



Integrate to Remediate Proven Attack Paths and Verify Every Fix Automatically

Business challenge

Security teams know more about their weaknesses than ever and fix fewer of them. Scanners produce thousands of theoretical findings ranked by generic severity, with no evidence any are reachable in the live environment. Even when a pentest proves a path is real, the findings land in a backlog, remediation crawls, and nobody verifies the fix actually broke the path.

Solution

Horizon3 and Torq turn proven exploitability into verified remediation. NodeZero®, Horizon3's autonomous pentesting platform, safely attacks production from an assumed-breach position, chaining weaknesses the way an attacker would across network, cloud, identity, and Active Directory to prove what is genuinely reachable. Torq, the AI SOC platform, queries NodeZero for those proven attack paths and compromised credentials, orchestrates remediation at machine speed, then launches a verification pentest to confirm the path is closed.

Value

The integration collapses the gap between proof and fix. Validated attack paths flow directly into Torq workflows that rotate exposed credentials, isolate impacted hosts, tighten cloud access, and route remediation to the right owner — no analyst toil, no backlog. Because every action targets a weakness NodeZero has proven exploitable, automation breaks real paths instead of clearing theoretical ones.

Verification closes the loop. Once remediation completes, Torq launches a targeted re-test and reads back the result, confirming the fix held rather than assuming it. The hack, fix, verify cycle runs continuously, MTTR drops from weeks to minutes, and leaders see evidence-backed risk reduction instead of a patch count.

Torq + Horizon3 Benefits

Remediate proven exploitability:

Torq acts only on weaknesses NodeZero has demonstrated are reachable in production, focusing automation where risk is real.

Attack-path-first response:

Impact-scored attack paths and impacted hosts drive Torq workflows, so remediation starts at the choke points that break the most paths.

Automatic fix verification:

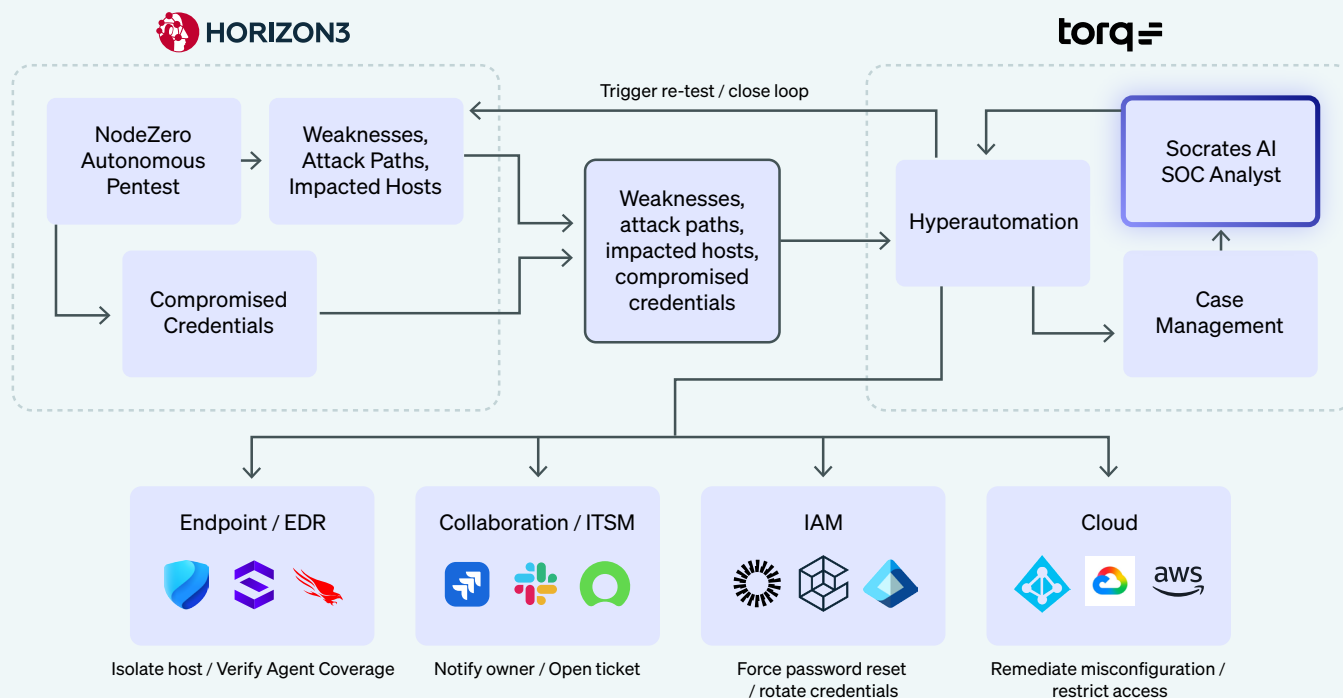
Torq launches a verification pentest after remediation and reads the result back, proving the path is closed without manual re-testing.

Credential exposure containment:

Compromised credentials surfaced by NodeZero trigger immediate rotation and session revocation across identity providers.

Continuous, autonomous validation:

Pentest operations run and scale under Torq orchestration, keeping validation continuous instead of periodic.



How it works

NodeZero autonomously pentests the live environment from an assumed-breach position, chaining vulnerabilities, misconfigurations, and credential weaknesses across network, cloud, and Active Directory into impact-scored attack paths. On a schedule or on demand, Torq queries Horizon3 to pull those proven findings into the SOC.

Signal enters Torq, where workflows enrich each finding with asset ownership and attack-path impact, and Socrates, Torq's AI SOC Analyst, determines what to fix first. Remediation runs in parallel across the stack — rotating credentials through IAM, isolating hosts through EDR, tightening cloud configurations, and notifying owners through collaboration and ITSM tools. Torq then launches a scoped verification pentest to confirm the path is closed. Verified findings resolve in Case Management; anything still exploitable routes back for another pass.

About Horizon3

Horizon3, the AI-Native Proactive Security Company behind NodeZero®, shifts the advantage from attackers to defenders by giving organizations the power to fight AI with AI. NodeZero, the World's Best AI Hacker™, autonomously tests your defenses at machine speed, safely finds and prioritizes exploitable attack paths, instantly verifies fixes, and drives a continuous hack, fix, verify loop. More than 7,000 organizations including the NSA, CISA, Fortune 100 enterprises, and major healthcare providers trust Horizon3 to prioritize what matters and for security you can prove.

Torq + Horizon3 use cases

Close proven attack paths automatically:
Torq pulls impact-scored attack paths and remediates them across identity, endpoint, and cloud, breaking multiple paths with each fix.

Contain exposed credentials on discovery:
Credentials NodeZero proves are compromised drive immediate rotation and session revocation, then re-verification.

Verify remediation without re-testing manually:
Torq launches a targeted verification pentest after every fix and resolves the finding only once the path is proven closed.

About Torq

Torq is the AI SOC platform transforming how enterprises manage risk. Using adaptive agentic reasoning and automation, Torq identifies, prioritizes, and remediates critical threats at machine speed, slashing MTI and MTTR while amplifying productivity. Global leaders like PepsiCo, Procter & Gamble, Siemens, Telefónica, and Virgin Atlantic trust Torq to power the next generation of AI-driven security operations. For more information, visit torq.io.