ATTACKIQ

READY

SOLUTION BRIEF

AttackIQ Ready

Continuous Adversary Exposure Validation Made Simple and Expertly Managed

Table of Contents

Executive Summary

AttackIQ Ready brings the power of continuous adversary exposure validation to organizations that need measurable assurance without the complexity of managing an enterprise testing platform. Operated with the guidance and support of AttackIQ experts, Ready continuously tests and validates the effectiveness of your defenses—across endpoint, email, network, and cloud controls—while you focus on remediation and improvement.

With **automated, MITRE ATT&CK®-aligned testing** and **expert-curated reporting**, Ready transforms validation into a frictionless, outcome-driven service. Results are distilled into **prioritized weaknesses, remediation guidance**, and **clear trend analysis** to show how your resilience improves over time.

By combining automation, intelligence, and expert oversight, AttackIQ Ready enables organizations to **validate continuously, act confidently, and reduce exposure—without the need to build or manage a testing program.**

The Need for Continuous Adversary Exposure Validation

Security teams face growing pressure to demonstrate that their defenses are effective, but manual validation is resource-intensive and limited in scope. Many organizations rely on point-in-time audits or red-team exercises that fail to keep pace with changing threats and environments.

According to IBM, the **average breach cost has risen to $4.88 million**, while Verizon's 2024 DBIR found that **68% of breaches involve the human element**—showing that prevention alone isn't enough. Continuous validation has become essential to ensure that controls function as intended against real adversaries.

AttackIQ Ready delivers that capability as a service. Customers get **enterprise-grade adversary testing, ATT&CK-aligned coverage, and expert reporting** that proves defensive effectiveness and guides exposure reduction.

Continued on next page.

The Value of AttackIQ Ready

Accelerate CTEM Maturity

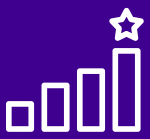
AttackIQ Ready aligns directly with the Continuous Threat Exposure Management (CTEM) framework, uniting validation, prioritization, and remediation within a single managed cycle. It helps organizations shift from reactive patching to proactive exposure management—continuously discovering, validating, and mobilizing fixes that close the most critical attack paths first.

Close Security Control Gaps

Continuously validate that controls perform as intended across endpoints, cloud, and boundary defenses. AttackIQ Ready identifies undetected exposures, misconfigurations, and detection gaps before attackers do—helping teams proactively close weaknesses and maintain defensive assurance.

Conserve Resources and Reduce Costs

Replace manual testing and fragmented validation efforts with continuous, automated testing at scale. Ready saves valuable analyst time and operational costs by identifying redundant controls, optimizing configurations, and minimizing the impact of breaches—while extending the lifespan of existing security investments.



Accelerate Mobilization and Accountability

Move from insight to action faster with prioritized weaknesses, step-by-step MITRE-aligned guidance, and integrated Jira/ServiceNow workflows. AttackIQ Ready mobilizes remediation across teams, enabling measurable progress and sustained security improvement.

Prove and Improve Resilience

Translate continuous testing into measurable business assurance. Ready helps organizations quantify progress over time, track ATT&CK coverage and key metrics, and communicate readiness to leadership—demonstrating a defensible, data-driven security posture.

The Value of AttackIQ Ready (cont.)

Gain Expert-Led Assurance and Clarity

AttackIQ's specialists act as an extension of your security team, analyzing test results, reviewing detection performance, and translating data into actionable guidance. Their insights help you **understand exposure in context**, communicate risk to leadership, and track measurable improvements in resilience over time.

Continuously Reduce Real Exposure (Add-On)

The Exposure Management Module (EMM) add-on enables you to **identify, understand, and mitigate what's truly exploitable** in your environment. It enhances **CTEM-aligned capabilities** across discovery, validation, and prioritization, allowing teams to focus on exposures that truly matter.

EMM unifies the power of Ready with **attack-path modeling** and **risk-based scoring**, you can rank vulnerabilities based on environmental context and identify choke points where a single fix breaks multiple attack paths. The outcome: measurable, continuous reduction of real organizational exposure—not just vulnerability counts.

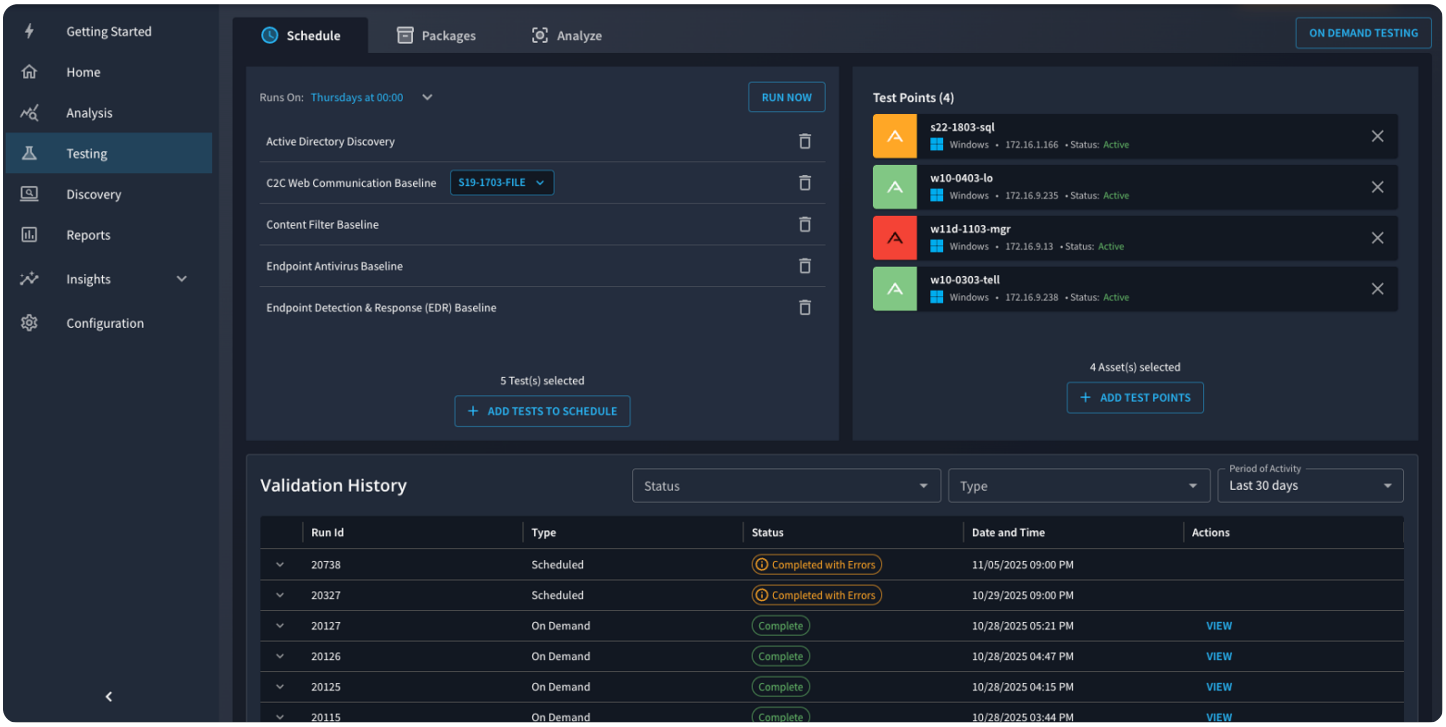
Continued on next page.

What You Can Do with AttackIQ Ready

AttackIQ Ready makes adversary exposure validation effortless. Customers receive continuous, automated testing, actionable reporting, and hands-on expert analysis —without needing to manage the platform themselves.

Optimize Defensive Posture

AttackIQ Ready helps you validate that the key layers of your defense are performing as intended. These capabilities enable continuous control assurance across your hybrid environment, ensuring that preventive and detective technologies stay effective as configurations evolve and threats change:



- ✓ **Validate endpoint security** by testing malware, lateral movement, and credential-theft defenses across Windows, macOS, and Linux.
- ✓ **Test boundary controls** by validating email, web, and WAF policies and replaying PCAPs against real attack traces.
- ✓ **Confirm DLP protections** by simulating data-exfiltration attempts and validating egress prevention policies.

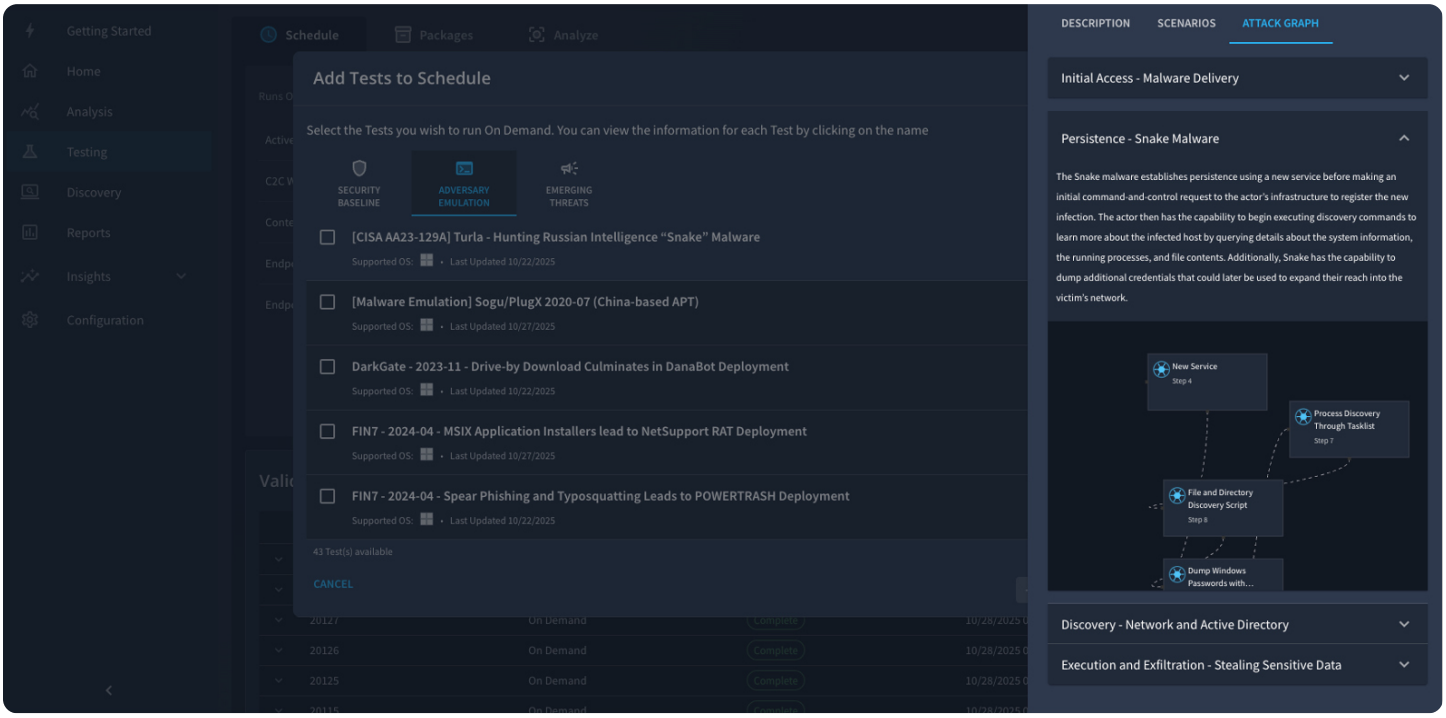
Optimize Defensive Posture (cont.)

- ✓ **Monitor posture over time** with dashboards, KPIs, and trend analysis to measure progress across repeated tests.
- ✓ **Prioritize exposures** with a weaknesses view ranked by impact, likelihood, and business relevance.
- ✓ **Follow prescriptive, MITRE-aligned mitigation steps** that guide security teams to actionable closure.
- ✓ **Integrate with Jira and ServiceNow** to assign and track remediation tasks directly from results.
- ✓ **Leverage expert insights** from AttackIQ consulting teams to refine remediation workflows and validate fixes.

Scale Offensive Testing

AttackIQ Ready gives you the ability to simulate adversary behaviors using MITRE ATT&CK-aligned emulations.

Ready enables you to run **adversary emulations** mapped to the MITRE ATT&CK framework, including **coverage of CISA advisories** that measure the effectiveness of your defenses against the latest adversarial tradecraft. It delivers results and mobilization strategies through enterprise-grade reporting.



Reduce Exposure

AttackIQ Ready supports **Continuous Threat Exposure Management (CTEM)**, enabling organizations to move beyond testing and validation to **scoping, discovery, and prioritization** of exposures across the attack surface. These capabilities help teams understand what's most exploitable, reachable, and impactful in their environment—and act faster to reduce risk.

Core capabilities allow you to:

- ✓ **Scope discovery** to specific endpoints, IP ranges, and domains, and import asset inventories from third-party sources to anchor the testing scope.
- ✓ **Assess identity risk in Active Directory**, including privileged accounts, risky relationships, and misconfigurations.
- ✓ **Audit endpoint and server exposure**, identifying open ports, services, and active RDP sessions that expand the attack surface.
- ✓ **Map the external attack surface**, including public IPs, TLS configurations, and internet-facing assets.
- ✓ **Reveal internal subnets, VLANs, and shared SMB/NFS resources** to detect lateral-movement opportunities.

Reduce Exposure (cont.)

- ✓ **Ingest vulnerability data** from leading scanners such as Rapid7, Tenable, Qualys, and CrowdStrike Spotlight.
- ✓ **Uncover business-sensitive applications and databases** hosting critical or regulated data.

As organizations face **vulnerability overload and alert fatigue**, most lack the context needed to focus remediation on what truly matters. The **Exposure Management Module add-on** extends **AttackIQ Ready** with **advanced threat modeling, attack-path intelligence, and business-aware risk scoring**—turning static vulnerability data into validated, prioritized, and measurable exposure reduction. By incorporating your environment's real-world context—such as **Active Directory relationships, network reachability, and control configurations**—EMM enables organizations to see where they are truly exposed and act decisively to reduce risk.

With the Exposure Management Module, organizations are able to:

- ✓ **Model attack paths** to crown-jewel assets using identity, network topology, and control validation to calculate the probability of an incident.
- ✓ **Identify choke points** where a single fix can collapse multiple attack paths, accelerating exposure reduction.
- ✓ **Deprioritize vulnerabilities** already blocked by effective controls and **rank remaining vulnerabilities** based on user privileges, AD relationships, and network reachability.
- ✓ **Score overall risk** through unified metrics that combine vulnerability data, control efficacy, and business impact.

Continued on next page.

The Value of AttackIQ Ready in Action

Gain Continuous Proof That Your Defenses Work

AttackIQ Ready transforms adversary validation into an always-on service, continuously testing against real-world attack behaviors. Each validation cycle delivers clear, evidence-backed results—**demonstrating control effectiveness without adding operational burden.**

Reduce Risk Faster with Targeted, Prioritized Remediations

Every Ready report prioritizes weaknesses that have the highest impact on your organization's resilience. Step-by-step, MITRE-aligned remediation guidance empowers teams to **fix what truly reduces risk**, eliminating guesswork and wasted effort.

Demonstrate Progress and Value to Leadership with Confidence

Track measurable improvement across testing cycles with intuitive dashboards that visualize **ATT&CK coverage, control performance, and trend KPIs**. Ready equips leaders with defensible metrics to communicate readiness and justify investment.

Advance CTEM Maturity Without Added Complexity

Ready operationalizes CTEM by pairing ongoing validation with prioritized mitigation insights—**accelerating exposure reduction with no new headcount, setup, or tooling required.**

Accelerate Exposure Discovery and Mitigation (EMM Add-On)

For organizations ready to take the next step, Ready seamlessly integrates with the Exposure Management Module (EMM) add-on, providing **attack-path modeling, exploitability-based prioritization, and exposure scoring**. Together, they transform testing insights into **real-time exposure management**.

Highlights

Test Safely and Continuously

Run weekly or on-demand tests across up to 50 test points continuously. AttackIQ Ready is designed to deliver safe, realistic adversary emulations that measure security effectiveness across Windows, macOS, and Linux.

MITRE ATT&CK Alignment

Maintain full transparency and traceability between adversary behaviors and your defensive posture. Every test aligns with MITRE ATT&CK, CISA advisories, and real-world adversary tradecraft, enabling measurable and repeatable control validation across your organization.

CTEM Enablement

AttackIQ Ready helps organizations operationalize Continuous Threat Exposure Management (CTEM) by aligning discovery, validation, prioritization, and remediation in a single workflow. This unified approach enables teams to reduce exposure iteratively and demonstrate continuous improvement in resilience.

Attack Surface Discovery

Continuously uncover external and internal assets to understand what's exposed to attackers. AttackIQ Ready identifies users and systems within your environment, helping you define the true scope of what needs testing and protection.

Attack Path Management (EMM Add-On)

Visualize and analyze how attackers could move through your environment to reach critical assets. EMM models attack paths and identifies choke points—where one fix can collapse multiple routes—enabling faster, evidence-based reduction of real exposure.

Expert Consulting & Advisory Services

Access on-demand expertise from AttackIQ's consulting and adversary research teams to refine your testing strategy, improve scenario design, and accelerate validation maturity. Get tailored guidance to implement best practices and improve control resilience.

Agentless, On-Demand Testing Anywhere

Run tests instantly using Flex packages—no agent deployment or setup required. AttackIQ Flex enables lightweight, agentless testing that can validate security controls on any Windows environment on demand, accelerating assessments without operational overhead.

Continuous Security Validation

Continuously validate that controls perform as intended across endpoints and boundary defenses. AttackIQ Ready identifies control gaps before attackers do—helping teams proactively close weaknesses and maintain defensive assurance.

Weakness Management

Identify and track weaknesses across the enterprise with prioritized remediation guidance aligned to MITRE mitigations.

Vulnerability Prioritization (EMM Add-On) Cut through vulnerability overload by focusing on what's truly exploitable. The EMM add-on ranks vulnerabilities based on exploitability and reachability, transforming endless CVE lists into focused, high-impact remediation priorities.

Risk Scoring (EMM Add-On)

Quantify exposure with unified risk scores that combine vulnerability data, control efficacy, and asset criticality. This risk-based view enables teams to communicate exposure clearly to executives and track measurable reductions over time.

Automated, Enterprise-Grade Reporting

Translate technical validation into actionable results you can track weekly or on demand through enterprise-grade reports and in-platform KPIs and MITRE-aligned scoring.

See AttackIQ Ready in action.

Schedule a technical consultation: attackiq.com/demo.

ATTACKIQ

U.S. Headquarters

171 Main Street
Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading provider of Adversarial Exposure Validation (AEV) solutions, is trusted by top organizations worldwide to validate security controls in real time. By emulating real-world adversary behavior, AttackIQ closes the gap between knowing about a vulnerability and understanding its true risk. AttackIQ's AEV platform aligns with the Continuous Threat Exposure Management (CTEM) framework, enabling a structured, risk-based approach to ongoing security assessment and improvement.

The company is committed to supporting its MSSP partners with a Flexible Preactive Partner Program that provides turn-key solutions, empowering them to elevate client security. AttackIQ is passionate about giving back to the cyber-security community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.