SafeBreach

CASE STUDY

Fortune 500 Drug & Device Development Company Implements SafeBreach to Take the Guesswork Out of Validation

Learn how the security team at one of the world's largest drug and device companies implemented SafeBreach to automatically execute attacks safely and continuously, gaining the data-driven intelligence needed to identify and address their most critical vulnerabilities.

Industry	Life Sciences
Challenge	Securing clinical trial data and other sensitive records was a constant imperative for the company's security team. Over the years, the organization had implemented an array of security controls, but they struggled to assess how effective those controls really were.
Solution	The team instituted automated testing of their security architecture with the advanced SafeBreach breach and attack simulation (BAS) platform, enabling them to execute attacks safely and continuously.
Results	With SafeBreach, the Fortune 500 drug and device company's security team achieved: ▪ Data-driven insights to more clearly assess the effectiveness of security controls ▪ Improved levels of operational efficiency and cost reduction with continuous automation ▪ Enhanced customer safeguards and confidence in security posture

Too Much Guesswork

As a Fortune 500 global provider of outsourced drug and device development and commercialization services, the company supports programs that advance every phase of clinical development, from compound selection to clinical trials.

As a clinical research organization, the team has to take security extremely seriously. The company operates in a highly regulated industry that must adhere to FDA requirements and strict agreements with its customers. Through the course of its work, the company collects a massive amount of clinical trial data. It would represent a huge exposure for the organization if any of this data was stolen, changed, released, or sold to competitors. Quite simply, any type of unauthorized access would be an issue—and it fell to the security team within to guard against these threats.

"Just like any other organization, we are subject to website attacks, users clicking on malicious links, and data loss," said the company's head of information security. "As a clinical research organization trying to get a drug to market, it's imperative that we secure a range of confidential information, particularly data on drug trials."

To establish appropriate safeguards, the security team has continued to implement an array of controls. However, they lacked an effective way to validate that the controls were working as expected. The team conducted penetration tests, but this approach posed significant limitations:

- **Time-consuming:** The security team had to devote a significant amount of time and effort to conduct these tests and gather results—they also weren't able to act on results very quickly. Ultimately, it took more than 12 months to plan, execute, and then address remediation.
- **Incomplete:** Over time, it became increasingly clear the penetration tests didn't accurately reflect the way organizations were getting compromised and only offered a limited view of exposure. For example, to assess whether anti-malware was working, they could upload a standard European Institute for Computer Antivirus Research (EICAR) test file that should trigger an antivirus process. But this approach wouldn't uncover whether an anti-malware solution would detect a trojan, rootkit, or a ransomware execution. The reality was that many breaches were perpetrated through techniques like phishing, which allowed attackers to move laterally and escalate privileges once in the network. Penetration testing wasn't assessing this type of activity, which left the team to make assumptions around the efficacy of their controls.
- **Inconsistent:** To augment penetration testing, the security team conducted red-team exercises as well. The relative thoroughness and ultimate success of these efforts was highly dependent on the skill sets of individual testers. Further, these efforts would vary depending on the specific experience and perspectives of the individuals in charge, which meant there was little consistency or predictability across tests.

The security team increasingly questioned the value and efficacy of these efforts, and started to seek out a better way to validate their security controls.

"We wanted the security assessment process to become faster, more consistent, and more thorough," said the head of information security. "We sought to move away from having to make assumptions and rely on guesswork. We needed to gain better insights into the strength of our existing protections and gain targeted direction on where to make improvements."

A Holistic Solution

To strengthen their security control validation capabilities, the team chose to deploy the SafeBreach BAS platform. SafeBreach conducts automated testing of the team's security architecture, using advanced technology that can execute real-world attacks safely and continuously.

They chose SafeBreach after conducting an in-depth analysis of the solutions in the market. During this investigation, they found other platforms only offered coverage of niche scenarios (e.g., only executing browser attacks). SafeBreach stood out because it offered complete coverage of multi-faceted attacks, including infiltration, lateral movement, and exfiltration.

> "After evaluating the solution, we found that, with SafeBreach, we could proactively predict attacks, validate security controls, and improve the responsiveness of our security operations center analysts. Further, we quickly found that the SafeBreach team was amazing to work with. Our contacts really helped us understand attack automation, including what it is and how to get the most out of it."
>
> **– Head of Information Security**
> **Fortune 500 Drug & Device Company**

A Range of Use Cases

The team was initially focused on applying the SafeBreach platform to a single use case. However, as new projects came up, so did new ways to use the platform. Following are a few of the ways the team uses SafeBreach today:

Tool Validation

Originally, the team had two competing anti-malware solutions running in their environment. While analysts had long suspected that one tool was more effective than the other, it was difficult to gather objective data to validate those suspicions.

With SafeBreach, the team could continuously and safely execute attacks, analyze results, and clearly determine which anti-malware tool was better, confirming the staff's original suspicions. The team was also able to make decisions about which anti-malware tool to consolidate on based on objective evidence rather than gut feelings.

Other projects came up around Internet gateways, proxies, and web filtering. The team used SafeBreach to assess different technologies, and in each case, the solution could point to clear

winners. Further, they could identify weaknesses or gaps in any solution. As a result, before they signed with a vendor whose solution came out on top, they could provide specific requests in terms of errors, issues, or gaps that came up during testing, and ensure they were addressed before the solution was procured and deployed.

"This wasn't general feedback about our opinions or preferences. This was us being able to point vendors to very specific issues, for example, 'Your proxy allowed malware from this site, which presented these specific exposures to our organization.'"

Control Validation

The organization's leadership team was understandably keen to know how susceptible they were to some of the major malware threats making headlines, including WannaCry, NotPetya, and Bad Rabbit. The security team used SafeBreach to determine how safe they were and report on that to management.

"SafeBreach was of vital assistance. We could provide an accurate assessment of our security posture that wasn't based on guesswork or opinions. We could explain, in black and white, where we were covered, where we were exposed, and what we were doing about it. Further, we could continue to report back, showing how we progressed based on those findings."

Combined with a vulnerability management solution, SafeBreach helped the team more intelligently target the problems that had to be addressed most urgently.

Mergers & Acquisitions

The drug and device company has been aggressive with growth and acquisitions in recent years. During a typical year, the team may acquire multiple companies. Once a company is acquired, there's an immediate emphasis on security and how robust the organization's safeguards are. SafeBreach gives them a current, data-driven picture of the new organization's defenses.

Without SafeBreach, the team would have to resort to significant manual testing, which would be a massive undertaking. For example, it would potentially mean testing every one of a company's thousands of servers. SafeBreach enables the team to avoid this manual effort, and quickly provides an accurate picture of the organization's security.

Another advantage SafeBreach provides is in terms of comprehensiveness. With penetration testing, the team was only able to examine the Internet perimeter and one specific application. But, if taking over a medium-size organization, there's little security value in inspecting one application, when there may be 200 or more that could present potential routes for hackers to exploit. With SafeBreach, they can more consistently assess controls across the board.

Industry Benchmarking

With SafeBreach, the team has been able to gain objective data and insights about its security controls and risks. This has given the team the ability to establish benchmarks and knowledgeably compare their environments and controls with other companies in their industry.

Ongoing Benefits & Improvements

By implementing SafeBreach, the security team at the Fortune 500 drug and device development company has been able to realize a number of benefits:

Data-Driven Security Insights

"SafeBreach provided the highly comprehensive metrics we needed to assess the state of our cybersecurity," said the head of information security. "The clarity and lack of ambiguity the solution delivers is brilliant. SafeBreach simulates infiltration, lateral movement, and exfiltration methods. The playbook encapsulates all the major cybersecurity threats. By simulating data breach, data loss, and malware threats, we're effectively assessing the effectiveness of our patching, network segmentation, security monitoring and detection, and prevention controls."

Improved Operational & Cost Efficiency

Now, the security team doesn't need to have people spending time dedicated to running manual testing—they use SafeBreach to do automated testing that is more thorough and more efficient. This frees up staff to focus on more strategic efforts. Further, this automation significantly enhances consistency, which yields improved insights.

"Skilled penetration testers are hard to find, and they will have constraints and time deadlines," said the head of information security. "SafeBreach enables testing that is comprehensive, automated, and continuous. SafeBreach has given us consistency and scale to test security controls in an intelligent way and improve our security."

Enhanced Customer Security & Confidence

Within the company, teams are often still running penetration tests because many customers put that requirement into contracts. This is often because customers may have a standard requirement for outsource service providers that mandates these steps are taken. With SafeBreach, the team can go well beyond these baseline requirements and expectations and demonstrate rigorous attack automation. By exceeding these baseline requirements, the team is better equipped to allay customer concerns and deliver strong safeguards.