SafeBreach Security Control Validation: Minimize Risk, Maximize the Return on Your Security Investments

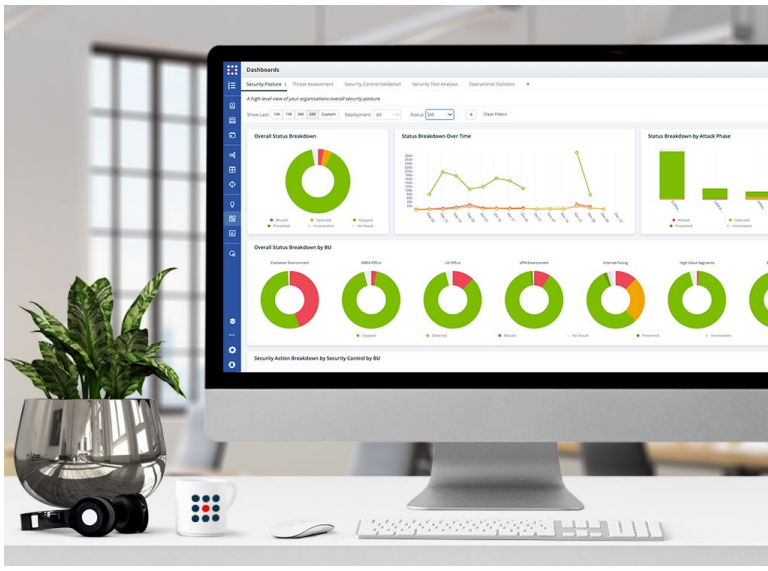
SafeBreach

Solution Brief

You may have deployed dozens of security controls, but that's not enough. You need to ensure those controls are working as intended and needed. To do so, you need to do security control validation. This brief reveals why traditional approaches are coming up short, and it shows how SafeBreach offers the advanced capabilities that enable effective, continuous security control validation.

Introducing Security Control Validation

To combat the threats posed by cyber attackers, security teams in enterprises and government agencies have continued to implement and enhance a range of controls. However, even after massive investments have been made and tools have been deployed, the job's not done. It's vital that teams validate their security controls and ensure they're providing the defenses required.



Align security investments to your business goals with SafeBreach Executive Dashboards

The Challenge:

The Limitations of Traditional Security Control Validation Approaches

Security teams can pursue a number of approaches for doing security control validation. Over the years, teams may have elected to do penetration testing, red team exercises, vulnerability scanning, and more. However, by and large, these approaches presented 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 insights.** The output of systems like vulnerability scanners can be a lot of "noise," uncovering a lot of issues that may, or may not, actually represent real security risks. By surfacing a high volume of issues, these systems can create a huge backlog of tasks for overworked security teams, while offering minimal insight to guide prioritization.
- **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, many organizations are significantly limited in the scope, frequency, and duration of their ability to do these types of tests. Typically, penetration tests are conducted intermittently, often annually or semi-annually, which means teams only gain point-in-time insights.

Introducing Security Control Validation From SafeBreach

Today, SafeBreach offers advanced breach and attack simulation capabilities that give teams an efficient, programmatic way to validate security controls. As a result, the platform enables you to address your organization's control validation 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.

Complete Coverage of the Security Ecosystem

With SafeBreach, you can assess the security of your entire security ecosystem, including the people, processes, and technologies in place. In addition, you can validate specific controls across all these areas:

- **Data loss prevention (DLP).** Make certain your DLP controls are correctly configured, so that data cannot be exfiltrated. Get the insights you need to maximize the performance of your DLP solution.
- **Email controls.** Ensure your email controls are configured correctly, so they identify all indicators of compromise (IOCs) that are known to signal the infiltration of an organization.
- **Endpoint controls.** Be certain that endpoint controls—including anti-virus, anti-malware, endpoint detection and response (EDR), and extended detection and response (XDR)—are configured correctly to prevent or detect malicious activity on your endpoints.
- **Network controls.** Make sure your network controls are configured optimally to guard against malicious activity. Do extensive validation of firewalls, next-gen firewalls, segmentation, intrusion prevention and detection systems, network behavior and traffic analysis, and more.
- **SIEM controls.** Correlate attack results to distinguish between the controls that detected or prevented attacks and those that failed. Map relevant events and rules for each attack to the appropriate compensating controls.
- **Web controls.** Determine whether your web gateways, proxies, and URL filtering controls are configured correctly to prevent or detect malicious activity.
- **Cloud & container controls.** Ensure your move to the cloud has control and data plane security controls that are configured correctly to maximize your cloud strategy.

After each validation, the SafeBreach solution generates a detailed remediation plan that helps you maximize the efficacy of your controls.

Security Control Validation

Execute Attacks Safely

Visualize Your Security Posture With Data-Driven Results

Remediate Holistically to Defend Your Enterprise

Security Control Validation: Use Cases

The SafeBreach platform can assist with a range of efforts in your enterprise. Following are just a few of the ways your organization can use this breach and attack simulation platform today:

- **Conduct authoritative, fact-based solution evaluations.** It is a challenge to evaluate and verify exactly how effectively a new tool will defend your enterprise against adversaries. With SafeBreach, you can quickly run thousands of attacks during the evaluation process to ensure you make the right investment.
- **Assess hardened system images.** After taking steps to harden a system image, you can execute attacks to quickly assess the efficacy of the changes—before rolling them into production. Assess system images on local, virtual, or cloud infrastructures, and get a detailed remediation plan.
- **Conduct realistic attack scenarios for training.** Take a mock scenario from theoretical to actual by executing attacks safely, and enabling teams to observe attacks and do incident response training.
- **Safeguard remote workforces.** Execute key attack methods to quickly identify and remediate security gaps, so you can safeguard the activities and data of your remote workforce.
- **Hold security vendors accountable.** Validate the security controls of your entire security ecosystem to identify solutions that prevent and detect attacks, and those that completely miss them. Gain the power to hold your vendors accountable, leveraging insights and objective evidence in terms of how their solutions really perform under attack.
- **Minimize endpoint tool bloat.** Too often, PCs and laptops are overloaded with too many security tools, degrading system performance, the machine's lifespan, and the user's experience. Execute attacks on each security tool to identify the optimal combination of controls, so you defend your enterprise—without weighing down your devices.

SafeBreach: Key Benefits

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

- **Reduce risk.** Identify vulnerabilities, gaps, and errors—before cyber attackers can exploit them. With SafeBreach, you can do 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.** Validate the efficacy of specific tools as well as the entire security ecosystem, including the people, processes, and technologies in place. Gain the objective insights needed to identify the most critical threats, and take steps to address them.
- **Enhance operational efficiency.** Streamline administration and operations by knowledgeably identifying overlapping and ineffective tools, and eliminating them.
- **Intelligently evaluate new controls.** Accurately test prospective solutions, so you can determine which will work best in your environment, before you make the purchase.
- **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.

SafeBreach

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

Conclusion

Enterprise security is too important to leave to guesswork, speculation, or wishful thinking. Security control validation is absolutely essential in enabling teams to ensure adequate defenses are in place—and understand what to do if not. Further, the need for security control validation is critical, but so is the need to manage these efforts constantly and cost effectively. With SafeBreach, your teams can harness advanced breach and attack simulation capabilities that provide an efficient, programmatic way to validate security controls. Now you can assess your controls and address vulnerabilities—before they're exploited.

To learn more, visit safebreach.com