SafeBreach

WHITE PAPER

The Four Pillars of Breach and Attack Simulation (BAS)

A breakdown of the continuous security validation processes and outcomes enabled by an automated BAS solution.

SAFEBREACH.COM

Contents

Introduction

2021 will be remembered as the year of the Log4 Shell. The super critical and nearly ubiquitous security vulnerability in the Apache Log4J logging system punched a massive hole in dozens of popular software packages, enabling a remote takeover of servers and systems. 2021 also saw attacks against critical systems and infrastructure accelerate and increase at an unprecedented rate, with Google's **Project Zero discovering more Zero Day exploits** than in any year previous.

50%

year-over-year increase in corporate network attacks in 2021 with an all-time peak in Q4

CHECK POINT

2022 is on pace to be another record year. In the first quarter alone, 8,051 vulnerabilities were published to the NVD database. **According to the 2022 Verizon DBIR report**, ransomware was one of the fastest growing breach types, increasing by 25% in the last year analyzed. Attackers are also leveraging the software supply chain more actively—the 2022 DBIR report found supply chain attacks and failures were responsible for 62% of system breaches.

This troubling trend of increasing numbers of breaches and attacks is compounded by the fact that the infrastructure required to mount attacks continues to become cheaper. Savvy operators are exploiting botnets or even free cloud computing accounts to scale out attacks. Given the state of high tensions between nations, state actors have occupied a growing role in creating new malicious hacking tools and propagating new forms of malware and attacks. This new reality means CISOs and their security teams are constantly having to validate security controls to remediate misconfigurations and patch or modify programs to improve security and performance.

Breach and attack simulation (BAS) solutions—designed to continuously test the effectiveness of security controls and identify potential vulnerabilities accessible to attackers—have emerged as a powerful tool to help organizations navigate this new reality. There are a number of BAS vendors on the market today, and BAS solutions are quickly becoming a key technology for CISOs looking to properly leverage existing security controls and guard against security drift. But, not all BAS platforms are created equal. In this white paper, we will discuss what BAS is, the value it provides, and common users who benefit from the technology. We'll also provide an overview of the four critical capabilities you should look for in a BAS platform to ensure it can effectively improve security posture and scale in a complex enterprise environment.

What Is BAS?

Automated BAS solutions run real-world attack simulations—based on real threat intelligence, real malware behavior, and real-world actions—against production applications and infrastructure within your environment safely and at scale. They test if systems are vulnerable to attacks by:

- Continuously validating that security controls are in place, properly configured, and working as intended
- Providing visibility into how the entire security ecosystem responds at each stage of the defense process

While often called "simulations," BAS scenarios utilize real exploits, tools, behaviors, and scripts to mimic real-world attacks that can be customized to focus on specific industries, attack methods, and actor types. BAS solutions can also be further tuned using integrations with:

- Security controls and security information and event management (SIEM) solutions to provide visibility and context around defense mechanisms and process effectiveness
- Threat intelligence and attack frameworks to operationalize threat intelligence and focus on the threats that matter most to an organization
- Workflow and SIEM solutions to streamline remediation processes and improve security posture

What Value Does BAS Provide?

BAS enables continuous security validation that **improves security operations efficiency,** enabling a faster and more effective way to reduce critical business risk. Rather than putting out fires or wasting time with manual and semi-manual control validation—like penetration testing—security teams can accomplish more with fewer resources and remain focused on new high-priority attacks and suspected vulnerabilities. By integrating with other parts of the security ecosystem, including SIEM solutions, security orchestration, automation, and response (SOAR) solutions and threat intelligence solutions, BAS can also generate a holistic view of security posture across the entire enterprise attack surface that is not otherwise available.

From a strategic perspective, this level of visibility enables stakeholders to formulate long-term security plans and inform resourcing decisions. It can also help justify security investments, secure additional budget, and ensure strategic alignment. The continuous nature of simulations also enables enterprises to progressively track, improve, and clearly communicate about their security posture over time. Taken together, BAS provides mission-critical functionality to help organizations quickly address gaps in security controls, gain unmatched visibility into how their security ecosystem is performing, and, ultimately, strengthen cyber resilience.

Who Benefits from BAS?

BAS is a platform technology with myriad users not only in security, but also IT, finance and procurement, and compliance.

Security Team

The core users of BAS have jobs that require them to interact daily or even hourly with BAS dashboards and remediation guidance.

Red Team	Use BAS to automate and streamline testing processes and allow them to focus on new ways to attack, while spending less time probing for flaws to exploit.
Blue Team	Use BAS to validate security control effectiveness, prioritize remediation requests to security engineers, and target rapid response exercises.
Security Operations	Use BAS to validate, monitor, and improve SIEM and security operations center (SOC) detection capabilities.
Threat Intelligence	Integrate their tools to automatically inform BAS administrators and security engineers on what simulations to run, using which TTPs and playbooks, and report on the organization's effectiveness against tracked threats.
Security Engineers	Use BAS to guard against security drift and to validate that security controls are protecting properly and are not misconfigured.

IT Team

Working in conjunction with the security team, IT teams are in charge of applying patches and handling hardware and endpoint protection configurations. IT teams use BAS to guide patching prioritization and to identify which employees require updates to their hardware and systems.

Finance & Procurement

Finance and procurement teams might use BAS data to create metrics measuring the value of different security control solutions and determine where money is best spent for expanding existing solutions or replacing them with better technology.

Compliance

Compliance teams can use the empirical data provided by BAS results to prove validation of security controls, which is a key component of compliance requirements for many organizations. BAS also continuously tests the entire security ecosystem, not just environments under compliance, which can help compliance teams ensure blindspots do not form from following compliance requirements alone.

How Is BAS Different from Alternative Methods?

There are a number of approaches to security control validation. However, by and large, these approaches come with limitations, requiring significant time and expense, while offering limited coverage. Below, we have provided a brief description of each method and its limitations as compared to BAS.

Penetration Testing

Penetration testing—also known as pen testing—is the process of evaluating the security of an environment by attempting to exploit weaknesses that may exist. This form of testing is inherently dependent on successful infiltration, meaning it will only continue to the next stages of an attack (e.g., lateral movement inside your network or attempted data exfiltration) if infiltration is successful. Pen testing is also reliant upon the relative skills and expertise of the people conducting the efforts. This means the scope, quality, efficacy, and results of pen testing can vary substantially, making it difficult to compare the results of different tests and track progress. Further, the manual nature of these tests means they can be costly, unscalable, time-consuming, and error-prone. Due to the high cost, these assessments can typically only be conducted annually or semi-annually and, as such, only provide point-in-time insights.

Red Teaming

Red teams work together to simulate a team of cyberattackers. These teams take an offensive approach, seeking to pursue vulnerabilities and conduct attacks. Typically, the types of experts needed to staff effective red teams are in short supply and demand high salaries, making the prospect of building a new red team costly and daunting. Also, due to the nature of red teaming, it can be difficult to scale out attacks or run multiple scenarios.

Attack Path Management

Attack path management is the process of validating external attack surfaces to understand how an attacker might leverage assets to gain access into your network—this generally includes solutions like attack surface management (ASM) and VM. Unlike pen testing, these forms of testing do focus on infiltration and lateral movement inside your network; however, they do not execute actual attacks. Instead, they run heuristics to deduce possible attack paths and do not, as a result, trigger controls or enable the evaluation of control efficacy. They also typically lack context about the likelihood of a vulnerability being exploited or the risks associated with an identified exposure. Consequently, the output of these systems can create a lot of "noise," while offering minimal insight to guide prioritization or consideration of overall business risk.

Four Critical Pillars of a BAS Platform

BAS solutions require several critical capabilities to effectively improve security posture and scale in a complex enterprise environment. The following section explains what these four important capabilities are and how they contribute to the best security outcomes that reduce business risk for an organization.

Four Pillars of BAS

Attack:

Generate highly realistic attack simulations that are indistinguishable from actual attacks

Analyze:

Provide real-time analysis of security control performance

Remediate:

Accelerate and focus remediation efforts to continuously reduce risk

Report:

Communicate results clearly with stakeholders via dashboards and automated findings

Attack: A Versatile, Fast Platform to Simulate Attacks

The primary role of a BAS platform is to simulate advanced attacks to help an organization continuously test the efficacy of existing security controls. These attacks provide instant feedback on an organization's level of preparedness against known and new threats. By providing these insights, a BAS solution can enhance the efficacy and breadth of security coverage and remediation activities. A modern and effective BAS solution must have the following attack capabilities.

Coverage of Major Attack Surfaces

A complete BAS platform must cover the major attack surfaces, including network, endpoint, cloud, applications, and email. For example, it will test all major operating systems run on-premises, on local and distributed machines, and in the cloud. The BAS platform should cover all security controls, as they are often subject to inadvertent misconfigurations or drift as part of normal IT processes—like patching and updating—that can make them vulnerable to attackers.

As organizations move to the cloud, it is imperative that a BAS solution simulates attacks against public and private cloud infrastructure (IaaS), addressing the control plane that includes identity and access management (IAM), network, storage, and administrator access. It is also crucial to move up the cloud technology stack and address the data plane, covering lateral movement, system abuse, privilege escalation, and running unapproved processes. With many attacks now focusing on container-based applications, a BAS platform should also have attacks geared specifically toward Docker containers and public cloud environments where containers are prevalent.

Coverage of New Threats with Guaranteed Service-Level Agreement (SLA)

The volatile and ever-changing nature of the threat landscape means a BAS platform must have a documented process in place to quickly add coverage for newly identified threats. When a new threat is identified and announced via a US-CERT alert, a security team must be able to quickly understand the threat, test against it, and identify what security gaps exist that may make an organization more vulnerable.

In these situations, timing is critical, so the SLA and response-time guarantees of a BAS vendor with regard to covering known threats is important. A BAS vendor should be able to ship a comprehensive set of simulations covering any new US-CERT threats within a day or two, so an organization can immediately validate its defenses against the threat. BAS platforms that take a week or more to add simulations against new US-CERT warnings should be viewed with caution; during that period of time, hackers can capitalize on newly released warnings to compromise an organization's infrastructure and wreak significant business impact.

Exhaustive Coverage of Known Threats

A BAS platform must have a comprehensive playbook to draw from that contains the attack tactics, techniques, and procedures (TTPs) for all advanced persistent threats (APTs), including but not limited to the TTPs of the MITRE ATT&CK framework. Having thousands of attack scenarios readily available to test across the enterprise frees up testing time for security teams and ensures red teams no longer have to build out every attack. But it is important to ensure the BAS platform does not require complex configurations in order to run attack simulations properly in the network, as this could burden security teams and slow down reporting.

99%

of attacks are the result of known security vulnerabilities

Easily Customizable to Accommodate Specific Threats or Create Hybrid Playbooks

For efficiency and better interpretation of results, the BAS platform should emphasize and give testing priority to attack methods most relevant and potentially damaging within today's infrastructure. It should also provide the flexibility to allow security teams to focus on specific TTPs and threat groups that are a high priority for an organization. For example, a security team should be able to run all TTPs associated with a specific threat group across all simulators in the enterprise to quickly answer inquiries from the executive suite or board members about the level of protection against specific threats.

While existing information about attack methods and vulnerabilities can help ensure protection against known threats, it can also be used to make educated predictions and simulations against future threats. Toward this end, a BAS platform should enable security teams to:

- Leverage the building blocks of known attacks within the platform to develop new attack combinations that may be relevant to an organization
- Build or upload its own attacks to the platform to better anticipate novel TTPs and attack progressions
- Add new attacks to the platform leveraging network recording packet capture (PCAP) or programming languages like Python
- Integrate with preferred threat intelligence providers—and other attack information sources like Securityfocus, GitHub, and Reddit—to update and inform personalized attack playbooks

This extensibility allows security teams—and red teams specifically—to quickly develop attacks, increase their testing coverage, and better scale their exercises. It also allows them to better address organization-specific risks that may not be covered in the various frameworks and to innovate around identifying new and undiscovered risks.

Enables High-Speed Simulations

A continuous simulation process is only as good as the speed at which it can execute. This is particularly important in a modern technology environment, where new code may be shipping multiple times per day and virtual infrastructure may deploy and shut down every few minutes. For a BAS tool to be effective, it must execute quickly with minimal load on compute and network resources. Rapid execution enables faster iteration on security stance, constant control validation, and up-to-the-hour detection and remediation of security gaps that may be created by security drift, patching failures, or control misconfiguration. BAS should be able to run continuously, multiple times per day to keep pace with modern infrastructure deployment and software update practices.

ATTACK CHECKLIST

- ☐ Coverage of all major types of attack surfaces, including device or asset type (e.g., hardware, software, software-as-a-service [SaaS]) and function (e.g., application, networking, cloud workload)
- ☐ Guaranteed SLAs for rapid coverage of new threats
- ☐ Exhaustive coverage of the largest possible number and type of proven TTPs and attack playbooks to ensure coverage of both major attacks and edge cases
- ☐ Customizable BAS attack simulations that enable security teams to design attacks specific to their needs
- ☐ The ability to run simulations quickly and continuously to provide comprehensive coverage, rather than snapshots of security posture

Analyze: The Ability to Turn Attack Results into Intelligence

A BAS platform provides insight into security posture by aggregating and visualizing security-control performance data an organization can use to analyze what their attack surface looks like, which network segments are most vulnerable, which threat groups present the highest risk, and what mitigation options will be most effective. Below are key analysis capabilities a BAS platform should have to enable this value.

Visualization of Real-Time Performance

A modern enterprise technology ecosystem is incredibly complicated, spanning thousands of endpoints, infrastructure elements, software applications, and connected Internet of Things (IoT) devices. Network topologies are also convoluted—a reality that has only increased with the rise of remote work. To quickly and effectively analyze security-control performance based on attack-simulation results, real-time visualization and dashboards are required and should:

- **Aggregate effectiveness of security controls:** Report what control failures were detected, which types of attacks were missed, which types of attacks were blocked, and other data to quickly identify areas for emphasis. This reporting can be pre-configured or can be anomaly based.
- **Visually interpret simulation data:** Provide visual tools for analysis of specific simulation exercises to drive easier comprehension of real-time security risk. This may include charts, maps and heat maps, scatter plots, and more. Visual tools allow stakeholders to easily zoom in and out on specific findings and data points. Visual tools enable more rapid digestion and comprehension of information, leading to smarter prioritization and faster mean time to repair (MTTR).

Incorporates MITRE ATT&CK Heat Map & Other Sources

This builds on the previous point but is a more specific requirement mapping to MITRE, which has become the industry standard for threat analysis. The MITRE knowledge base of adversarial tactics, techniques, and common knowledge (ATT&CK) provides a framework that organizes and categorizes thousands of threats into a "landscape map" security teams can use to apply their resources on a more informed basis. A BAS platform should readily enable simulation results to be incorporated into the MITRE ATT&CK framework to develop heat-map exposures that can:

- Produce a threat intelligence-based view of an organization's security posture against all tested attacks
- Provide highly visual guidance about areas of exposure that security teams can use to select tests that drill down into specific attack techniques for a detailed view of what simulations were prevented or detected
- Help security teams understand and pursue shared remediation goals

While incorporating results into the MITRE ATT&CK framework is valuable, it's important to note that it is not sufficient. The framework itself is not exhaustive, further underscoring the importance of leveraging a BAS platform with a comprehensive playbook that contains the attack TTPs for all APTs.

SafeBreach curates and maintains the Hacker's Playbook, the largest collection of TTPs and attack data based on real-world activities culled from MITRE, NVD, and many other data sources. SafeBreach is the only BAS vendor that actively contributes new techniques to the MITRE ATT&CK knowledgebase and framework. SafeBreach Labs has contributed four new techniques to the framework. Commitment to original research is a fundamental requirement for a BAS provider to drive the platform's capabilities ahead of fast evolving security threats.

Maps Attack Paths

All attacks are made up of a sequence of logical steps. More sophisticated attacks may incorporate decision trees and attempts against multiple entry points to optimize attack behavior. Organizations that gain a detailed understanding of how attacks may reach an asset from the outside can then control choke points to prevent lateral movement or data exfiltration.

A BAS platform should provide a rich ability to map and visualize potential attack paths across the entire kill chain to help security teams accurately assess the organization's attack surface. This mapping capability generally covers the entire attack life cycle, from first penetration or compromise through lateral movements and later data exfiltration or system compromise.

By mapping the steps of an attack, from initial infiltration modalities, host compromises, lateral movements, and propagation to exfiltration, sequestration (ransomware), or destruction (wiping attacks), security teams can identify how to break the chain most efficiently. Visualization is even more effective if a team can zoom into or out of different parts of the infrastructure or filter results based on key attributes.

Attack path mapping and visualization also helps with prioritization by enabling teams to see and analyze the kill chains of the highest-threat security risks identified by the BAS platform. For example, visualization can help:

- Identify whether there is a path from the external attacker to the target segment for infiltration or exfiltration
- Determine how exposed the target segment is from other segments
- Discover bottleneck segments or connections that allow many attack paths

Risk Scoring & Gap Prioritization

A BAS solution should bring together critical data to help an organization understand its overall security posture. BAS can also bring together different security teams by applying a risk-rating approach driven by comprehensive data. To make this capability broadly useful, it will include particular consumer-grade features, such as:

- A variety of visual tools including heat maps, lists, scatter plots, and pie charts to quickly communicate risk data
- Top risks and action items customized by stakeholders
- A query engine to enable rapid report and dashboard creation based on risk scores or type of security gap
- A clear way to communicate prioritization of remediations and team focus

ANALYZE CHECKLIST

- ☐ Visual tools to analyze findings and comprehend trends faster
- ☐ Sufficient data points, such as MITRE ATT&CK and other threat intelligence information, to provide a comprehensive picture of the threat landscape
- ☐ The ability to map attack paths through IT and application environments to enable analysts to track and analyze the entire attack life cycle
- ☐ Risk scoring and gap prioritization rules that interpret BAS data and other integrated data to clearly indicate which suggested fixes are the most critical

Remediate: Guidance to Help Teams Address the Biggest Risks

A BAS platform will continually run hundreds of thousands of breach methods and automatically prioritize remediation targets based on business risks and priorities. BAS will also provide specific remediation guidance mapped to attacks. Advanced BAS solutions, however, go beyond simply supplying remediation next to each security flaw finding.

Provide Remediation Guidance by Severity

A well-designed BAS platform will aggregate results from all simulations and rank them by severity or potential impact to the organization. This improves operational efficiency by focusing team efforts on the security gaps that pose the greatest risk. The BAS solution should group threats by clear categories, such as network, web, endpoint, and email, and by vendor and operating system. This makes it more feasible to coordinate efforts of security, IT, network, endpoint, and risk teams in ongoing but holistic and targeted remediation efforts. Key elements of this effort include:

- Building a set of prioritization rules to guide BAS remediation hierarchies and heuristics
- Creating a unified workspace or dashboard where each team can focus on the highest priority remediations in their area of responsibility (e.g., netsec, appsec, opsec)
- Running BAS shortly after remediations are applied to verify that the BAS solution's remediation guidance was effective

SafeBreach integrates with dozens of security solutions out-of-the-box and provides an API to allow security teams to move data into and out of the SafeBreach environment. This makes it easy to improve the user experience and aggregate information customized to each stakeholder's needs.

Automated Workflows & Remediation Processes

BAS should have tight workflow integrations with SOAR, SIEM, and ticketing solutions for automated breach remediation. Integrations with workflow systems can be used to trigger processes for additional information gathering, configuration changes, and analyst approvals required to direct mitigation and remediation of issues. Over time, these bi-directional workflow integrations improve the security posture and reduce the risk of a breach by improving the ability of the security team to quickly and effectively mitigate issues discovered by BAS.

REMEDIATION CHECKLIST

- ☐ The ability to integrate business criticality data into BAS security gap findings to better prioritize remediation guidance
- ☐ The ability to automate remediation processes and workflows leveraging the BAS API to improve efficiency

Report: Communicating Findings & Metrics

For BAS to be effective beyond the core security audience, it must clearly communicate findings and impacts. To do this, a BAS solution must make it simple to create a wide variety of report types and structures with charts, tables, and graphs. BAS should also enable admins to create automated reports that fire off either when triggered or with weekly or monthly data. Advanced BAS must not only have strong reporting and dashboarding inside the product but also make it simple to export findings and data to other security solutions—hence, the need for a flexible API and out-of-the-box integrations with leading security solutions.

Reporting BAS Basics

Because BAS can act as a "before-and-after" viewpoint for control changes and other remediations, it is a natural provider of metrics on security control improvement initiatives. BAS should also be flexible enough to serve, if needed, as a key reporting and metrics tool for security teams to monitor and evaluate security-control management and responses to BAS findings. To fulfill all of the above, BAS must:

- Convey a clear picture of the organization's security posture with dashboards, charts, and reports
- Allow for configurable views tailored to specific stakeholders
- Communicate real security posture trends and trackable metrics
- Detail the security posture against specific threat groups, threat types, and playbooks or TTPs
- Support requests for changes in security control configuration, budget allocations, or resource shifts
- Track progress (or lack of progress) over time to build accountability

Key Risk Indicators

Risk indicators help to track your organization's progress, validate that your security posture is indeed improving, and understand trends over time. Communicating the status of key risk indicators is an essential value of BAS. The types of risk indicators tracked should reflect what your organization cares about most. For example, overall attack surface is measured as the percentage of attack attempts which pass through defenses.

Another indicator might be the success rate of defense against attacks, measured as the percentage of MITRE framework attacks that are blocked. An organization may want to calculate risks against its critical segments, or elevate the risk value of services that involve financial transactions or store financial data and PII. BAS should make it easy to select, calibrate, and then measure against these indicators. Additionally, BAS should be able to calculate the exposure time from discovery of a breach until it is resolved, as well as the success rate of remediation, in order to track:

- The efficiency and responsiveness of a security team
- The effectiveness of improving security posture
- Trends over time of reductions (or increases) in critical security gaps or attacks blocked as a percentage

Integrate Communications Where Appropriate

Because not everyone consuming BAS data will have a BAS seat or even understand how the tool works, it's important to design communications to fit into the workflows of the stakeholders.

- For IT teams and those in charge of patch management, BAS communications should populate help desk tickets
- For blue teams and security operations, BAS data should be automatically pushed into their primary workspaces (e.g., SIEM or SOAR)
- For red teams, BAS data may be added to customized dashboards or consoles that incorporate their chosen penetration and analytical tooling
- For non-technical stakeholders, BAS reports can populate common dashboarding programs like Tableau or Looker, or be sent out as emails or links to BAS dashboards

REPORTING CHECKLIST

- ☐ Create a grid of stakeholders and communications they should receive
- ☐ Discuss and define your key risk metrics to shape communications
- ☐ Make sure you utilize charts and graphs to convey large volumes of data in digestible formats
- ☐ Enable stakeholders to create reports that serve their needs
- ☐ Design communications to integrate into existing workflows and tooling rather than forcing everyone to log into the BAS solution

Beyond Functionality: Enterprise Readiness Capabilities

Over the past several years, many organizations focused on purchasing numerous security solutions to defend against cyberattacks. These include network tools, endpoint solutions, secure gateways, data-loss prevention, SIEM, and SOAR. Most security teams suffer from "tool sprawl," which has added significant complexity to their jobs. Ironically, tool sprawl has actually made it harder to maintain security due to the complexity of deploying, configuring, and managing the 70 to 100 security controls most organizations have in place on average. Any security tool can be useless if misconfigured or not properly integrated into other systems. Thus, any new solution should reduce complexity, not increase it, in order to be accepted and leveraged properly. BAS solutions should excel in the following readiness capabilities:

Ease of Use

A BAS platform should be easy to use, with minimal training and tuning time required. Its user interface should be intuitive enough that security teams and other users can self-educate quickly. Secondarily, an effective BAS solution should fit without friction into existing workflows and not require significant professional services to be effectively integrated and work properly.

Speed & Flexibility of Deployment Options

A BAS solution should be accessible as both a SaaS and an on-premises system. At present, most regulated environments (e.g., financial services, health care, government) require on-premise deployment or deployment as an instance inside a private cloud. Additionally, an enterprise-ready BAS platform must be able to deploy simulators of various operating systems, including Windows, Linux, and MacOS. The BAS platform must also be deployable in major cloud environments, including Amazon Web Services, Microsoft Azure, Google Compute Platform, and others. This necessarily means easy deployment on containerized environments. In reality, most large organizations now have a hybrid infrastructure that spans hosted infrastructure, private cloud, and public clouds. A BAS solution must accommodate these evolving hybrid architectures.

Gauging Ease & Speed of Deployment

When asking about the standard timeline for deployment, confirm that estimates include testing and tuning time required to make the BAS platform production ready. Ascertain how much customization is required for configurations, dashboards, and report templates—and whether these are DIY or require administrator assistance. For attack simulator configurations, ask to see the specific steps required to set up attacks that cover your network and endpoints. If this is complicated and requires many steps, then the BAS tool will require significant deployment time and may contain significant hidden complexity. Find out how much training is required for your team to become proficient on the platform. Excessive rollout time only delays improvements to security posture and ROI.

Intelligent Scale Up

To scale intelligently and easily, a BAS platform needs to determine which types of attacks to run, where to run them in the infrastructure, and in what sequences or rotations. For example, a BAS platform should run Windows attacks only on Windows machines, MacOS attacks only on Macs, Linux attacks only on Linux servers, and Windows Servers attacks only on Windows Servers. Similarly, the BAS platform should recognize the context of IT assets and, for example, run data exfiltration exploits only against databases and other parts of the data infrastructure. This intelligence is crucial for BAS to scale easily without stressing the operations team or becoming a resource hog. If scaling requires extensive manual tuning, this introduces human bias and errors, potentially generating security blindspots and, ironically, misconfigurations of security controls. In addition, BAS needs to be able to test attack playbooks across the entire kill chain and life cycle of attacks to spot enhanced security remediation opportunities. This is true even if the attack was blocked higher up in the chain by a control or other remediation measure.

Support for Granular Role-Based Access

Because BAS can and should assist multiple teams within an organization—from executives to blue and red teams—BAS platforms must support role-based assignments. Executives can view reports and dashboards, while blue teams can configure and execute the various simulations, and red teams can create new and custom breach methods. Supporting granular, role-based access is essential for sharing the right information and capabilities in the right way with the right stakeholders.

Conclusion: The Right BAS Makes a Big Difference

A BAS solution that lacks critical capabilities and integrations can cause lack of clarity, consume valuable staff time and other resources, and even hamper production services. On the other hand, a full-featured, well-integrated BAS platform significantly improves security posture through better analysis of the attack surface and remediation. Such a solution can pay for itself in a matter of months by enabling information security teams to be more effective, without adding more people and purchasing more security tools.

Applying the right framework to the BAS selection process can simplify the decision and cut through marketing speak. In this paper, we identified the four key pillars of that framework—along with the critical capabilities associated with each—that CISOs and their teams can use to select a BAS solution that can serve as a critical component in their security posture improvement efforts.

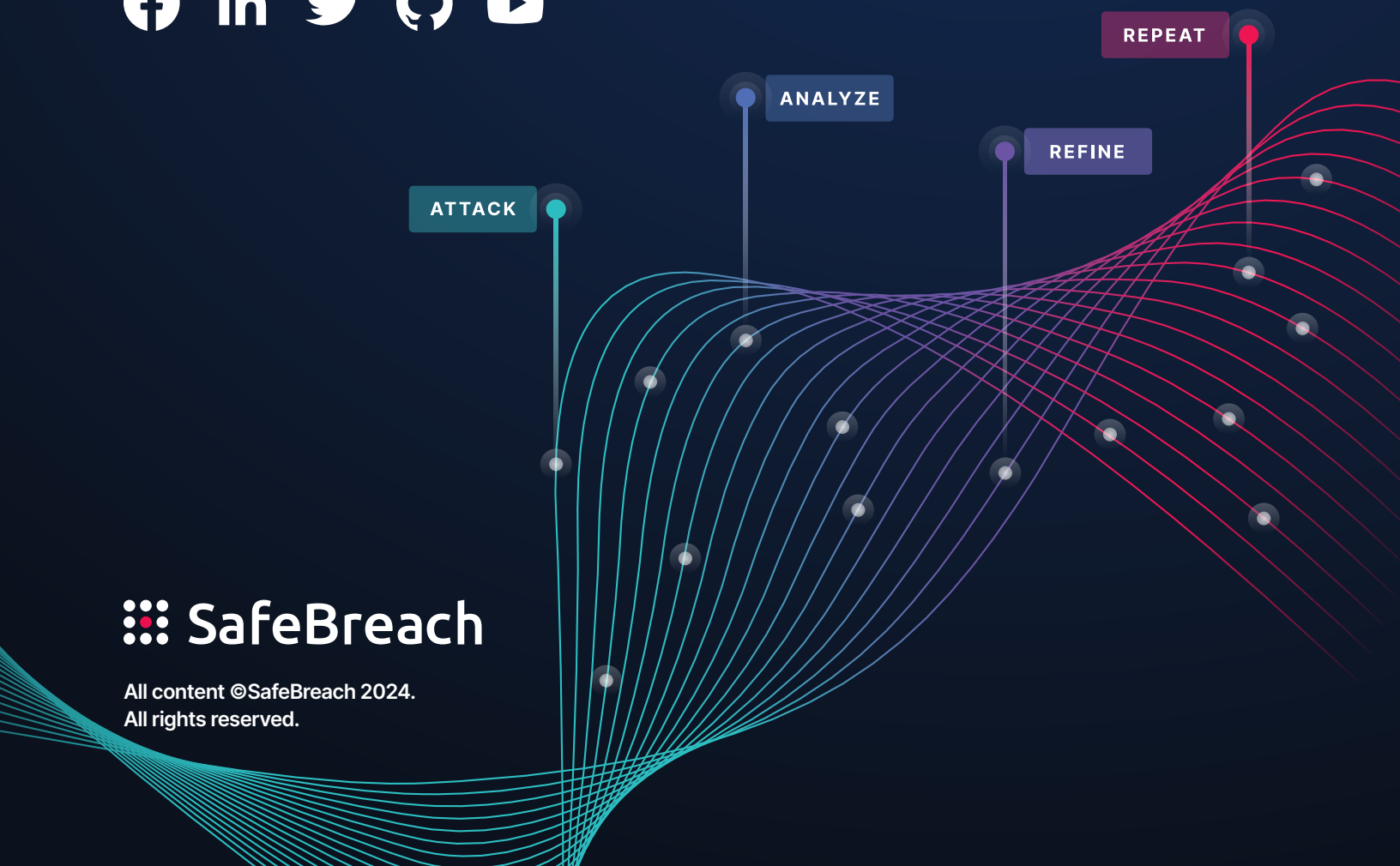
Want to learn more about why leading organizations—like PayPal, Netflix, Experian, and Johnson & Johnson—use the SafeBreach BAS platform to support their continuous security validation programs? **Connect** with a SafeBreach cybersecurity expert or **request a demo** of the platform today.

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