SafeBreach

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

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

Powered by the SafeBreach Helm AI Agent and grounded in Adversarial Exposure Validation (AEV), the CTEM by SafeBreach solution enables organizations to continuously identify, prioritize, validate, and eliminate real cyber risk at scale.

THE CHALLENGE

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 System (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

CTEM by SafeBreach

SafeBreach delivers an enterprise-grade, AI-powered CTEM solution that brings together fragmented security activities into a continuous, closed-loop program. It combines the **SafeBreach Exposure Validation Platform** (the AEV foundation), SafeBreach Helm (the AI CTEM agent), and **AI Remediation** with ecosystem integrations.

Together, these capabilities operationalize the full CTEM lifecycle—Scope, Discover, Prioritize, Validate, and Mobilize—within a single, unified platform. By connecting each stage in a continuous loop, SafeBreach enables organizations to move beyond theoretical exposure and focus on what can actually be exploited and fixed.

Unlike traditional approaches and other AEV providers, SafeBreach turns exposure management into measurable risk reduction, grounded in real-world validation.

HOW IT WORKS

CTEM Lifecycle Mapped to SafeBreach

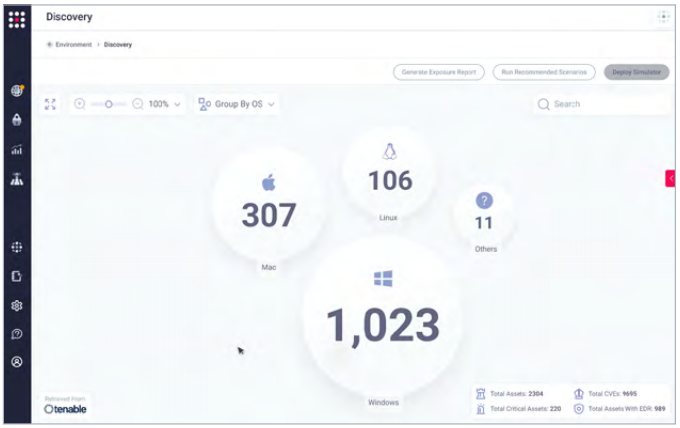
1. SCOPE
Define What Matters Most

Objective: Focus on critical assets, business priorities, and relevant threats

SafeBreach Capabilities:

- Helm AI Agent contextualizes assets and business risk via natural language interaction
- Security ecosystem integrations (e.g. Threat Intelligence) align validation scope to real-world attacker TTPs and operational security context

Outcome: A validation strategy aligned to business-critical risk not generic coverage



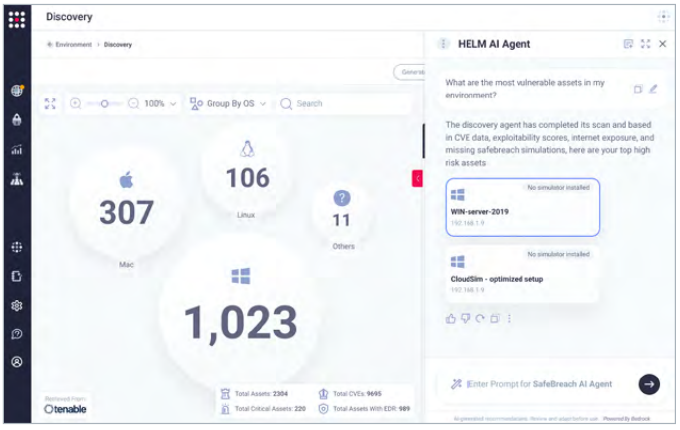
2. DISCOVER
Continuously Identify Exposures

Objective: Aggregate exposure data across the entire attack surface

SafeBreach Capabilities:

- Exposure Hub (upcoming) for unified exposure correlation from Vulnerability Management (VM) and External Attack Surface Management (EASM) tools
- Platform-wide integrations across endpoint, network, and cloud

Outcome: Continuous, unified visibility into all exposures—internal and external



3. PRIORITIZE

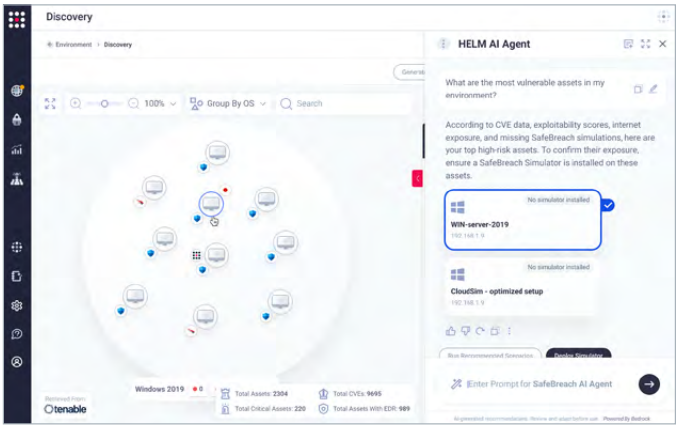
Focus on What Actually Matters

Objective: Identify exposures that pose real, exploitable risk

SafeBreach Capabilities:

- AEV correlation (Exposure Validation Platform)
- Attack path context via Propagate
- Helm AI-driven analysis and investigation

Outcome: Prioritization based on exploitability, attack paths, and business impact not noise



4. VALIDATE

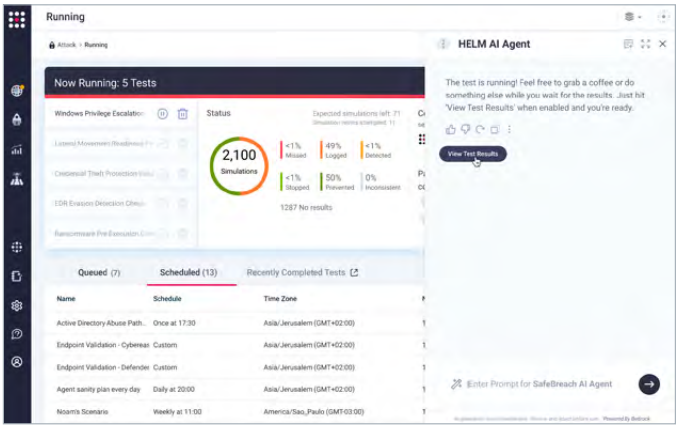
Prove What Is Exploitable

Objective: Confirm real-world exploitability of exposures

SafeBreach Capabilities:

- **Validate (BAS)** executes full kill-chain attack simulations and enables teams to build custom attacks with VS Studio
- **Propagate (APV)** simulates lateral movement and attack paths
- Threat Intelligence (TI) ensures realism and relevance

Outcome: Empirical proof of what attackers can actually achieve



5. MOBILIZE

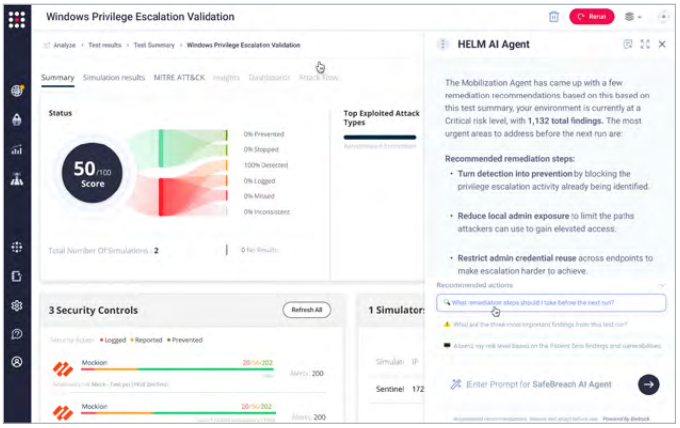
Turn Insight into Action

Objective: Remediate validated risk efficiently and effectively

SafeBreach Capabilities:

- **AI Remediation** provides context-aware, simulation-based fixes
- Ticketing/SIEM/SOAR integrations operationalize workflows
- Closed-loop validation confirms remediation success

Outcome: Faster remediation with measurable risk reduction



Why SafeBreach

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

At its core is AEV, delivering 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, an AI-native CTEM orchestration layer that enables natural language investigation and action, applies AI-driven capabilities across every stage of the CTEM lifecycle, and unifies intelligence across tools and data sources.

SafeBreach operationalizes CTEM as a continuous, closed-loop process—Scope, Discover, Prioritize, Validate, Mobilize—with built-in feedback to confirm remediation effectiveness. 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

Get Hands-On With CTEM by SafeBreach

CTEM isn't a framework you adopt—it's a discipline you execute. CTEM by SafeBreach turns exposure management into a continuous, AI-driven, closed-loop operation that gives 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