SafeBreach

Top Security Developer Gives Red Teams the Ultimate Security Tool

Validates Security Controls with SafeBreach Continuous Security Validation Platform

SafeBreach

CHALLENGES

A developer of cyber and data security products that protect business-critical data and applications in the cloud and on-premises, needed a solution to unearth security vulnerabilities, risks and data exfiltration routes, while continuously validating security across its dynamic environment.

SOLUTION:

The security developer 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:

- Validated the impact of a breach scenario to enable quick corrective action
- Identified and mitigated data exfiltration risks and focused resources on the right breach mitigation techniques
- Achieved continuous validation of security controls for entire infrastructure

An industry-leading security solutions company creates innovative cyber and data security products for the cloud and on-premises. The firm's integrated security platform includes tools to combat attacks, theft and fraud, mitigate risk, and streamline regulatory compliance.

The firm's environment is very dynamic and growing quickly. As a company that develops security products, it clearly understands the importance of working to constantly improve its own security. The person charged with safeguarding the security developer's operations, data and users is its Chief Information Security Officer (CISO). "My team is responsible for the security and compliance of our enterprise footprint and for cloud operations for several product lines," he says.

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. As a result, security executives are seeking tools that can consistently probe and test their security products, validate their security posture, identify security risks and morerisks and more

Focused on the Right Issues?

The security firm sought a solution to address multiple security challenges. "We wanted to be more efficient in our firewall operations," says the CISO. "We need to know if our security products are configured the right way, and relying on log reviews isn't efficient enough. In addition, our environment is really dynamic – with changes made weekly – so we wanted to reduce the man hours it took to validate the efficacy of our security controls."

The security solutions provider also wanted to verify that its assumptions about its security were correct. "We wanted a tool that could confirm our security posture and our beliefs about what our people are doing, and that we're addressing the things that adversaries may want to exploit," says the CISO.

Lastly, the company has an open environment, so the CISO and his team sought to better understand potential data exfiltration vulnerabilities. "We needed a product to identify, limit and close outbound channels, and prioritize which channels don't need to be open and should be closed first."

Finding Safe Harbor in SafeBreach

The security provider considered the options on the market and found that only the SafeBreach Security Validation Platform met all of its criteria. 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. "It was clear that SafeBreach had the ability to identify the critical issues that we needed to address," says the CISO.

Top Security for Top Security Developer

The leading security developer deployed SafeBreach and realized the results it desired. SafeBreach quickly spotlighted potential routes for outbound data. "We were able to see potential data exfiltration methods and limit the risk posed by outbound channels," says the CISO.

"SafeBreach constantly challenges my security controls to ensure they are working as expected and improves the quality of the findings of my red teams. It enhances security by identifying potential outbound channels for data, and makes our red teams more efficient and effective by focusing them on the right issues."

– Chief Information Security Officer for a leading security solutions developer

SafeBreach helped the security firm become more secure and achieve better efficiencies. "SafeBreach has significantly reduced the man hours it takes to identify and solve security issues," he says.

SafeBreach also speeds up decision-making about risks. "It tells me how external communication channels enabled on our firewall infrastructure can be used for threat activities, so we can decide whether to block or allow a given protocol," says the CISO. "By gaining the perspective of an attacker, we can make better decisions about whether to block particular activities or not."

The deployment of SafeBreach has generated more insights into security and operational efficiencies. "In a dynamic, fast-growing environment, it's important to prioritize the right things," says the CISO. "SafeBreach enables us to address potential security vulnerabilities and enhance the performance of our red teams so they can spend their time finding the more unique, specific things for their environment that might be potential targets for hackers."

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

"With SafeBreach, there's more awareness and clarity about what the major risks are –beyond simply identifying foundational issues. SafeBreach also challenges the efficacy of my security defenses and my security assumptions; this is where SafeBreach's real value comes into play," says the CISO.

SafeBreach

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

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