LivePerson Deploys the Hacker’s Playbook

Validates Security Posture with the SafeBreach Continuous Security Validation Platform

CHALLENGES

LivePerson drives communication to foster relationships between brands and consumers. The company needed a solution that could probe for and identify vulnerabilities, risks and changes to its network and continuously validate its security across numerous environments.

SOLUTION:

LivePerson 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. The solution empowers LivePerson to identity 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
- Resources focused on the right breach mitigation techniques
- Achieved continuous validation of security controls for entire infrastructure – network, cloud and endpoints

Over 18,000 brands – including leaders in banking, telecom, retail and transportation – connect with thousands of consumers 24/7 on LivePerson's bustling mobile and online messaging platform. To support its clientele, the company's global operations and 1,200 employees use multiple IT environments with assets in corporate, production and cloud-based networks and mobile devices.

The person responsible for LivePerson's strategy to protect critical data, information systems, users and infrastructure – throughout all business operations – is Chief Security Officer Ron Peled. "The primary challenge with having multiple environments is that they are very dynamic," says Peled. "There are change management challenges – despite the fact everything is documented – and the changes are very rapid." Each of LivePerson's development operations, system or network engineers can make changes to the network. "We need to understand the ramifications of each change in terms of its security risk in those environments," he says.

A lack of awareness of every change made to an IT environment, and whether it invites risk, are major headaches for businesses. In fact, 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.

Underwhelming Security Validation Options

LivePerson deployed a variety of vulnerability assessment and change management tools to help it identify, assess and efficiently manage security risks. "Even though we had a lot of sensors, none of them could show us the actual risk or breach scenarios once someone was inside the network," says Peled. "Our existing tools could only let us see this on a point-in-time basis."

LivePerson wanted a better solution and began its due diligence. "The challenge with hiring ethical hackers or penetration testers is that they are very focused on finding vulnerabilities and exploiting them, which can impact the environment." Peled also evaluated using 'red teams,' which can go beyond standard vulnerabilities exercises and practices and perform drills on a company's entire ecosystem without anyone's knowledge.

"Most of this validation via specialized humans is very costly, takes a lot of time, shows only a limited point of view and is no longer valid after five minutes," says Peled.

Why Only Play Defense?

After reviewing the options, LivePerson 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.

“We liked SafeBreach’s combination of simulators that are constantly testing our infrastructure – not just point-in-time – and that we get updates on breach scenarios in real-time,” says Peled. “The fact that SafeBreach does not impact stability or uptime in the environment is also a big advantage.”

Building A Proactive Framework

LivePerson quickly and seamlessly deployed SafeBreach, with simulators placed both inside and outside of its data center. This allowed the company to simulate breach scenarios across the entire kill chain, and validate both internal and external threats.

“The SafeBreach platform enables us to find and remedy any security issues in our networks before an attacker has the chance to potentially do anything to exploit it,” says Peled.

Challenging Security Controls

Peled and his team quickly noticed the contributions of SafeBreach. “For the first time, we were able to see multiple breach scenarios displayed in one consolidated view or screen, rather than reading endless pages of a report on confusing environments,” says Peled.

> “Hackers don’t rest, and that means neither can we. Buying and implementing the latest defensive technologies and patching the latest bugs are necessary, but not sufficient. We need to be able to anticipate what an attacker will do next, and get there first. SafeBreach helps us with do this.”
>
> **– Ron Peled, Chief Security Officer, LivePerson**

“In addition, some of our security controls that we thought were fully deployed were missing in certain segments of the network.”

The ability to challenge security controls, and identify which ones were not performing adequately, was important for better overall and proactive security. LivePerson is so pleased it plans to try SafeBreach’s new endpoint simulator, which can execute simulated attacks on endpoints.

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.

Peled has advice for other companies that may be evaluating the benefits of offensive security. “The most important thing is validation -- validating your controls and assumptions," he says. "We all know assumptions break easily when checked. It's not just about offense versus defense, because over time we have invested money in both areas. The bottom line is you must validate your controls, your beliefs and that the concept in your mind is true. Having a platform like SafeBreach that can reassure and constantly confirm the tools you have in place, and that they're doing what they are supposed to do, is a real game changer."

SafeBreach answers the key question organizations struggle to answer, "Am I secure?" The 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. That's powerful security.