SOLUTION BRIEF

AttackIQ Exposure Management Module

Expose Real Risks and Focus Remediation Where It Strengthens Resilience

Table of Contents

Executive Summary 3

The Challenge: Visibility without Context 4

The Value of AttackIQ EMM 5

Turn Vulnerabilities into Validated Weaknesses 5

Model Attack Paths to What Matters Most 5

Prioritize with Business Context and Exploitability 6

Quantify Exposure Reduction Over Time 6

Align to CTEM and Risk Frameworks 7

What You Can Do with AttackIQ EMM 8

Prioritize & Model 8

Validate & Measure 8

The Value of EMM in Action 9

Accelerate Risk Reduction with Patch Prioritization 9

Prove Protection of Critical Assets 9

Maximize Remediation Impact While Saving Time & Resources 9

From Vulnerability Lists to Validated Exposure Reduction. 9

Highlights 10

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

> Organizations spend millions patching vulnerabilities that attackers can’t reach while exploitable paths to critical assets remain open. The result is wasted effort, blurred visibility into real risk, and limited proof that remediation actually strengthens resilience.

The **AttackIQ Exposure Management Module (EMM)** is an add-on that extends **AttackIQ Ready** and **AttackIQ Enterprise** (coming soon) with advanced attack path management, threat modeling, scoring, and prioritization capabilities that help organizations **identify and reduce the exposures** that matter most.

EMM bridges the gap between vulnerability management and adversary validation. It aggregates vulnerability, asset, network, user privileges, and configuration data, then applies **attack-path modeling, exposure scoring, and control validation** to reveal which risks are actually exploitable and which can be safely deprioritized.

By combining **environmental context and control performance**, EMM enables security teams to focus on high-impact fixes that measurably reduce exposure.

With EMM, organizations can:

- Model and visualize attack paths to critical assets.
- Prioritize vulnerabilities by exploitability, reachability, and business value.
- Quantify exposure reduction over time using a unified scoring and analytics framework.

This enables more intelligent decisions, faster remediation, and clear proof that every action taken meaningfully strengthens resilience.

The Challenge: Visibility without Context

Security teams are drowning in vulnerability data but starving for context. Typical enterprises have thousands of open findings across their environment—yet often a small fraction is truly exploitable.

- ✓ **Vulnerability overload lacks context:** Organizations face massive Common Vulnerabilities and Exposures (CVEs) backlogs while attackers exploit only a handful of reachable flaws. The Cybersecurity and Infrastructure Security Agency (CISA)'s Known Exploited Vulnerabilities (KEV) catalog highlights that not all vulnerabilities matter equally.
- ✓ **Traditional scanning doesn't reflect reality:** Common Vulnerability Scoring System (CVSS) scores measure severity, not exploitability. Many "critical" vulnerabilities remain unexploited because of existing controls or limited attack paths.
- ✓ **Exposure needs validation, not just discovery:** Without tying vulnerabilities to control performance or attack paths, teams can't prove that remediation actually reduces risk.

Continuous Threat Exposure Management (CTEM) focuses on *scoping, discovery, prioritization*, *validation*, and *mobilization*, not merely scanning lists. EMM operationalizes that model, turning discovery into validated, actionable exposure reduction.

Continued on next page.

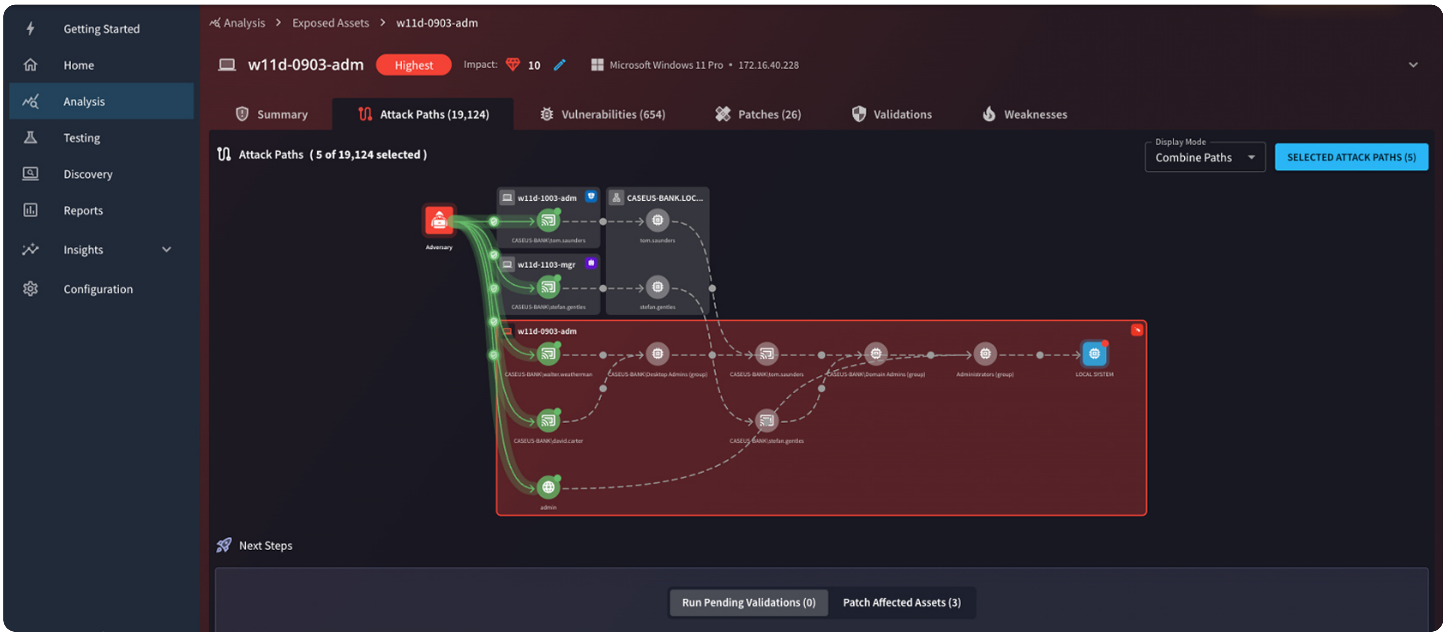
The Value of AttackIQ EMM

Turn Vulnerabilities into Validated Weaknesses

EMM correlates vulnerability data with control validation results to distinguish between *theoretical* risks and real exposures. Teams can focus on vulnerabilities that are exploitable in their environment, backed by AttackIQ's adversarial exposure validation results.

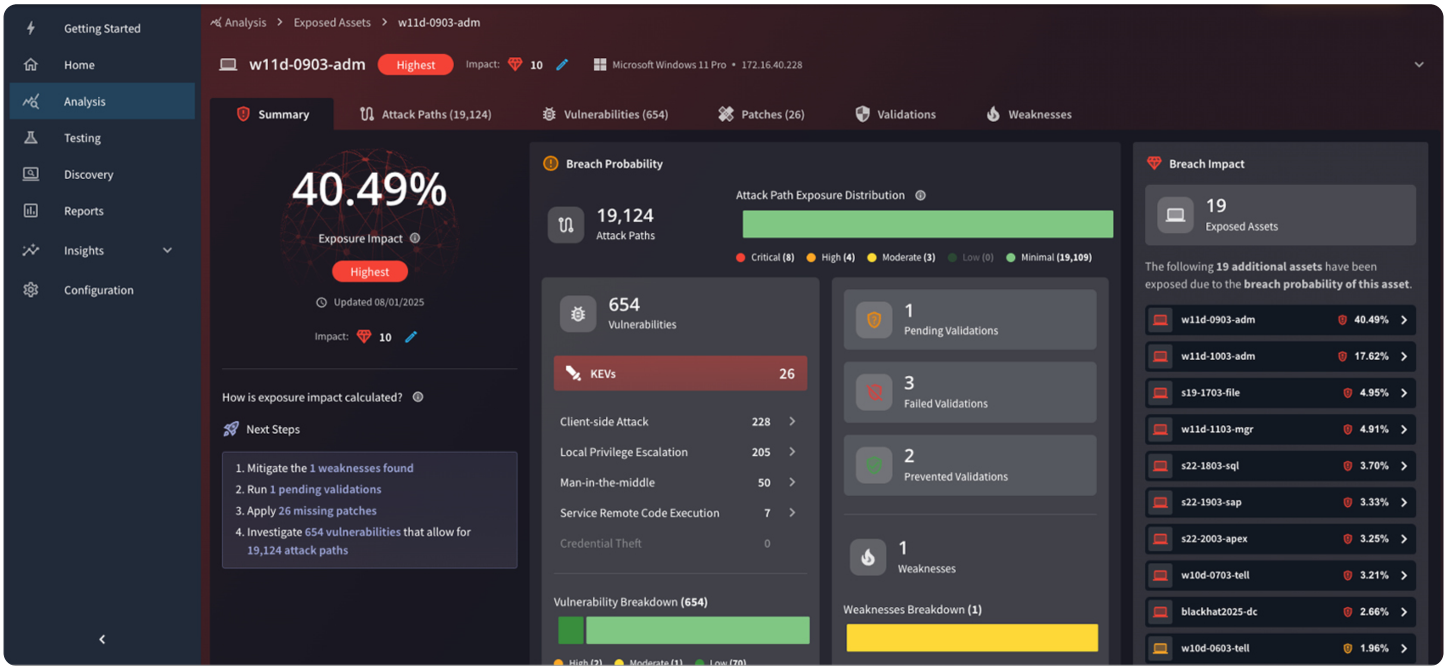
Model Attack Paths to What Matters Most

Go beyond lists. EMM builds **attack-path** maps that visualize how an adversary could traverse your network from the point of entry to high-value assets. It identifies choke points—places where one fix collapses multiple paths—so teams can maximize impact with minimal effort.



Prioritize with Business Context and Exploitability

Rank vulnerabilities based on **reachability, exploit difficulty, and asset criticality**, not just severity. Combine vulnerability data with **Active Directory relationships, network data**, and **existing control coverage** to determine actual business risk.



w11d-0903-adm Highest Impact: 10 Microsoft Windows 11 Pro • 172.16.40.228

40.49%
Exposure Impact
Highest
Updated 08/01/2025
Impact: 10

How is exposure impact calculated?

Next Steps

1. Mitigate the 1 weaknesses found
2. Run 1 pending validations
3. Apply 26 missing patches
4. Investigate 654 vulnerabilities that allow for 19,124 attack paths

Breach Probability

19,124 Attack Paths

Attack Path Exposure Distribution

● Critical (8) ● High (4) ● Moderate (3) ● Low (0) ● Minimal (19,109)

654 Vulnerabilities

KEVs	26
Client-side Attack	228
Local Privilege Escalation	205
Man-in-the-middle	50
Service Remote Code Execution	7
Credential Theft	0

Vulnerability Breakdown (654)

● High (2) ● Moderate (1) ● Low (70)

1 Pending Validations

3 Failed Validations

2 Prevented Validations

1 Weaknesses

Weaknesses Breakdown (1)

Breach Impact

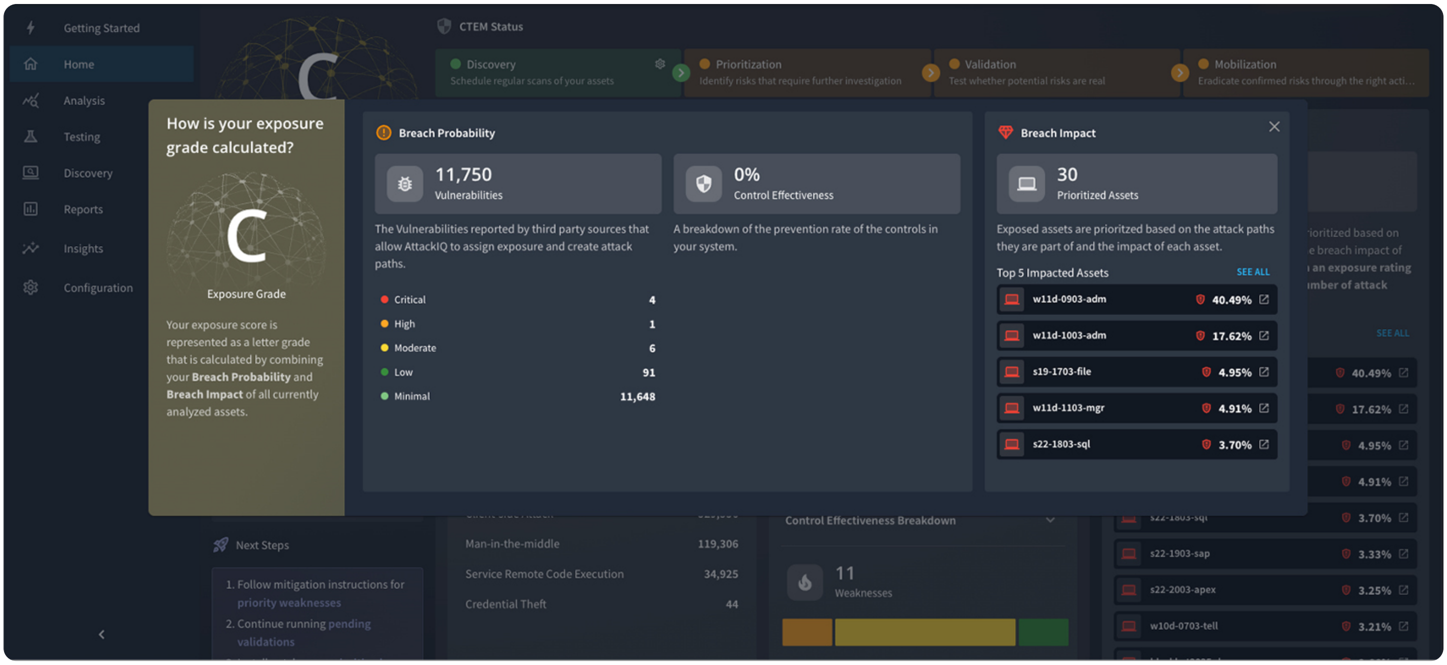
19 Exposed Assets

The following **19 additional assets** have been exposed due to the **breach probability of this asset**.

w11d-0903-adm	40.49%
w11d-1003-adm	17.62%
s19-1703-file	4.95%
w11d-1103-mgr	4.91%
s22-1803-sql	3.70%
s22-1903-sap	3.33%
s22-2003-apex	3.25%
w10d-0703-tell	3.21%
blackhat2025-dc	2.66%
w10d-0603-tell	1.96%

Quantify Exposure Reduction Over Time

Measure improvement with unified **risk scoring** that accounts for vulnerabilities, misconfigurations, control performance, and asset value. Dashboards show how remediation and validation efforts reduce exploitable pathways across testing cycles.



Discovery — Schedule regular scans of your assets

Prioritization — Identify risks that require further investigation

Validation — Test whether potential risks are real

Mobilization — Eradicate confirmed risks through the right acti…

How is your exposure grade calculated?

C
Exposure Grade

Your exposure score is represented as a letter grade that is calculated by combining your **Breach Probability** and **Breach Impact** of all currently analyzed assets.

Breach Probability

11,750 Vulnerabilities

The Vulnerabilities reported by third party sources that allow AttackIQ to assign exposure and create attack paths.

● Critical	4
● High	1
● Moderate	6
● Low	91
● Minimal	11,648

0% Control Effectiveness

A breakdown of the prevention rate of the controls in your system.

Breach Impact

30 Prioritized Assets

Exposed assets are prioritzed based on the attack paths they are part of and the impact of each asset.

Top 5 Impacted Assets

w11d-0903-adm	40.49%
w11d-1003-adm	17.62%
s19-1703-file	4.95%
w11d-1103-mgr	4.91%
s22-1803-sql	3.70%

Next Steps

1. Follow mitigation instructions for priority weaknesses
2. Continue running pending validations

Man-in-the-middle	119,306
Service Remote Code Execution	34,925
Credential Theft	44

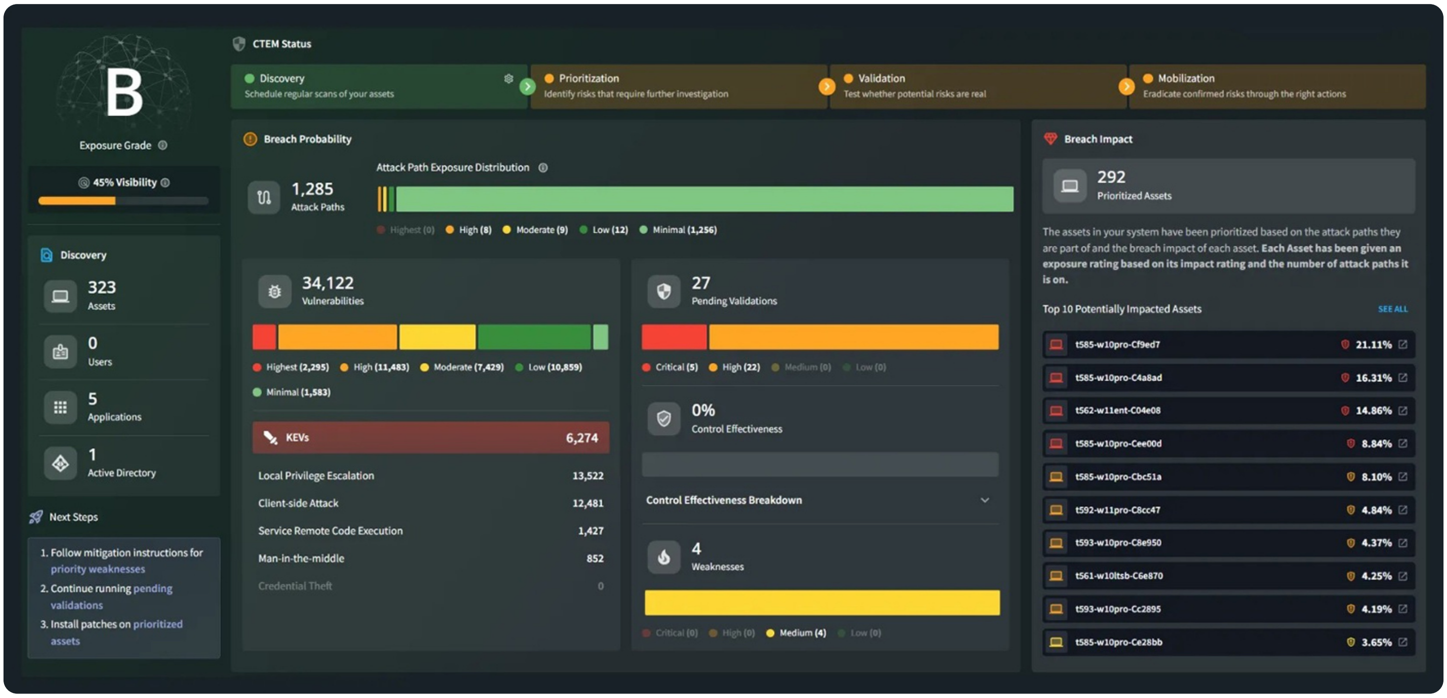
Control Effectiveness Breakdown

11 Weaknesses

s22-1903-sap	3.33%
s22-2003-apex	3.25%
w10d-0703-tell	3.21%

Align to CTEM and Risk Frameworks

EMM operationalizes **CTEM's five phases** (*Scoping* → *Discovery*→ *Prioritization* → *Validation* → *Mobilization*), ensuring every mitigation step contributes to measurable exposure reduction.



B

Exposure Grade

45% Visibility

Discovery

323 Assets

0 Users

5 Applications

1 Active Directory

Next Steps

1. Follow mitigation instructions for priority weaknesses
2. Continue running pending validations
3. Install patches on prioritized assets

CTEM Status

- Discovery: Schedule regular scans of your assets
- Prioritization: Identify risks that require further investigation
- Validation: Test whether potential risks are real
- Mobilization: Eradicate confirmed risks through the right actions

Breach Probability

1,285 Attack Paths

Attack Path Exposure Distribution

Highest (0) · High (8) · Moderate (9) · Low (12) · Minimal (1,256)

34,122 Vulnerabilities

Highest (2,295) · High (11,483) · Moderate (7,429) · Low (10,859) · Minimal (1,583)

KEVs	6,274
Local Privilege Escalation	13,522
Client-side Attack	12,481
Service Remote Code Execution	1,427
Man-in-the-middle	852
Credential Theft	0

27 Pending Validations

Critical (5) · High (22) · Medium (0) · Low (0)

0% Control Effectiveness

Control Effectiveness Breakdown

4 Weaknesses

Critical (0) · High (0) · Medium (4) · Low (0)

Breach Impact

292 Prioritized Assets

The assets in your system have been prioritized based on the attack paths they are part of and the breach impact of each asset. **Each Asset has been given an exposure rating based on its impact rating and the number of attack paths it is on.**

Top 10 Potentially Impacted Assets — SEE ALL

t585-w10pro-Cf9ed7	21.11%
t585-w10pro-C4a8ad	16.31%
t562-w11ent-C04e08	14.86%
t585-w10pro-Cee00d	8.84%
t585-w10pro-Cbc51a	8.10%
t592-w11pro-C8cc47	4.84%
t593-w10pro-C8e950	4.37%
t561-w10ltsb-C6e870	4.25%
t593-w10pro-Cc2895	4.19%
t585-w10pro-Ce28bb	3.65%

Continued on next page.

What You Can Do with AttackIQ EMM

EMM extends the power of AttackIQ Ready and AttackIQ Enterprise (coming soon) with context-rich discovery and prioritization capabilities.

Prioritize & Model

- ✓ **Correlate vulnerabilities, assets, and validation data** to reveal real exploit paths and identify weaknesses that matter most.
- ✓ **Rank vulnerabilities by exploitability, reachability, and business value** to focus remediation on the areas that pose the most significant risk.
- ✓ **Model attack paths to crown-jewel assets**, showing how adversaries could traverse your network and isolate dead-end findings that pose no real risk.
- ✓ **Identify choke points** where one fix collapses multiple attack paths, helping teams act efficiently and maximize remediation impact.
- ✓ **Deprioritize vulnerabilities already blocked by controls**, saving time and effort by focusing only on validated exposures.

Validate & Measure

- ✓ **Confirm whether compensating controls block exploit paths**, ensuring defenses are effective before spending remediation effort.
- ✓ **Integrate directly with AttackIQ testing results** to verify that mitigations and compensating controls work as intended.
- ✓ **Quantify exposure reduction** over time using unified scoring (A–F) and trend analytics that combine vulnerability data, control efficacy, and asset criticality.
- ✓ **Track measurable progress** toward CTEM objectives by linking discovery, validation, and prioritization in a single workflow.

EMM transforms traditional vulnerability management into exposure-based decision-making. By connecting vulnerabilities to real-world exploit paths and validated control performance, it helps security teams focus on the few issues that truly matter—**reducing risk faster and proving continuous resilience improvement.**

The Value of AttackIQ EMM in Action

Accelerate Risk Reduction with Patch Prioritization

Thousands of critical CVEs compete for limited patch windows.

EMM ranks vulnerabilities by exploitability and reachability, allowing you to deprioritize findings already blocked by controls and identify choke points.

This helps you pinpoint the high-impact fixes that measurably reduce exposure.

Prove Protection of Critical Assets

Leadership needs evidence that critical applications are protected, not just patched.

EMM models attack paths to critical assets and validate control efficacy, allowing organizations to demonstrate measurable reduction of business risk and verifiable protection of their most vital assets, aligning technical validation with executive-level assurance.

Maximize Remediation Impact While Saving Time & Resources

Remediation teams often work from vulnerability lists disconnected from real exploitability or defensive performance.

EMM unifies vulnerability, control, and asset context into a single view, prioritizing fixes that most effectively reduce validated exposure, and integrates with AttackIQ testing to ensure every mitigation is verified post-remediation.

The result is that remediation efforts become faster, more targeted, and directly tied to risk reduction, transforming patching from a maintenance task into a measurable security outcome.

From Vulnerability Lists to Validated Exposure Reduction.

Request a demo of the AttackIQ Exposure Management Module (EMM) and see how attack-path modeling, exploitability scoring, and business-aware prioritization turn visibility into measurable resilience.

Highlights

Attack-Path Modeling: Visualize how adversaries can move through your environment to reach critical assets, highlighting exploitable paths and dependencies that matter most.

Choke Point Identification: Pinpoint single fixes that eliminate multiple attack paths, helping teams maximize efficiency and accelerate measurable exposure reduction.

Identity and Network Context: Analyze Active Directory relationships, group memberships, and network segmentation to understand how identity and access misconfigurations contribute to attack paths.

CTEM Alignment: Operationalize CTEM by connecting scoping, discovery, prioritization, validation, and mobilization in a single, iterative workflow.

Vulnerability Prioritization: Focus remediation on what's most impactful by ranking vulnerabilities based on exploitability, reachability, and validated control gaps, eliminating noise from issues already blocked by defenses.

Exposure Scoring: Quantify your organization's overall risk posture by combining vulnerability data, control efficacy, and asset criticality into a unified exposure score.

Control-Aware Prioritization: Integrate with AttackIQ validation results to confirm control efficacy and focus remediation on exploitable weaknesses.

See AttackIQ EMM 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 turnkey solutions, empowering them to elevate client security. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.