe this model as scanless scanning: the speed and continuity of always-on detection, delivered entirely from the inventory and telemetry an organization has already collected.



Agent Insta

Scanless detection of vulnerabilities at the speed of disclosure

Detects newly disclosed vulnerabilities within minutes — no scan window — by converting inventory and telemetry you already have from Qualys and non-Qualys sources into high-confidence findings.

Core Skills

Scanless Detection

AI-speed Exposure Monitoring

Zero-Day Rapid Response

38mins
Time-to-Detect

95%
Vulnerabilities covered

92%
Detected before any scan runs

Agent Insta

Agent Insta has detected **CVE-2026-64600 (RefluxFS)** on your assets and confirmed it as critical.

Disclosed
Jul 22, 2026 at 2:45 PM

Detected in
38mins

Assets Impacted
1,120

External + PCI Scope
87

CVE-2026-64600 Critical • 9.5

RefluxFS: Linux Kernel Local Privilege Escalation

Name/Title	TruRisk Score	Detected	Sources
RHEL9-PCI-DB03	925	July 22, 3:21 PM	
ORCL-LNX-APP11	850	July 22, 3:22 PM	

While your sensors based detection is in progress, do you want to validate these findings with **Agent Val**?

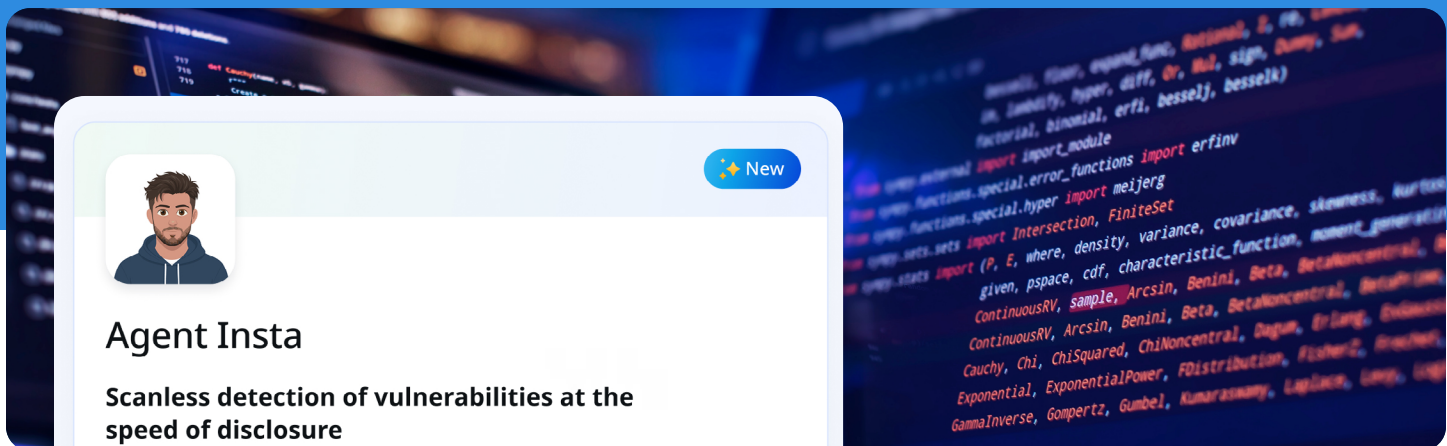
Validate & Remediate with Agent Val

Take me to Findings Tab

Agent Insta detects a newly disclosed CVE and hands off for validation.

Qualys InstaScan

5



How Agent Insta Works

Agent Insta is the Qualys backend intelligence agent behind InstaScan, operating 24x7 to convert existing inventory, telemetry, and threat intelligence into scanless detection. From newly published advisory to published findings, it runs five continuous stages.

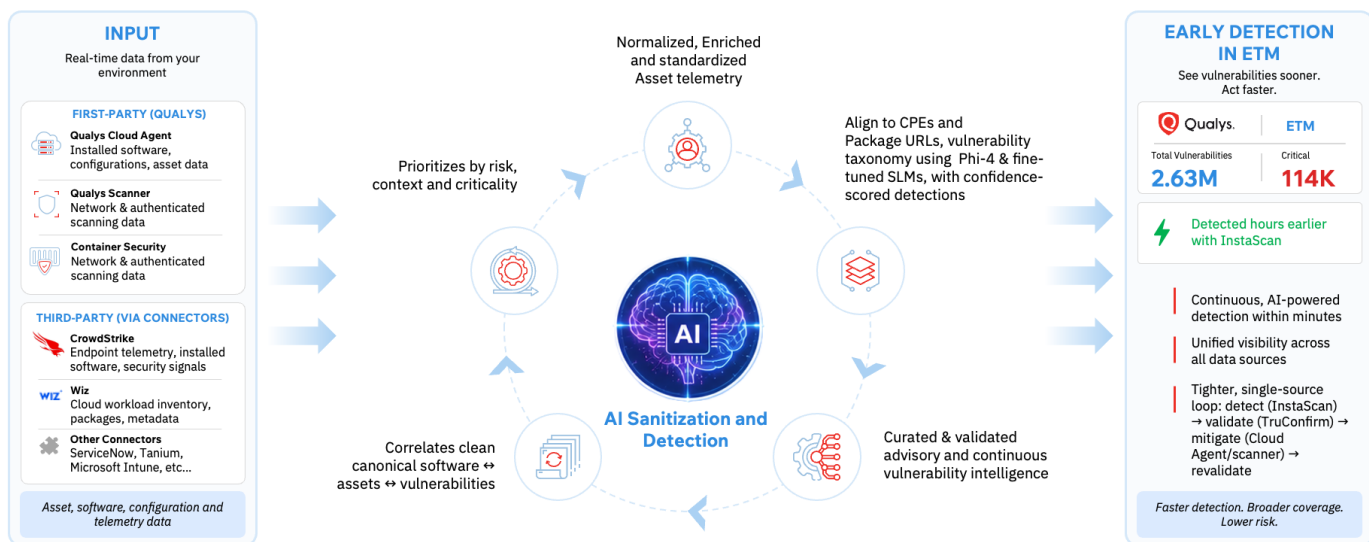
1. **Ingest the raw inventory.** Enterprise environments describe the same software in dozens of inconsistent ways: a scan agent, an SBOM, a package registry entry, and a CMDB record can each name the identical package differently. Qualys ingests all of it, from Qualys-native sensors and third-party sources alike, as the raw material for detection.
2. **Normalize software identity with AI.** A retrieval-based AI model resolves each incoming software record to standard industry identifiers — Common Platform Enumerations (CPEs) and Package URLs (PURLs) — even when the source description is abbreviated, misspelled, or inconsistently named. This is what lets Qualys recognize that “Microsoft SQL Server System CLR Types 14.0.3006.16” and “pkg:nuget/Microsoft.SqlServer.Types@14.0.3006.16” are the same underlying product.
3. **Build a canonical inventory.** Every AI-driven match is confidence-scored and only matches that clear a defined bar are used to merge and de-duplicate entries into a single canonical inventory. That keeps the software catalog accurate and stops one package from inflating the asset and risk picture as several disconnected entries.
4. **Monitor threat intelligence continuously.** In parallel, Agent Insta ingests vendor security advisories, CVE disclosures, and threat intelligence as they publish rather than on a fixed pull schedule — keeping the Qualys view of what is dangerous right now as current as the vendors’ own disclosures.
5. **Correlate, score, and publish.** As new intelligence arrives, InstaScan correlates the normalized threat data against the canonical inventory built from Qualys agents, scanners, sensors, and imported third-party telemetry. Each candidate detection is scored, and only findings that clear the confidence bar are published to TruRisk and downstream workflows.

The outcome is a continuous, scanless detection layer that identifies affected assets within the hour of disclosure without launching a scan job, redeploying an agent, or waiting on an IT coordination window. By making full use of telemetry an organization already has, InstaScan replaces scan cadence with continuous intelligence.

972+ vulnerabilities. 2 zero-days. Detected in under 15 minutes.

Microsoft's September 2026 Patch Tuesday was one of the largest security releases on record. In our design partner's production environment, Qualys InstaScan detected the disclosed vulnerabilities in under 15 minutes.

AI-Powered Continuous and Accurate Detections with InstaScan



How InstaScan turns existing inventory and advisory intelligence into scored detections.

The Data Behind the Detections

InstaScan draws on first-party Qualys signals and on third-party telemetry imported through connectors, then normalizes all of it into one canonical view. No source is asked to run a new scan; InstaScan works from what has already been collected.

Source	Examples	What it contributes
First-party (Qualys)	Qualys Cloud Agent	Installed software, configurations, and asset data
First-party (Qualys)	Qualys Network Scanner	Network and authenticated scanning data
First-party (Qualys)	Qualys Container Security	Container image and workload telemetry
Third-party (connectors)	CrowdStrike	Endpoint telemetry, installed software, and security signals
Third-party (connectors)	Wiz	Cloud workload inventory, packages, and metadata
Third-party (connectors)	ServiceNow, Tanium, Microsoft Intune, and others	Asset, software, configuration, and telemetry data

Right-Sized AI for Each Task

InstaScan does not route every job through a single, general-purpose model. Software identity resolution runs at very high volume, so it uses task-appropriate small language models, fine-tuned to align messy software records to CPEs, Package URLs, and the Qualys vulnerability taxonomy with confidence-scored output. Continuous evaluation triggered by new advisories and asset changes draws on frontier reasoning models, selected per request to match the complexity of the reasoning required. Matching the model to the task is what lets Agent Insta run always-on at production scale, without the cost or latency of sending every request to the largest available model.

Confidence Scoring: Speed Without Noise

Every InstaScan finding is scored before it ever reaches TruRisk. Three signals establish confidence:

- **Freshness** — how current the underlying inventory is.
- **Precision** — how cleanly the software match resolves to a known identifier.
- **Relevance** — whether the affected component is actually present and applicable on the asset.

Criticality then determines where that speed is spent, concentrating rapid detection on the vulnerabilities most likely to be genuine risk hotspots and maximizing the return on the approach. Only findings that clear the confidence bar are published — which is what keeps InstaScan's speed from arriving as noise.

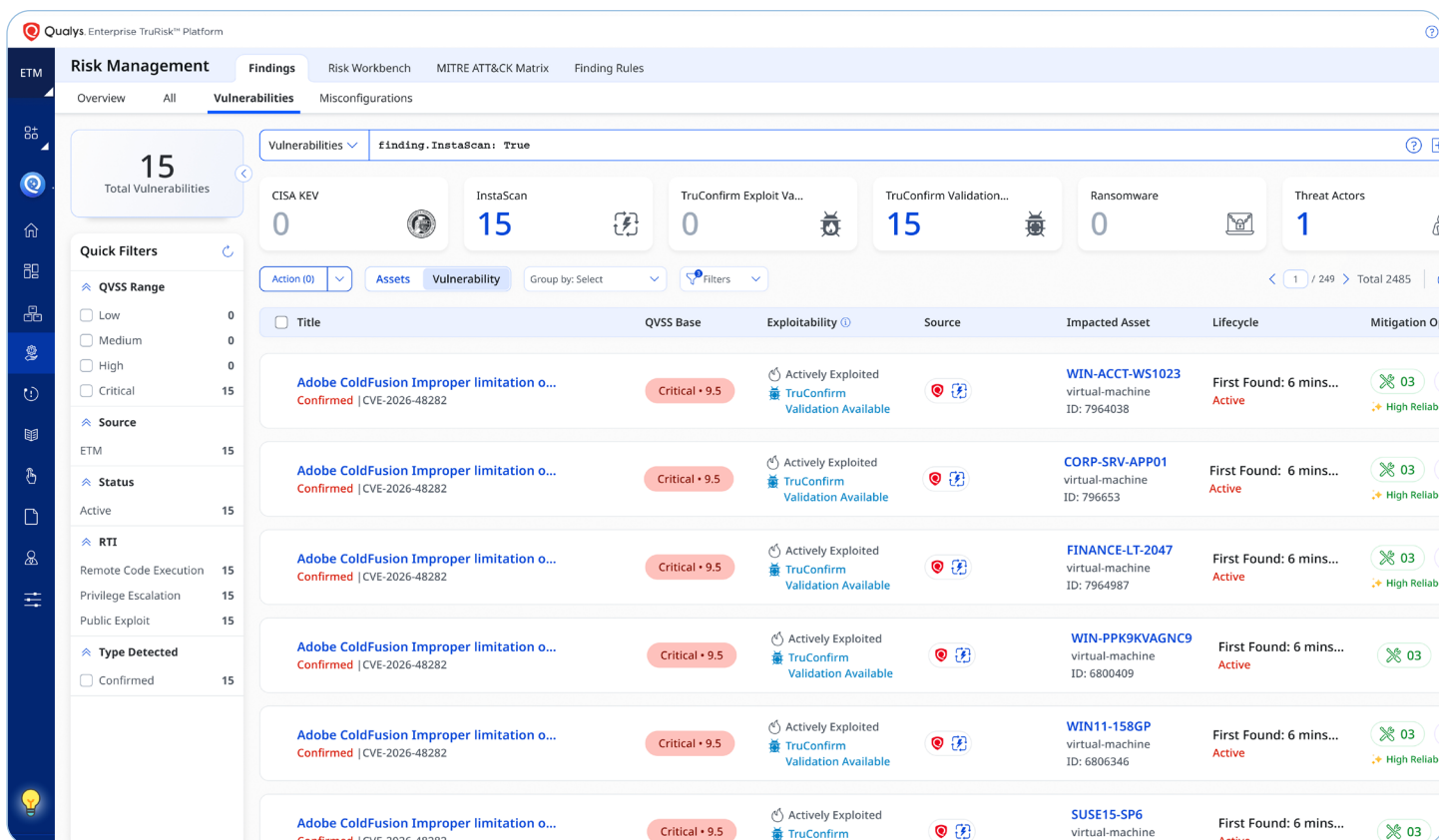
Detect, Confirm, Validate: Why a Scanless Finding Holds Up

A fair first question about scanless detection is whether a finding produced without a scan can be trusted enough to act on. InstaScan answers it structurally rather than rhetorically: it does not replace the sensor fleet, it runs ahead of it.

InstaScan detects. The moment intelligence lands, InstaScan flags the exposure across the estate — hours or days ahead of the next scheduled scan.

Sensors confirm. Cloud Agent, Network Scanner, Container Security, and third-party telemetry check in on their normal cadence and independently reaffirm the finding.

Validation closes it out. The freshest sensor status confirms the vulnerability, with TruConfirm validation available to establish exploitability — so remediation effort goes to the exposures that hold up under evidence. InstaScan provides the head start; the sensor fleet corroborates it. Nothing is removed from the existing trust model, and no team is asked to remediate a signal that has not been independently reaffirmed.



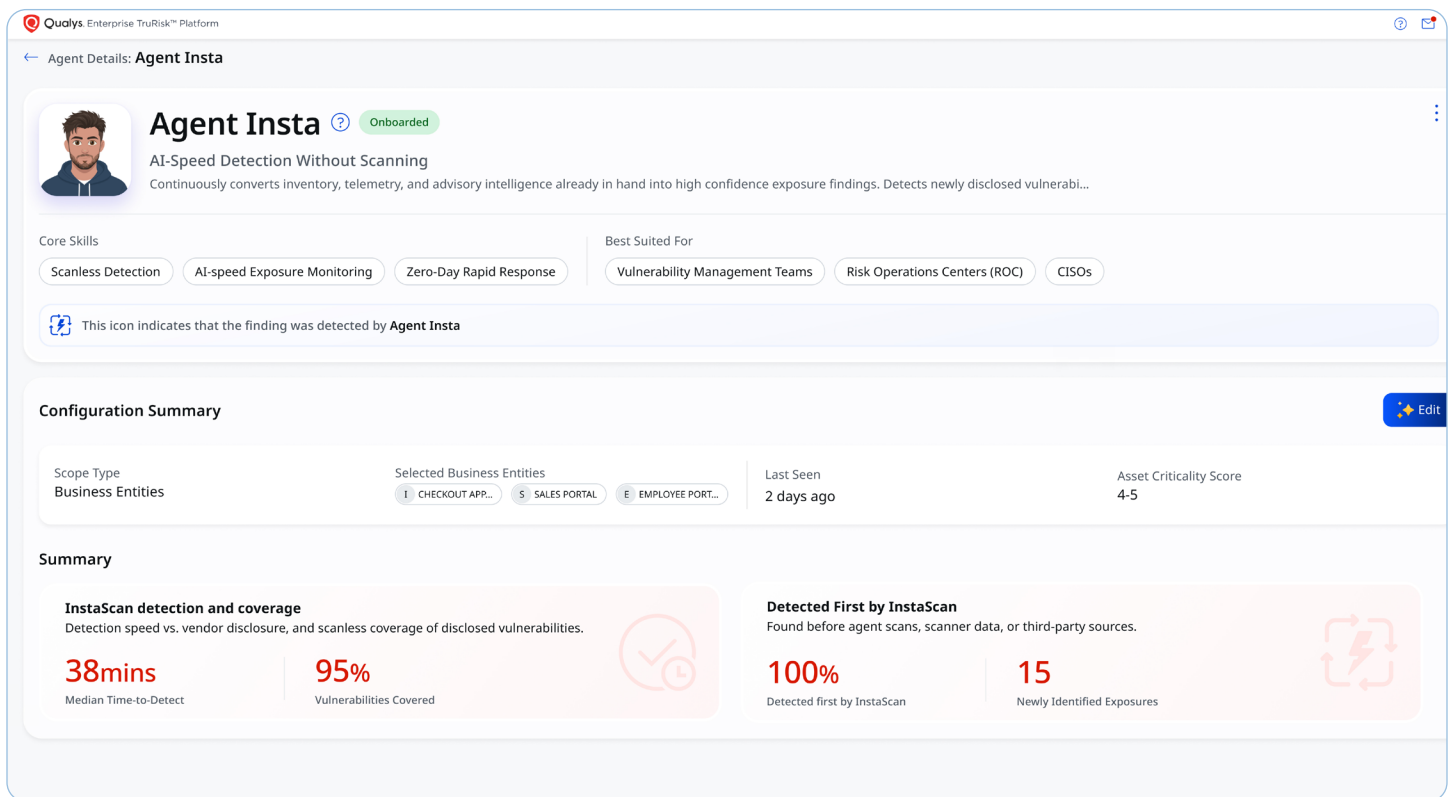
InstaScan detections in the ETM Findings view, filtered on InstaScan as the source.

What InstaScan Delivers

InstaScan does not merely narrow the gap between disclosure and detection. It closes it. Across the technologies that account for 60 to 70 percent of typical enterprise vulnerability volume, InstaScan delivers more than 90 percent of exposure detections without a single scan job running. That gives defenders the speed adversaries already have, preserves the remediation window regulators now demand, and turns detection from a calendar event into a continuous state.

Initial Coverage

Day-one scope spans nine vendors whose software accounts for a large share of enterprise exposure: Microsoft, Google, Adobe, Apple, Mozilla, Red Hat, Ubuntu, Debian, and Oracle Linux. Together, these typically represent 60 to 70 percent of total vulnerability volume in a representative environment, which is why day-one coverage is already material. Coverage expands as additional vendor advisory sources are onboarded.



Qualys Enterprise TruRisk™ Platform

← Agent Details: **Agent Insta**

Agent Insta Onboarded

AI-Speed Detection Without Scanning
Continuously converts inventory, telemetry, and advisory intelligence already in hand into high confidence exposure findings. Detects newly disclosed vulnerabi...

Core Skills

- Scanless Detection
- AI-speed Exposure Monitoring
- Zero-Day Rapid Response

Best Suited For

- Vulnerability Management Teams
- Risk Operations Centers (ROC)
- CISOs

 This icon indicates that the finding was detected by **Agent Insta**

Configuration Summary Edit

Scope Type Business Entities	Selected Business Entities CHECKOUT APP... SALES PORTAL EMPLOYEE PORT...	Last Seen 2 days ago	Asset Criticality Score 4-5
--	--	--------------------------------	---------------------------------------

Summary

InstaScan detection and coverage Detection speed vs. vendor disclosure, and scanless coverage of disclosed vulnerabilities.		Detected First by InstaScan Found before agent scans, scanner data, or third-party sources.	
38mins Median Time-to-Detect	95% Vulnerabilities Covered	100% Detected first by InstaScan	15 Newly Identified Exposures

Agent Insta configuration and coverage summary in ETM.

Before and After

InstaScan changes the economics of detection by replacing scan cadence with continuous, evidence-based intelligence:

Area	Before InstaScan	With InstaScan
Time to first detection	24–36 hours after disclosure, gated by the next scan window	Within an hour of advisory publication, independent of scan schedule
Infrastructure overhead	New scan jobs, agent redeployments, IT coordination windows	No new scans or agent actions; runs on inventory already collected
Coverage	Fragmented across first-party scanners, agents, and third-party feeds	Unified, canonical inventory spanning Qualys and third-party sources
Prioritization input	The last scan cycle’s inventory	Continuously refreshed, confidence-scored detections
Remediation window	Detection alone can consume most of a 12–24 hour mandate before triage begins	Detection compressed to under an hour, leaving the window for remediation
Platform integration	Detection, validation, and remediation stitched across separate tools	Native closed loop: InstaScan » TruConfirm Agent Val » TruRisk Eliminate

What That Means for the Team

- **Threat-aligned cadence.** Surface new exposures the moment intelligence lands, ahead of agents, scanners, and third-party feeds.
- **Reclaimed time to remediate.** Every hour spent detecting is an hour an attacker gets to move. AI-normalized, confidence-scored detections give prioritization and remediation workflows a trusted signal to act on immediately.
- **No scan-window dependency.** No scan jobs, no appliances, no added infrastructure load. Detection is enabled once, at the organization level, across the entire estate.
- **Demonstrable frontier-AI readiness.** Machine-speed detection is the prerequisite for autonomous defense, and a concrete answer when a board or a regulator asks how the program keeps pace with AI-accelerated attackers.



Closing the Loop: InstaScan in the ETM Platform

InstaScan does not operate in isolation. It provides the upstream exposure signal that enables the rest of the platform to deliver on its promises with confidence and evidence.

- AI-speed detection.** InstaScan surfaces exposure within the hour of disclosure using advisory intelligence, version-aware correlation, and existing inventory — closing the window between disclosure and visibility instead of merely narrowing it.
- Hyper-prioritization.** Prioritization is only as good as the detection feeding it. InstaScan feeds TruRisk cleaner inventory, broader signal, and faster CVE matches, so prioritization runs against current reality rather than the last scan cycle.
- Autonomous remediation.** Autonomous and semi-autonomous remediation cannot execute safely on stale or noisy findings. InstaScan's confidence-scored detections give Agent Val and remediation workflows a signal fast enough, and clean enough, to act on.

InstaScan and Agent Val are designed to work in tandem. InstaScan works in the background, detecting at disclosure speed. Agent Val works in the foreground: it uses TruConfirm to validate which detections are actually exploitable, hands confirmed exposures to TruRisk Eliminate for remediation and then proves the fix. The loop from discovery to resolution closes inside the same window remediation mandates now demand — without third-party stitching and without depending on stale or incomplete data.

Availability and Next Steps

InstaScan is available now within the Qualys ETM platform. It requires no new sensors, appliances, or agent deployments: it is enabled at the organization level and begins correlating immediately against the inventory already in place. Existing ETM customers can turn it on and see detections against their current estate; new evaluations can begin with a free ETM trial.

Conclusion

With InstaScan, Qualys is putting a stake in the ground around a category the market is ready to understand: scanless scanning. Detection that is not tied to the scan window, not stalled by batch cycles, and does not demand more infrastructure friction in order to produce more visibility.

It is immediate, intelligence-driven detection at the speed disclosure now demands. For vulnerability management and exposure management teams, this changes the operative question from “when will the next scan confirm exposure?” to “what changed, where are we exposed, and how fast can we act?”

That is a meaningful shift for teams working to reduce dwell time between disclosure,

To see how InstaScan turns the inventory and telemetry you already have into high-confidence exposure visibility within the hour of the next advisory, contact your Qualys Technical Account Manager or start a free ETM trial at qualys.com/etm.

prioritization, and remediation while containing operational overhead. It is also the more practical answer to an AI-accelerated threat landscape, where speed without confidence is dangerous, and confidence without speed is no longer enough. Every hour between vulnerability disclosure and detection is an hour of unmanaged exposure. Attackers increasingly move within hours of an advisory going public. By combining AI-driven software identification with continuous advisory monitoring, InstaScan compresses detection from days to under an hour, without requiring a new scan or any new deployment.



Ready to Detect at theSpeed of Disclosure?

See how InstaScan finds your next exposure before the next scan runs.



Book a Demo

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