SafeBreach

SafeBreach Helm

The AI Infrastructure Layer Powering Enterprise CTEM

Continuous Threat Exposure Management (CTEM) promises a more strategic, operational approach to risk reduction, but most security teams still struggle to operationalize it across fragmented tools and disconnected workflows—until now.

SafeBreach Helm is the AI infrastructure layer of the **SafeBreach CTEM Platform** that unifies the full CTEM lifecycle, orchestrating three purpose-built AI agents—the Analyst Agent, Validation Agent, and SecOps Agent—through a single natural-language interface. As a result, teams can continuously discover, validate, and remediate exposures based on real attacker behavior at enterprise scale.

THE CHALLENGE

Siloed Tools & Systems

Most organizations already have the core technologies required for exposure management—Vulnerability Management (VM), External Attack Surface Management (EASM), Threat Intelligence (TI), Breach and Attack Simulation (BAS), Security Orchestration, Automation, and Response (SOAR), and remediation workflows—but these systems remain siloed. Security teams must manually correlate findings, prioritize exposures without full context, and validate risk across disconnected tools.

The result is predictable: alert fatigue, low confidence in exposure exploitability, remediation bottlenecks, and operational inefficiency.CTEM was designed to address this challenge, but operationalizing CTEM at enterprise scale requires more than a framework. It requires continuous orchestration across each of the framework's phases: scoping, discovery, prioritization, validation, and mobilization.

THE SOLUTION

SafeBreach Helm

SafeBreach Helm operationalizes the entire CTEM lifecycle through three AI agents that continuously discover, validate, and remediate exposures based on real attacker behavior. This capability is enabled using a single, natural-language interface that removes the need for security leaders to manage multiple AI systems.

Instead, teams can ask SafeBreach Helm one question and get one actionable answer in return—for example, "Where could Volt Typhoon threat actors gain traction in my environment and what gaps should I fix first?" In response, SafeBreach Helm automatically coordinates:

The result is a unified, validated remediation workflow instead of fragmented findings across disconnected tools.

HOW IT WORKS

The Three Agents

Analyst Agent

CTEM PHASE: SCOPE | DISCOVER | PRIORITIZE

Continuously scopes, discovers, and prioritizes exposures by correlating:

- Vulnerability management (VM)
- External attack surface management (EASM)
- Threat intelligence (TI)
- Asset intelligence

The Analyst Agent helps teams focus on the exposures most likely to impact the business.

Validation Agent

CTEM PHASE: VALIDATE

Validates exploitable exposures using:

- Adversarial Exposure Validation (AEV)
- Continuous attack simulation
- Attack path analysis

Powered by **SafeBreach Validate** and **SafeBreach Propagate**, the Validation Agent replaces theoretical risk scoring with evidence-based validation grounded in real attacker behavior.

SecOps Agent

CTEM PHASE: MOBILIZE

Continuously scopes, discovers, and prioritizes exposures by correlating:

- SOAR platforms
- Ticketing systems
- Security operations tooling

The SecOps Agent reduces mean-time-to-respond (MTTR) by prioritizing fixes based on validated business impact rather than raw vulnerability volume.

Why It Matters

Continuously operationalizes CTEM instead of treating it as a static framework

Reduces remediation fatigue by prioritizing exposures that materially impact risk

Replaces theoretical risk scoring with validated exploitability from real attacks

Continuously aligns defenses to evolving attacker behavior at enterprise scale

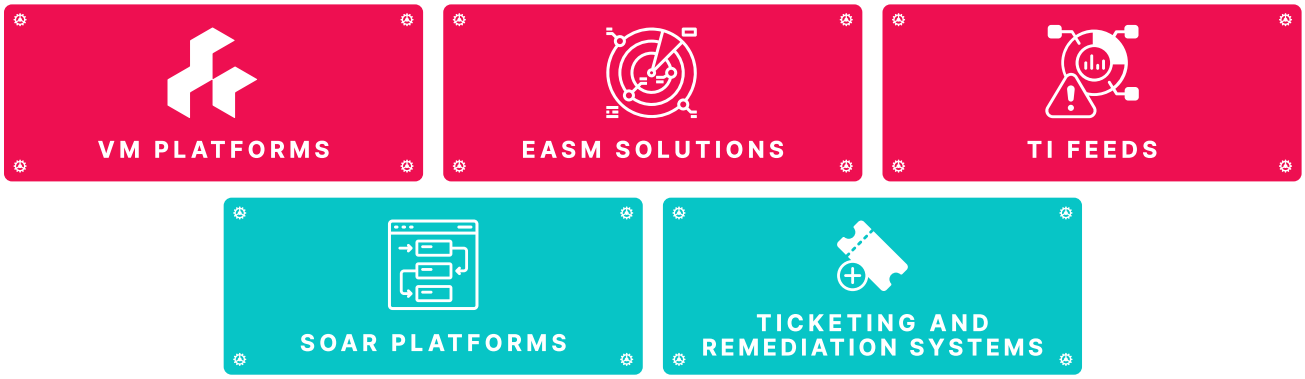
Unifies discovery, validation, and remediation into a single workflow

Enables teams to leverage existing security investments

How to Activate SafeBreach Helm

SafeBreach Helm is available to organizations running SafeBreach Validate or SafeBreach Propagate, providing the foundation for activating the Validation Agent and validating exploitability through continuous adversarial testing.

Organizations can extend Helm across the CTEM lifecycle by integrating existing:



This allows teams to operationalize CTEM incrementally while leveraging their existing security stack.

Take the Helm with SafeBreach Today

Schedule a personalized demo today to learn why enterprise security leaders choose SafeBreach Helm to operationalize the CTEM framework and continuously discover, validate, and remediate exposures at scale.

About SafeBreach

SafeBreach is on a mission to help organizations have certainty in their security. Long trusted as the global leader in adversarial exposure validation (AEV), SafeBreach empowers organizations to take command of risk by operationalizing the full CTEM lifecycle. Powered by the SafeBreach Helm AI Agent and grounded in the award-winning SafeBreach Exposure Validation Platform, CTEM by SafeBreach is the first enterprise-grade, closed-loop solution designed to move organizations beyond siloed security activities toward a continuous, intelligence-driven exposure management program. Backed by world-renowned threat researchers and an unrivaled customer success team, SafeBreach provides the capabilities enterprises need to holistically understand threat exposure, make data-driven decisions that reduce risk, and measurably improve cyber resilience—safely and at scale. To learn more about SafeBreach, visit **www.safebreach.com**.

SafeBreach

US Headquarters

526 W Fremont Ave #2880
Sunnyvale, CA 94086

Israel Offices

HaMasger St 35, Sky Tower, Floor 8
Tel Aviv-Yafo, Israel

SAFEBREACH.COM