ATTACKIQ

Continuous Threat Exposure Management (CTEM) Platform

Scope, discover, validate, prioritize, and reduce exposure—*continuously.*

AttackIQ operationalizes Continuous Threat Exposure Management (CTEM) by identifying exploitable exposures, prioritizing them by likelihood and impact, and validating defenses through MITRE ATT&CK®-aligned adversary emulation—delivering measurable risk reduction.

Break Critical Attack Paths, Reduce Risk.

Security findings alone are not risk. AttackIQ connects vulnerabilities, identity exposures, misconfigurations, and control gaps to reveal where attackers can successfully move through your environment.

- Discover and correlate exposure across infrastructure, identity, and cloud

- Prioritize by likelihood of exploitation and impact of compromise

- Validate defensive effectiveness against real-world attack behavior

- Drive remediation and tracks progress over time

This is not vulnerability management. It is threat-informed, attack-path-aware, and grounded in defensive effectiveness—ensuring security controls perform as intended under real attack conditions.

HIGHLIGHTS

Discover Gaps Before Attackers Strike

Continuously discover | assets, vulnerabilities, and misconfigurations across your environment to eliminate blind spots and reduce risk.

Validate Security Controls with Real-World Scenarios

Emulate the latest adversary behaviors to ensure your defenses are prepared for threats that matter most to your organization.

Prioritize What Matters Most

Get prioritized, MITRE ATT&CK®-aligned recommendations based on your most critical exposures, so you spend time and resources where they have the greatest impact.

Turn Data into Prioritized Mobilization

Receive clear, step-by-step remediation guidance to shorten resolution times and quickly strengthen your security posture.

Track Exposure Reduction with Ease

Monitor improvements at a glance with an Exposure Management Score, enabling you to demonstrate security wins and justify investments to stakeholders.

Operationalize CTEM at Enterprise Scale

AttackIQ enables CTEM execution across the enterprise or targeted sub-scopes—by business unit, cloud, application, or regulated system—while maintaining centralized governance. Agent-based, agentless, and hybrid coverage extends across remote, on-prem, cloud, and container environments.
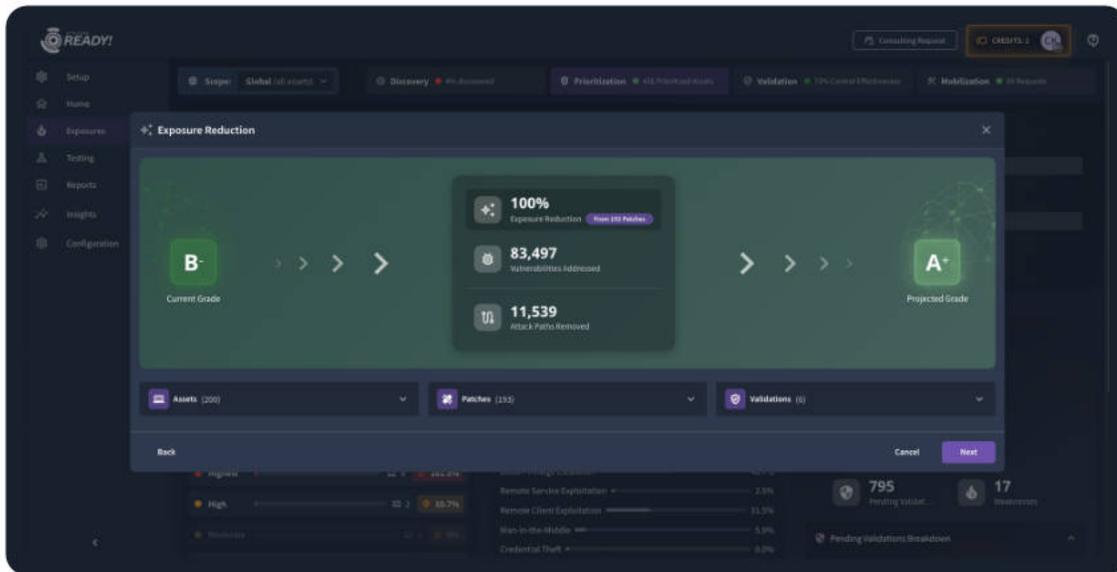
Continuous Exposure Correlation

AttackIQ discovers live attack surface through native discovery and ingestion from existing security tools. Findings are correlated into prioritized attack paths ranked by likelihood of attacker success.

AI-Driven Decision Support

AttackIQ leverages AVA, its AI Virtual Advisor, to turn fragmented findings into prioritized action—recommending what to remediate first, identifying follow-on validations, previewing mitigation impact, routing tickets into existing workflows, and tracking progress through the Exposure Management Score.

Prove your defenses perform under real attack conditions. [Schedule a demo.](#)