SafeBreach

SafeBreach Validate

Put Your Cyber Defenses to the Test with Pioneering Breach & Attack Simulation

Enterprise security leaders spend millions annually on security tools to protect their organization, but often lack complete confidence in these very tools when dealing with the rapidly evolving threat landscape. Organizations need a way to continuously validate their controls against newly emerging attacks to decrease the risk of a breach and understand the overall impact of threats on organizational security posture.

SafeBreach Validate is an award-winning breach and attack simulation (BAS) tool that uses patented technology to test the efficacy of deployed security controls against real-world threats. Leveraging the tactics, techniques, and procedures (TTPs) used by malicious actors, Validate automates adversarial attacks to help you:

- Reduce the attack surface and improve security posture by running simulation techniques across the entire MITRE ATT&CK® kill chain to identify security gaps and misconfigurations.
- Support a proactive and continuous threat exposure management program.
- Leverage the largest attack playbook and the ability to create custom attacks to validate your entire organizational security control stack automatically and at scale.
- Minimize the overall time to detect and respond through contextual remediation insights and a comprehensive integration ecosystem.
- Uncover empirical evidence about control efficacy, threat exposure, and cyber risk to empower data-driven business and security decisions.
- Automate the execution of multi-stage attacks across the entire cloud stack, including end-user devices, networks, cloud services, and applications.

Validate Benefits

Continuously Test Your Defenses

Continuously test the efficacy of your security controls with 30,000+ attack methods from our patented Hacker's Playbook™—including SafeBreach Original Attacks you won't find anywhere else—or create your own customized attacks.

Understand Your Exposure

Analyze your organizational posture broken down by category, including the MITRE ATT&CK® framework, known attacks, and threat groups, so your team can understand the efficacy of existing systems at a glance, inform resourcing decisions, and enhance strategic alignment.

Accelerate Remediation

Uncover actionable insights about the root cause of successful breach simulations to identify and visualize gaps, collaborate to speed remediation, and efficiently reduce the attack surface.

Monitor Your Risk

Enhance stakeholder visibility with customizable dashboards and reports to help key stakeholders quickly understand existing gaps, evaluate risks, and recognize security drift.

Validate Use Cases

Security Control Validation

See what's happening in your security ecosystem with contextualized data that helps you understand exposure across the entire kill-chain and explore mitigation approaches. Evaluate and compare control technologies to make the most informed implementation decisions.

Detection Engineering Efficiency

Automatically and continuously validate detections and alerts for thousands of known attack methods. Create custom detections more efficiently to allow detection engineering teams to focus more resources on remediation or other high-value initiatives.

Security Posture & Resilience Reporting

Benchmark and continuously measure organizational security posture, align security programs with business outcomes, and justify security investments by highlighting their return on investment (ROI). Demonstrate resiliency through a composite scoring approach that identifies performance gaps and quantifies exposure across the enterprise.

Enterprise Safety & Scalability

SafeBreach Validate was purpose-built for enterprise organizations and provides the highest level of protection against risks that other forms of security testing can introduce. SafeBreach Validate does not execute actual malware, but instead simulates phases of the malware cycle, including:

Malware Delivery

This phase is simulated by transferring the real malware payload to the endpoint. This is done on the network level and malware is not written to disk or executed at any time during this phase.

Malware Infection

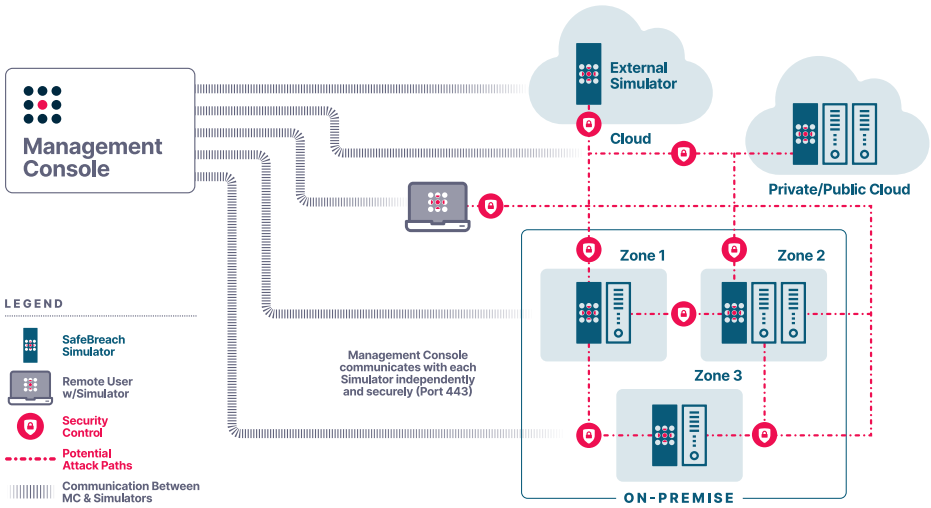
During this phase, the real malware payload is written to disk and removed at the end of the simulation. No malware is triggered or executed at any time during this phase.

Malware Activity

To imitate real malware activity—including changing system configurations, creating scheduled tasks, and simulating ransomware—SafeBreach Validate leverages simulations involving actions derived from reverse engineering of real malware.

Malware Propagation

Malware propagation is simulated against SafeBreach services (on the same or other simulators) and certain pre-approved services to prevent any risk to the production infrastructure.



How Validate Works

1. Deploy Simulators

Lightweight simulators are deployed in critical network segments, in the cloud, or on endpoints to play the attacker and simulate the entire kill chain.

2. Simulate Attacks

The SafeBreach Management Console continuously orchestrates and executes attacks from our industry-leading Hacker's Playbook™ or custom attacks designed by you.

3. Analyze Results

Automated analysis functionality correlates simulation results and event logs from integrated security devices to help analysts quickly identify gaps and control misconfigurations.

4. Prioritize Threats

In-depth simulation results can be broken down by category—including MITRE ATT&CK®, known attacks, and threat groups—to prioritize threats based on their impact on organizational security posture.

5. Accelerate Remediation

Simplified integrations with SIEM, SOAR, and workflow management tools enable remediation insights to be easily shared with other teams, reducing the MTTD and MTTR and improving overall SOC efficacy.

6. Monitor & Communicate Risk

Simulations can be re-run after gaps and misconfigurations have been addressed to validate modifications, monitor drift, and ensure a hardened security posture. Customizable dashboards and reports provide a security baseline, track improvement over time, and support communication with key stakeholders.

Why Validate?

SafeBreach Validate is a pioneering and award-winning BAS solution for enterprise security teams that need to validate the efficacy of their deployed security controls against today's advanced attacks so they can quickly identify and remediate security gaps and control misconfigurations. With Validate, security teams can:

Uncover empirical evidence about control efficacy, threat exposure, and cyber risk.

Speed and simplify detection engineering and remediation by quickly and accurately exposing potential security gaps.

Deliver actionable insights and remediation guidance to help key business and IT stakeholders make data-driven business- and security-spending decisions.

Get Hands-On with Validate

Schedule a personalized demo today to learn why enterprise security leaders choose SafeBreach Propagate to enhance the quality, efficacy, and value of their security programs.

ABOUT SAFEBREACH

SafeBreach is the leader in enterprise-grade exposure validation, providing the world's largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach Exposure Validation Platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit **www.safebreach.com.**

SafeBreach