SafeBreach

CASE STUDY

Two Fortune 100 Financial Services Organizations Implement Continuous Security Validation with SafeBreach

Learn how a renowned financial-services CISO leveraged the unparalleled value of the SafeBreach platform to aid in overall security validation at two organizations.

Industry	Financial Services
Challenge	Without clear insight into current attacks and other relevant security issues, a financial-services CISO sought a more effective and efficient way to prioritize vulnerabilities and threats to remediate.
Solution	The CISO invested in SafeBreach to execute safe, automated attack scenarios, continuously validate control effectiveness, and provide visibility into the impact and feasibility of legitimate cyber attacks.
Results	With SafeBreach, both financial services organizations achieved: ▪ Comprehensive validation and verification of security controls ▪ Real-time, quantifiable effectiveness of overall security program ▪ Ability to re-prioritize remediation efforts ▪ Increased assurance of the board and key stakeholders ▪ Time saved previously spent on manual data collection

The Rising Financial Services Threat

With cyber warfare targeting key financial institutions 300 times more frequently than organizations of other industries, providing assurance to key stakeholders can be a daunting task for financial security leaders. Faced with this rising threat landscape, the former CISO of a multinational financial services company turned to his military background for guidance.

"Any student of military studies understands that a strong defense is the key to offensive success," said the CISO. "When it comes to protecting critical infrastructure, cybersecurity resilience is the center of gravity for the financial services industry. As a result, a security team's approach must provide the highest level of defense and assurance that the business's critical operations can continue to run during a cyber attack."

Without clear insight into current attacks and other relevant security issues, the CISO felt it would be an impossible task to properly prioritize vulnerabilities and threats to remediate. The CISO knew a more proactive approach would be needed to gain an accurate and comprehensive understanding of the organization's security posture and control effectiveness. He determined the best way to achieve this would be through the implementation of an advanced breach and attack simulation (BAS) platform.

A Partner in Proactive Defense

With its industry-leading capabilities to provide automated, continuous security validation, the SafeBreach BAS platform won out as the best choice for the financial services organization. With the largest attack playbook in the industry, SafeBreach delivered the relevant threat-intelligence coverage the CISO needed. Additionally, the platform provided the security team a thorough understanding of their tools' current capabilities, including their configuration and ability to function productively with other tools in the environment.

To best communicate results with the board, the CISO insisted on having quantifiable metrics to speak to their current security posture. SafeBreach's real-time reporting delivered the data needed and drastically improved organizational understanding of the current environment. This helped to ensure a realistic comprehension of security-tool effectiveness as well as validate and verify any assumptions made. The reports reaffirmed existing risks, identified new risks based on simulated attacks, and were crucial in the mission to provide unwavering confidence to the board and other key stakeholders. Additionally the reports created articulate evidence packages for audit and regulatory examination purposes.

> "SafeBreach was instrumental in validating and verifying our current security posture. The platform allowed for irrefutable and quantitative data to back up additional risks and findings previously missed, allowing my team to focus on other key parts of our overall cybersecurity strategy."
>
> **– Fortune 100 Financial Services CISO**

But the CISO knew reports are extraneous if they are not action-oriented and results-driven. To achieve full confidence in his organization's posture, his team leveraged pertinent information in the reports to inform risk-based decisions, prioritize security goals, and perform proactive remediation efforts.

Ongoing Risk Reduction & Assurance

The compiled source of prioritized information allowed the cybersecurity team to continuously and efficiently act on identified gaps while quantifiably measuring the organization's full security posture. And each time the SafeBreach platform runs in the environment, an update on the security posture and prioritization of risks is automatically recreated. This automation enabled the CISO and his team to focus on how they use the information to make intelligent decisions rather than having to focus on daily information gathering.

"Safebreach's automation and validation allowed my team to focus on defensive remediations rather than the compilation of data to determine priorities and other time-consuming housekeeping tasks," said the CISO. "Beyond leveraging SafeBreach's attack playbook, anytime we got a new TTP or IOC, we were able to utilize SafeBreach to provide key stakeholders renewed assurance in our organization's current ability to handle a serious attack. Without such a platform, this level of ongoing assurance would never have been possible."

When the CISO decided to pursue a new opportunity with another Fortune 100 financial services corporation, he knew his previous organization would continue to be in good hands with the continuous validation and risk reduction SafeBreach enables. And the decision to bring SafeBreach along to his next organization was a no-brainer for the CISO. He was once again able to leverage SafeBreach's leading BAS platform to successfully deliver comprehensive security validation, quantifiable effectiveness, prioritized remediation, and increased assurance for his new organization's leadership team.

"Over the past five years, SafeBreach has validated and verified my organizations' security controls," said the CISO. "They have provided a customized platform that is easily implemented and allows for seamless integration with other third-party tools. The clarity provided in the reporting has maximized my teams' ability to proactively defend against threat-enriched exploits, allowing me, as the CISO, the ability to assure my key stakeholders and board of directors of our ability to withstand complex cybersecurity events."