SafeBreach

CASE STUDY

Fortune 500 Healthcare Provider Establishes Continuous Security Validation with SafeBreach

Learn how the security team for one of the largest not-for-profit healthcare insurance providers leveraged the SafeBreach platform to safeguard its systems, services, and sensitive data against constantly evolving threats and vulnerabilities.

Industry	Healthcare
Challenges	For this healthcare provider's security team, threats are constantly evolving—and so are the environments that need to be protected. The team needed to ensure effective defenses were in place at all times.
Solution	The team deployed the SafeBreach platform to safely execute real-world attack simulations to continuously validate their security controls.
Results	With SafeBreach, this Fortune 500 healthcare provider: ▪ Gained critical insight to strengthen their defenses ▪ Enhanced the maturity of their security team ▪ Established a more consistent, efficient security operation ▪ Laid the foundation for a self-defending infrastructure

Seeking a Holistic, Proactive Approach

With nearly one million subscribers, this Fortune 500 healthcare provider is one of the largest not-for-profit healthcare insurance providers. Its security team is responsible for safeguarding the organization's systems and services, as well as a range of sensitive data, including financial records, personally identifiable information, protected health information, and more.

That is an increasingly challenging task in the healthcare industry, which repeatedly tops the charts in terms of the number of publicly disclosed breaches and the average cost of each breach. Rather than a security strategy solely targeting compliance requirements, the organization's team sought a more holistic, proactive approach that would help them continuously evolve to guard against the ever-changing cybersecurity threats faced by the healthcare industry. They wanted to build effective threat models, have greater visibility into their vulnerabilities, and take proactive steps to reduce their overall attack surface.

They started by asking several fundamental questions:

- Do we have visibility where we need it?
- If we see an issue, do we know what to do about it?
- How do we measure the effectiveness of our controls?

The team conducted penetration testing and red team exercises on an annual basis. However, these efforts only provided point-in-time assessments, and team members weren't convinced the results were conclusive. They needed a more continuous way to ensure they were protecting the sensitive data of both their organization and their customers, day in and day out.

"Just because we have controls in place doesn't mean they're working, and our security posture is changing all the time," said the CISO at the Fortune 500 healthcare provider. "A mistaken configuration change in a VPN service could open up a new vulnerability at any time. That's why it's so vital to continuously validate our tools and overall security posture.

An Automated, Continuous & Simple Solution

The team chose to deploy the SafeBreach breach and attack simulation (BAS) platform for continuous security validation. SafeBreach enabled the team to safely execute real-world attack simulations across the cyber kill chain to validate security controls, uncover possible attack paths, identify and prioritize critical gaps, and remediate based on quantitative evidence before a breach occurred.

Compared to alternative vendors they had evaluated, SafeBreach was much easier to implement and use. Other platforms required significant time and effort to stitch things together, and staff had to manually build all attacks. The SafeBreach Hacker's Playbook, on the other hand, offered over 25,000 attacks the healthcare provider's team could use right out of the gate.

> "SafeBreach already had a library with a lot of attacks," said the CISO. "You could press a button and start running. My team loves the SafeBreach platform. We have agents running on premises and in the cloud, and we're continuously running the solution. We rely on the platform extensively to generate different reports that we can use to communicate with management. The platform provides the vital insights that enable us to continually fine-tune our defenses."

Since implementing the SafeBreach platform, the team has continued to expand the ways in which the solution is used, including:

Threat Assessment

SafeBreach handles all the activities associated with advanced cyberattacks, including sending and opening emails, detonating payloads, triggering alarms in simulators, and so on. The healthcare provider's security team is able to run advanced attacks that are composed of a number of steps, and assess each phase in detail.

They also rely heavily on SafeBreach's service level agreement that ensures coverage for US-CERT and FBI Flash alerts are added to the SafeBreach Hacker's Playbook within 24 hours. This helps them manage ongoing threat assessments and ensure they are aware of heightened threat levels from malicious actors—including nation states—targeting the healthcare industry. Based on what they know about the actor, and their tactics, techniques, and procedures, the team can wage similar attacks, test their defenses, and assess whether there are vulnerabilities the actor could exploit.

Mock Scenario Training

With SafeBreach, the team can execute regular mock scenario training. This ensures their staff members are prepared to respond to new and emerging threats, regardless of things like turnover or paid time off.

"Our staff changes occasionally, but what's even more challenging is the fact that everything else is changing constantly, including malware, tactics, and environments," said the CISO. "We wanted to establish continuous training, so teams would always be best prepared to respond when issues arose."

Tool & Service Validation

With its robust capabilities, SafeBreach helps the team vet the efficacy of the solutions they implement, which was difficult to do in the past. For example, if the team employed a new anti-malware tool, and the vendor claimed to catch 90% of malware, how could they tell whether that was true? How could they track exactly how it worked in their specific environment?

With SafeBreach, the team can test and validate the efficacy of the tools they have in place, and hold their vendors accountable for the claims and commitments they make. They can even test products during proof-of-concept phases to validate that they work as advertised.

In addition, they use SafeBreach to verify whether operations staff from the managed security service provider they use to operate their network operations center are following up according to established policies when events occur.

Ongoing Benefits & Improvements

By using the SafeBreach platform, the team has realized several key benefits:

Boosted Team Maturity

By harnessing the solution to conduct mock scenario training, the team is able to refine their expertise, workflows, and policies. With SafeBreach, the team can establish the continuous training that helps ensure team members are optimally prepared for the latest threats.

Strengthened Safeguards

SafeBreach has delivered the insights that enable the team to identify gaps and weaknesses before they're exploited. Now, they proactively report to senior leadership about breaches in the news. The security team can assess whether the healthcare provider is exposed to the same risk, and, if so, take steps to mitigate it. By revealing the gaps that can actually be exploited, SafeBreach helps the team more intelligently prioritize their remediation efforts.

Enhanced Efficiency & Consistency

With SafeBreach, the healthcare provider doesn't need to have multiple people spending significant time running manual tests. This frees staff up to focus on more strategic efforts on an ongoing basis. Further, the automation of test execution ensures that testing is more consistent, which yields significantly improved insights.

Established A Foundation for a Long-Term Strategy

Over the course of the deployment, the team and SafeBreach have established a partnership, working together to advance the solution's capabilities.

"Over the years, SafeBreach has responded to a number of requests and input we've provided, including adding support for the MITRE ATT&CK framework, offering more flexibility in running specific attacks, and providing increasingly robust integration with the Cortex SOAR solution," said the CISO.

SafeBreach's integration and automation capabilities are also helping support the team's longer-term goal to establish a self-defending infrastructure. Instead of having team members responding when alerts arise, their goal is to employ orchestration and automation to handle incident response more quickly and consistently.

"People often think about security in binary terms, focusing on whether they're winning or losing," said the CISO. "When it comes to security, you need to stay in the game—at all times. We need to be focused on defense constantly. That's why we're continuously training and improving."