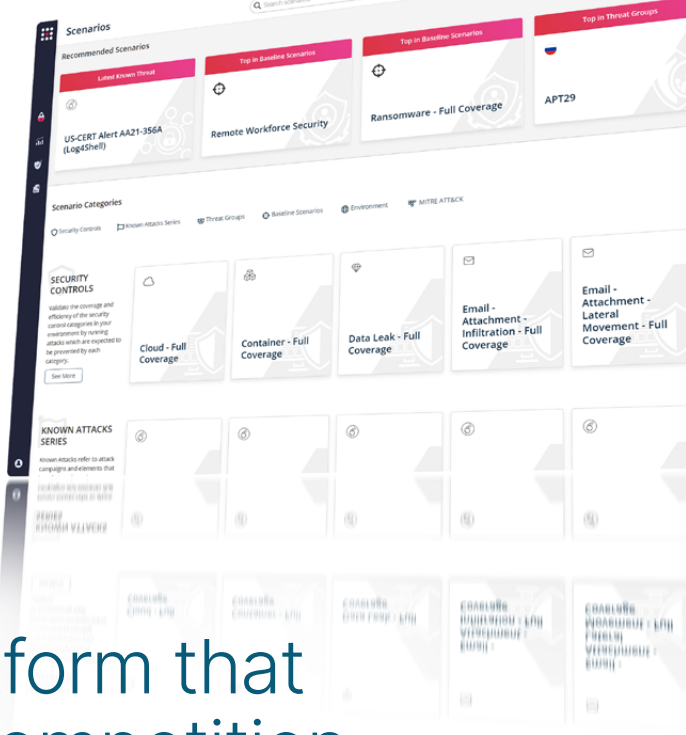
SafeBreach

WHITE PAPER

Why Enterprises Switch to SafeBreach

Learn why more enterprise security leaders are choosing the SafeBreach breach and attack simulation (BAS) platform to enhance the quality, efficacy, and value of their security programs.

SAFEBREACH.COM



An enterprise-ready platform that stands out against the competition.

As the pioneer in breach and attack simulation (BAS), SafeBreach launched the industry's first continuous security validation platform in 2014. As security professionals themselves, our co-founders were frustrated by the realization they could spend a fortune on security controls, yet still be unable to confidently validate their security investments against specific threats. The SafeBreach BAS platform was born, and early adopters found it provided previously unattainable insight into the true efficacy of their security controls with rapid time-to-value.

Since then, the SafeBreach platform has continued to evolve, with the continuous addition of new features, functionality, and content. As demand for security control validation has expanded, several competitors have entered the market with their own BAS platforms. While we believe competition drives innovation and customer focus, it has also created confusion and frustration among enterprises seeking BAS capabilities. And it's no wonder; the marketing messages from competitive platforms often make bold claims, while the actual product experience offers something different.

This sentiment has been echoed in dozens of conversations we've had with enterprise security leaders who have voiced their frustrations about the shortcomings of their previous BAS offering. This paper highlights some of the points we hear most often in these conversations, including the reasons many companies are switching to SafeBreach. The purpose isn't to call out any specific competitors—we won't be doing that anywhere in this paper—but rather to encourage enterprises to evaluate whether their BAS platform is fully delivering the capabilities they expect and to highlight specific areas where SafeBreach provides a more comprehensive BAS program.

Timely access to new attack content for emerging threats reduces critical risk.

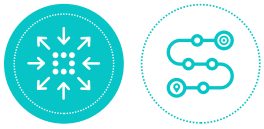
With the rate of change in the threat landscape, enterprises are most keenly interested in validating their controls against the newest emerging threats. Yet, we regularly hear from security leaders that one of the primary drivers for replacing their incumbent BAS platform is that it often takes weeks—or even months—for their vendor to make a new threat available for use in attack simulations. This latency not only increases the risk of falling victim to an emerging threat, but also makes it much more difficult for security leaders to understand whether they are protected in the critical early days after a new attack.

> **"A great value to us is that SafeBreach immediately updates the Hacker's Playbook with new attacks based on the US-Cert alerts. In the case of attacks used against SolarWinds, this was exceptionally helpful to quickly test our controls, processes, and our teams. To be able to report to the board that we launched attack simulations and the team was able to quickly discover the attack provided them with additional assurance that our team is alert and has the capability to detect and respond fast—something we didn't have with our previous BAS tool."**
>
> **CISO**
> Top 10 US Insurance Company

Certainly, most BAS platforms provide the ability for users to create their own custom attack scenarios. But this functionality is best reserved for modeling novel or specialized attacks based on unique requirements in your environment, not keeping your BAS platform current with publicly known emerging threats. After all, you expect your endpoint detection and response (EDR) vendor to issue prompt updates for emerging threats, why should BAS be any different?

Ensuring the content within a BAS platform accurately reflects the changing threat landscape requires an ongoing commitment from the vendor to maintain the advanced threat research capabilities necessary and the operational capacity to deliver consistently; yet, the number of BAS vendors who do this is surprisingly small. SafeBreach is one of the few BAS vendors to maintain a ***dedicated*** threat research team, and ***the only BAS vendor*** to maintain a 24-hour service-level agreement (SLA) to add new attacks based on **critical US-CERT and FBI Flash alerts**. In addition, SafeBreach publishes **Original Attacks** to the Hacker's Playbook to enable customers to future-proof their protection. Original Attacks are novel attack methods discovered by SafeBreach threat researchers that have not yet been seen in the wild.

> **"We switched to SafeBreach as their playbook encapsulates all the major cybersecurity threats. SafeBreach simulates infiltration, lateral movement, and exfiltration methods. The clarity and lack of ambiguity the solution delivers is brilliant. Yes, many security vendors have a research team, but SafeBreach is the only BAS vendor who develops original content based on the team's findings, allowing us to test against novel attacks."**
>
> **CISO**
> Clinical Research Company



Strong integrations provide key line of sight to security controls.

In our conversations with security leaders, we are often asked about our technology partnerships and how the SafeBreach platform can integrate with their key security and workflow technologies. Their questions are usually driven by specific challenges they have experienced with their incumbent BAS platform, including:

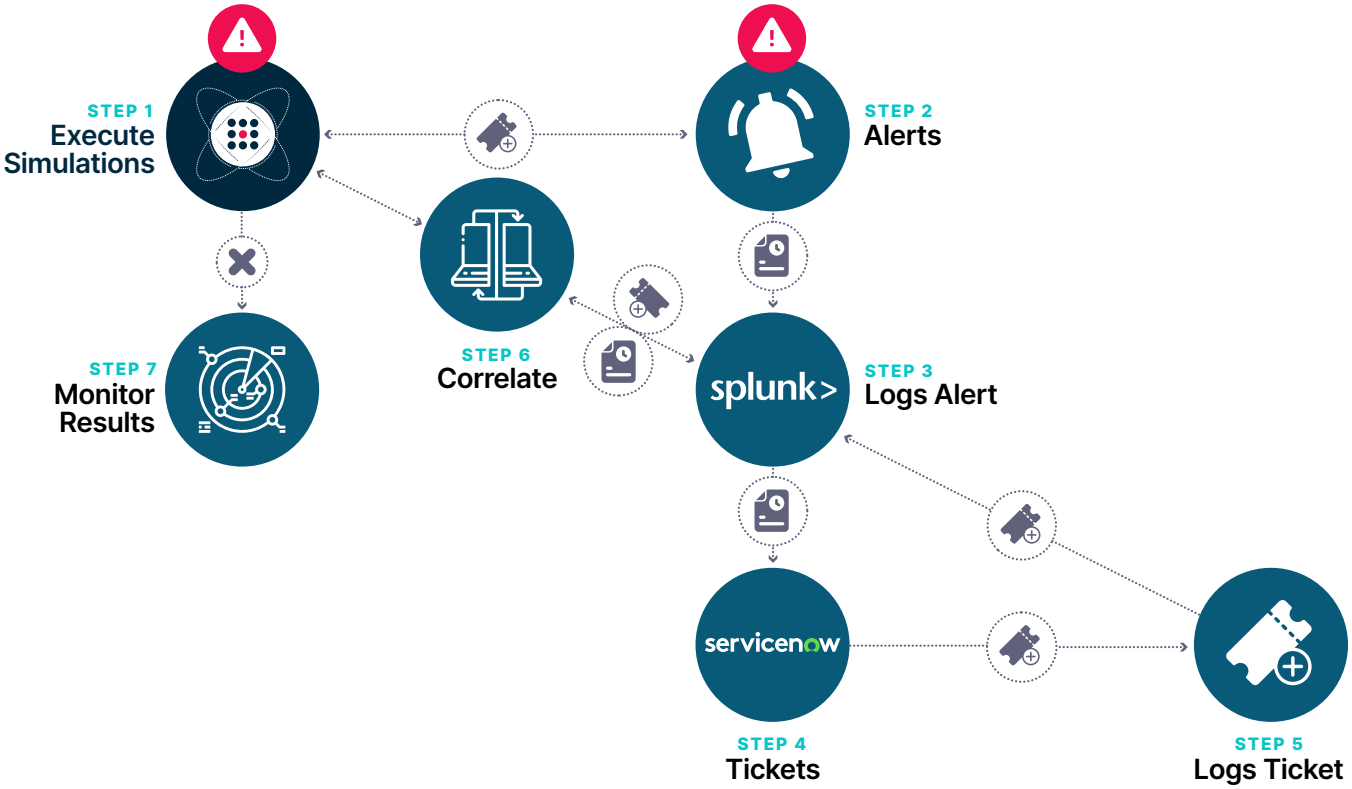
- Lack of a native integration for certain key security controls
- Integration functionality that is limited or difficult to customize
- Integrations that place too much additional load on security controls
- The inability to simultaneously integrate with more than one vendor in a control category or with multiple tenants of the same control

A BAS platform's ability to analyze the result of attack simulations and validate security controls requires integration with a variety of technologies for preventing, detecting, and responding to threats within the user's environment. A BAS solution should include a broad collection of core integrations with:

- Endpoint, network, and cloud-level controls and security information and event management (SIEM) solutions to provide visibility and context around defense mechanisms and process effectiveness
- Threat intelligence sources and attack frameworks such as MITRE ATT&CK® to operationalize threat intelligence and focus on the threats that matter most to an organization
- Vulnerability management solutions to help prioritize remediation activities
- Workflow and security orchestration, automation and response (SOAR) solutions to streamline remediation processes and improve security posture

SafeBreach has a robust partner ecosystem that includes industry-leading solution providers in critical categories, and the platform includes connectors for dozens of these third-party providers. Our dedicated integrations team is continuously adding new integrations each month, and the platform also provides the ability to create custom connectors to integrate with proprietary applications and data feeds. Connectors work out-of-the box but can also be customized and "tuned" to meet the user's unique needs. For example, to reduce the load on their Splunk instance, many users customize when SafeBreach queries the SIEM.

The SafeBreach platform can also simultaneously integrate with multiple vendor platforms within a control category—for example, multiple EDR or firewall platforms running simultaneously—or multiple tenants of the same platform—for example, multiple CrowdStrike licenses spread across different business units.



A global financial services institution that recently switched to SafeBreach leveraged our out-of-the-box integrations for both their ServiceNow ticketing system and Splunk SIEM. This allowed them to establish a closed loop, where simulated attacks automatically trigger notifications that traverse the typical alert pipeline to reach the appropriate incident responders, just as they would in a real-world scenario. As a result, the customer was able to discover and correct several issues that were impacting their ability to respond to threats quickly. See the detailed case study to learn more.

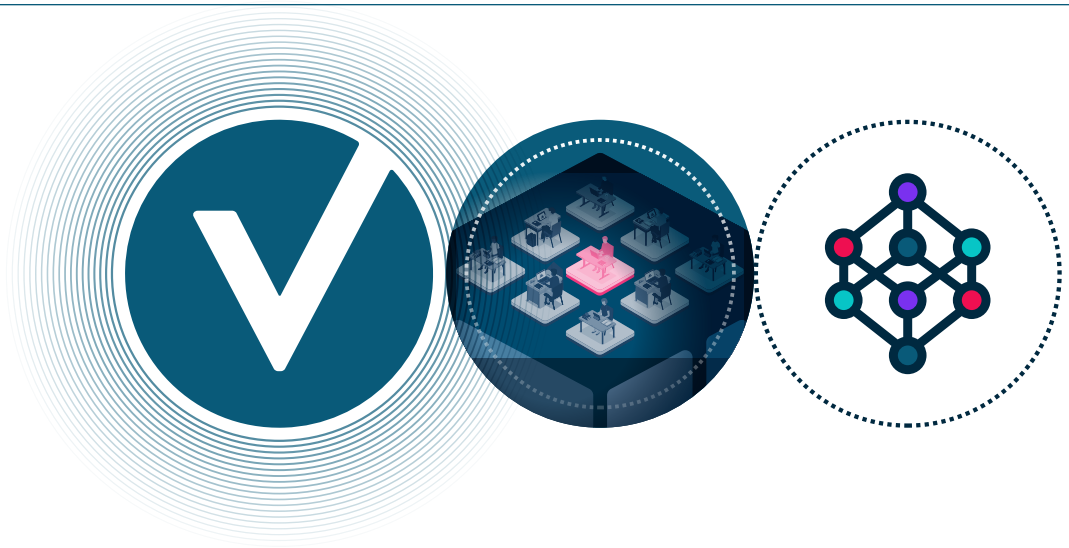
Simplified deployment and high-touch support ensure greater success.

We frequently hear that difficult deployments have reduced (sometimes quite significantly) the value enterprise security leaders feel they received from their BAS investment with competitive providers. Several security leaders who have either switched solutions or are looking to do so have complained that they still did not have their BAS solution fully deployed and/or working as expected after more than two years.

Other security leaders also noted areas of frustration with deployment difficulty, simulation setup, report customization, and—most importantly—challenging support experiences when trying to resolve these issues. Complaints included lack of technical support during initial proof-of-value testing, a generally poor quality of support, and add-on charges for what was expected to be standard on-boarding support. Again, this is surprising given that support is consistently listed as top purchase driver among technology decision makers. In fact, quality of customer support, ease of implementation, ease of use, and rapid return on investment (ROI) were all ranked higher as purchase considerations than number of product features and price in **G2's 2023 Software Buyer Behavior Report**. So, focusing on these areas just makes good business sense.

> **"We started looking at new BAS vendors, as our previous one was not providing the support we needed and we weren't able to deploy our platform. Not only has SafeBreach provided excellent service support and design/deployment collaboration, but they are also helping us define our BAS program, including staffing, areas of focus, and number of simulators."**
>
> **Director - Risk Management**
> Technology Provider

The SafeBreach architecture reduces time to deploy and maintenance overhead, resulting in a significantly lower cost of ownership than competing BAS technologies. SafeBreach's single simulator agent performs multiple endpoint and network attacks in parallel, reducing the time of execution and the total number of simulators needed. By comparison, competitive BAS offerings require many more agents or virtual appliances to deliver similar results, which increases their cost. Once deployed, SafeBreachs's Getting Started scenarios can have users running their first attack simulations in as few as three clicks. And, for select migrations, SafeBreach can help port over custom attacks customers may have already developed to ensure previous time and effort doesn't go to waste.



SafeBreach also understands the critical role service and support plays in ensuring customers can successfully deploy, manage, and derive value from our platform. That's why we offer:

Comprehensive user manuals, support documentation, and videos designed to help customers quickly implement the SafeBreach platform

The SafeBreach Academy, which provides a personalized and self-paced onboarding experience to help customers utilize the platform's extensive feature set and integrate it with existing business systems and workflows

The SafeBreach Community, where customers can find FAQs, submit questions to SafeBreach support experts, and actively engage with each other about common use cases, challenges, and more

The SafeBreach Validate Summit, a recurring customer event that brings together experts in the security community to discuss challenges, best practices, and key considerations for building a proactive security program

In addition, most SafeBreach customers are partnered with a dedicated support and success team that includes:

A Customer Success Manager to serve as the customer's single point of contact for all needs and coordinate all training and support activities

A Technical Account Manager to serve as the customer's technical advisor and ensure successful deployment, onboarding, training, and adoption of the platform

A Technical Support Engineer to provide premium 24/7/365 support for technical issues that arise at any hour

Built-in support for key stakeholders enhances internal adoption and extends value.

BAS is a dynamic technology with the potential to empower individuals across an organization—not only in security, but also IT, finance and procurement, compliance, and more. Yet, security leaders often cite the challenges they face with conveying the value of BAS to a wider organizational audience to support internal buy-in, increase adoption, and enhance collaboration.

From its simple deployment model and robust integrations, to its customizable onboarding capabilities and reporting features, the SafeBreach platform was designed to incorporate, support, and educate a broad audience. As a result, our customers are able to extend the value of their BAS solution to stakeholders across their organization, including:

C-Suite and Boards
Enable clear, data-based reporting on security risk posture; inform future security investments and validate existing ones; and support business-level initiatives, like digital transformation, cyber insurance, compliance, and M&A activities.

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.

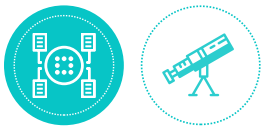
Blue Team
Use BAS to validate security control effectiveness, prioritize remediation requests to security engineers, and target rapid response exercises.

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.

Vulnerability Management
Uses BAS to identify the most critical vulnerability areas and security gaps and appropriately target patching where compensating controls are not effective.

Security Engineers
Use BAS to guard against security drift and to validate that security controls are protecting properly and are not misconfigured.



An experience that fits enterpise organizations now and in the future.

As demand for security posture assessment has increased rapidly over the last five to eight years, it's clear that more and more enterprises have recognized the value of BAS. Whether it is continuously testing your security response to new threats in a safe and controlled way, optimizing your mix of security controls and prioritizing future security investments, or improving security due diligence as part of mergers and acquisitions (M&A) initiatives, the benefits of a world-class BAS platform are immense.

However, since the category's inception, many competitors have entered the space with varied and—in our opinion—incomplete approaches to attack simulation and security control validation, as seen in the table below.

FEATURE / USE CASE	SafeBreach	Competitor A	Competitor B	Competitor C
24-hour SLA on new US-CERT and FBI Flash Alerts	✓			
The Largest & Most Up-to-Date Playbook	✓			
Flexible Reporting Dashboards	✓	✓		
Most Diverse and Mature Partner Ecosystem	✓			
Easy-to-Deploy Enterprise Coverage	✓			✓
Dedicated Threat Research Team	✓		✓	
Novel Attack Simulations	✓			
Simultaneous Integration With Multiple Vendors Within a Control Category	✓			
Integration With Multiple Tenants of the Same Control Platform	✓			
Single Simulator Architecture Performs Multiple Endpoint and Network Attacks in Parallel	✓	✓		
Run First Attack Simulations in as Few as Three Clicks	✓			
Dedicated CST, TAM, and TSE at No Additional Cost for Life of the Contract	✓			

Based on the increased volume of inquiries SafeBreach receives from enterprises looking to make a switch, it is clear that many organizations have faced significant challenges in establishing, expanding, and scaling their enterprise-level BAS programs with less mature BAS vendors.

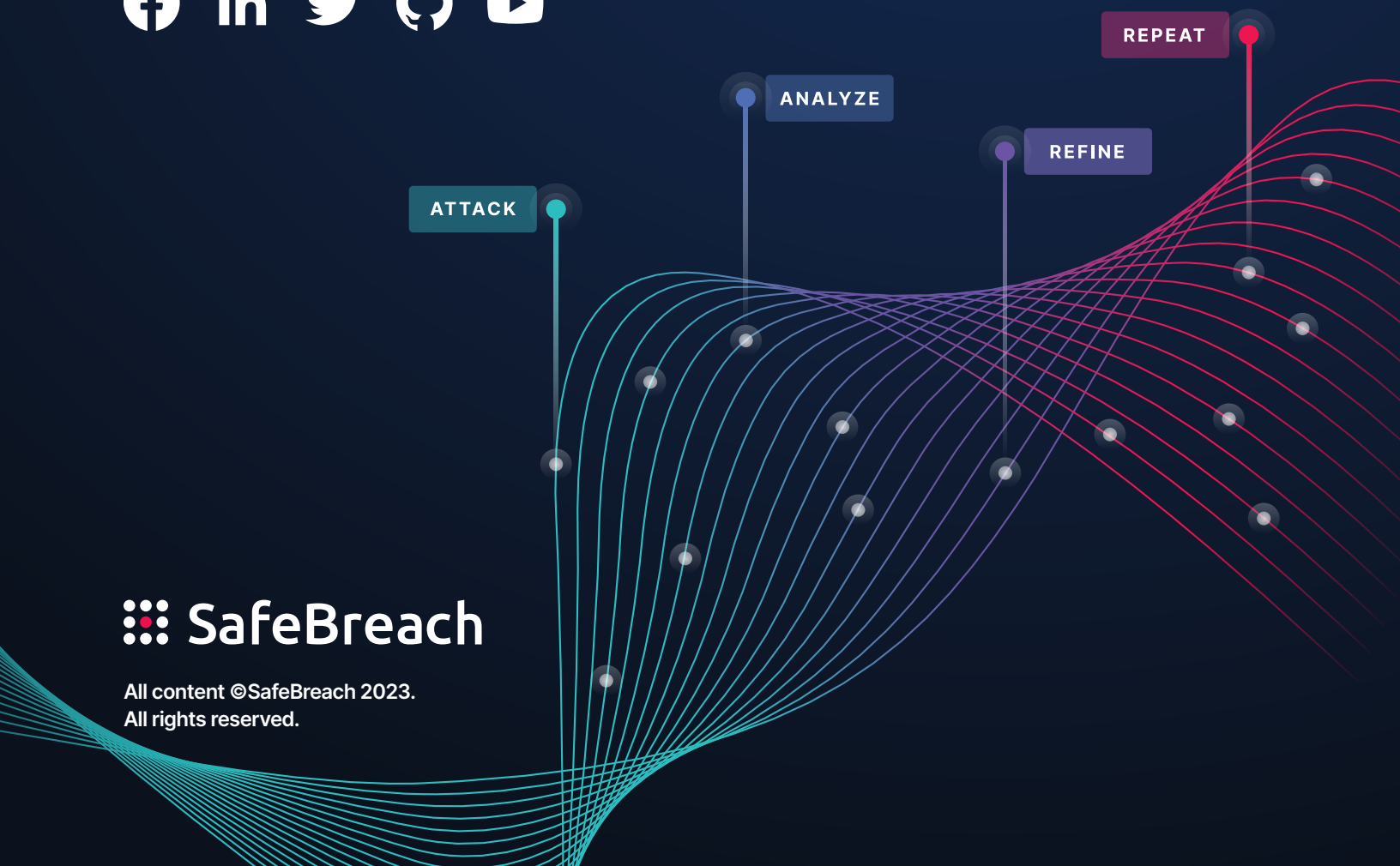
SafeBreach offers a world-class BAS solution that is scalable and easy to deploy across your environment, from your endpoints and servers to your cloud estate. Our world-renowned research team provides a large—and continuously updated—library of attack scenarios for immediate use, while also enabling users to plug in their own threat intelligence feeds. Our platform integrates with your existing security controls and workflow tools and enables you to customize those integrations or easily develop your own. And finally, our BAS platform is backed by an award-winning customer success team that is committed to ensuring you—and your entire organization—find success with our technology. If you're not getting all of this from your current BAS vendor, perhaps it's time to explore the alternatives.

To learn more about SafeBreach's advantages, **contact us to 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