SafeBreach

CASE STUDY

A Top Global Bank Switches to SafeBreach to Improve Security Control Validation & Enhance M&A Due Diligence

Learn how this bank's security team achieved 30% threat coverage improvement and time savings equal to one full-time security analyst when it replaced its previous breach and attack simulation (BAS) platform with SafeBreach.

Industry Banking

Challenge Information provided by the bank's previous BAS platform could not be trusted, leading to hours of additional manual validation by the security team.

Solution The team switched to SafeBreach to continuously test its own security posture, something it could not do before. SafeBreach also allowed the security team to track and communicate progress in their security posture over time.

Results With SafeBreach, the global bank's security team achieved:

- 30% improvement of threat coverage
- Time savings equal to one full-time security analyst
- Continuous and real-time security posture testing
- Quick and easy integration with their Splunk platform

The Security Challenges

With more than $200 billion in assets, one of the world's largest global banks offers a range of services, including merchant and retail banking, investment banking, asset management, and credit cards. The bank also has several partnerships with innovative financial technology (fintech) companies and an active mergers and acquisitions (M&A) pipeline.

The bank has a diverse technology ecosystem across multiple subsidiaries, including Windows and Linux servers and Windows desktop environments. The bank also has a large cloud computing footprint, with key assets of subsidiaries and the main bank operating in public and private cloud environments.

Using BAS for Continuous Risk Management

The bank was an early adopter of BAS, recognizing the critical need to continuously validate security controls to manage risk more proactively. The key challenge facing the bank was to protect against hackers accessing payment and transaction environments and exfiltration of key data from bank systems.

"Banks are constantly under cyberattack and being probed by nation-state sponsored advanced persistent threat (APT) groups. These attacks are very sophisticated," said the bank's CISO. "We also aim to have the best possible security in place to protect our infrastructure and our customers."

The bank began working closely with a BAS provider, but found over time that it not only needed better BAS capabilities, but also a more holistic approach to managing risk and validating security controls. The bank needed a security control validation and risk-management solution that could integrate with all of its existing systems, including security incident and event management (SIEM) solutions, log file analysis, and more.

This was particularly crucial for Splunk, the bank's primary platform to analyze cyber threats. The bank's security analysts found that their existing BAS solution often provided inaccurate readings as to whether a security control could or could not block an attack. This inability to trust the results of their adversarial attack exercises forced analysts to manually validate security controls, generating many hours of additional, tedious work.

"You don't want to take your precious analyst resources and have them spend it checking results from an automatic tool," the CISO said. "To gain a holistic understanding of our entire security posture, we needed to look at different siloes inside that product. It was not a great user experience."

While the BAS system had worked initially in serving basic use cases, the bank found that for more advanced use cases and control validations, their BAS tool would require extensive customization and modifications. In addition, the tool lacked the flexibility to pivot between the ability to replicate threat actor behavior and run multiple attack simulations in quick succession. This complexity and lack of flexibility reduced the value of the BAS tool considerably.

Using BAS for M&A Due Diligence

Due to its M&A activity, the bank also wanted to be able to quickly assess the security posture and validate security controls of the companies it intended to acquire before signing the acquisition papers. With their existing BAS solution, this was complicated. Due to the same issues noted above, the bank could not easily use its BAS capabilities to validate the security posture of key suppliers and partners in its digital supply chain.

“It was too hard to set up and run and was not lightweight enough to easily install and then run inside other organizations,” said the CISO, who added the lack of accuracy also diminished usefulness for M&A due diligence and supply chain security posture validation.

Validation Solution Requirements

The bank laid out specific criteria for what it needed from a continuous control validation and risk management solution based on its experience with their previous BAS tool. Specifically, the bank wanted a solution that could:

- Integrate with other key systems such as SIEM, threat intelligence, and vulnerability management solutions to provide a more holistic view of its security posture and to make risk management more efficient and effective.
- Deliver high accuracy in validating whether security controls were properly configured to block attacks and breach attempts.
- Run attacks and playbooks from a wide variety of threat actors and against the entire universe of common vulnerabilities and exposures (CVEs) and known risks on a continuous basis, also using the MITRE ATT&CK framework.
- Understand and improve the bank’s own security posture continuously and provide detailed reports on indicators of compromise (IOCs) and other risk elements as part of a risk-based security management process.
- Stand up a security posture assessment and control validation capability quickly and easily inside of potential acquisitions or environments of key partners.

A Best-in-BAS Solution

The bank’s CISO and security team began evaluating other BAS solution providers and continuous validation tools to identify which ones met all their criteria. After looking at various products, they identified SafeBreach as the continuous security control validation solution that best met their needs. SafeBreach had already pre-configured integrations with **Splunk SIEM** and many other key cybersecurity applications. In a proof-of-concept test, SafeBreach delivered superior accuracy with minimal false positives or false negatives in simulated adversarial engagements.

The bank appreciated that SafeBreach—via its Hacker's Playbook, the largest collection of attack methods in the industry—provided a flexible and simple way to apply more than 25,000 different attack types and test controls for efficacy against specific threat actors and APT attack patterns. The agility of SafeBreach also allowed the bank to continuously test its own security posture, something it could not do before.

SafeBreach also allowed the security team to track and communicate progress in their security posture over time. Lastly, SafeBreach was lightweight and easy enough to install so the bank could use it for cyber due diligence in M&A processes and to check the security stance of fintech partners in the digital supply chain.

Tangible Results

SafeBreach represented a significant improvement over the bank's previous BAS solution. Within a matter of weeks, SafeBreach was fully integrated with the bank's Splunk system and shared a continuous stream of IOC information to the security operations team in a seamless handoff. The accuracy of SafeBreach's security control validation was spot on.

> "The difference in accuracy was night and day. Our analysts could trust the SafeBreach results and stopped worrying about manually verifying them. It saved our security analysts many hours."
>
> – Global Bank CISO

The CISO added that SafeBreach improved his team's threat coverage by 30%. The security team also uses SafeBreach in M&A due diligence projects and to validate the security posture of key supply chain partners.

Because SafeBreach has an intuitive user interface and is inherently easy to use, the bank's security team quickly learned how to operate the solution and customize it for their specific needs by running particular APTs and threat types. SafeBreach also allowed the bank to customize the platform to highlight and prioritize the security control failures that posed the greatest business risk. The intuitive user interface of SafeBreach generated a holistic view of all control validations, threat warnings, and remediation steps to fix gaps in controls. The security team can create on-the-fly reports on any aspect of SafeBreach attacks and coverage results.

"With the flexibility of SafeBreach, we are implementing it as part of our operational capabilities and part of our ongoing cybersecurity lifecycle processes," said the CISO. "This is much more than traditional breach and attack simulation. It gives us real-time security posture and robust connectivity plus recommendations that make our teams smarter and more effective."