SafeBreach

The SafeBreach CTEM Platform

Command Your Risk with an AI-Powered, Closed-Loop Continuous Threat Exposure Management (CTEM) Platform

Security teams are overwhelmed with exposure data but lack clarity on what is truly exploitable and impactful. The **SafeBreach CTEM Platform** transforms exposure management into a continuous, intelligence-driven program—operationalizing the full CTEM lifecycle with real-world validation, AI-driven orchestration, and closed-loop remediation.

Grounded in Adversarial Exposure Validation (AEV) and integrated across the broader security ecosystem, the platform enables organizations to continuously identify, validate, prioritize, and eliminate real cyber risk at scale.

THE PROBLEM

Exposure Without Proof

Modern organizations face a fundamental gap between visibility and action:

- **Too many findings, not enough context.**
  Vulnerabilities and exposures lack proof of exploitability.
- **Fragmented security ecosystem.**
  Vulnerability Management (VM), External Attack Surface Management (EASM), Breach and Attack Simulation (BAS), and remediation tools operate in silos.
- **No consistent prioritization model.**
  Teams rely on Common Vulnerability Scoring Systems (CVSS) scores instead of real attacker behavior.
- **Lack of validation and closure.**
  Organizations cannot confirm whether risk is exploitable or fixed.
- **Limited understanding of real attack paths.**
  Static models fail to reflect how attackers actually move.

The Result: Inefficient remediation, wasted resources, and persistent cyber risk.

THE SOLUTION

The SafeBreach CTEM Platform

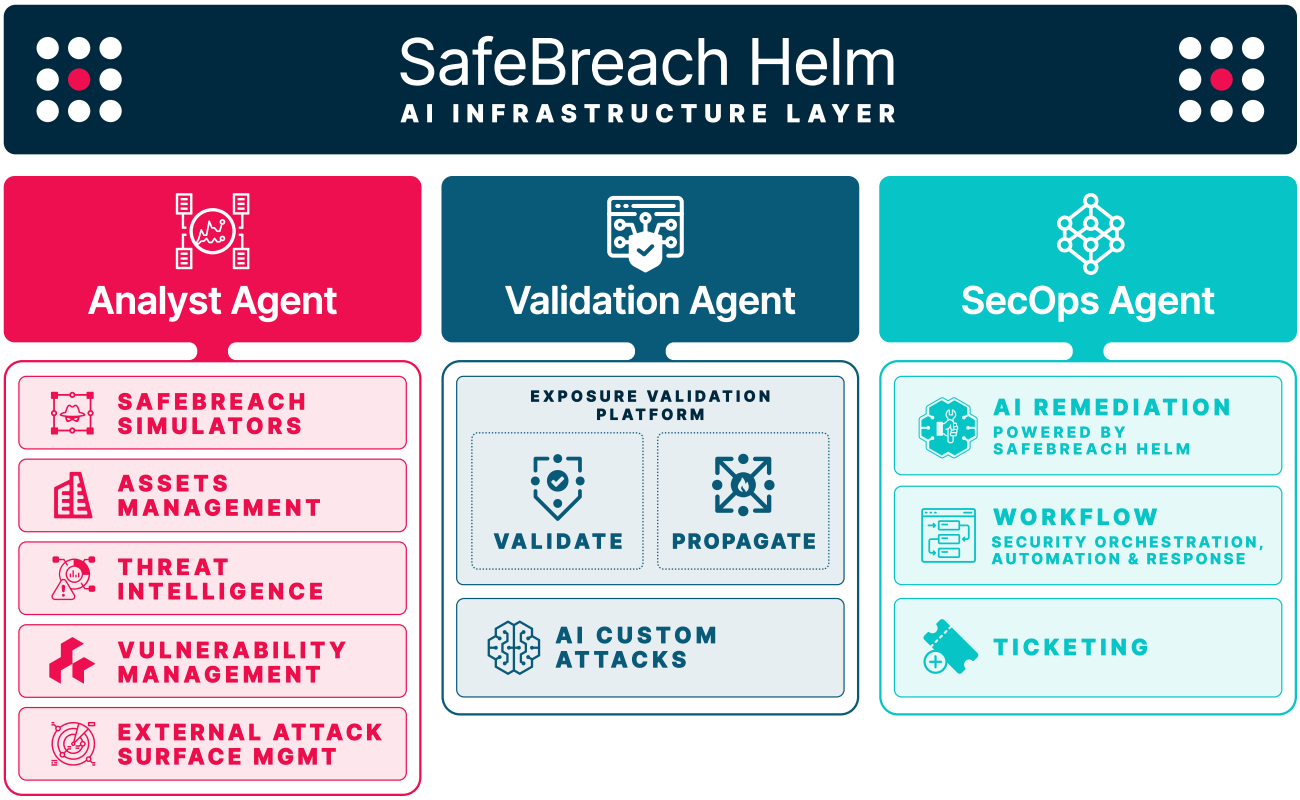
The SafeBreach CTEM Platform is an enterprise-grade, AI-powered platform that brings together fragmented security activities into a continuous, closed-loop program. At its core, SafeBreach Helm—the AI infrastructure layer—orchestrates three purpose-built AI agents to operationalize the full CTEM lifecycle: the Analyst Agent, Validation Agent, and SecOps Agent.

It is powered by the **SafeBreach Exposure Validation Platform** (the AEV foundation), **AI Remediation**, and ecosystem integrations spanning VM, EASM, and Threat Intelligence (TI). Together, these capabilities operate as a single, continuous, closed-loop program. Unlike traditional approaches and other AEV providers, SafeBreach turns exposure management into measurable risk reduction, grounded in real-world validation.

HOW IT WORKS

SafeBreach Helm & the AI Agents

The SafeBreach CTEM Platform operationalizes the full CTEM lifecycle, with every stage powered by purpose-built AI agents orchestrated by SafeBreach Helm.



SAFEBREACH HELM

The AI Infrastructure Layer

Role: The AI infrastructure layer that orchestrates the CTEM platform and coordinates three purpose-built AI agents through a single, intelligent interface.

SafeBreach Capabilities

- Natural language investigation, validation triggering, attack path analysis, and remediation orchestration via simple prompts.
- Unifies data from AEV, VM, EASM, TI, and Asset Management sources.

Outcome: A coordinated, closed-loop CTEM program where every agent shares the same intelligence—not siloed tools or fragmented workflows.

Analyst Agent

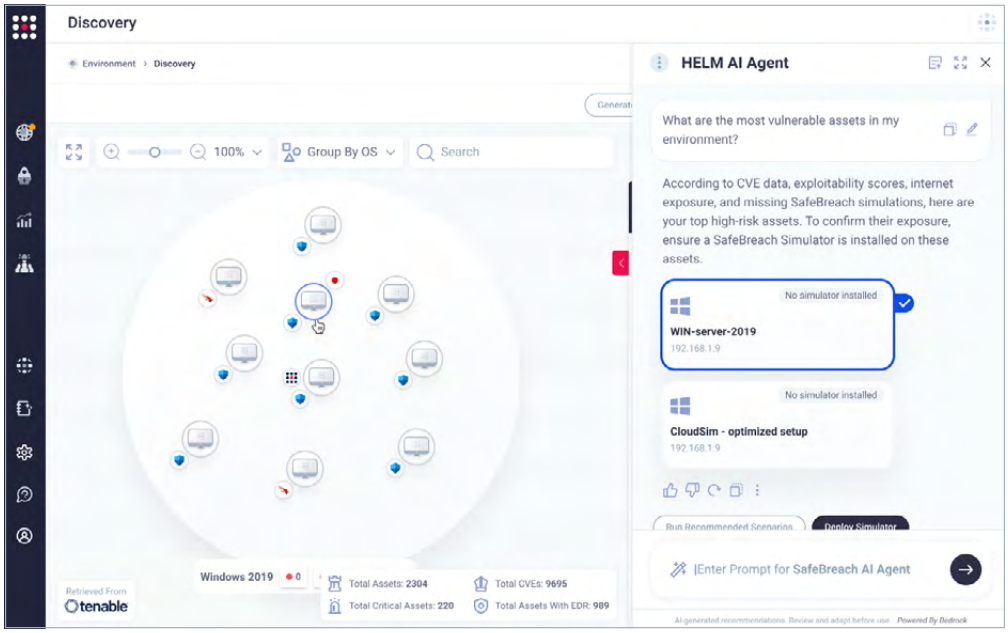
CTEM PHASE: SCOPE | DISCOVER | PRIORITIZE

Role: Continuously scopes, discovers, and prioritizes exposures across internal and external attack surfaces.

SafeBreach Capabilities

- Powered by Asset Management, TI, EASM, and VM integrations.
- AI-driven correlation of exposure, asset, and TI data to focus teams on exploitable, business-critical risk.

Outcome: Risk-prioritized exposures aligned to business impact—not raw vulnerability counts.



Validation Agent

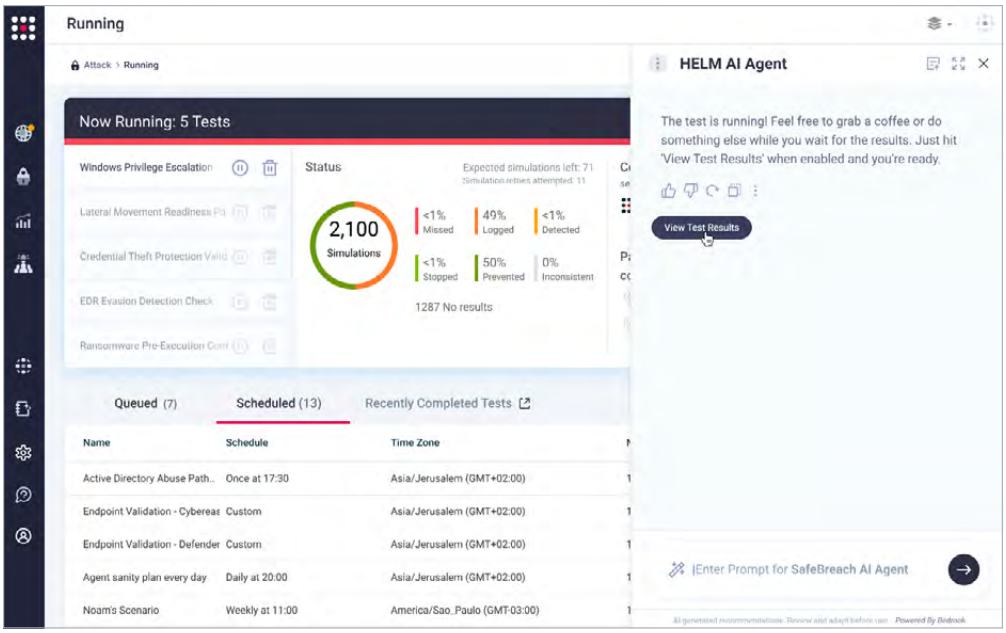
CTEM PHASE: VALIDATE

Role: Validates real-world attack exposure through AEV—including BAS, attack path validation (APV), and AI-driven adversarial testing.

SafeBreach Capabilities

- Powered by the SafeBreach Exposure Validation Platform: **Validate (BAS)** for full kill-chain simulations and **Propagate (APV)** for attack path validation.
- AI Custom Attacks via Breach Studio, including a VS Code extension for environment-specific testing.
- Continuously updated TI to ensure realism and currency against active adversary tactics, techniques, and procedures (TTPs).

Outcome: Empirical proof of how attackers could actually compromise



SecOps Agent

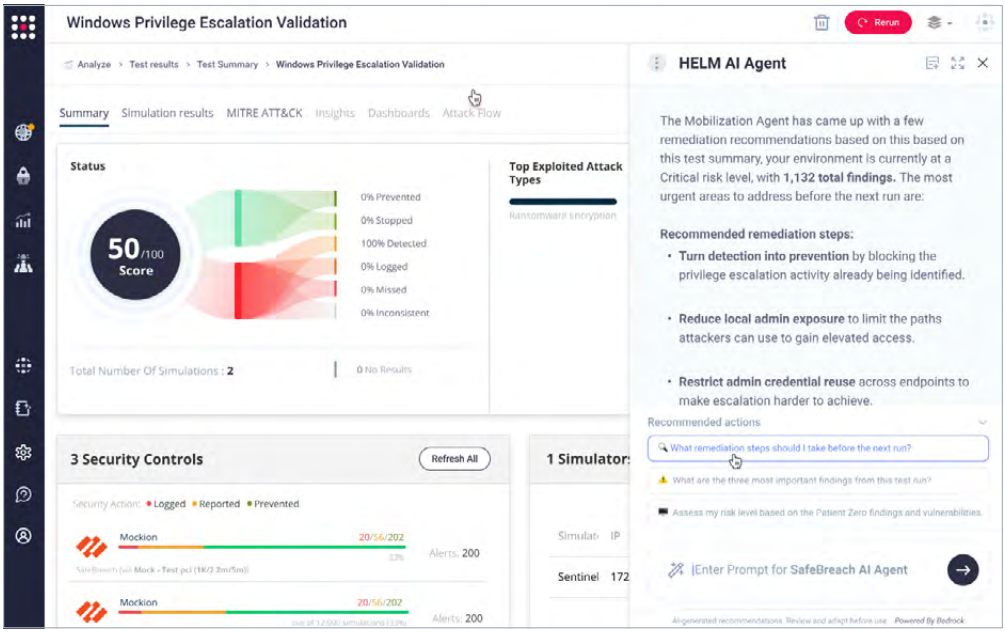
CTEM PHASE: MOBILIZE

Role: Operationalizes remediation through AI-guided workflows, automation, and security operations integrations.

SafeBreach Capabilities

- Powered by **AI Remediation** for context-aware, simulation-based fixes tied to validated exposures.
- Ticketing, Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) integrations to operationalize remediation workflows.
- Closed-loop validation to confirm remediation success and measurable risk reduction.

Outcome: Faster, measurable risk reduction with remediation tied directly to validated exposures.



Why SafeBreach

SafeBreach is uniquely positioned to deliver CTEM by combining proven AEV, AI-native orchestration, closed-loop execution, and a truly unified platform.

SafeBreach's core AEV offering delivers real-world attack simulation across the full kill chain, autonomous validation of attack paths, and continuous testing of security controls and detections. This is paired with SafeBreach Helm, the AI infrastructure layer that orchestrates the Analyst Agent, Validation Agent, and SecOps Agent. Together, they enable natural language investigation and action across the full CTEM lifecycle and unify intelligence across tools and data sources.

All of this is delivered through a single platform that integrates VM, EASM, TI, and validation—eliminating siloed workflows and fragmented tooling.

Business Value

FOR CISOs & SECURITY LEADERS

- Command enterprise risk with confidence
- Prove security effectiveness with measurable outcomes
- Prioritize investments based on real-world impact
- Strengthen cyber resilience continuously

FOR SECURITY PRACTITIONERS

- Test defenses against real attacker behavior
- Validate exploitability and eliminate false positives
- Understand real attack paths and blast radius
- Accelerate remediation with precise, actionable guidance

Take the Helm with the SafeBreach CTEM Platform

CTEM isn't a framework you adopt—it's a discipline you execute. The SafeBreach CTEM Platform turns exposure management into a continuous, AI-driven, closed-loop operation—giving you the power to:

- Focus on what truly matters
- Prove real-world exploitability, not theoretical risk
- Eliminate the exposures that actually reduce risk

This isn't more visibility. It's decisive control over cyber risk. Stop managing exposure. Start commanding it. **Request a demo today** to learn how.

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