ATTACKIQ

# Adversarial Exposure Validation Platform

## Cut the Noise. Validate Continuously. Strengthen Resilience with Adversarial Exposure Validation

Cyber threats are evolving at an unprecedented pace, leaving security teams overwhelmed by a flood of vulnerabilities and a fragmented view of their expanding attack surface. Traditional point-in-time assessments and reactive patching are no longer sufficient. Continuous Threat Exposure Management (CTEM) offers a strategic framework to discover, prioritize, and address real security gaps on an ongoing basis.

Gartner's insights reinforce this. They predict that:

***"By 2026 organizations that prioritize their security investments based on a continuous exposure management program will be three times less likely to suffer a breach."***

Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023

## Continuous Threat Exposure Management Challenges

### Expanding Attack Surfaces

Hybrid cloud environments, remote work, and mobile devices create new entry points daily.

### Legacy, Siloed Testing

Point-in-time assessments and sporadic pentests leave extended periods of untested security gaps.

### Rapidly Exploited Vulnerabilities

From software vulnerabilities to missed patches, attackers capitalize on exposures within days—or even hours—of discovery.

### Overwhelming Noise

Traditional vulnerability scanners and generic threat feeds generate endless alerts, obscuring the critical few that truly matter.

## HIGHLIGHTS

### Uncover Gaps Before Attackers Strike

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

### Test Security Controls with Real-World Scenarios

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

### Prioritize What Matters Most

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

### Turn Data into Actionable Insights

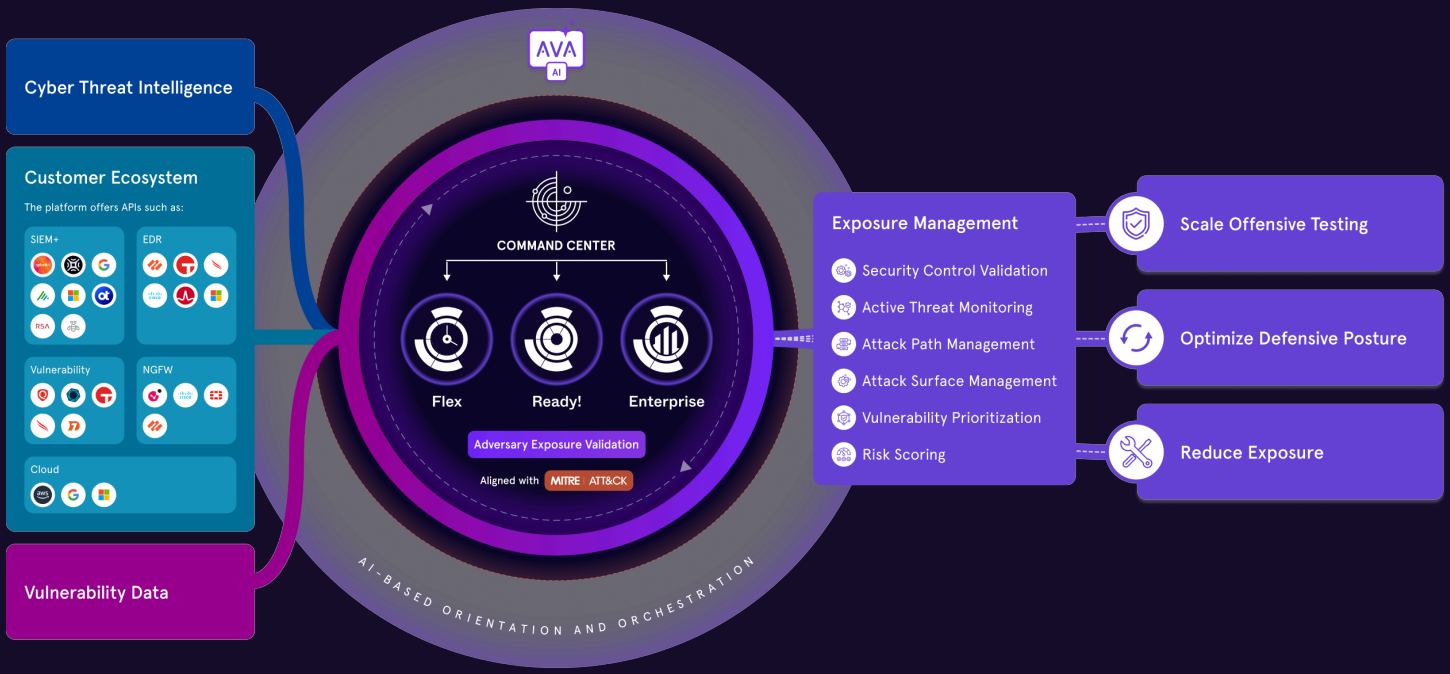
Receive clear, step-by-step remediation guidance to shorten resolution times and quickly strengthen your security posture.

### Track Progress with Ease

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

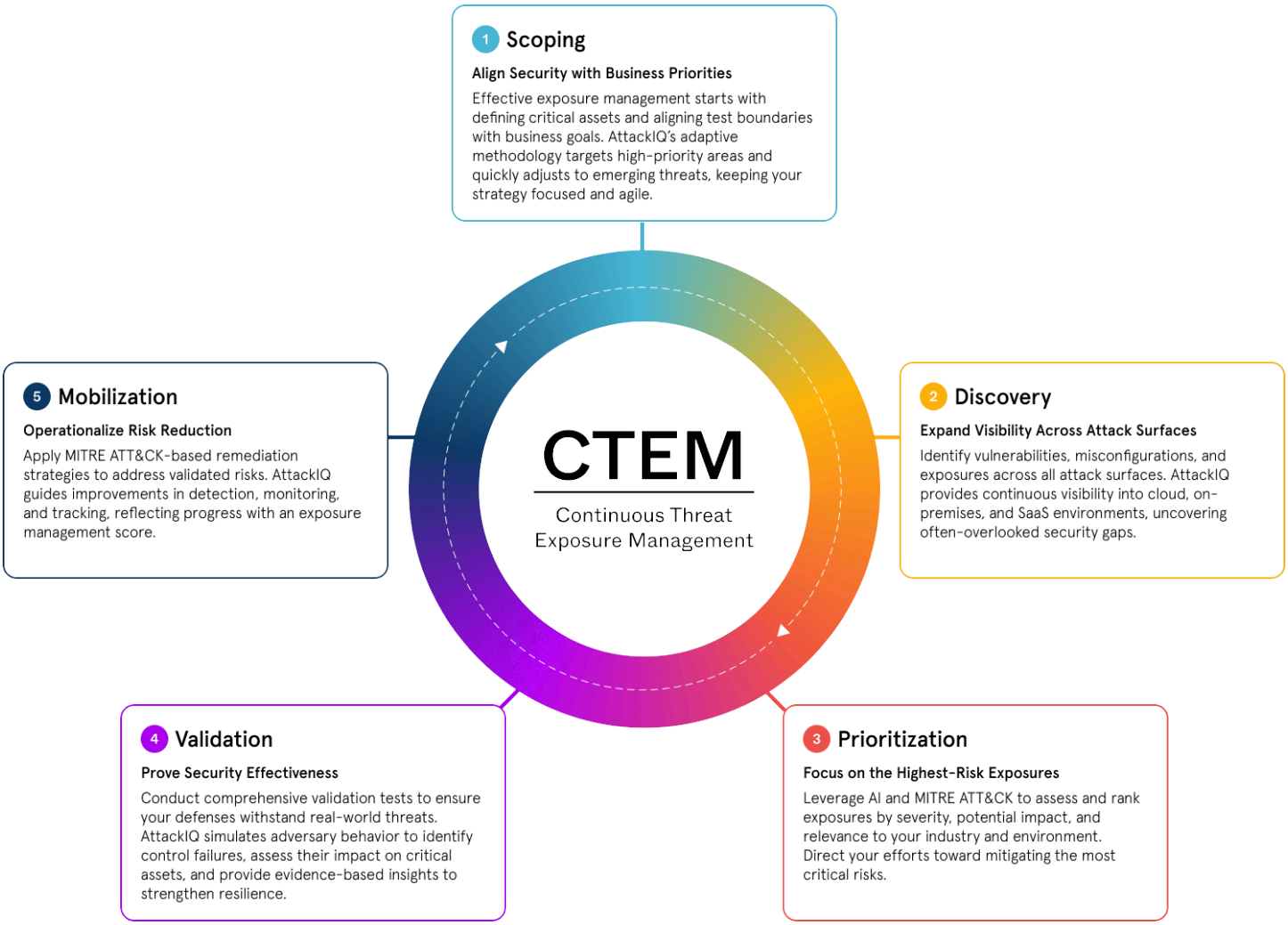
# Introducing the Adversarial Exposure Validation Platform

The AttackIQ Adversarial Exposure Validation (AEV) platform goes beyond traditional exposure management by continuously validating security controls and simulating real-world adversary tactics, techniques, and procedures (TTPs). With insights grounded in the MITRE ATT&CK® framework, you can identify exposures, prioritize mitigations, and reduce risks, enabling your organization to enhance readiness and build long-term resilience.



# Proactively Manage Threat Exposure with CTEM + AEV

AttackIQ's Adversarial Exposure Validation Platform supports every phase of CTEM by combining attack surface discovery, vulnerability intelligence, and adversary validation. This integrated approach delivers a continuous, data-driven defense against evolving threats.



# How AttackIQ Powers CTEM

AttackIQ's Adversarial Exposure Validation Platform operationalizes CTEM by delivering advanced automation, actionable insights, and real-world adversary emulations—all seamlessly integrated to scale your security operations.

### Reduces Risk & Threat Exposure

Continuously validate security controls, prioritize critical exposures, and adapt defenses in real time to minimize risk and prevent breaches.

### Enhances Operational Efficiency

Streamline repetitive security tasks, gain unified visibility into your attack surface, and integrate seamlessly with existing tools for a more efficient security strategy.

### Strengthen Compliance and Reporting

Conduct continuous security assessments and generate compliance-ready reports to meet evolving regulatory requirements and audit needs.

### Demonstrates Security Excellence

Improve security outcomes with measurable metrics like mean-time-to-detect (MTTD) and mean-time-to-remediate (MTTR), backed by clear, actionable reports.

Take the guesswork out of threat exposure management. Validate your defenses with real-world attack scenarios and focus on what matters most—manage your risk. Get a 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 cybersecurity community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.