SafeBreach

SOLUTION BRIEF

SAFEBREACH CTEM PLATFORM

The SafeBreach Validation Agent:
AI-Powered Adversarial Exposure Validation

Executive Summary

Most organizations struggle to determine whether identified exposures are actually exploitable. Vulnerability findings and attack surface data alone cannot reveal how attackers would realistically compromise the environment.

The **SafeBreach Validation Agent** operationalizes the validation phase of Continuous Threat Exposure Management (CTEM) by continuously testing security defenses against real-world attacker behavior.

Powered by the SafeBreach Exposure Validation Platform—including SafeBreach Validate and SafeBreach Propagate—the Validation Agent uses adversarial exposure validation (AEV) to determine how attackers could exploit exposures, move laterally, and impact critical assets.

How the Validation Agent Works

Operating within **SafeBreach Helm**, the Validation Agent continuously validates real-world attack exposure using:

- ☐ SafeBreach Validate · BAS
- ☐ SafeBreach Propagate · APV
- ☐ AI-driven adversarial testing
- ☐ Distributed simulators
- ☐ The SafeBreach Hacker's Playbook™

The agent executes realistic attack scenarios to reveal:

- Which exposures are **truly exploitable**
- How attackers could **move laterally**
- Which **controls fail**
- What **assets are reachable**
- The true **blast radius** and business impact

> Security teams can trigger validations, investigate findings, and analyze attack paths through **SafeBreach Helm's** natural language interface.

Key Benefits

01
Move Beyond Theoretical Risk
Validate whether exposures are actually exploitable in the real environment.

02
Understand Real Attacker Behavior
Gain visibility into how attacks unfold across systems, identities, and critical assets.

03
Prioritize Based on Proven Risk
Focus remediation efforts on validated attack paths and exploitability.

04
Strengthen Cyber Resilience
Continuously test defenses against evolving attacker techniques before adversaries strike.

Business Outcomes

Organizations using the Validation Agent can:

- ☐ Eliminate **blind spots** before exploits happen
- ☐ Demonstrate **measurable risk reduction**
- ☐ Stay current against evolving threat landscape
- ☐ Quantify **blast radius** and business impact
- ☐ Improve **prioritization accuracy**
- ☐ Prove your security stack is working—before an incident occurs
- ☐ Strengthen resilience against evolving threats

BUILT ON PROVEN ADVERSARIAL VALIDATION

30,000+ attack methods in the Hacker's Playbook™

- Continuous threat research and rapid updates
- Enterprise-safe simulations for production environments
- Proven deployment across Fortune 500 organizations

CONCLUSION

The SafeBreach Validation Agent enables organizations to continuously validate defenses against real attacker behavior, strengthening resilience and proving defense-readiness.

Powered by **SafeBreach Helm** and the **SafeBreach Exposure Validation Platform**, the Validation Agent helps organizations move beyond theoretical risk and prioritize exposures based on proven exploitability.