ATTACKIQ

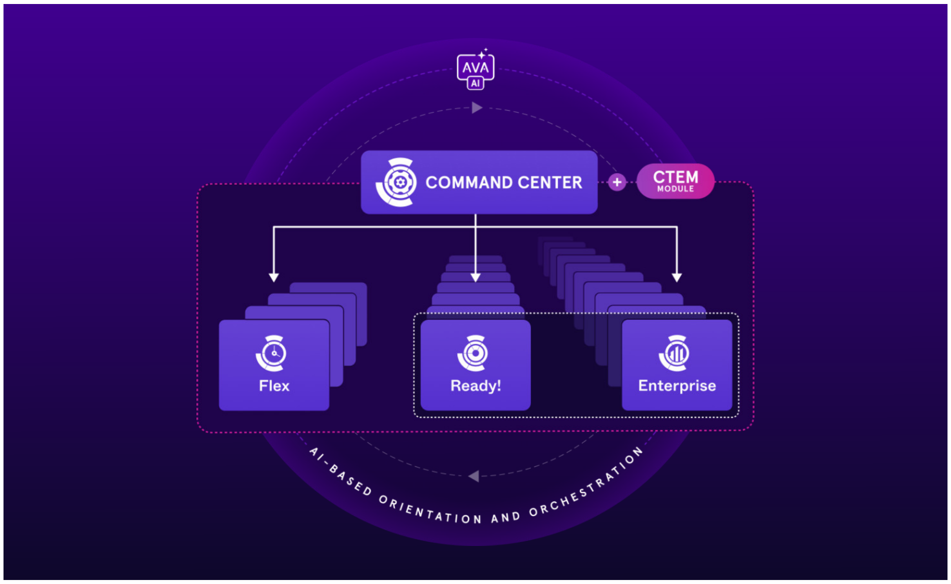
AttackIQ Command Center

The Challenge: Fragmented Security and Operational Silos

Security governance is often centralized, but cyber defense execution spans distributed teams using fragmented tools and siloed data—creating gaps, inefficiencies, and limited visibility into true security posture.

For enterprises, this means inconsistent validation practices, varying levels of maturity across business units, and difficulty standardizing security metrics. For MSSPs, it creates a management nightmare with separate toolsets for each client, inefficient resource allocation, and challenges scaling service delivery. And for partners, it limits the ability to deliver scalable solutions while maintaining consistent quality and reporting across diverse client environments.

The Solution: One Powerful Console to Simplify Complexity



HIGHLIGHTS

Unified Management Console
A single interface to manage deployments, users, agents, and third-party integrations while streamlining workflows.

Customizable Validation Framework
Configure validation scenarios—from baseline assessments to emerging threats and attack simulations—tailored for each business unit or client.

Automated Assessment Scheduling
Schedule recurring assessments or initiate on-demand testing as requirements evolve, maintaining continuous validation across your ecosystem.

Comprehensive Visibility
Transform assessment data into strategic insights with visualizations that highlight performance patterns and prioritize improvement efforts.

Advanced Governance Controls
Implement multi-layered access management, content filters, and security boundaries to maintain operational integrity across your validation program.

AttackIQ Command Center provides centralized oversight for exposure validation—tailored to each environment and built to scale across teams, deployments, and partners:

User Management

Control access and permissions across all deployments

Test Orchestration

Automate and coordinate assessment timing and execution

Validation Scenarios

Configure and customize testing for each team or client

Performance Monitoring

Track metrics and results in one place

Whether you're an enterprise managing business units, an MSSP handling client deployments, or a partner delivering validation services at scale, Command Center adapts to your specific operational needs.

Operate Securely. Govern Globally. Validate Continuously.

Unified Control, Reduced Overhead

- Centrally orchestrate validation across business units, partners, and clients from one secure console
- Automate user management, test provisioning, and reporting workflows to reduce manual effort
- Maintain secure separation between tenants while preserving global oversight

End-to-End Visibility, Zero Blind Spots

- Correlate testing results, control performance, and adversary behavior in real time
- Drill down into unit-level metrics or roll up into executive-ready dashboards
- Benchmark exposure trends across units to uncover systemic gaps and guide strategic investment

Flexible Validation, Faster Outcomes

- Deploy right-sized solutions matched to team maturity without losing standardization
- Scale from basic controls baseline to advanced simulations—all from the same platform
- Preserve historical performance data when upgrading between Flex, Ready, and Enterprise

Verified Third-Party Security, No Guesswork

- Replace manual vendor assessments with automated, evidence-backed validation
- Enforce testing and reporting standards across partners and suppliers with minimal friction
- Centralize third-party testing data to expose risks before they impact your supply chain

Tailored Solutions for Every Organization

For Enterprises

Overcome inconsistent validation practices and varying maturity levels across business units with a unified approach. Command Center helps you:

- Configure validation scenarios based on specific team requirements
- Compare results across business units to identify security gaps
- Streamline compliance reporting organization-wide

For MSSPs

Transform the management nightmare of separate toolsets, inefficient resource allocation, and scaling challenges into a streamlined operation. Command Center enables you to:

- Manage multiple client deployments from a single console
- Offer tiered services aligned to client needs
- Scale your validation business efficiently

For Partners

Deliver scalable solutions while maintaining consistent quality and reporting across diverse client environments. Command Center helps you:

- Create white-labeled offerings that maintain your brand identity
- Deliver measurable security improvements across client environments
- Offer third-party assessment as a value-added service

Customer Spotlight: Scaling Exposure Validation Across 52 Business Units

The Challenge

A global enterprise managing 52 business units needed centralized visibility into its cybersecurity posture—without sacrificing flexibility at the edge. Each unit operated under different regulatory, staffing, and operational conditions, making standardization difficult.

The Approach

Instead of enforcing a one-size-fits-all model, the organization adopted a tiered exposure validation strategy tailored to the needs of each business unit:

Smaller Teams

Implemented automated assessments for core control hygiene and emerging threats—minimizing setup and effort while reporting results centrally.

Mid-Scale Teams

Ran continuous validation aligned to enterprise baselines, with the ability to prioritize exposures and benchmark performance consistently.

Advanced Teams

Deployed high-fidelity adversary emulations informed by threat intelligence, conducting regular purple team exercises and continuous discovery.

The Impact

With layered validation in place, the organization unified security oversight across 15+ business units, gained real-time visibility into vulnerabilities and attack paths, and aligned exposure scoring with business risk to inform strategic decisions.

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.