SafeBreach

Establish Continuous Visibility Into the Evolving Threat Landscape

Executive Summary

Even yesterday's most advanced, stringent security controls won't cut it if a new vulnerability, attack method, or misconfiguration arises today. To make sure your organization's critical digital assets remain secure, it's vital to perform continuous, intelligent threat assessment. Find out how SafeBreach offers the advanced breach and attack simulation capabilities you need to stay in front of threats.

Introduction

If your organization is like most, you've implemented a number of advanced security technologies, and you're continuing to add to the mix of tools in place.

However, no matter how advanced or comprehensive your toolsets are, the reality is new threats arise all the time. In the wake of news about organizations being breached or high-profile vulnerabilities being discovered, your teams can't just assume they're covered.

Your teams need to be able to ascertain whether the organization is exposed, and, if so, where the gap is and how to address it. Teams need access to the latest threat methodologies so they can objectively and accurately assess the range of controls implemented and ensure those controls are effectively blocking a specific vulnerability or method of attack.

The Challenge:
The Limitations of Traditional Threat Assessment Approaches

Given the fact the threat landscape constantly evolves and changes, you need to continue to shift focus in your search for security gaps. Ultimately, you need to ensure your security operations move as fast as cyber attackers. Unfortunately, many of the tools and approaches available in the past have fallen short in enabling these objectives.

Security teams can pursue a number of approaches for doing threat assessments, such as penetration testing, red team exercises, vulnerability scanning, and more. Many teams also employ threat intelligence solutions. However, by and large, these approaches present significant limitations:

- **Inconsistency.** The manual, individual nature of white hat hacking and red team approaches can leave businesses exposed to inconsistency and unpredictability at best, and errors, oversights, and omissions at worst.
- **Minimal, limited insights.** Threat intelligence helps in understanding the attacks being executed. However, it doesn't address how and whether your organization is vulnerable to those attacks, and, if so, what the potential damage may be. Further, the output of systems like vulnerability scanners can be a lot of "noise," uncovering issues that may, or may not, actually represent real security risks. By surfacing a high volume of issues, while offering minimal insight to guide prioritization, these systems can create a huge backlog of tasks for overworked security teams.
- **High costs.** The types of experts that are needed to staff effective red teams or conduct white hat hacking are in short supply and demand high salaries.
- **Constrained frequency, scope.** Given the high cost and the difficulty of finding the right experts for exercises like red team testing, many organizations are significantly limited in the scope, frequency, and duration of these exercises. Typically, penetration tests are conducted intermittently, often annually or semi-annually, which means teams only gain point-in-time insights.

Introducing Breach and Attack Simulation from SafeBreach

SafeBreach offers advanced breach and attack simulation capabilities that give your teams an efficient, programmatic way to assess threats. As a result, the platform enables you to address your organization's threat assessment objectives, while overcoming the limitations of manual, labor-intensive activities like penetration testing and red teaming. Further, unlike other breach and attack simulation platforms, SafeBreach enables teams to run continuous attacks automatically, without the need to hire dedicated teams to manage the platform.

The SafeBreach platform safely executes real attacks in production environments to prove where security can withstand such attacks—and where it needs to be improved. The platform automates testing of an organization's security architecture, using advanced, patented technology that can execute attacks safely and continuously.

Offering a 360-degree view of your environment, the solution can simulate attacks against all your assets and domains, including endpoints, networks, security information and event management (SIEM) platforms, cloud environments, containers, email, and data loss prevention (DLP) solutions.

Key Threat Assessment Capabilities

Gain a Hacker's Perspective

With SafeBreach, you can gain a hacker's perspective of whether specific attacks can breach your organization. The solution makes it practical to track threats across the entire "kill chain." The solution visually depicts attack paths within your infrastructure, helping you assess whether an attack can infiltrate, exploit hosts, move laterally, or exfiltrate data. Gain insights to determine whether attacks can leave critical business assets exposed to theft, being held for ransom, and so on. Proactively report to executives on your risk posture and get a mitigation plan in place—before attackers exploit the gaps.

Gain Timely Threat Updates

SafeBreach solutions are supported and optimized by SafeBreach Labs, our dedicated team of researchers who continuously update the SafeBreach Hacker's Playbook with new attack scenarios and the attack methods highlighted in US-Cert alerts. New attack methods are automatically made safe and built into the playbook, which contains more than 10,000 breach methods.

In addition, the solution can be integrated with a range of threat intelligence platforms. By integrating with your threat intelligence solutions, you can push active threats into SafeBreach in real time, where threats are correlated with methods in the playbook.

In this way, a comprehensive, current set of attacks can be run across your infrastructure to expose where controls are working and where they're not. The SafeBreach platform gives you visibility into your security posture against specific threats and enables you to focus on the highest-risk attacks. Effectively understand the impact of real-world threats on your business and gain valuable insights on how to update your security controls to reduce threat impact and mitigate overall risk.

Security Control Validation

Execute Attacks Safely

Visualize Your Security Posture With Data-Driven Results

Remediate Holistically to Defend Your Enterprise

Leverage the MITRE ATT&CK® Framework

SafeBreach gives you a practical, highly flexible way to put the MITRE ATT&CK framework to work for your business. The solution enables your team to assess threat intelligence within the organized structure of ATT&CK. Quickly see the effectiveness of your security controls by safely executing thousands of attacks and automatically mapping the results to the ATT&CK framework.

SafeBreach: Key Benefits

By employing the SafeBreach platform to perform security control validation, your teams can realize a number of key benefits:

- **Reduce risk.** With SafeBreach, you can identify vulnerabilities, gaps, and errors—before cyber attackers can exploit them. SafeBreach enables you to do targeted assessments and continuous validation to ensure that new risks, whether due to new attack techniques or new vulnerabilities that have emerged in your enterprise environment, are quickly identified and addressed.
- **Strengthen security.** SafeBreach enables you to validate the efficacy of specific tools, as well as the entire security ecosystem, including the people, processes, and technologies in place. SafeBreach makes it possible to test continuously, so you can ensure configuration changes haven't introduced any exposure. Gain the objective insights needed to identify the most critical threats, and take steps to address them. Plus, after remediation, you can rerun tests to ensure controls address the gap.
- **Enhance operational efficiency.** With SafeBreach, you can assess which controls are defending your business, and which aren't. The solution can do correlation with vulnerability scans to help ensure you focus on vulnerabilities that are exploitable. The solution delivers the actionable insights teams need to assess security gaps based on potential impact, prioritize remediation work, and effectively focus efforts on securing critical assets. These insights help reduce your staff's administrative burden, while enabling them to be more productive. Also, the solution can help streamline administration and operations by enabling your team to knowledgeably identify overlapping and ineffective tools, and eliminate them.
- **Maximize the return on existing investments.** Objectively assess various tools in place and determine which are working and which aren't. In this way, your teams can make the most of your existing controls and ensure these systems are optimized to deliver the highest levels of security.
- **Intelligently evaluate new controls.** With SafeBreach, your teams can accurately test prospective solutions, so you can determine which will work best in your environment—before you make the purchase.

SafeBreach

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

Conclusion

Whatever security controls were implemented yesterday won't matter if new threats or vulnerabilities arose today. Leverage SafeBreach and get the advanced breach and attack simulation capabilities you need to stay in front of fast changing environments, vulnerabilities, and threats. Find out how SafeBreach can help your team spot gaps and address them—before they get exploited.

To learn more, visit safebreach.com