ATTACKIQ

# Adversarial Exposure Validation Platform

## From Exposure Validation to Real Risk Reduction

Only 1% of published security vulnerabilities are actually exploited in the wild, yet organizations still struggle to identify which exposures pose genuine risk to their specific environment.

Attackers don't focus on isolated weaknesses—they discover attack paths by chaining exposures and bypassing security controls to reach high-value assets. Even patched systems may remain vulnerable if compensating controls are misconfigured or ineffective.

The AttackIQ Adversarial Exposure Validation (AEV) Platform operationalizes the Continuous Threat Exposure Management (CTEM) framework by continuously discovering, validating, prioritizing, and mobilizing responses to exposures in your unique environment. Focus where it matters—validate, remediate, measure, repeat.

> ***“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

### HIGHLIGHTS

**Identify Exploitable Security Gaps**

Continuously discover and validate which exposures are actually exploitable in your environment—so teams can focus remediation efforts where they’ll have the most impact.

**Discover Complex Attack Paths**

Map how attackers chain multiple exposures to reach critical assets, revealing hidden risks that traditional vulnerability scanners miss.

**Test Control Effectiveness Against Real Attacks**

Verify if your security controls actually withstand exploitation using MITRE ATT&CK®-aligned techniques that simulate real-world adversary behavior.

**Prioritize Based on Validated Risk**

Focus resources on exposures with confirmed exploitability and business impact rather than relying on generic severity scores.

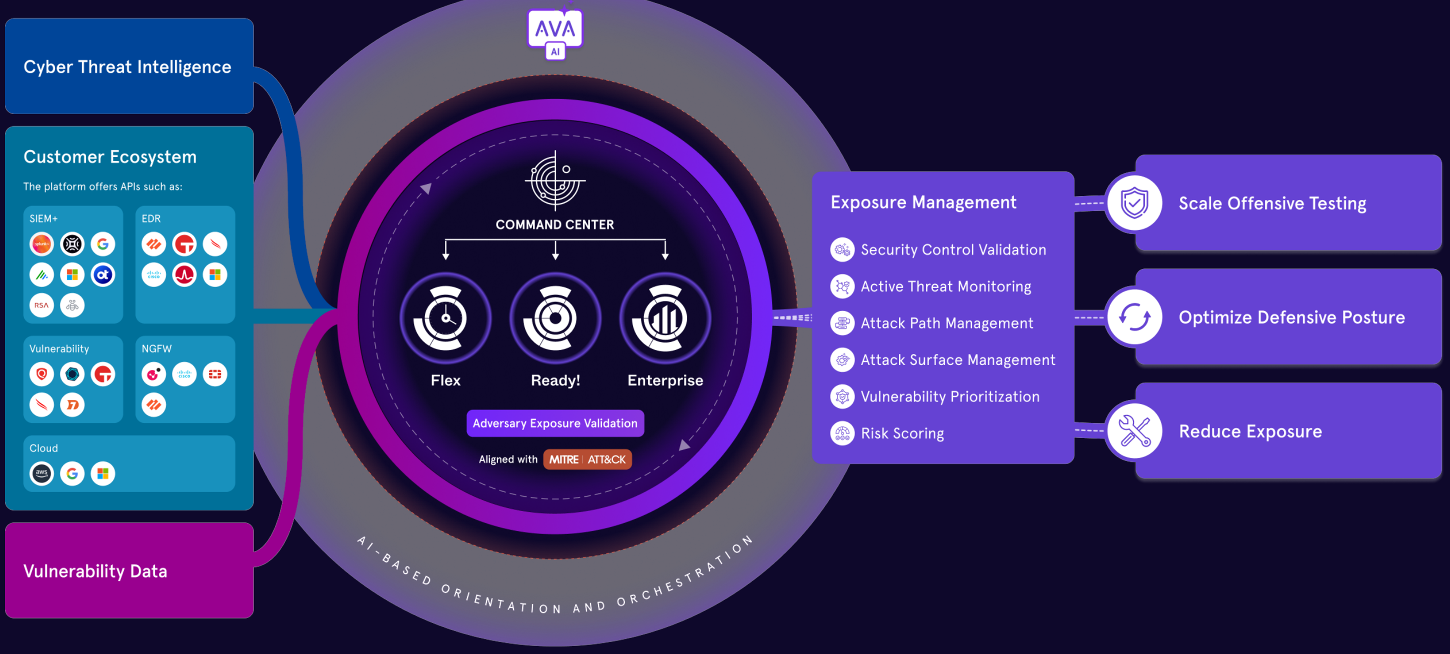
**Measure Exposure Reduction Over Time**

Track your security posture improvements with quantifiable metrics that demonstrate risk reduction to technical and executive stakeholders.

# Introducing the Adversarial Validation Platform

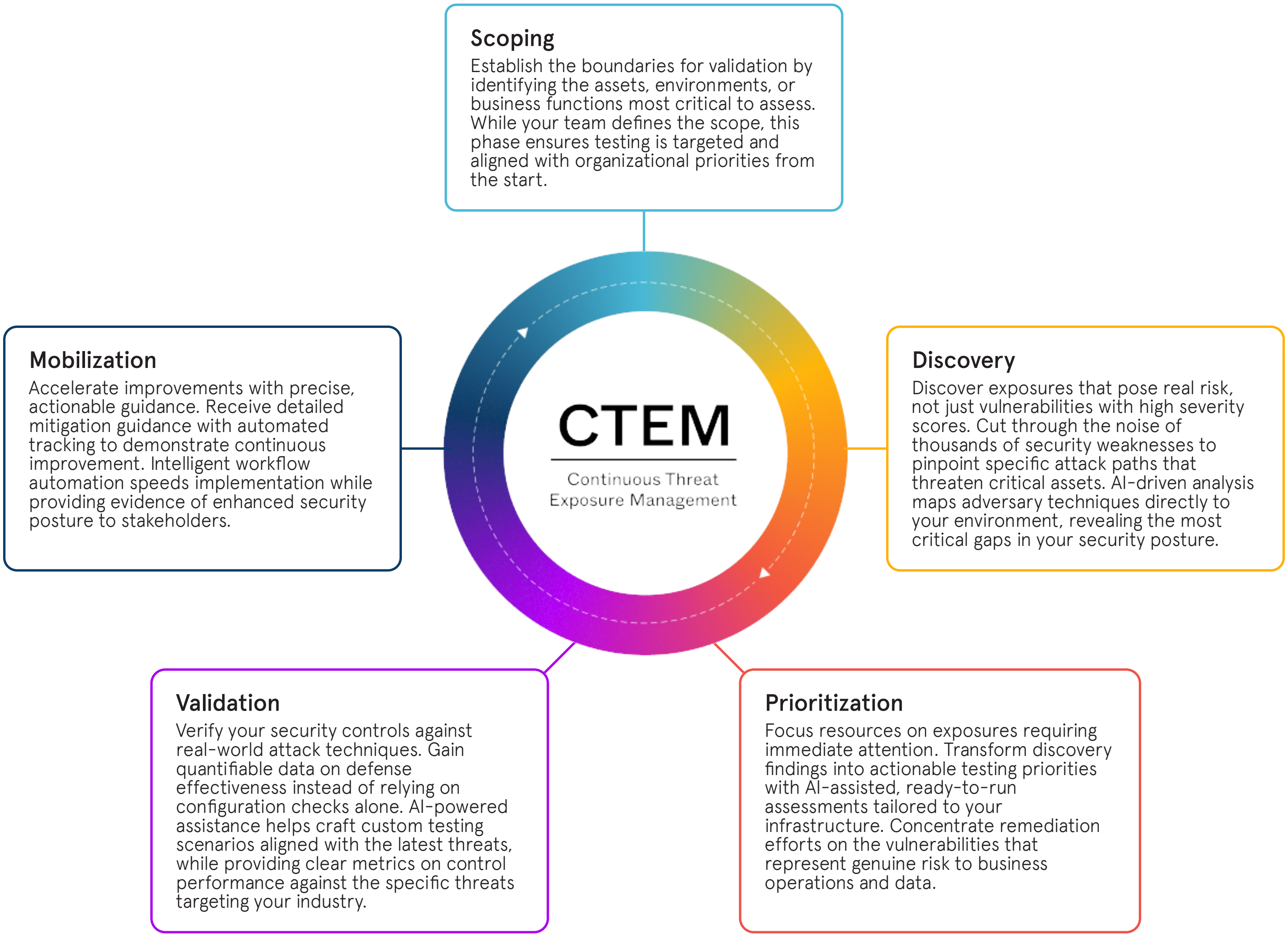
The AttackIQ Adversarial Exposure Validation (AEV) provides continuous, intelligence-driven insight into how adversaries move, what they can exploit, and whether your controls can stop them.

By simulating real-world attack behavior, AEV helps validate exposures, prioritize what matters, and take targeted action across the entire CTEM lifecycle. It's a unified, operational platform designed to reduce risk, improve control performance, and strengthen resilience.


Cyber Threat Intelligence
Customer Ecosystem
The platform offers APIs such as:
SIEM+
EDR
Vulnerability
NGFW
Cloud
Vulnerability Data
AVA
AI
COMMAND CENTER
Flex
Ready!
Enterprise
Adversary Exposure Validation
Aligned with MITRE | ATT&CK
AI-BASED ORIENTATION AND ORCHESTRATION
Exposure Management
Security Control Validation
Active Threat Monitoring
Attack Path Management
Attack Surface Management
Vulnerability Prioritization
Risk Scoring
Scale Offensive Testing
Optimize Defensive Posture
Reduce Exposure

# Operationalize Every Phase of CTEM

Take action across every stage of the CTEM lifecycle—moving from reactive defense to proactive, risk-driven exposure management.



### Scoping

Establish the boundaries for validation by identifying the assets, environments, or business functions most critical to assess. While your team defines the scope, this phase ensures testing is targeted and aligned with organizational priorities from the start.

### Discovery

Discover exposures that pose real risk, not just vulnerabilities with high severity scores. Cut through the noise of thousands of security weaknesses to pinpoint specific attack paths that threaten critical assets. AI-driven analysis maps adversary techniques directly to your environment, revealing the most critical gaps in your security posture.

### Prioritization

Focus resources on exposures requiring immediate attention. Transform discovery findings into actionable testing priorities with AI-assisted, ready-to-run assessments tailored to your infrastructure. Concentrate remediation efforts on the vulnerabilities that represent genuine risk to business operations and data.

### Validation

Verify your security controls against real-world attack techniques. Gain quantifiable data on defense effectiveness instead of relying on configuration checks alone. AI-powered assistance helps craft custom testing scenarios aligned with the latest threats, while providing clear metrics on control performance against the specific threats targeting your industry.

### Mobilization

Accelerate improvements with precise, actionable guidance. Receive detailed mitigation guidance with automated tracking to demonstrate continuous improvement. Intelligent workflow automation speeds implementation while providing evidence of enhanced security posture to stakeholders.

## Adversary-Informed. Intelligence-Driven. Built for CTEM.

AttackIQ delivers the only complete platform purpose-built to operationalize CTEM—combining adversary emulation, threat intelligence, and automation to continuously reduce exposure and drive long-term resilience.

### Reduce Risk & Threat Exposure

Continuously validate security controls against real adversary behavior to uncover hidden attack paths, prioritize exposures that pose genuine risk, and disrupt attack chains before adversaries reach critical assets.

### Enhance Operational Efficiency

Automate repetitive security tasks, streamline manual exposure validation, gain unified visibility into your attack surface, and scale your program with integrations across the entire security stack—from SIEM and EDR to vulnerability management.

### Strengthen Compliance and Reporting

Stay audit-ready with continuous assessments mapped to leading frameworks like MITRE ATT&CK®, and generate compliance-grade reports that satisfy regulators and reassure stakeholders.

### Demonstrate Security Excellence

Track progress over time with executive-ready dashboards that visualize exposure reduction, control effectiveness, and security posture trends—backed by real testing data that reflects actual risk reduction.

# AttackIQ Products

AttackIQ offers multiple product solutions tailored to your specific exposure validation needs:

### AttackIQ Flex!

*On-Demand Exposure Validation*

A flexible, agentless solution that delivers rapid security testing with minimal setup and no long-term commitment. Flex enables targeted validation of controls against specific threats without requiring permanent infrastructure changes.

Perfect when you require:

- Targeted validation of key security controls or vulnerabilities
- Point-in-time assessments without agent deployment
- Quick results for specific security questions with limited budget impact

### AttackIQ Ready!

*Fully Managed, Continuous Validation*

A turnkey service providing automated discovery, continuous exposure validation, and prioritized remediation guidance. Ready! combines expert-managed validation with comprehensive reporting to strengthen security posture with minimal operational overhead.

Ideal when you require:

- Continuous validation without specialized expertise
- Expert-managed service with actionable remediation guidance
- Regular effectiveness reporting for security leadership and boards

## AttackIQ Enterprise

*Complete Control of Your Security Readiness*

An enterprise-grade platform offering maximum customization, extensive integrations, and tailored testing. Enterprise enables comprehensive validation across complex environments with advanced workflow automation and detailed control assessment.

Optimal when you require:

- Advanced customization and security stack integration
- Custom attack scenarios with automated validation workflows
- Enterprise-scale deployment with comprehensive analytics and detailed reporting

## AttackIQ Command Center

*Centralized Orchestration for Security Validation*

A unified command hub for coordinating validation activities across multiple environments with granular access control. Command Center provides centralized management with flexible execution across environments—enabling unified oversight and secure operational autonomy.

Essential when you require:

- Multi-tenant security validation management
- Segregated testing environments with centralized oversight
- Unified reporting with role-based access controls

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.