

See what attackers see. Break the path before they take it.

Tanium External Attack Surface Management & Attack Path Mapping

The Problem

Internet-facing assets accumulate through cloud sprawl, SaaS adoption, and M&A activity, often without ever appearing in an internal inventory. 76% of organizations have suffered a cyberattack because of an unknown, unmanaged, or poorly managed internet-facing asset¹. According to Verizon 2026 Data Breach Investigations Report, 31% of breaches now start with vulnerability exploitation².

But the entry point is never the target; it's the first hop on a path. Security teams face tens of thousands of findings, and only a small fraction sits on a real path to a business-critical asset. Attackers don't exploit one asset in isolation; they chain exposed assets, identities, and cloud permissions together to reach their objective.

Best Practice: See. Prioritize. Act.

Closing the gap between exposure and breach comes down to three disciplines, in order. Skipping any one of them is why most exposure management programs stall out at a spreadsheet of findings nobody acts on.

Continuous visibility. An organization can't defend what it can't see. That means a complete, continuously refreshed inventory of every asset exposed to the internet, combined with what's already known internally about those same assets.

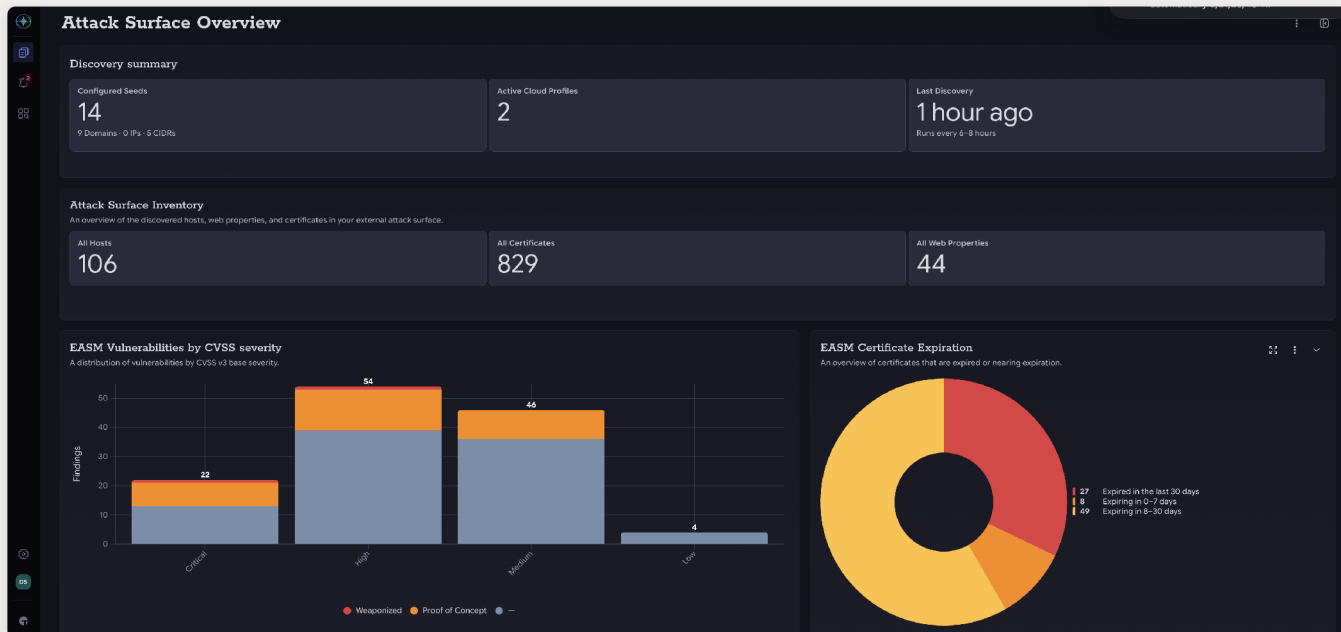
Impact-driven prioritization. Not every exposure deserves the same urgency. The right approach ranks exposures by whether they sit on a real path to something the business cares about, using business context and relationship data, not technical severity scores alone.

Closed-loop remediation. Visibility and prioritization only pay off if they lead somewhere. The fewer tools and handoffs, the faster the exposure gets fixed. And with the confidence that a remediation closed the vulnerability, without breaking anything else in the process.

Continuous visibility: Tanium External Attack Surface Management

Know your attack surface before attackers do.

Tanium EASM gives security teams a continuously updated inventory of internet-facing hosts, web properties, and TLS/SSL certificates associated with their organization. The attack surface changes daily; Tanium refreshes the scanning every 6–8 hours, so defenders work from close to the same picture of the attack surface that adversaries already have.



Graph 1 – Tanium Attack Surface Overview

How It Works

Configure Seeds

Identify and add the known domains, IP addresses, CIDRs, and ASN identifiers that belong to your organization. These seeds are the starting points for discovery. It is easy to get started, and expandable as the organization's footprint grows.

Discover External Attack Surface

Set scope and discovery parameters for each seed, and control who can see and manage them through role-based access control so external visibility can be extended safely without exposing the full environment.

Reduce Exposures

From those seeds, Tanium EASM continuously and comprehensively discovers and inventories the internet-facing hosts, web properties, and certificates that belong to the organization, refreshed every 6–8 hours.

Most external scanners run on a weekly or on-demand cadence. Continuous internet-facing scanning closes that gap, adding a real-time outside-in view on top of the real-time endpoint context Tanium already collects from the inside out.

Once assets are discovered, Tanium EASM evaluates and prioritizes them for open ports, services, CVEs, and misconfigurations. Security teams get a prioritized view of what attackers would exploit first, not just a list of exposures.

Key Capabilities

Continuous external inventory. Continuously refreshed inventory of internet-facing hosts, web properties, and certificates, updated every 6–8 hours.

Exploitability-prioritized CVEs. CVEs on external assets are ranked by real-world exploitability signal — not CVSS score alone. This helps remediation efforts focus on what's being exploited in the wild.

Enterprise readiness. Grant and restrict EASM access by role, so security teams can extend external visibility safely.

Full asset context in one place. Drill into any external asset's services, open ports, certificates, discovery path, and identified software.

Misconfiguration detection built in. HTTP header and service-level risk findings surface misconfigurations across external web properties and hosts directly in Tanium, without licensing a separate scanner.

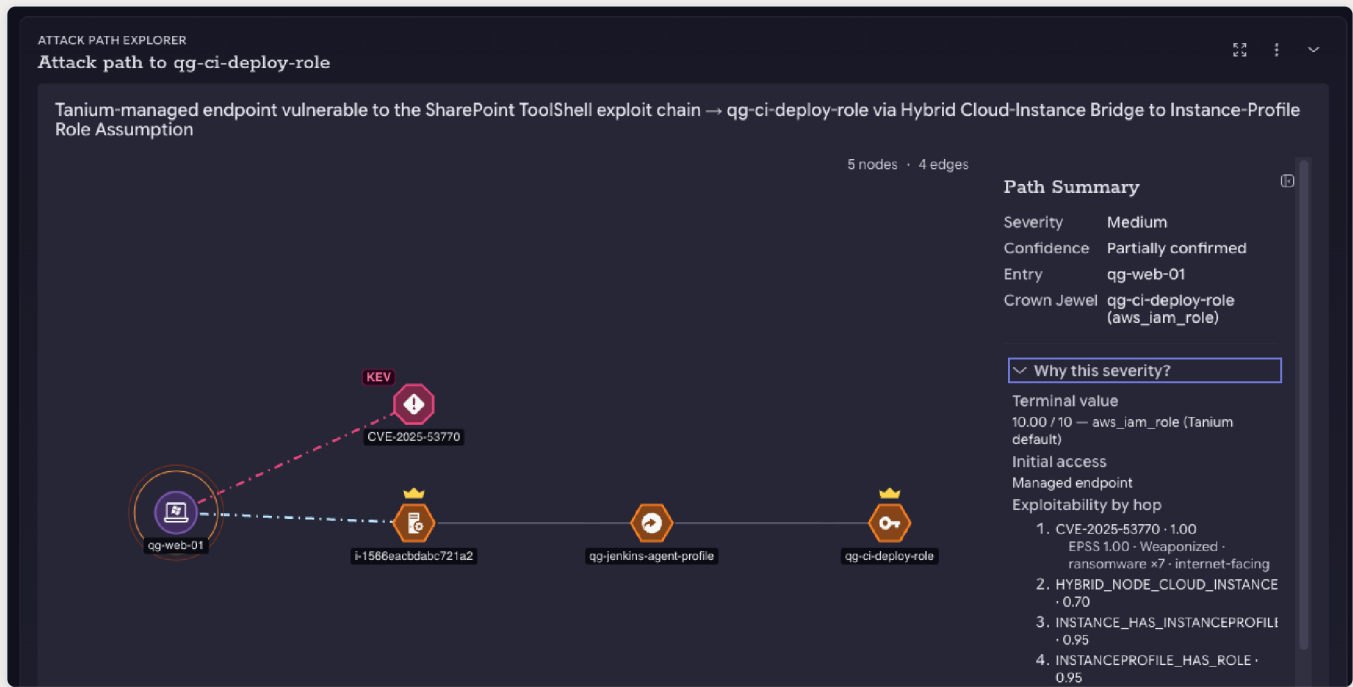
Impact-driven prioritization: Tanium Attack Path Mapping

See your environment the way an attacker does.

Tanium APM models how an attacker would chain vulnerabilities, exposures, misconfigurations, and permission relationships from an entry point to mission critical systems and customer-designated crown jewels. Instead of another list of findings, APM ranks paths by business impact: which ones lead somewhere that matters, which single fix breaks the most of them, and how far an attacker could get from here.

Tanium APM's unified correlation bridges an on-premises Windows endpoint or Microsoft Active Directory user to the synchronized cloud identity, cloud endpoint, AWS and Azure resource it controls, not a set of disconnected findings across separate tools.

Endpoint	Tanium APM continuously tracks the live configuration, local privileges, credentials cached, and sessions active on the endpoints.
Identity	Enterprise intrusions still travel through on-premises Microsoft Active Directory before reaching the cloud, moving laterally through group memberships, nested privileged groups, Kerberos delegation, and domain trusts. Tanium APM maps those permission relationships to show lateral movement as a path, not as findings scored in isolation. That correlation extends into Microsoft Entra ID for identity and device relationships, including the link from a Windows endpoint/Microsoft AD user to its synchronized cloud identity.
Cloud	Once an identity is correlated into the cloud, Tanium APM follows it into AWS resources and permissions as well as Azure subscriptions, resources, and RBAC role assignments. This enables true multi-hop paths: cloud-to-cloud and endpoint-to-cloud, following the specific resources and permission grants an attacker would traverse.



Graph 2 – Tanium Attack Path Mapping

How It Works

Attack Paths

The hop-by-hop route an attacker could walk from an initial compromise to a highest-value asset, whether a crown jewel or another critical asset. Each path's severity is ranked by how exploitable its traversals are and how critical the targeted asset is. Each hop and the path also carries a confidence score reflecting how difficult it would be for a real attacker to execute.

Choke Points

The highest-leverage fix: the one node where the most paths converge, and the remediation that breaks the most paths to crown jewels at once, eliminating unnecessary triage.

Blast Radius

Shows which crown jewels are reachable from a given node, forward and in reverse. It helps answer the question: "if this were compromised right now, what could attackers reach next?"

Key Capabilities

Attack Path Explorer — Inspect, filter, and pivot through detected paths on the Tanium Atlas graph, hop by hop, from entry point to crown jewel.

Attack Paths List — Every path ranked by severity, with terminal crown-jewel class, designation source, CVSS/KEV status, EPSS, Ransomware & botnet association, exploit maturity & weaponization, and path length.

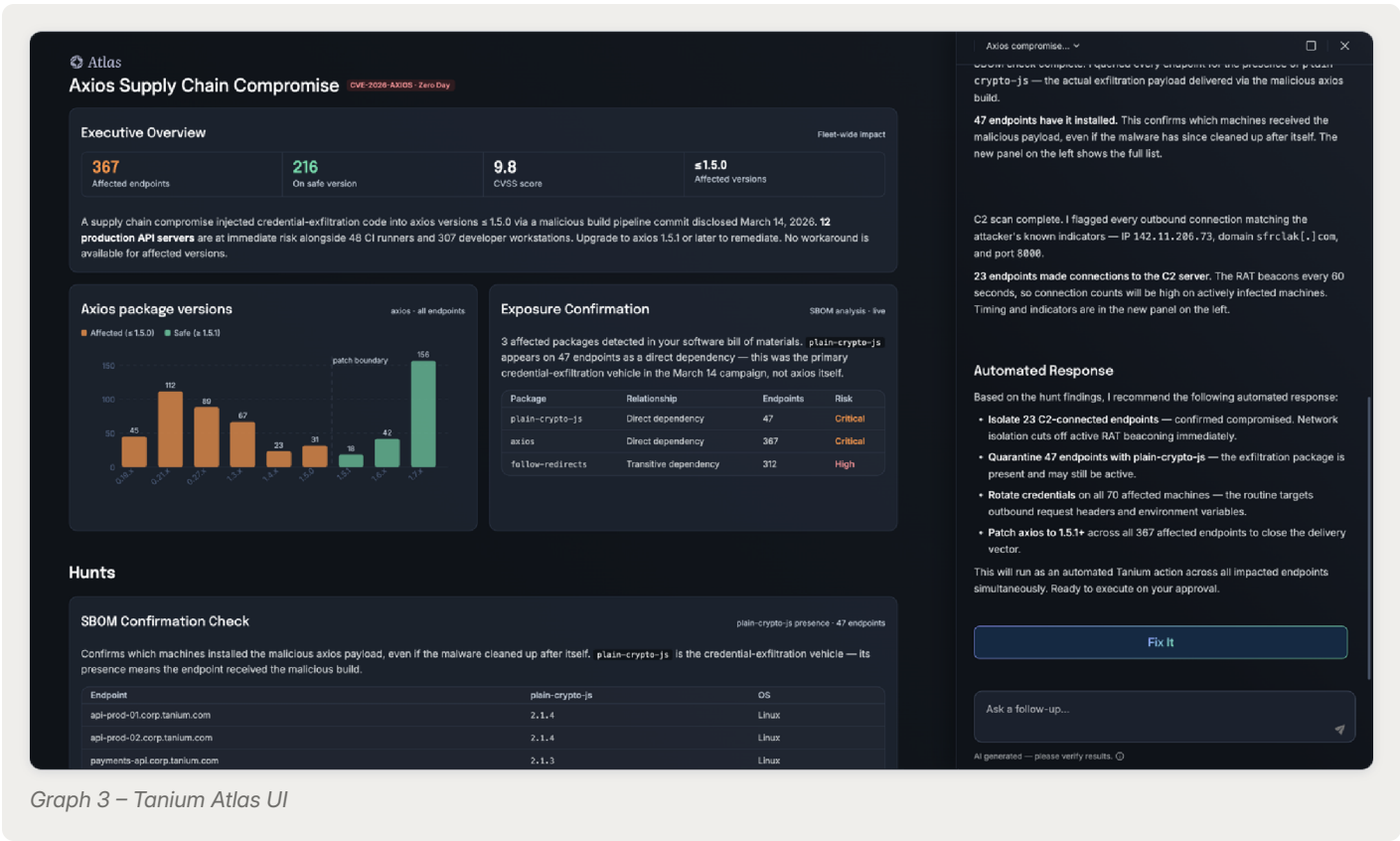
Crown Jewels, customer designation — Tanium designates crown jewels via automated logic and best practices; customers can designate or override any node, and customer designations always win.

Detection & remediation — Built on Tanium Atlas, it can quickly remediate a choke point and deploy an approval-gated fix in place, without exiting the platform.

Closed-loop remediation: Tanium Atlas

Fix the risks before they're exploited.

Tanium EASM and APM are both native to Tanium Atlas, so an analyst's investigation doesn't stop at a finding. Tanium Atlas correlates the finding, the path, and the fix in one graph: from the discovered exposure to the attack path it sits on, to the choke point that breaks the most paths at once. The whole investigation happens there, and so does the fix.



Graph 3 – Tanium Atlas UI

Governed remediation Tanium Atlas can quickly remediate a choke point or an external exposure and deploy the fix directly from the endpoint control plane. Autonomous but approval-gated, a human sign off before anything changes, with no handoff to a separate ticketing or remediation tool. The agent that gives Tanium real-time endpoint and attack-surface visibility is the same one that executes the fix, so there's no gap between finding an exposure and acting on it.

Closed-loop verification That same agent that does the remediation also verifies the attack path is actually broken, not just marked resolved. The loop closes with proof, not an assumption.

That's the advantage standalone tools can't replicate: continuous discovery, business-context prioritization, governed remediation, and verification – all on one platform.

The Bottom Line

In the new AI era, speed is the new perimeter. Where the market stops at visibility and AI recommendations, Tanium acts.

See the full Exposure Management platform: tanium.com/platform/exposure-management

Source:
1. Enterprise Strategy Group by Tech Target, Elevating Security with Risk-based Vulnerability Management, June 2024.
2. Verizon Data Breach Investigations Report, May 2026.