SafeBreach

A Top Global Bank Deploys SafeBreach for Control Validation, M&A Due Diligence, and Ongoing Security Posture Improvements

Case Study

Security Control Validation, Security Posture Tracking, and M&A Due Diligence Use Cases

For the security team at one of the 300 largest banks in the world, it was critical to protect the bank's payment and transaction environment from advanced persistent threats (APTs). Additionally, the bank wanted to quickly assess the security posture and validate security controls of any companies it intended to acquire. SafeBreach has allowed the bank to not only continuously validate its security controls against APTs, but it has also allowed them to successfully perform cyber due diligence in its M&A processes.

Challenges

Information provided by the existing Breach and Attack Simulation (BAS) solution could not be trusted, leading to hours of additional manual validation by the security team.

Solution

The team employed 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.

Benefits

Improvement in threat coverage and continuous, real-time security posture testing.

Challenges

Company Background

One of the 300 largest banks in the world with over $200 billion in assets. The company is headquartered in Israel with operations all around the globe. Bank activities include 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 pipeline.

The bank has diverse technology infrastructure 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.

Challenge 1—Using BAS for Continuous Risk Management

The company was an early adopter of breach-and-attack simulation (BAS) software, recognizing the 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," explains 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 startup in Israel but over time found that it not only needed a better BAS capability, 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) systems, log file analysis, and more. This was particularly crucial for Splunk, the bank's primary platform to analyze cyber threats. As time went on, 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. The product design also siloed different types of complementary information. This created more work. "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," said the bank CISO.

While the BAS system had worked well initially and served basic use cases, the bank found that for more advanced use cases and control validations, their BAS tool required extensive customization and modifications. In addition, the tool lacked 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. "We found that we could not easily use it to check our posture against the latest threats," explained the CISO.

Challenge 2—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. For the same reason, the bank could not easily use its BAS capability 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," explained the CISO, who added the lack of results accuracy also diminished usefulness for M&A due diligence and supply chain security posture validation.

The Requirement:

The bank laid out specific criteria for what it needed from a continuous control validation and risk management solution based on its experience with the previously used 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 CVEs and known risks on a continuous basis, also using the MITRE framework.
- Understand and improve the bank's own security posture continuously and provide detailed reports on 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.

Solution and Results

The bank CISO and their team began talking to other solutions providers to identify the ones that met 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 very few false positives or false negatives in simulated adversarial engagements.

The bank appreciated that SafeBreach—via it's Hacker's Playbook™, the largest collection of breach & attack methods in the industry—provided a flexible and simple way to apply more than 30,000 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 enough and easy enough to install so that 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.

Results:

- 30% improvement of threat coverage
- Time savings equal to one FTE cyber security analyst
- Enabled continuous and real-time security posture testing
- Integrated quickly and easily with the Splunk platform

SafeBreach represented a significant improvement over the bank's previous BAS-only 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 like night and day. Our analysts could trust SafeBreach results and stopped worrying about manually verifying the results. It saved our security analysts many hours of time," the CISO said, adding that SafeBreach improved his team's threat coverage by 30%. With a simple installation and set-up, the security team will plan on using SafeBreach in several M&A due diligence projects and to validate the security posture of key supply chain partners in the near future.

Because SafeBreach had an intuitive user interface and was inherently easy to use, the bank's security team quickly learned how to operate the solution and to 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 could 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," explained the bank 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."

SafeBreach
111 W. Evelyn Avenue
Sunnyvale, CA 94086 408-743-5279
safebreach.com

Learn More

If you're interested in learning more about how SafeBreach can benefit your organization, be sure to visit safebreach.com.

Here