

SOLUTION BRIEF

AttackIQ Enterprise

Comprehensive Adversary Exposure Validation
for Large and Complex Environments

Table of Contents

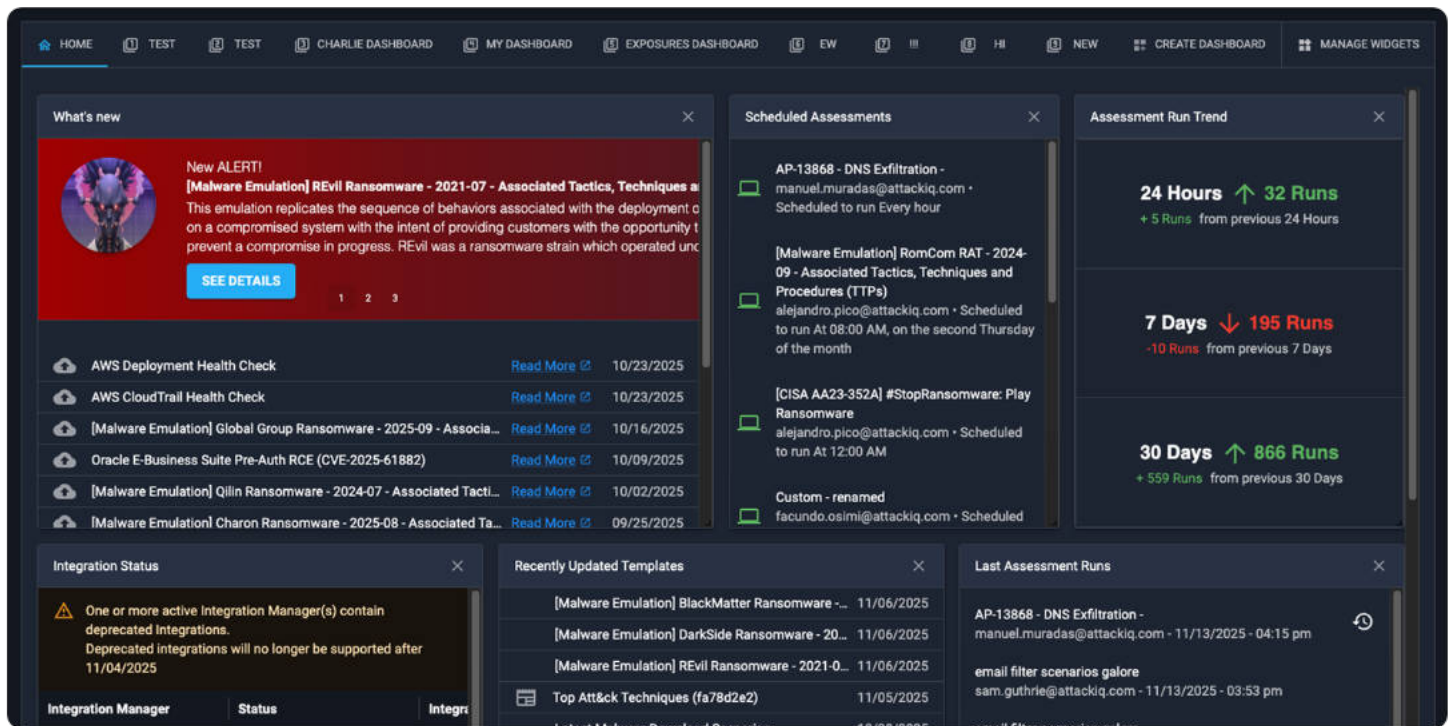
- Executive Summary 3
- The Need for Continuous Adversary Exposure Validation 4
- The Value of AttackIQ Enterprise 5
 - Close Security Control Gaps 5
 - Conserve Resources and Reduce Costs 5
 - Detect and Stop Threats Faster 5
 - Accelerate Mobilization and Accountability 5
 - Prove and Improve Resilience 5
 - Accelerate CTEM Maturity 6
 - Continuously Reduce Real Exposure 6
 - Validate Readiness Against Threats Targeting You 6
- What You Can Do with Enterprise 7
 - Optimize Defensive Posture 7
 - Scale Offensive Testing 9
 - Enhance Detections 10
 - Reduce Exposure 11
- Highlights 14
 - Fully Customizable Testing 14
 - Test Safely at Scale 14
 - MITRE ATT&CK-Aligned 14
 - Detection Engineering 14
 - SIEM Pipeline Validation 14
 - Boundary & Email Controls 14
 - Cloud Security Validation 14
 - Weakness Management 14
 - Expert Consulting & Advisory Services 14
 - Detailed Reporting & Executive Insights 14
 - Hyper-Local Threat Intelligence 14

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.

The screenshot displays the AttackIQ Enterprise interface for an assessment titled "Windows Credential Theft (Results)". The interface includes a sidebar with navigation options like Setup, On Demand, Scheduled, Results, Summary, Detections, History, MITRE ATTACK, Mitigations, Reports, Team, and Notifications. The main content area shows a table of results with columns for Run ID, MITRE tactics, Test, Scenario, User Privileges, Asset, Prevention, Detection, Alerted, and Notes. The table lists five entries, all with a "Prevented" status and "No" alerts. The detection column shows various security tools like Falcon and Windows Defender.

Run ID	MITRE tactics	Test	Scenario	User Privileges	Asset	Prevention	Detection	Alerted	Notes
09/11/2025 04:50 pm	Credential Access	Multi-source	Dump Passwords using LaZagne	SYSTEM	bcrow8888w10x5	Prevented	Falcon, Windows Defender	No	View (0)
09/11/2025 04:50 pm	Credential Access	Windows	Dump Passwords using gsecdump	SYSTEM	bcrow8888w10x5	Prevented	Falcon, Windows Defender	No	View (0)
09/11/2025 04:50 pm	Credential Access	Windows	Dump Passwords using PwDump7	SYSTEM	bcrow8888w10x5	Prevented	Falcon	No	View (0)
09/11/2025 04:50 pm	Execution, Credential Access	Windows	Dump Windows Passwords with Obfuscated Mimikatz	SYSTEM	bcrow8888w10x5	Prevented	Falcon, Windows Defender	No	View (0)
09/11/2025 04:50 pm	Credential Access	Windows	Dump Windows Passwords	SYSTEM	bcrow8888w10x5	Prevented	Falcon	No	View (0)

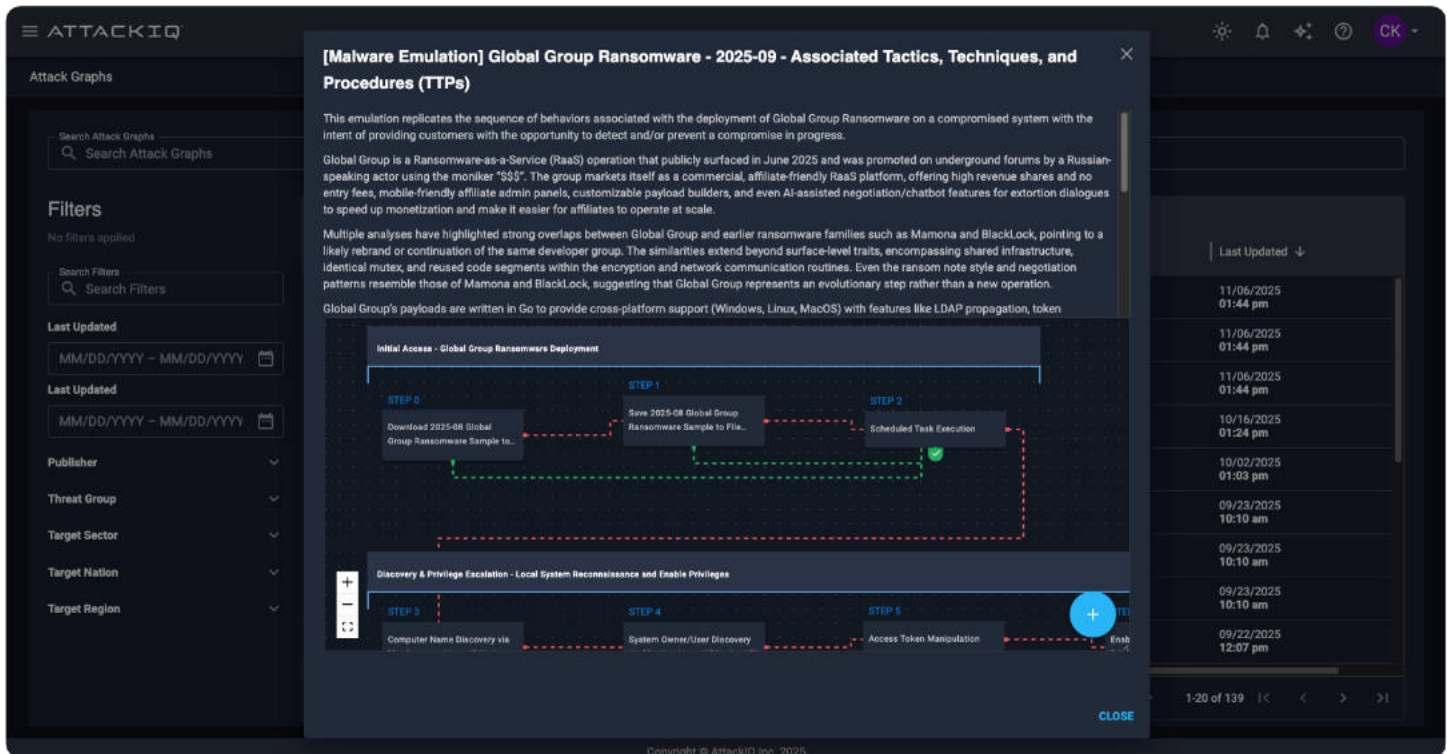
Optimize Defensive Posture (cont.)

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.

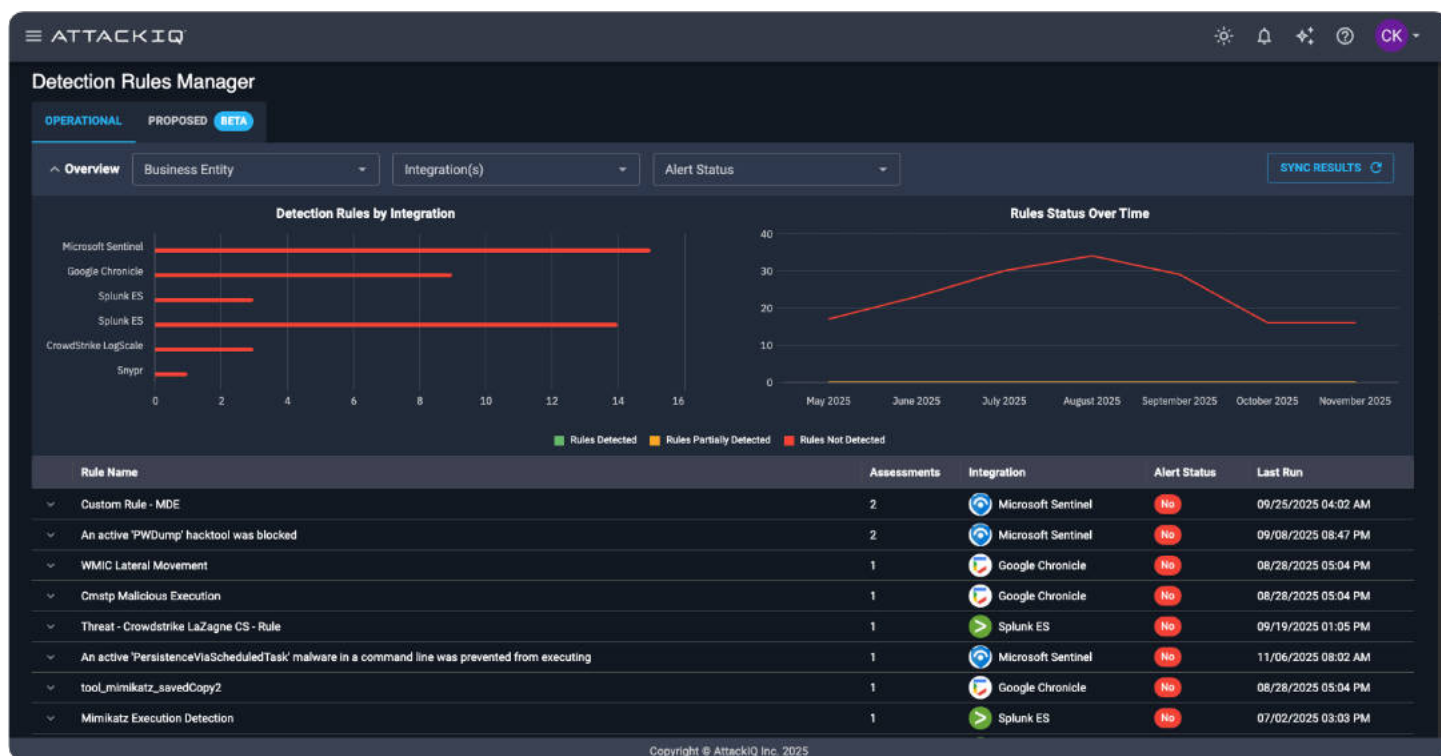
Continued on next page.

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.

The screenshot displays the AttackIQ interface for viewing weakness details. The main heading is "User credential hashes were obtained". Below this, there are tabs for "GENERAL INFORMATION", "MITIGATION", and "RAW RESULTS". The "RAW RESULTS" tab is active, showing a table of results. The table has columns for Date, Test Name, Scenario, Test Point, Prevention, and Detection. The first row shows a test on 09/24/2025 at 09:11 AM, titled "Tanium Threat Response Baseline for Default Profile", with the scenario "Dump Windows Passwords with Obfuscated Mimikatz". The prevention status is "Failed" and the detection status is "Not Detected". Below the table, there is a detailed log of events, including the execution of the Obfuscated Mimikatz command and the successful retrieval of credential hashes for the user "admin" on the domain "TANIUM-EDC".

Date	Test Name	Scenario	Test Point	Prevention	Detection
09/24/2025 09:11 AM	Tanium Threat Response Baseline for Default Profile	Dump Windows Passwords with Obfuscated Mimikatz	tanium-edc	Failed	Not Detected
10/13/2025 04:46 PM	Cisco XDR	Dump LSASS Process to Minidump File	b8888spadew10m3	Failed	Not Detected

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 in **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 Proactive 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.