SafeBreach

WHITE PAPER

How Breach and Attack Simulation Supports Continuous PCI Compliance

Increase visibility and confidence that your cardholder data environment is both compliant and protected by continuously testing your security controls against real-world attack scenarios.

SAFEBREACH.COM

Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements designed to ensure organizations who store, process, or transmit payment (credit, debit, or prepaid) cardholder data maintain, at minimum, a defined set of security policies and procedures to detect, mitigate, and prevent cyberattacks and breaches targeting cardholder data.

In this whitepaper, we provide some context on PCI and compliance requirements and discuss the difference between "compliant" and "secure." We'll also explain how to achieve "continuous compliance" with breach and attack simulation (BAS) and lay out how the SafeBreach platform can help ensure your environment is continuously both compliant and secure.

PCI Compliance Overview

PCI DSS was developed by the Payment Card Industry, a consortium of the largest payment card transaction processors. The standard is "self-regulating," meaning it is not associated with, or enforced by, any government mandates or agencies. However, any organization that stores, collects, or transmits payment card information is subject to compliance.

Merchants are subject to one of two compliance methods, depending on the volume of transactions they process. High-volume merchants (over 6 million card transactions per year) must submit a report on compliance prepared by an external qualified security assessor (QSA) or an internal security assessor (ISA). A QSA will go onsite to conduct an audit, while an ISA can be a member of your team properly trained to perform an assessment and liaise with external auditors. All other merchants are not subject to an onsite PCI audit, but must complete a Self-Assessment Questionnaire (SAQ).

All details on PCI DSS requirements and compliance procedures can be found on the PCI Standards Council website: **www.pcisecuritystandards.org**

Non-Compliance and Data Breach Penalties

Penalties for non-compliance with PCI standards are complex because several parties are involved, including the card provider, the merchant's bank or transaction processor, and the merchant themself. If a merchant is consistently non-compliant, or experiences a security event in which cardholder data is impacted and they are found to have been non-compliant with PCI DSS at the time, they can expect severe sanctions. Penalties may include being fined, having increased transaction fees applied or being suspended from accepting payment cards, providing credit monitoring services for customers whose data was compromised, and being exposed to class-action and governmental lawsuits.

Version 4.0 Compliance Deadline is Approaching

Announced in March 2022, PCI DSS Version 4.0 is a substantial update from version 3.2.1, with over 60 new or revised requirements. In response to the scope of updates in v4.0, PCI defined a phased approach to compliance, where most of the requirements must be met by March 31, 2024, while certain others can be treated as best practices until March 31, 2025, at which time full compliance is required. These 2025 requirements are called out in the "Applicability Notes" section for each requirement (see example below).

Requirements and Testing Procedures		Guidance
8.5 Multi-factor authentication (MFA systems are configured to prevent misuse		
Defined Approach Requirements ▪ The MFA systems is not susceptible to replay attacks. ▪ MFA systems cannot be bypassed by an users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. ▪ At least two different types of authentication factors are used. ▪ Success of all authentication factors is required before access is granted. **Customized Approach Objective** MFA systems are resistant to attack and strictly control any administrative overrides. **Applicability Notes** *This requirement is a best practice until March 31, 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **8.5.1.a** Examine vendor systems documentation to verify that the MFA system is not susceptible to replay attacks. **8.5.1.b** Examine system configurations for the MFA implementation to verify it is configured in accordance with all elements specified in this requirement. **8.5.1.c** Interview responsible personnel and observe processes to verify that any requests to bypass MFA are specifically documented and authorized by management on an exception basis, for a limited time period. **8.5.1.d** Observe personnel logging into system components in the CDE to verify that access is granted only after all authentication factors are successful. **8.5.1.e** Observe personnel connecting remotely from outside the entity's network to verify that access is granted only after all authentication factors are successfully.	**Purpose** Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE. **Definitions** Using one type of factor twice (for example, using two separate passwords) in not considered multi-factor authentication. **Further Information** For more information about MFA systems and features, refer to the following: *PCI SSC's Information Supplement: Multi-Factor Authentication* *PCI SSC's Frequently Asked Questions (FAQs) on this topic*

Note which of the two compliance deadlines applies when reviewing each v4.0 requirement.

Source: PCI DSS Version 4.0 Requirements and Testing Procedures

Despite the relatively long runway for full compliance, the window is closing rapidly for the first deadline. So, if your business is subject to PCI DSS, and your v4.0 compliance initiative is not already underway, it should be a major priority over the next 2–3 quarters. Use of a BAS platform can help meet or validate several of the v4.0 requirements and may accelerate your efforts to meet the deadlines. We'll discuss exactly how later in this paper.

Compliant Does Not Always Equal Secure

While compliance with regulations and standards should be a byproduct of good security practices, it doesn't always equate to actual security. While standardized security requirements provide tremendous value in driving consistent practices within an industry, it's important to remember that security regulations reflect the lowest acceptable level of security policies and protections, not what is optimal for your unique environment. Think of compliance as the floor, not the ceiling, of your security strategy.

It's also important to be mindful of risks created by the schedule on which you must prove compliance. Many regulations, including PCI DSS, require organizations to undergo an annual audit to prove compliance. However, this proof only reflects your security posture at the point in time the audit is conducted. This is the fatal flaw in focusing on compliance rather than security. How many organizations have passed a PCI audit, only to be seen in the headlines due to a major breach? Certified PCI-compliant companies continue to suffer theft of cardholder data; however, this is not always caused by a failure to put adequate security practices or controls in place. Drift from baseline policies and configurations is a fact of life in information security. Hardware upgrades, ad-hoc fixes to network, operating system, and application issues, and poor communication between teams can all create unintentional drift, which results in vulnerabilities that can lead to a breach.

The more frequently you assess your environment against your baseline, the lower the risk of significant drift, and the easier it is to realign the environment with the baseline. The focus needs to be on continuous compliance. This approach continuously validates that the security controls protecting Cardholder Data Environments (CDEs) are working as expected, enables teams to react quickly when something changes, and evolves security strategy—both compliance and security—at any given time. This is continuous compliance.

PCI Compliance Framework and Requirements

The requirements set forth by the PCI DSS are both operational and technical, and the core focus of these rules is always to protect cardholder data. PCI DSS includes 12 core requirements that fall within six domains as follows:

GOALS	REQUIREMENTS	
Build and maintain a secure network	Requirement 1:	Install and maintain a firewall configuration to protect cardholder data
	Requirement 2:	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	Requirement 3:	Protect stored cardholder data
	Requirement 4:	Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	Requirement 5:	Use and regularly update anti-virus software or programs
	Requirement 6:	Develop and maintain secure systems and applications
Implement strong access control measures	Requirement 7:	Restrict access to cardholder data by business need to know
	Requirement 8:	Assign a unique ID to each person with computer access
	Requirement 9:	Restrict physical access to cardholder data
Regularly monitor and test networks	Requirement 10:	Track and monitor all access to network resources and cardholder data
	Requirement 11:	Regularly test security systems and processes
Maintain an information security policy	Requirement 12:	Maintain a policy that addresses information security for employees and contractors

Table 1: PCI DSS Requirements

Each of the 12 requirements contains several sub-sections and defined approaches, which explain the requirements in greater detail. Not all of these apply to every entity, though, so we won't cover all of them here. Rather, we will focus on those areas where breach and attack simulation (BAS)—and, more specifically, the SafeBreach platform—can be most helpful in achieving continuous compliance.

BAS Reduces Time and Effort of Compliance

BAS platforms should be an essential part of any CISO's security portfolio to validate security assumptions about their PCI environment and ensure their cybersecurity strategy is working. BAS validates security controls by simulating sophisticated real-world attacks against your environment, testing external and insider threat vectors, lateral movement, and data exfiltration. By automatically running these simulated attacks, BAS enables an enterprise to continuously validate their security posture, identify risks, and challenge the efficacy of security controls—all without creating risk of disruption or data loss in production environments.

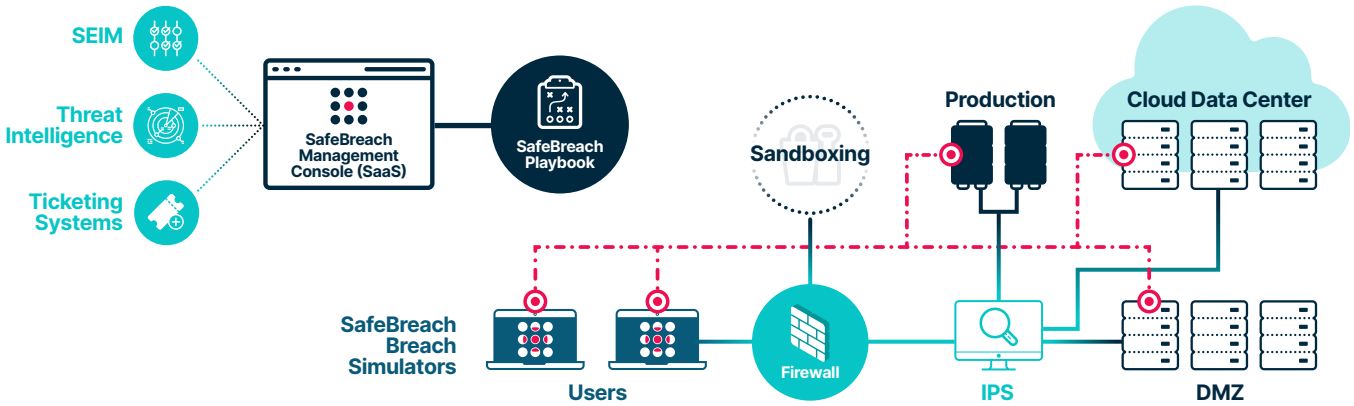
Using BAS to assist with PCI compliance offers several unique advantages:

- **Continuously validates security posture:** BAS platforms can run simulations continuously or very frequently, so security teams know at all times — not just annually or biannually — whether security measures are working properly. This enables security teams to continuously address security gaps with respect to the CDE rather than face a mountain of remediation tasks in preparation for an audit.
- **Reduces or validates the true scope of compliance:** Changes in system or network configuration — for example, a new firewall rule that permits connectivity between a system in the CDE and another system — could bring additional parts of the environment into scope for PCI DSS. Unauthorized, undocumented, or forgotten changes happen constantly and can open a gap and unknowingly bring a CDE into scope. BAS can be used to validate connectivity is not possible, thus reducing or validating the true scope of compliance.
- **Lets you understand true PCI exposure:** BAS uses a black-box approach (i.e., no prior knowledge of the environment is required) and incorporates a library of attack scenarios including brute force, exploits, malware, and remote access tools. BAS provides a more accurate real-world sense of what a hacker can do in an organization's environment, accurately predicting if the PCI environment can be breached and the exposure of data if that were to occur. Through this, an organization is better able to accurately measure their level of risk.
- **Proactively updates PCI scope:** Changes—whether new systems, new users, or organizational changes (merger and acquisition, for example)—can create security and compliance gaps. Compound this with the accelerated rate of change and you add an infinite multiplier to the creation of gaps. BAS can pinpoint new PCI requirements for the environment due to change. For example, imagine that simulators are placed in three zones in the data center—Segment A, Segment B, and Segment C. Today, credit card data may reside only in Segment A. If changes are made such that Segment B will soon gain access to credit card data, BAS analysis can provide an immediate understanding of the impact of this change, so that security teams can proactively update their PCI scope and implement appropriate security controls. Identifying these gaps and having the ability to proactively remediate them ahead of an audit saves a lot of headaches for security teams. Essentially, you have continuous validation of segmentation.
- **Validates compensating controls:** Compensating controls may be considered for most PCI DSS requirements when an organization cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints. When this occurs, the organization can mitigate the risks associated with the requirement via compensating security controls. BAS can demonstrate to PCI auditors that these compensating controls are working and are effective alternatives, or they can help organizations identify where they are needed and where they can be placed.

How SafeBreach Helps Maintain Continuous Compliance

The SafeBreach platform is well suited to address PCI requirements because of our database of over 30,000 hacker breach methods, our focus on the business impact, and our ability to integrate with existing security solutions.

As shown in the diagram below, the platform consists of the management console and the simulators that play the role of the "virtual hacker."



MANAGEMENT CONSOLE

The centralized management console incorporates SafeBreach's Hacker's Playbook of over 30,000 different attack methods and manages a distributed network of breach simulators from a centralized location. Capabilities include the ability to manage all aspects of simulator configuration, review breach methodologies that have been successful or blocked, and generate reports on breach patterns. Deployment scenarios are extremely flexible. The management server can be deployed on-premise or in an enterprise cloud infrastructure (AWS, Azure and GCP*).

SIMULATORS

The SafeBreach simulators perform the role of the attacker, simulating traffic within the cyber kill chain. Three different types of simulators are supported:

- **NETWORK SIMULATORS:** Network simulators are deployed as virtual machines on VMware servers and run a variety of network breach methods.
- **HOST SIMULATORS:** Host simulators are supported on Windows, Mac OS, and Linux operating systems and are deployed as lightweight agents on endpoint or server systems.
- **CLOUD SIMULATORS:** These are network simulators that act as infiltration and exfiltration points, located in the enterprise cloud infrastructure. Cloud simulators participate in network breach methods only.

SafeBreach simulations are based on proven models of attacker breach methods spanning exploits, malware, brute force, password harvesting, and more. This comprehensive database of breach methods is managed and updated by SafeBreach Labs, the research arm of the company. Unlike penetration testing or vulnerability assessment platforms, SafeBreach provides the full kill chain perspective of an enterprise's impact from a breach, using comprehensive breach methods instead of vulnerabilities, but doing so safely.

*Q4 2023

Specifically for PCI compliance, BAS can demonstrate attacker success with infiltration, lateral movement to the PCI environment, and finally, exfiltration of credit card data. Credit card data is self-generated by SafeBreach, and the type and format can be customized to match your parameters. No actual customer data is ever exfiltrated.

SafeBreach and the PCI V4.0 Requirements

By continuously testing, validating, and documenting that your security controls are delivering the protections defined in many of the PCI DSS 4.0 requirements and sub-sections, SafeBreach can significantly reduce your compliance and operations costs and the risks associated with interacting with payment card data. Below is a summary of the PCI DSS 4.0 requirements where SafeBreach can help.

REQUIREMENT 1
INSTALL AND MAINTAIN NETWORK SECURITY CONTROLS

Section 1.2 Network security controls (NSCs) are configured and maintained.

Section 1.3 Network access to and from the cardholder data environment is restricted.

Section 1.4 Network connections between trusted and untrusted networks are controlled.

Section 1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Unauthorized attempts to access cardholder account data may occur as the result of a malicious external party looking to steal the data, or they may be the result of an internal party attempting to access confidential data without malicious intent, but also without proper authorization. Regardless, effective network security controls are key to controlling both internal and external network traffic to and from the CDE. PCI DSS Requirements 1.2–1.5 mandate that network security controls are properly configured and maintained, only authorized network traffic is allowed to and from the CDE, the network hosting the CDE is segmented from untrusted networks, and security controls are implemented on devices that can access the CDE as well as untrusted networks (such as the Internet).

HOW SAFEBREACH CAN HELP

SafeBreach validates network security controls by simulating a wide range of attack scenarios from both inside and outside the corporate network. Specific to requirements 1.2–1.5, SafeBreach can validate the presence and effectiveness of network firewalls, segmentation schemes, and other network access controls. SafeBreach network attack scenarios simulate not only malicious attempts to infiltrate your network externally and move laterally to your CDE, but also unauthorized attempts to access the CDE from inside the network.

REQUIREMENT 2

APPLY SECURE CONFIGURATION TO ALL SYSTEM COMPONENTS

Section 2.2 System components are configured and managed securely.

PCI DSS Section 2.2 requires entities to implement and maintain secure configuration standards to ensure their system components are configured consistently and securely. Even if you have multiple layers of best-in-class security technologies in place, your protection can be seriously compromised if these controls are not properly configured. Whether because admin account credentials were not changed from the vendor default, or a control was misconfigured by an administrator (e.g., conflicting firewall rules, etc.), insecure configurations can create serious security exposure that goes unnoticed unless controls are "pressure-tested" with realistic attack scenarios. In fact, based on running millions of attack simulations in customer environments, SafeBreach found that **92% of successful attack simulations could have been blocked** by optimizing configuration settings in existing controls.

HOW SAFEBREACH CAN HELP

SafeBreach attack simulations identify which controls blocked, detected, or missed attacks, so you can pinpoint ineffective settings, underperforming tools, and incident response gaps. And through SafeBreach's integration with other security tools, such as leading security information and event management (SIEM) and security orchestration, automation and response (SOAR) platforms, security teams can quickly correlate simulated attacks with alerts and events from multiple sources to grant real-time visibility into the effectiveness of those controls. Additionally, actionable insights provided by SafeBreach can help automate the process of breach investigation and remediation, making it more effective and efficient, and enabling teams to close security gaps faster.

SafeBreach then closes the loop by re-running attacks to ensure that the updated configurations can successfully detect or prevent the attack. This continual security control validation ensures a hardened security posture that can withstand advanced attacks.

REQUIREMENT 5

PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE

Section 5.2 Malicious software (malware) is prevented or detected and addressed.

Section 5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

Section 5.4 Anti-phishing mechanisms protect users against phishing attacks.

Malware and phishing continue to be among the most common tactics used in cyberattacks, and new variants tend to evolve very quickly. As such, virtually all enterprises have already implemented some level of anti-malware and anti-phishing protection. PCI DSS requirements 5.2–5.4 define that anti-malware and anti-phishing solutions are deployed and kept up to date for all system components in scope for PCI DSS, and the personnel who access them.

HOW SAFEBREACH CAN HELP

SafeBreach can run thousands of predefined malware simulations from our Hacker's Playbook, or enable users to create custom scenarios using their own malware samples. Simulations test for detection of signature and behavioral-based malware, malware pre-

execution, and ransomware encryption. Attacks can be customized to specifically target the CDE or other critical data. Though there is no specific anti-malware efficacy requirement in PCI DSS, any organization will also want to know if their solution is doing its job. SafeBreach's real-world malware scenarios emulate the full kill-chain and document exactly where your controls detected, blocked, or missed the attack.

Additionally, SafeBreach validates security controls at the email gateway by simulating phishing attacks using an external, SafeBreach-hosted email address to send malicious payloads and URLs to a test mailbox on the corporate network. These attack simulations determine if the controls at the email gateway successfully block, quarantine, or reject these test messages.

REQUIREMENT 6
DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE

Section 6.3 Security vulnerabilities are identified and addressed.

Section 6.4 Public-facing web applications are protected against attacks.

Section 6.5 Changes to all system components are managed securely.

Cyberattacks tend to follow the path of least resistance, often exploiting known vulnerabilities to gain access to a target environment. Promptly patching known, high-risk vulnerabilities is a standard security best practice and one of the greatest "bang-for-the-buck" defensive strategies in cybersecurity. PCI DSS Requirements 6.3–6.5 requires:

- All applicable system components have appropriate software patches installed to protect against the exploitation and compromise of cardholder account data and industry-recognized sources for security vulnerability information be utilized to identify new security vulnerabilities.
- Web applications must be protected by an automated security solution configured to detect and prevent web-based attacks.
- Pre-production environments are separated from production environments, so that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

HOW SAFEBREACH CAN HELP

Through its integration with leading vulnerability management (VM) tools, the SafeBreach solution can reveal the organization's accessibility and exploitability of existing vulnerabilities. By continuously and safely executing attacks in your environment, SafeBreach calculates the risk of both network-based and host-based attacks. By combining SafeBreach insights with VM scan results, security teams can prioritize the remediation of the vulnerabilities that pose the greatest risk of accessibility and exploitation by a potential adversary.

Web applications are a favorite target of hackers, so most enterprises deploy web application firewalls (WAFs) to provide a layer of security that filters traffic and defends against malicious behavior, and yet, web applications are still the second-most used infiltration method for cyberattacks. Simply having a WAF deployed meets some of the compliance requirements for PCI DSS, but you can't know if your WAF is actually protecting your web apps without testing it against real-word attacks. SafeBreach runs multiple attack scenarios to simulate

injection attacks, cross-site scripting attacks, cryptographic failures, insecure application design, remote exploitation of web application vulnerabilities, server-side request forgery, and more.

PCI DSS requires separation of pre-production and production network environments to ensure vulnerabilities created as a result of development and testing activity aren't accidentally introduced into the "live" or production network with access to the CDE. Most enterprises maintain separate, segmented networks to minimize the risk of spillover from one environment to the another. However, firewall and network access mis-configuration can create unintended weaknesses in this security scheme. SafeBreach validates that networks are properly segmented by executing attack scenarios that include different tactics, techniques, and procedures (TTPs) to gain access, escalate privileges, and move laterally to other networks and endpoints after the initial compromise of a single system.

REQUIREMENT 8
IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

Section 8.6 Use of application and system accounts and associated authentication factors is strictly managed.

Ensuring any user, system, or application attempting to access cardholder data is authorized to do so is foundational to the purpose of PCI DSS. Requirement 8.6 focuses on the controls that must be applied specifically to system or application accounts. These are accounts, often with elevated privileges, that execute processes or perform tasks on a computer system or application. They are not typically accounts that an individual logs into, but there are some legitimate reasons an enterprise would allow certain users to do this. Attackers often target system or application accounts to gain access to cardholder data as there is no accountability and traceability of actions taken by the user logged into these accounts. Requirement 8.6.1 defines how these accounts must be managed.

HOW SAFEBREACH CAN HELP

Interactive login is the ability for a person to log into a system or application account in the same manner as a normal user account. SafeBreach attack scenarios include the ability to impersonate user accounts at different levels. This capability can be used to either demonstrate that interactive logins are blocked or, if allowed, that they are properly tracked throughout the various control mechanisms.

REQUIREMENT 10

LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA

Section 10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Similar to Requirement 2.2, which stipulates system components must be securely configured, Requirement 10.7 requires a process for detection and remediation if the component is not operating correctly; for example, if a firewall spontaneously erases all its rules or suddenly goes offline. Such system failures could indicate an undetected attack, or could simply be caused by a failure within the system component. Regardless, if the malfunction goes undetected for extended periods, it can provide attackers the time and opportunity to compromise your environment and steal account data from the CDE.

HOW SAFEBREACH CAN HELP

SafeBreach's attack simulations test multiple security controls along the entire kill-chain and provide detailed results showing which controls detected, blocked, or missed the indicators of a compromise. These insights can then be imported into an integrated SIEM to launch remedial workflows or trigger alerts for further investigation in the case of a suspected mechanical failure.

REQUIREMENT 11

REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

Section 11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

Any experienced cybersecurity or risk professional knows that safe today does not necessarily mean safe tomorrow. With the dynamic nature of both the IT environment and the threat landscape, change is constant. Regularly testing your controls to ensure your CDE and other critical data assets remain protected from unauthorized internal or external access is critical to maintaining a strong security posture.

HOW SAFEBREACH CAN HELP

Continuous validation of security systems and processes and identifying the most critical vulnerabilities based on risk is at the heart of what SafeBreach delivers. SafeBreach continuously validates how your security controls respond based on real-word threats executed in a safe and controlled manner, enabling security teams to not only meet this PCI requirement, but also to ensure best practices are being followed and the environment is actually secure.

PCI DSS's Requirement 11.4 calls for testing to be performed at least every 12 months. We understand the reason for this interval, as traditional penetration testing can be expensive and disruptive. However, we believe this interval creates too much risk of vulnerability due to new attacks and drift from standard IT configurations and policies. Because the SafeBreach platform is automated, simulations can be run as frequently as the user desires to prevent drift or test against new attack methods.

Summary

For virtually any businesses managing cardholder data, PCI DSS compliance is a significant challenge. There are many complex requirements for security controls reaching across the IT environment. The challenge is made even greater for organizations that focus their compliance thinking around external forcing functions such as an annual audit. The nature of IT environments is dynamic, and drift from baseline policies, configurations and compliance requirements is inevitable. Forward-thinking organizations treat compliance as an everyday responsibility, not an annual project.

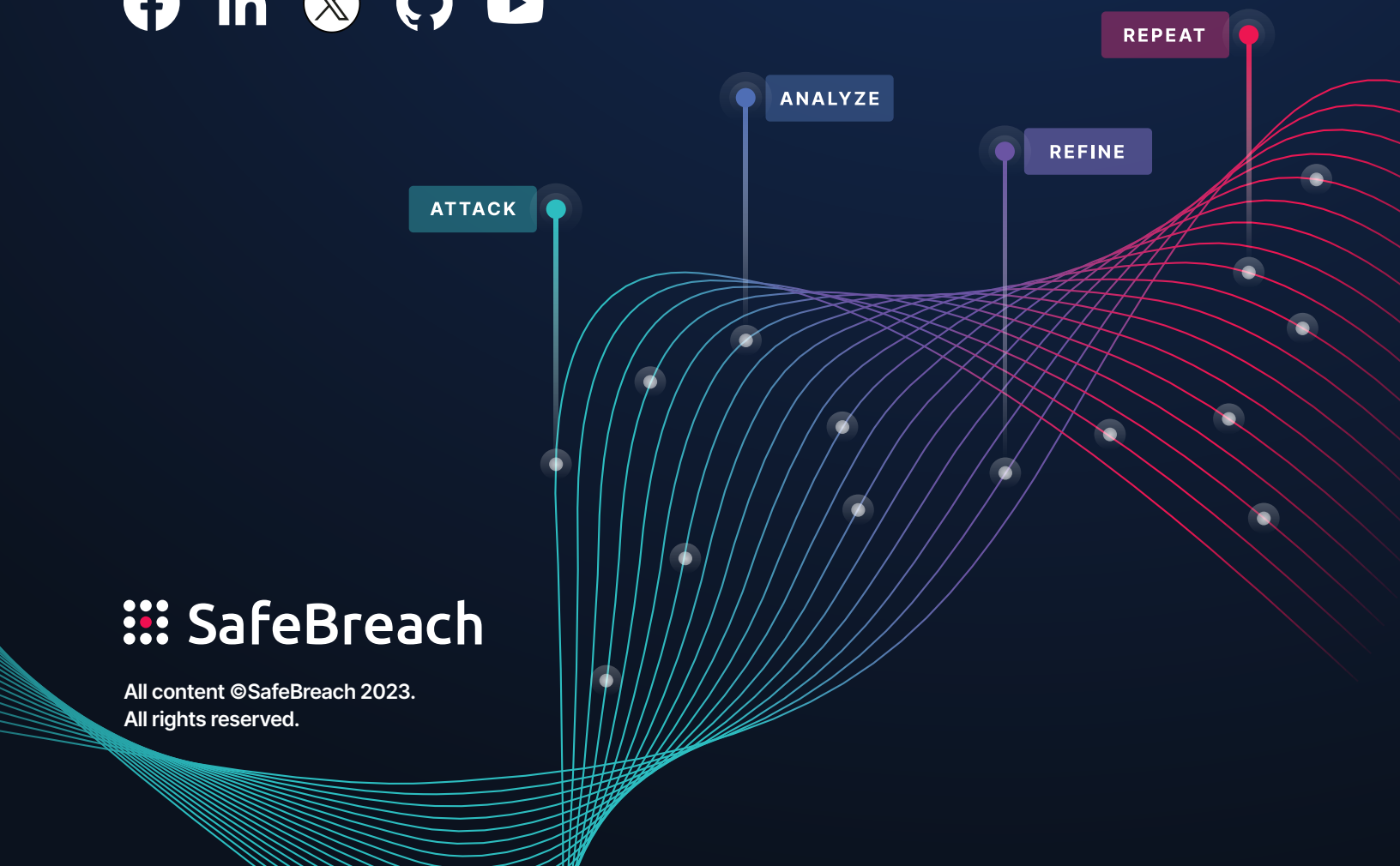
By frequently assessing your environment against your baseline, you can identify and correct drift before the problem becomes larger. This is what we call continuous compliance. But maintaining this level of diligence without an automated process would be impossible, even for businesses with mature teams, extensive policies and procedures, and the best of intentions. This is where the SafeBreach BAS platform can be transformative. By automatically running simulated attacks from our Hacker's Playbook of 30,000+ scenarios, SafeBreach enables enterprises to continuously monitor their security posture against a baseline, identify risks, and automate remediation steps.

If you'd like to learn more about the SafeBreach platform, **contact us and schedule a personalized demo**.

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at **SafeBreach.com.**



SafeBreach