SafeBreach

Financial Technology Leader Boosts its Security Score

Ends Data Exfiltration Risks with SafeBreach Continuous Security Validation Platform

SafeBreach

CHALLENGES

A leading provider of a free credit and financial platform for consumers needed a solution that could probe for and identify vulnerabilities, risks and data exfiltration routes on its network, while continuously validating security across its environment.

SOLUTION:

The financial firm deployed the SafeBreach Continuous Security Validation Platform, which simulates hacker breach methods inside its environment, analyzing what a hypothetical attacker would do and how security systems respond. SafeBreach enables the company to identify exfiltration routes and fix breach scenarios in its network before an attacker exploits them, acting like an "automated, continuously-validating red team" on a platform – all without impacting their environment.

BENEFITS:

- Understanding the impact of a breach before it happens to enable quick corrective action
- Identified and mitigated data exfiltration risks
- Achieved continuous validation of security controls for entire infrastructure

With millions of members, the free financial platform for a well-known financial technology firm helps people make educated financial decisions and pursue new opportunities. Because it handles sensitive financial data from consumers and its partners, network security is a primary focus.

A lack of awareness of potential outbound routes for data in an IT environment, and whether they invite risks, are top of mind for IT security teams. Despite almost $70B in security investment, organizations continue to face an uphill battle against breaches. The 2015 Verizon DBIR report found that in 60% of breaches attackers were able to compromise organizations within minutes, while these breaches remain undiscovered for weeks or months.

This leading financial technology firm consistently strives to proactively gain awareness of all network security risks. "We had long talked about whitelisting data leaving (and to specific locations, like partners, etc.), to close the threat window," says the company's senior security architect. "We wanted to address the last step in the kill chain; getting an actionable list of "outbound channels" we could close to prevent data from being exfiltrated."

What Happens on Your Watch?

To achieve its objectives, the financial technology company reviewed options on the market and chose the SafeBreach Security Validation Platform. SafeBreach simulates the Hackers' Playbook™ of hacker breach methods to find holes in an organization's infrastructure before an attacker does. Organizations can quantify their risks from breaches and validate their security controls, without impacting their environment, acting like an automated, continuously-validating red team on a platform. The SafeBreach platform validates all possible breach methods within an attack kill chain in real-time.

"If you're a C-level executive, your goal is for nothing bad to happen on your watch," says the senior security architect. "If an executive is coming into a new environment or inherits "technical debt", they don't know where the problems are. They assume someone is already in their network and looking for data, and trying to find the way out. What got us excited is how SafeBreach addresses this final piece in the kill chain by providing a list of things an attacker can do."

Sealing in Data

The financial technology firm quickly and seamlessly deployed SafeBreach and began receiving updates on breach scenarios in real-time – all without affecting the stability or uptime of its environment.

"SafeBreach gave us more visibility and supported what we knew about the issues with some of our outbound connections – especially those with partners," says the senior security architect. "SafeBreach also gave us a definitive list of about 50 ways data could get out, which significantly reduced the attack surface."

With action items from SafeBreach in hand, the company's network engineering team began to close all egress ports. "If you step through everything SafeBreach identifies as risks, you close all the "unknowns," which is huge," says the senior security architect. "The automation of SafeBreach helps achieves continuous validation of risks while keeping users and infrastructure running seamlessly".

The company implements rather stringent network segmentation best practices, such as "air gapping" its corporate and production networks, and using different user identities on its corporate and production network. "We don't co-mingle these two segments because you can't even use the same email and password for access," says the senior security architect. "Even though we do all of this, we are very aware of the risks of an attacker somehow gaining access into the production network and pivoting to corporate. Our next project will be to simulate the lateral movement of data between our corporate and production networks to assess potential exposure, and to ensure PII (personal identifiable information) cannot ever leave the corporate network."

"With cyberattacks, the key to understand is that only when the data gets out, does it become an actual breach. This is where the brilliance of SafeBreach comes in. By giving you an actionable inventory of egress methods so data cannot be exfiltrated, SafeBreach prevents the final step in the kill chain."

– Senior Security Architect for an industry-leading financial technology company

A consumer's credit score is a number that gives financial institutions the confidence to lend money to a person. "You could say that SafeBreach improves our security score, which increases the confidence users and partners have in us," says the senior security architect. "It's a high-confidence, independent way to score risks based on whether data can leave the network. Our compliance people also appreciate SafeBreach because they can run a report to categorically demonstrate there is no way data can get out."

Security Through Validation

SafeBreach delivers a new approach through which organizations are empowered to act like hackers and simulate breach methods to proactively find holes in their network – before an attacker does. By taking an offensive approach to security, security professionals can understand the hackers' perspective, gain visibility into exactly how vulnerable their organization is and focus their resources appropriately.

SafeBreach answers the key questions organizations struggle to answer, "Am I secure? What are the ways in which data can get out? Are my SOC teams ready for a breach? Are my security defenses working as expected?" The SafeBreach platform simulates hacker breach methods so that security professionals can quantify their actual risks from breaches, validate their security controls and empower their security red teams. "SafeBreach is the arrow you need in your quiver to make sure nothing bad happens on your watch."

SafeBreach

SafeBreach

HQ
111 Evelyn Avenue #119
Sunnyvale, CA 94086
contact@safebreach.com

R&D
108 Igal Alon Street
4th floor Tel Aviv, 6789146
ISRAEL