Service Definition: AttackIQ Platform

This service description provides additional information for buyers of the AttackIQ Platform.

Bright Cyber is an authorised reseller of the AttackIQ Platform. This service is offered through the G-Cloud framework in accordance with the published service listing and associated documentation.

Further information about the platform is available in the brochures provided as part of this service description. Buyers may also contact Bright Cyber using the details below for clarification or support.

Service Roles and Responsibilities

Bright Cyber Responsibilities
Bright Cyber is responsible for the commercial relationship with the buyer and for ensuring service delivery. This includes:

Account Management
- Provision of a named account manager
- Availability Monday to Friday, 9:00am to 5:00pm (excluding public holidays)
- Response to email queries within 4 working hours
- Direct telephone contact details will be provided

Service and Advisory Support
- Advice relating to use of the AttackIQ Platform
- Guidance on information security matters relevant to the service

Commercial Management
- Contracting under the G-Cloud agreement
- Billing and invoicing
- Management of service variations, extensions, and additional services where agreed
- All commercial activities managed in accordance with G-Cloud terms and conditions

Bright Cyber will ensure the service is delivered in line with the agreed scope and will support the buyer in using the service effectively.

This may include:
- Coordinating onboarding activities
- Attending service review or progress meetings where required
- Supporting issue escalation and resolution

- Ongoing service coordination and governance

AttackIQ Responsibilities
AttackIQ is responsible for delivery and technical operation of the platform, including:

- Platform provisioning and onboarding
- Delivery of the service in line with the published service description and specifications
- Provision of technical support for the platform

Service Contact Details

Service Contact: Murray Pearce
Email: murray.pearce@bright-cyber.co.uk
Telephone: 0345 257 0071
Website: https://bright-cyber.co.uk

See AttackIQ brochure following this page for futher service information.

ATTACKIQ

ENTERPRISE

SOLUTION BRIEF

AttackIQ Enterprise

Comprehensive Adversary Exposure Validation for Large and Complex Environments

© 2025 AttackIQ, Inc. All Rights Reserved.

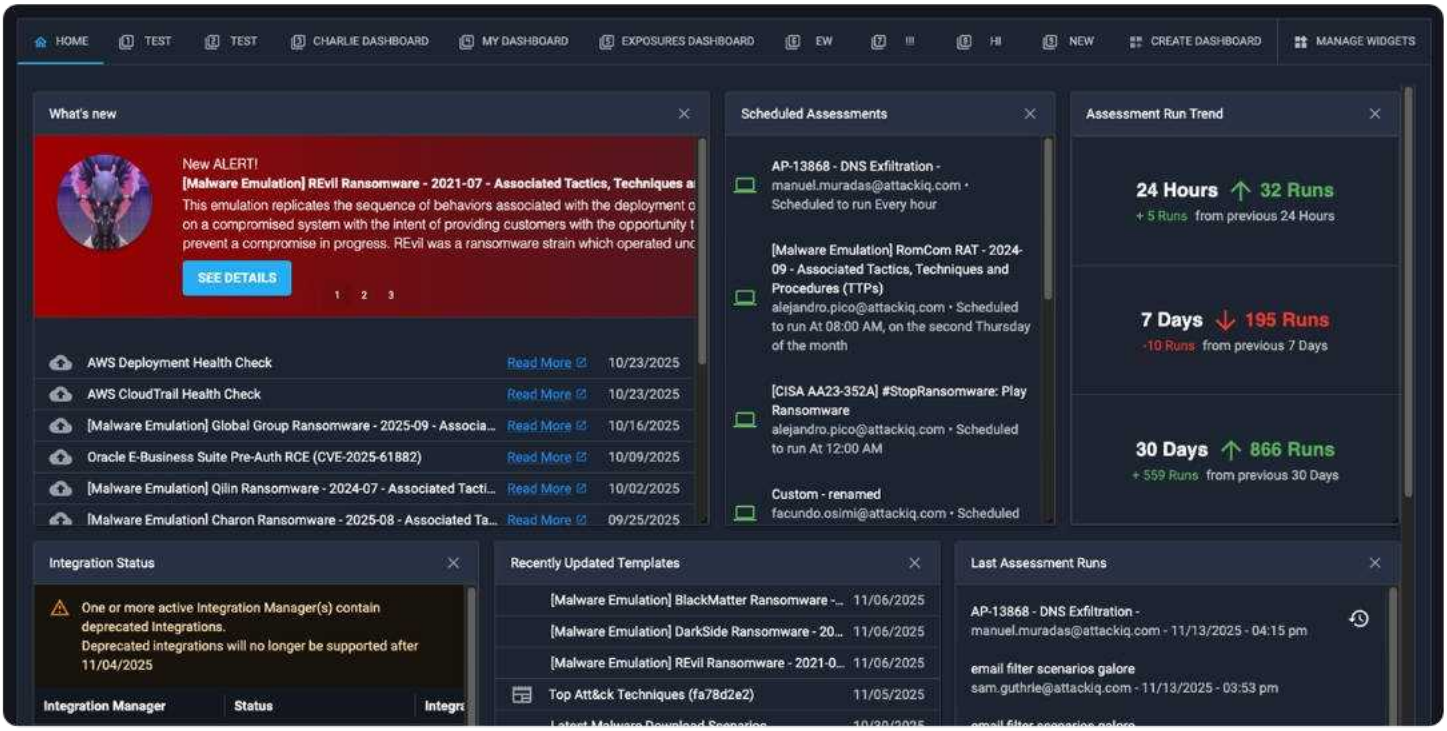
Table of Contents

Information and Use: The information contained in this document is provided for informational purposes only and is subject to change. Nothing herein should be interpreted as a commitment or guarantee of future functionality, performance, or delivery.

No Public Disclosure Permitted: This document is not to be used, copied, modified, reproduced, or distributed without the express written consent of AttackIQ. Please report postings of this document on public servers or websites to support@attackiq.com.

Executive Summary

AttackIQ Enterprise is a comprehensive adversary exposure validation platform that enables security teams to continuously test, measure, and improve their defenses across endpoints, cloud, and Security Information and Event Management (SIEM) pipelines. Designed for complex, hybrid environments, it gives organizations the flexibility to run unlimited, anytime testing, validate how well their controls perform against real adversary behaviors, and turn technical findings into evidence of measurable resilience.



With an extensive **MITRE ATT&CK-aligned test library** and AI-assisted automation, AttackIQ Enterprise empowers users to simulate sophisticated attacks, verify detections end-to-end, and uncover control gaps before adversaries exploit them. Teams can track ATT&CK coverage and defensive performance through dashboards, delegate reporting by business unit, mobilize remediation with step-by-step, MITRE-aligned guidance, and enhance detections with out-of-the-box or AI-generated detection rules.

By unifying **exposure visibility, validation, and mobilization** with automation and scalability, AttackIQ Enterprise transforms testing outcomes into actionable intelligence that **reduces organizational exposure over time**. It integrates with leading **security controls and SIEM platforms** to validate detections, while a **prioritized weakness view** helps teams focus on the exposures that matter most. The result is a **continuous, adversary-informed readiness** — allowing organizations to **strengthen critical controls, sustain measurable resilience gains, and maintain adversary-informed readiness** against evolving threats.

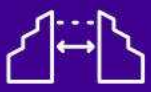
The Need for Continuous Adversary Exposure Validation

Every organization has a broad range of security controls in place; yet, effectiveness remains inconsistent, and adversaries evolve faster than defenses. Teams struggle to prove controls work as intended, prioritize exposures, and scale testing across complex hybrid estates spanning endpoints, cloud, and the SIEM pipeline. The average cost of a data breach climbed to $4.88 million in 2024, with 68% of breaches involving the human element, such as phishing, credential misuse, or error. In AttackIQ production analyses, endpoint detection and response tools stopped the top seven adversary techniques only 39% of the time, underscoring that traditional defenses alone are insufficient, and that performance must be verified continuously.

Evolving attacker tradecraft, expanding control surfaces, and faster attack cycles further shrink the window for detection and response—**median attacker dwell time has dropped to just 10 days**. Manual testing methods, like penetration testing or red teaming, cannot scale to cover enterprise-wide controls, leaving organizations blind to detection rule decay and control drift. To stay ahead, enterprises require **repeatable, ATT&CK-aligned validation at scale**, with **outcome-driven reporting and prescriptive mobilization guidance**—a continuous adversary exposure validation program that closes the gap between control assumptions and real-world resilience.

Continued on next page.

The Value of AttackIQ Enterprise



Close Security Control Gaps

Continuously validate that controls perform as intended across endpoints, cloud, and boundary defenses. AttackIQ Enterprise 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. Organizations save valuable analyst time and operational costs by identifying redundant controls, optimizing configurations, and reducing breach impact—while extending the lifespan of existing security investments.

Detect and Stop Threats Faster

AttackIQ Enterprise transforms detection from guesswork into precision. By validating and refining detection rules across your SIEM pipeline, security teams can identify and respond to real adversary behaviors with speed and accuracy. **AI-assisted detection engineering** continuously optimizes Sigma, KQL, and SPL rules, eliminating blind spots and stale detections. The result: a leaner, more responsive detection stack that spots threats early, shortens dwell time, and stops attacks before they escalate.

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 Enterprise mobilizes remediation across teams, enabling measurable progress and sustained security improvement.

Prove and Improve Resilience

Translate continuous testing into measurable business assurance. AttackIQ Enterprise 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 Enterprise (cont.)

Accelerate CTEM Maturity

AttackIQ Enterprise will align directly with the **Continuous Threat Exposure Management (CTEM)** framework, uniting validation, prioritization, and remediation within a single managed cycle. This will help organizations transition from reactive patching to proactive exposure management—**continuously discovering, validating, and mobilizing fixes** that close the most critical attack paths first.

Continuously Reduce Real Exposure

AttackIQ Enterprise is evolving to help you **see, understand, and minimize what's truly exploitable** in your environment. With upcoming **CTEM-aligned capabilities**, the platform will unify discovery, validation, and prioritization, allowing teams to focus on exposures that truly matter. The **Exposure Management Module (EMM)** add-on extends this power with **attack-path modeling** and **risk-based scoring**, helping you identify choke points where one fix breaks multiple attack paths. The outcome: measurable, continuous reduction of real organizational exposure—not just vulnerability counts.

Validate Readiness Against Threats Targeting You (Add-On)

Threats evolve every day—your testing should, too. With the **Watchtower add-on**, AttackIQ Enterprise turns live, **hyper-local threat intelligence** into **actionable validation**. It automatically detects adversaries targeting your IPs and domains, then generates **ATT&CK-mapped, ready-to-run test plans,** so you can confirm your defenses block what's actively hitting you right now. The result: faster adaptation, stronger assurance, and a threat response program that stays one step ahead.

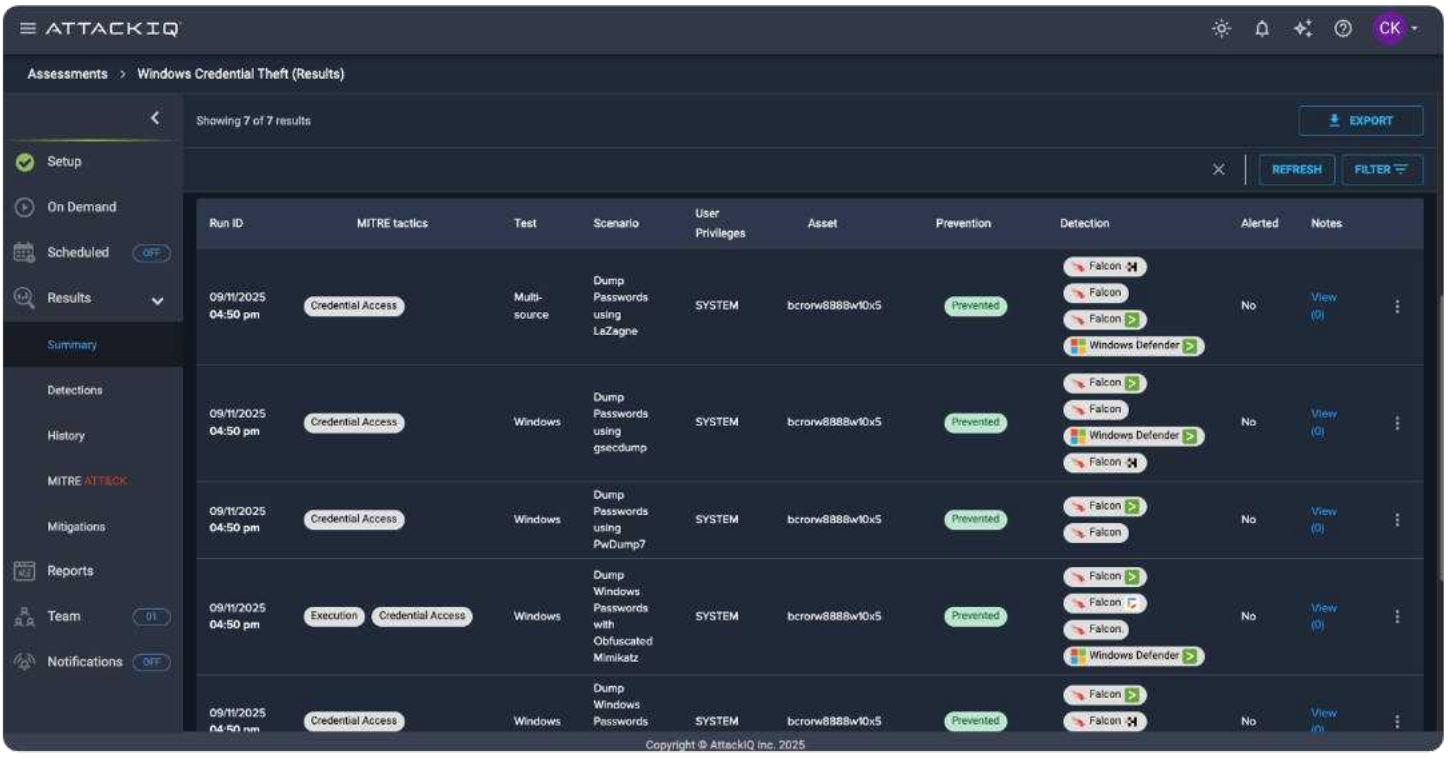
Continued on next page.

What You Can Do with AttackIQ Enterprise

AttackIQ Enterprise empowers security teams to continuously validate, optimize, and mature their defensive posture against adversary behaviors. From testing control performance and simulating advanced adversaries to improving detections and driving mobilization, it delivers the flexibility and depth needed to strengthen readiness across hybrid environments. The following sections outline what you can achieve with AttackIQ Enterprise today—and what's coming soon as the platform expands towards exposure reduction through Continuous Threat Exposure Management (CTEM).

Optimize Defensive Posture

AttackIQ Enterprise helps you validate that every layer of your defense is performing as intended—from endpoints to cloud workloads and SIEM pipelines.



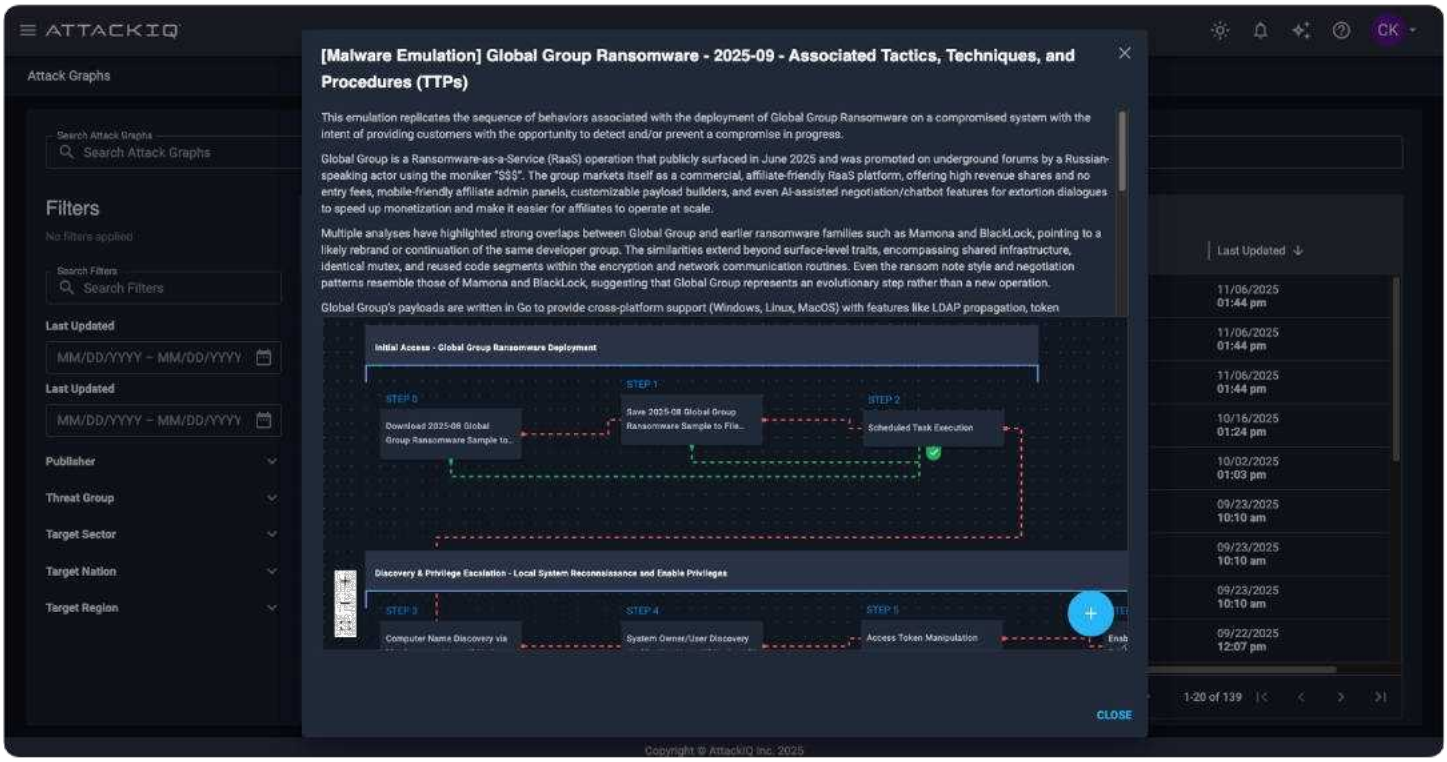
Optimize Defensive Posture (cont.)

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.
- ✓ **Verify SIEM performance** by testing rule logic, log ingestion, and detection latency, with AI-assisted rule-to-test matching.
- ✓ **Assess cloud guardrails** by testing AWS and Azure controls against internal and external threats.
- ✓ **Monitor posture over time** with dashboards, KPIs, and trend analysis to measure progress from repeated tests.
- ✓ **Delegate by business unit** with entity-specific reporting and role-scoped views to support executive accountability.
- ✓ **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.
- ✓ **Receive advanced alerts and notifications** for new exposures or validation failures across critical systems
- ✓ **Leverage expert insights** from AttackIQ consulting to refine remediation workflows and validate fixes.

Scale Offensive Testing

AttackIQ Enterprise gives you the ability to simulate adversary behaviors at scale using MITRE ATT&CK-aligned emulations. Whether you're running out-of-the-box scenarios, tailoring tests to your environment, or converting intelligence reports into ready-to-run simulations, you can continuously measure how well your defenses perform against the latest adversarial tradecraft.



- ✓ **Run adversary emulations** mapped to the MITRE ATT&CK framework, including CISA advisory coverage.
- ✓ **Create custom attack scenarios** tailored to your environment, assets, or threat profile.
- ✓ **Act on real-world threat intelligence** by automatically converting CTI reports (URLs, PDFs, Excel) into ready-to-run, ATT&CK-aligned tests with AI.
- ✓ **Plan and automate testing schedules** across environments and OSs for continuous coverage.
- ✓ **Report and communicate ATT&CK coverage** and test success metrics through intuitive dashboards.

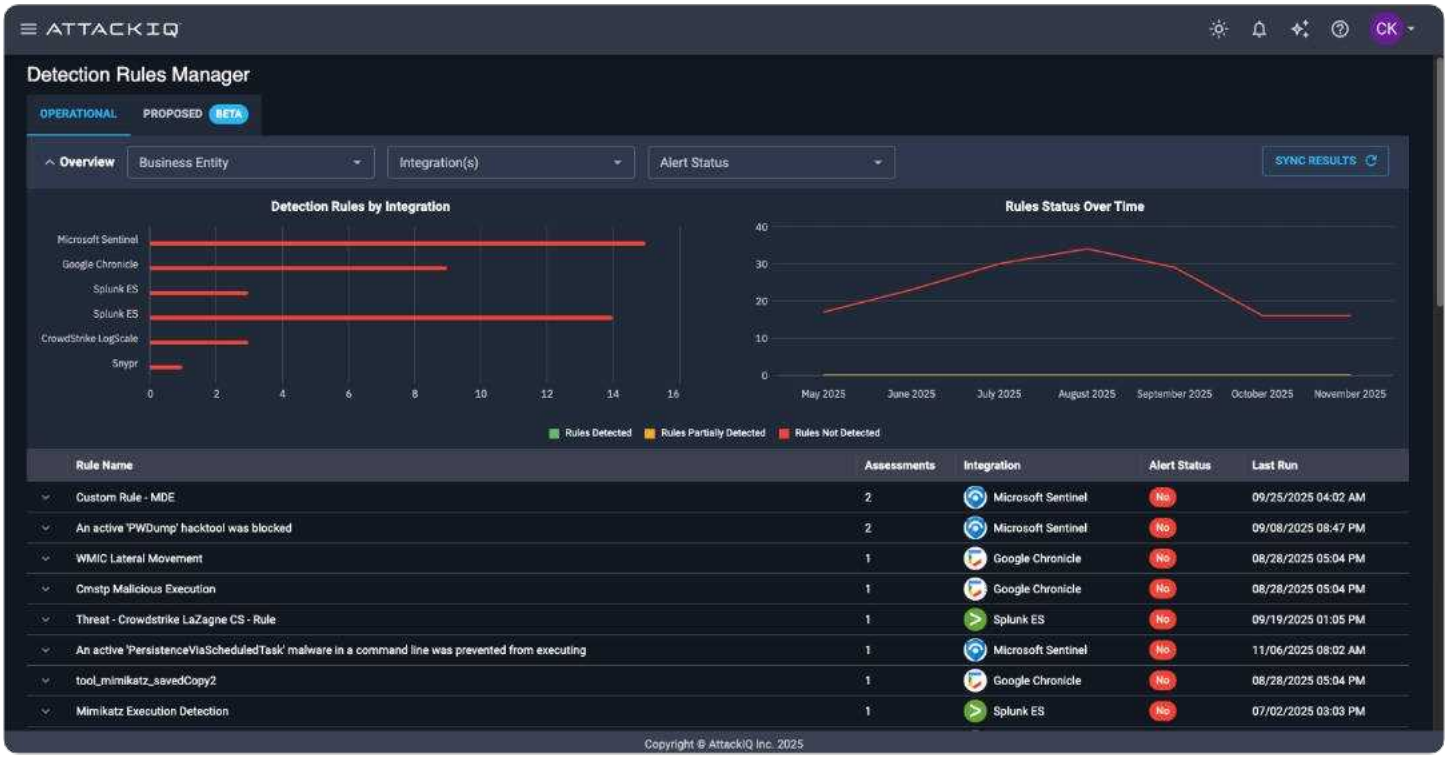
Continued on next page.

Scale Offensive Testing (cont.)

- ✓ **Analyze results directly in the ATT&CK Matrix** and import ATT&CK layers or generate new tests from Top Techniques.
- ✓ **Leverage hyper-local threat intelligence** with the AttackIQ Watchtower add-on, which identifies threats targeting your IPs and domains and automatically generates ATT&CK-mapped, ready-to-run test plans—enabling you to validate defenses against the attacks most relevant to your organization.

Enhance Detections

Beyond testing controls, AttackIQ Enterprise helps you strengthen your detection program by validating, optimizing, and scaling detections across your security stack. These capabilities make it easier to keep detection logic fresh, eliminate redundancy, and ensure analytics remain tuned to catch evolving attacker behaviors across your SIEM and related platforms:



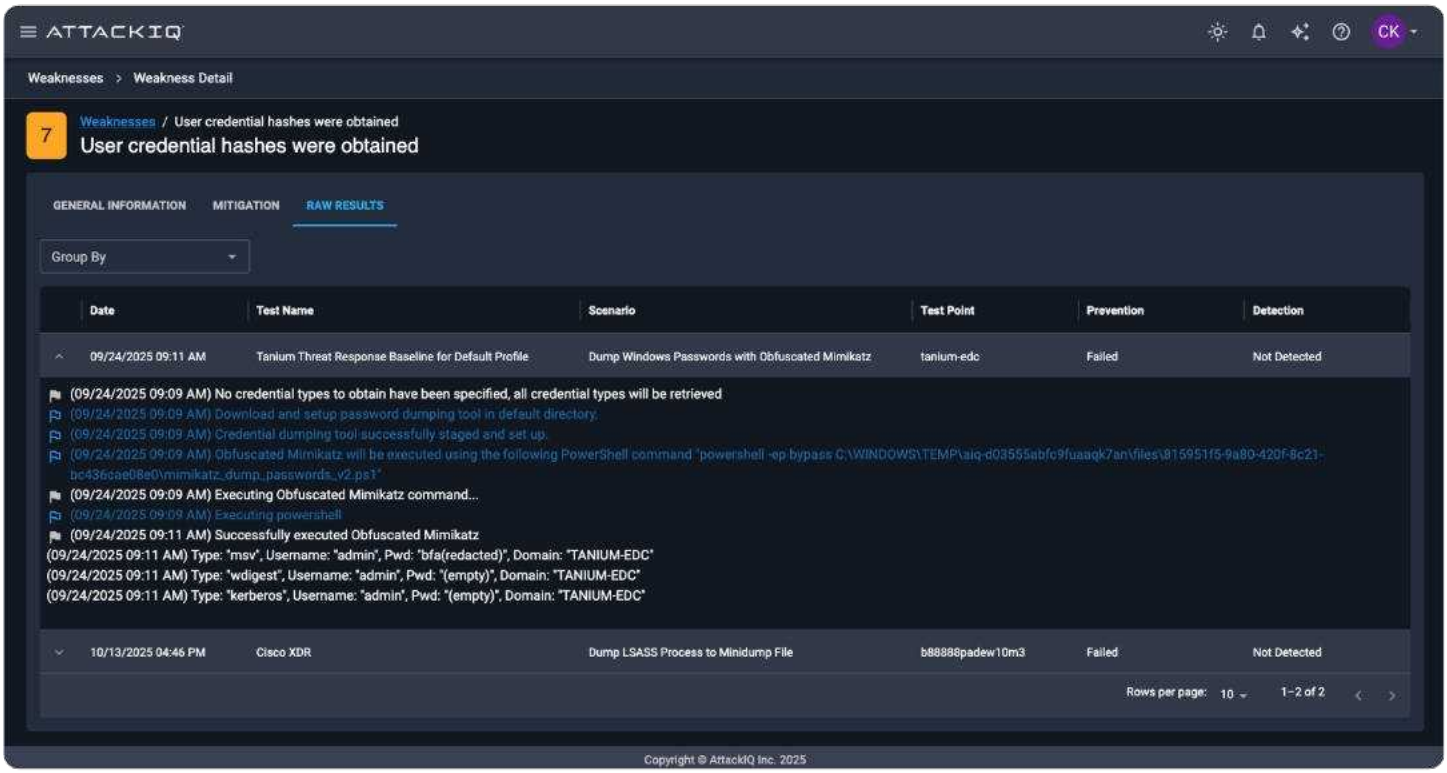
- ✓ **Strengthen detection rules** at scale by deploying vendor-provided rules or generating new ones (Sigma, KQL, SPL, YARA, Snort).
- ✓ **Validate existing detections** by linking tests to rules, measuring precision, recall, and decay to ensure they remain effective.

Enhance Detections (cont.)

- ✓ **Correlate detections to ATT&CK techniques** to understand which behaviors are covered—and where gaps exist.
- ✓ **Use AI-assisted detection engineering** to summarize detection performance and suggest rule improvements.
- ✓ **Automate detection lifecycle management** by identifying decayed, redundant, or missing detections and regenerating replacements with AI.
- ✓ **Integrate with SIEMs and analytics tools** (Splunk, Sentinel, Elastic, and others) to streamline detection validation and tuning.

Reduce Exposure (Coming Soon)

AttackIQ Enterprise is expanding to support **Continuous Threat Exposure Management (CTEM)** workflows, enabling organizations to move beyond testing and validation to **scoping, discovery, and prioritization** of exposures across their entire attack surface.



Reduce Exposure (cont.)

These upcoming capabilities will help teams understand what's most exploitable, reachable, and impactful in their environment—and act faster to reduce risk.

- ✓ **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.
- ✓ **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 to focus remediation on what truly matters. The upcoming Exposure Management Module (EMM) add-on extends AttackIQ Enterprise 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.

Continued on next page.

Reduce Exposure (cont.)

With Exposure Management Module, organizations will be 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, thereby accelerating exposure reduction.
- ✓ **Deprioritize vulnerabilities** already blocked by effective controls and rank remaining ones based on your user privileges, active directory relationships, and network reachability.
- ✓ **Score overall risk** through unified metrics that combine vulnerability data, control efficacy, and business impact.

Outcome: Gain visibility into your true exposure landscape, prioritize what to fix first, and strengthen your testing program with CTEM-aligned discovery and prioritization—enhanced by attack-path-driven exposure reduction and threat-aware validation through the EMM add-on.

Continued on next page.

Highlights

Fully Customizable Testing

Run **on-demand or automated testing** anytime, anywhere—scaling seamlessly across your enterprise. Customize every aspect of testing with **unlimited test points** and **advanced configuration options** to align with your organization's unique architecture, controls, and risk priorities.

MITRE ATT&CK-Aligned

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 enterprise.

SIEM Pipeline Validation

Ensure end-to-end visibility and reliability by validating **log ingestion, parsing, rule logic, and detection latency**. AttackIQ Enterprise's integrations with leading **SIEMs and analytics tools** verify that detections trigger as intended and events flow accurately across your telemetry stack.

Cloud Security Validation

Validate configurations and controls in **AWS and Azure** environments against both **internal and external threat scenarios** to ensure optimal security. Confirm that cloud guardrails enforce the intended protections and that misconfigurations don't expose your critical workloads.

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.

Hyper-Local Threat Intelligence (Watchtower Add-On)

Leverage **hyper-local threat intelligence** with the **AttackIQ Watchtower add-on**, which identifies threats targeting your IPs and domains and automatically generates **ATT&CK-mapped, ready-to-run test plans**—allowing you to validate defenses against the attacks most relevant to your organization.

Test Safely at Scale

Execute testing i**n production environments** with confidence. AttackIQ Enterprise is designed to deliver **safe, realistic adversary emulations** that measure security effectiveness across Windows, macOS, Linux, and **Kubernetes** (beta) without disrupting operations.

Enhanced Detection Engineering

Accelerate detection lifecycle management through **AI-assisted rule creation, validation, and tuning**. Generate, interpret, or explain detections across **Sigma, KQL, SPL**, and other formats while tracking **precision, recall, and decay**—ensuring detections remain accurate and resilient over time.

Boundary & Email Controls (Add-on)

Replay real **PCAP scenarios** to test the efficacy of **IDS/IPS, WAF, and email security** against attack traces. Validate boundary-layer defenses and ensure inspection and filtering controls perform as expected under real-world attack conditions.

Weakness Management

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

Detailed Reporting & Executive Insights

Translate technical validation into actionable intelligence. Use **role-specific dashboards, trend KPIs, and ATT&CK coverage metrics** to demonstrate progress over time, communicate readiness to leadership, and support risk-based decision-making.

See AttackIQ Enterprise 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.

ATTACKIQ®

READY

SOLUTION BRIEF

AttackIQ Ready

Continuous Adversary Exposure Validation Made Simple and Expertly Managed

© 2025 AttackIQ, Inc. All Rights Reserved.

Table of Contents

Information and Use: The information contained in this document is provided for informational purposes only and is subject to change. Nothing herein should be interpreted as a commitment or guarantee of future functionality, performance, or delivery.

No Public Disclosure Permitted: This document is not to be used, copied, modified, reproduced, or distributed without the express written consent of AttackIQ. Please report postings of this document on public servers or websites to support@attackiq.com.

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

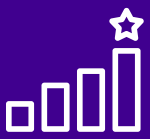
AttackIQ Ready aligns directly with the Continuous Threat Exposure Management (CTEM) framework, uniting validation, prioritization, and remediation within a single managed cycle. It helps organizations shift from reactive patching to proactive exposure management—continuously discovering, validating,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

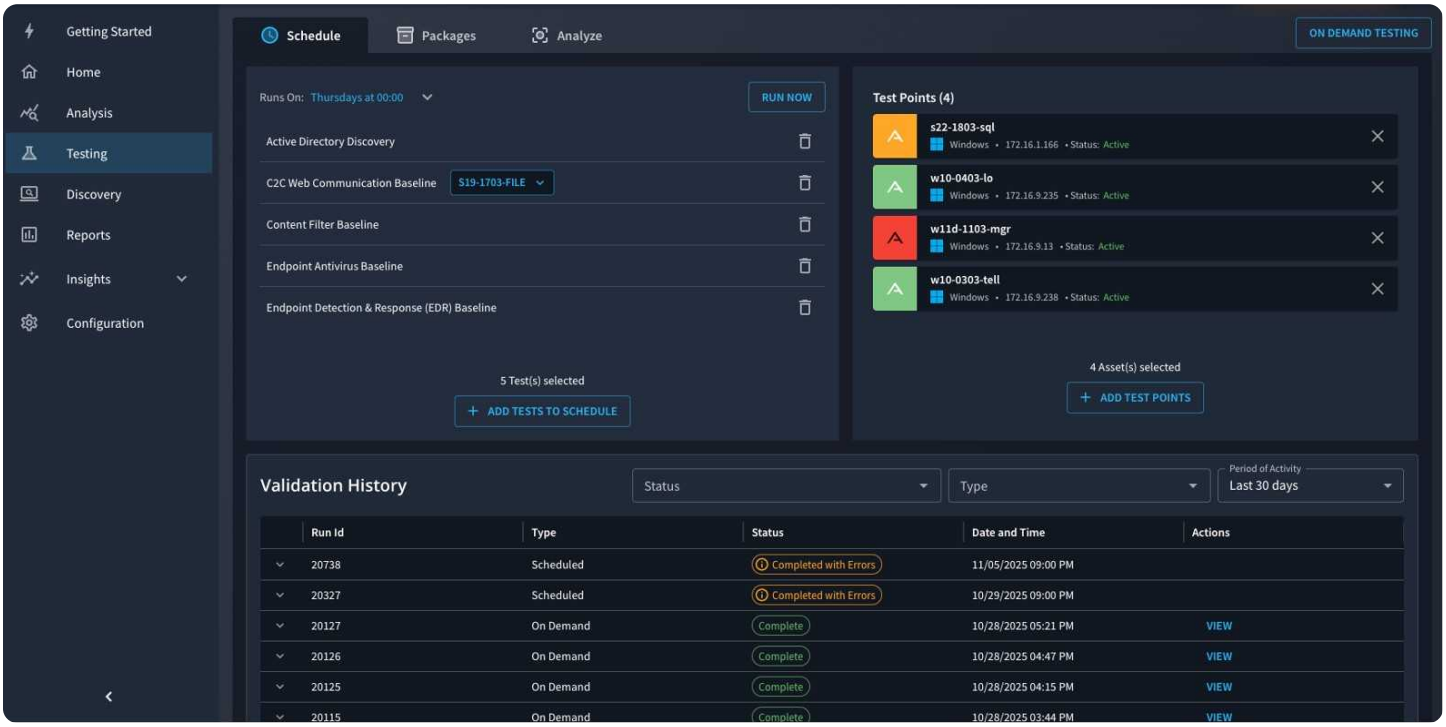
Continued on next page.

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.

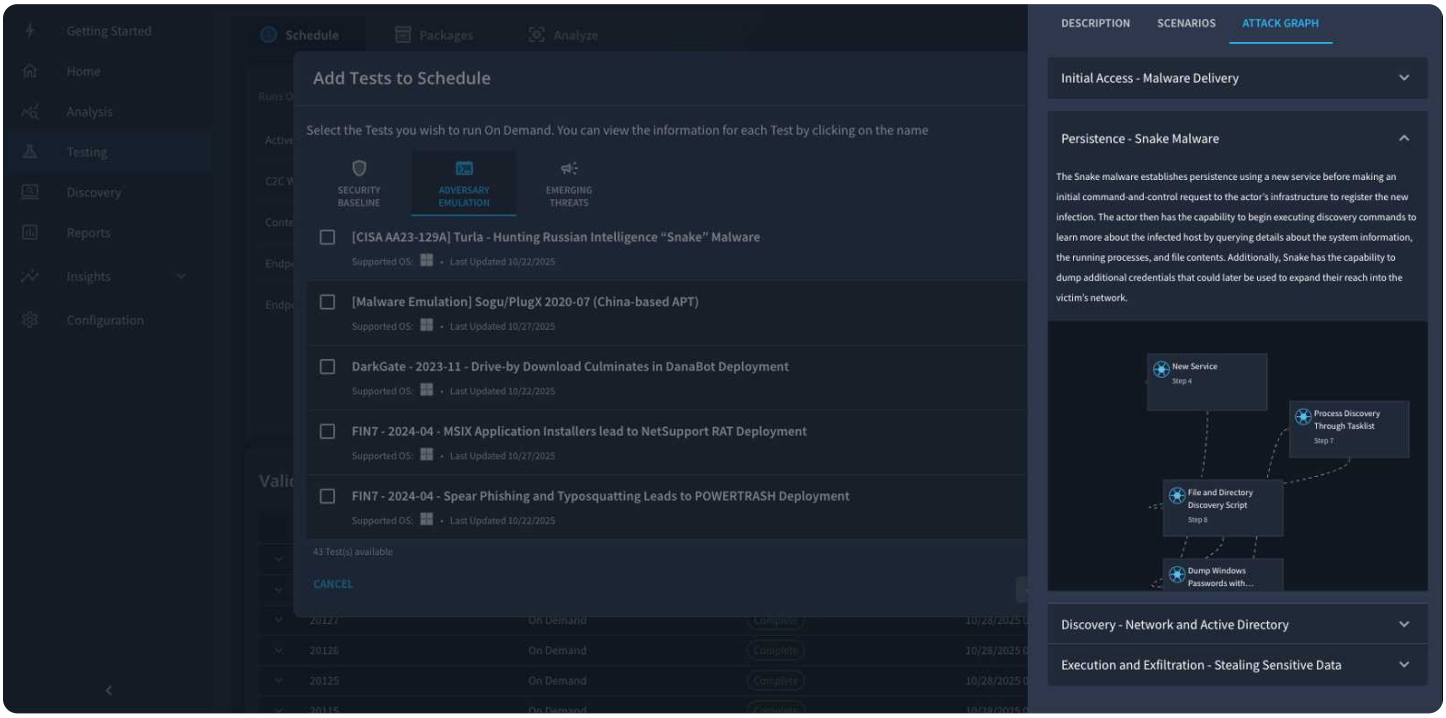
Optimize Defensive Posture (cont.)

- ✓ **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

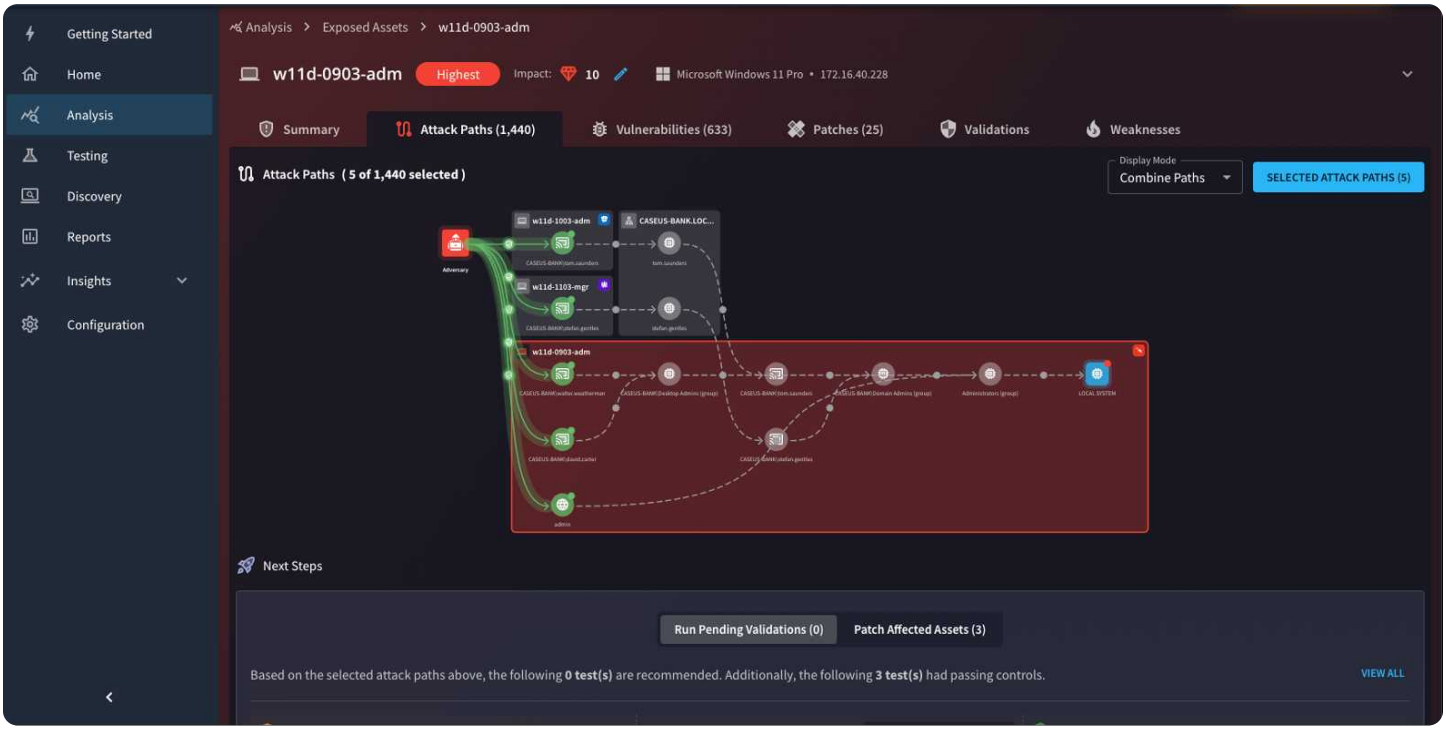
AttackIQ Ready gives you the ability to simulate adversary behaviors using MITRE ATT&CK-aligned emulations.

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.

ATTACKIQ

FLEX

ATTACKIQ FLEX

Transforming Testing

Testing is critical for maintaining an adaptive defense, but most organizations neglect to do it, leaving them exposed to threats and potential compromise. There are major hurdles organizations need to overcome for testing to be accessible—and AttackIQ Flex resolves these obstacles through an agentless test-as-a-service model.

The Need to Democratize Testing for Everyone

Traditional security testing methods like penetration testing are costly and time-consuming, require expertise that security teams often lack, and are difficult to do regularly, leaving visibility gaps between assessments.

Introducing Flex

AttackIQ Flex empowers organizations to rapidly test their security controls on demand. It revolutionizes the breach and attack simulation market by offering full adversary and security control test suites at the click of a button. It removes the obstacles of price, complexity, and time constraints that have kept organizations from comprehensive testing in the past.

HIGHLIGHTS

Lightweight and Agentless

Agentless architecture enables you to run tests on any network, anywhere rapidly.

MITRE Aligned Insights

Get detailed test findings with MITRE-aligned results and recommendations to fix security gaps.

Enterprise-Grade

Comprehensive adversary, compliance, and security control testing developed by industry-leading researchers.

Simplified Experience

Tests you can run at the click of a button, with results in minutes.

Pricing Fit for Your Budget

A flexible consumption model - pay-as-you-go or subscription-based – gives you the flexibility to test your way.

Detection Insights

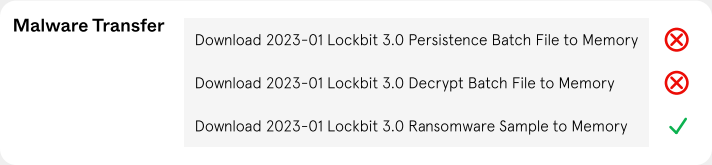
Direct integration with Splunk to validate security control detections and alert pipeline without configurations.

How It Works

1 Select Your Test | 2 Run Your Test | 3 View Your Results | 4 Fix Your Gaps

Comprehensive Reports

Detailed reports provide pentest-grade insights into your test results, including TTPs prevented, overall score, and global comparisons.



MITRE Aligned

See your overall security performance by MITRE tactic and technique in a simplified interface and intuitive scoring system.

Expertise on Demand

Access our industry-leading experts for testing support and guidance

Adversary and Security Control Testing

Adversary and security control tests were developed by industry-leading threat researchers.

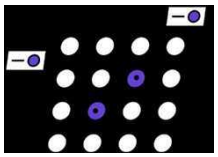
Compliance Testing Made Easy

Dedicated tests aligned to common compliance frameworks, including NIST and DORA.

Detailed Mitigations

Detailed recommendations on how to fix any security gaps that have been identified.

Value of Flex

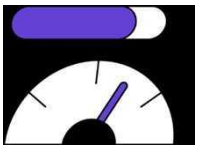


Emulate the Enemy

Built on AttackIQ's advanced adversary emulation software to realistically emulate attacker behaviors

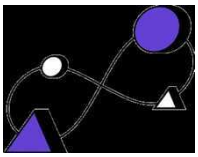
Testing for Everyone

Self-contained test packages lower the knowledge bar for validating security controls by simplifying key steps in the design and execution process



Save Time & Resources

Provides an economical means of validating security controls without the need for expensive and time-consuming manual testing.



Pay as You Go

Test as little or as much as you want at a price that's right for you.

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation (BAS) solutions, built the industry's first BAS Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

For more information visit www.attackiq.com and follow AttackIQ on Twitter, LinkedIn, and YouTube.

© 2024 AttackIQ, Inc. All rights reserved.