SafeBreach

CASE STUDY

Fortune 500 Biopharmaceutical Company Reduces Endpoint Tool Sprawl With SafeBreach

Learn how the security team at one of the largest biopharmaceutical companies in the world established continuous security control validation to ensure the most effective safeguards, while minimizing the cost, complexity, and risk of tool sprawl.

Industry	Biopharmaceutical
Challenge	To establish the safeguards needed, a number of security tools were employed on endpoints. Over time, the proliferation of tools began to introduce increased complexity and risk.
Solution	The security team trusts SafeBreach to execute safe, automated attack simulations, enabling them to rigorously test their endpoint security tools.
Results	With SafeBreach, the security team can more knowledgeably assess the effectiveness of the tools in place and establish the mix of tools that delivers optimized security and user experiences. The team leverages SafeBreach to: ▪ Identify ways to strengthen safeguards and intelligently prioritize vulnerabilities ▪ Boost efficiency and consistency by automating ongoing, low-level tasks ▪ Gain insights to address tool sprawl and attain a strong return on investment

Contending with Tool Proliferation

For the team at one of the largest biopharmaceutical companies in the world, delivering life-saving medicines is a core mission. In the process, an array of sensitive records need to be managed and secured against the constant specter of threats, including ransomware and Internet protocol (IP) theft. The security team is tasked with safeguarding a wealth of critical assets, including data related to financials, patients, employees, patents, clinical trials, and more.

Across the organization, there are core security mechanisms in place, and there are also security frameworks employed to address the needs of specific business units, such as labs and manufacturing departments. Given the multi-layered, varied nature of their security environments, the number of tools employed on endpoints has continued to expand in recent years. Further, as new risks, technology environments, and security technologies emerge, tools continued to be added. Over time, this increasing number of security tools has become problematic.

First, tools may not be foolproof, and they may not be kept current. For example, one study based on data from more than six million devices found that, at any given time, around 28% of devices had missing or outdated antivirus or antimalware protections.

Second, the complexity introduced by having many tools in place can lead to its own problems. Various tools can perform similar or overlapping functions. Different agents can be applied that may introduce conflicts or errors. This complexity can ultimately introduce failures and erode the very security benefits the tools were implemented to deliver. Plus, the proliferation of tools can have a direct and significant impact on users.

“Just because we have implemented a tool doesn’t mean we’re safe,” said the organization’s CISO. “We often hear users complain that they have too many tools running on their systems. They were seeing degraded performance. And users and our system administrators also had to contend with administrative complexity on an ongoing basis.”

Seeking Actionable Insights into Endpoint Tools

Users may experience outages and degraded performance based on the tools implemented, not to mention being exposed to the possibility that their devices may be compromised by an attack. In response, the security team sought out to strengthen security, enhance employee productivity, and reduce cost and overhead. To do so, it was vital to gain greater visibility into their security posture on a sustained basis.

“It is one thing to detect an event, but another to gain a complete understanding of how many attacks were executed, how many were caught, and how they were caught,” said the CISO.

Consequently, they looked to leverage a solution that could help validate tools they had in place, and determine which were working and which weren't. They sought to find a solution that could execute attacks safely and continuously, and provide the critical visibility they needed.

A Safe, Continuous Security Validation Solution

After an extensive evaluation of tools available, the team chose to deploy SafeBreach. The SafeBreach platform conducts automated testing of the team's security architecture, using advanced technology that can execute attacks safely and continuously. With SafeBreach, they can run accurate testing of endpoint tools and verify their efficacy in blocking attacks.

Working with SafeBreach, the team starts by running tests against machines with a clean corporate image. Then they add a security tool and rerun the tests to gauge the efficacy of the tool. They then repeat the process with each additional tool, gaining insights into how effective each tool is, and how it interacts with others.

In this way, the SafeBreach solution provides an accurate view of which tool blocks which type of attack. Ultimately, over time, this enables the team to determine whether existing tools can be removed, without introducing any risk, and whether because they introduce conflicts with other tools, they're redundant, or they're simply ineffective.

An Extensive, Flexible Playbook

With SafeBreach, the team has been able to leverage a playbook they can use to map out all the steps in an entire attack scenario. The solution offers comprehensive threat coverage, featuring capabilities for executing ransomware, nation-state attacks, and more. The solution can execute the cyber kill chain from end to end, including sending an email, opening it, detonating a payload, and triggering alarms.

A Consistent, Repeatable Scenario Execution

By using SafeBreach to safely automate attacks, the team saves significant time. Plus, the implementation of automation helps ensure far more consistency than having multiple staff members performing a lot of manual tasks.

"SafeBreach agents intelligently scale and are equipped to automatically determine what attacks to run on which agents," said the CISO. "Not only does this ease the burden on security teams, but it helps remove bias as well."

Flexibility to Support a Range of Use Cases

Given the solution's flexibility, the team was able to rapidly expand the ways the solution was used. In addition to tool-bloat testing, they're able to validate security controls, investigate the security of potential acquisition candidates, run mock scenario training, conduct red-team exercises, and more.

Ongoing Security Benefits & Improvements

By implementing SafeBreach, the security team at the Fortune 500 biopharmaceutical company has been able to realize a number of benefits.

Identifying Ways to Strengthen Safeguards

With SafeBreach, the team is better equipped to identify gaps and weaknesses before they're exploited. Further, by revealing gaps that can actually be exploited, SafeBreach helps the team intelligently prioritize the vulnerabilities they need to focus on.

"When we hear about breaches in the news, we know senior leadership wants to know if the same type of attack can expose the company," said the CISO. "With SafeBreach, we can establish automated attack execution based on the specifics of the reported attack and determine if we're exposed to the same risk."

Boosting Efficiency & Consistency

Now, instead of having different team members doing manual testing, they can employ automation. This automation significantly enhances consistency, which yields improved insights. With SafeBreach, the team can boost operational efficiency by streamlining and automating many ongoing, low-level tasks. As a result, they can spend more time focusing on strategic efforts.

Gaining Insights to Address Tool Sprawl

With SafeBreach, the team can now test how effective the tools they have deployed really are. With these insights, they'll be far better equipped to determine which solutions they need and which solutions they don't.Through this visibility, they'll be better able to strike the optimal balance between keeping endpoints and the organization secure, while delivering quality user experiences. This will also help them maximize the utilization of the tools they do have in place, and it will enable them to extend the usage of their endpoint devices.

"Right now, it's not uncommon for users to be running 15 security tools on their laptops," revealed the CISO. "In the long run, if SafeBreach helps us reduce that number to five tools, we will have realized an extremely strong return on our investment."