SafeBreach

LIFE SCIENCES CASE STUDY

Improving Visibility of Supply Chain Security Controls to Achieve Greater Resiliency

OVERVIEW

The security team at a global life sciences organization approached SafeBreach to investigate how they could gain greater visibility into identifying risk in their supply chain ecosystem. Recent industry attacks infiltrating the supply chain have gained access into organizations' internal infrastructure via third-party software components, causing our customer to focus on identifying and mitigating risk associated within their supply chain.

Challenges

The security team had multiple challenges, all centered around implementing a zero-trust architecture and leveraging the principle of least privilege to protect their network. Building a more resilient supply chain meant enabling comprehensive testing of security controls. This testing was designed for identifying and closing gaps to restrict unauthorized access while also permitting the flow of legitimate traffic between the organization and supply chain vendors.

Business Outcomes

Security Segmentation Validation Decreases Attack Surface

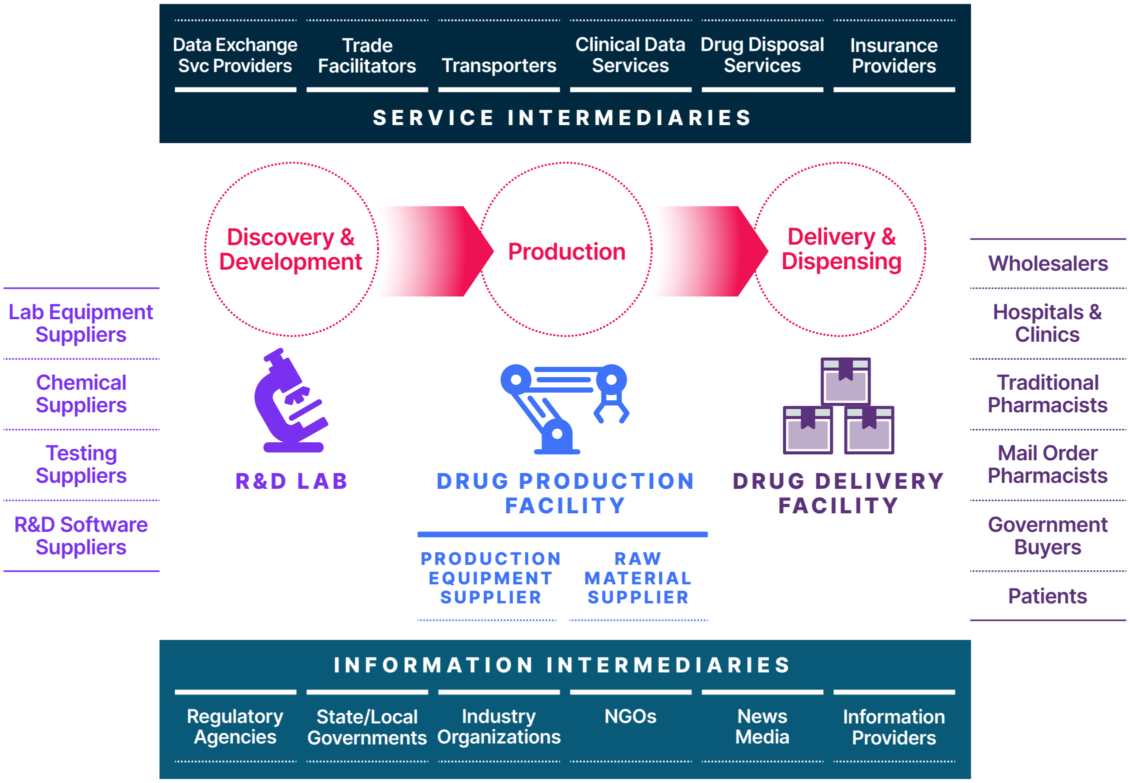
Closing Gaps at Network Perimeter

Greater Visibility into Open-Source Applications

The Life Sciences Supply Chain

Life sciences organizations have traditionally been concerned with managing only third-party suppliers. But, due to the industry's growing complexity, organizations now find themselves in a vast, new, risk-laden supply chain world of a fourth-, fifth-, and even sixth-party partner ecosystem.

This ecosystem includes the cloud services, IT providers, partners, and affiliates that define today's modern extended enterprise. But the global life sciences supply chain is much more far-reaching and includes lab equipment suppliers, chemical suppliers, lab testing suppliers, R&D software suppliers, and more. Once a drug has been approved by the FDA, pharma companies will work with wholesalers, hospitals and clinics, government buyers, pharmacies, and many others to distribute and prescribe their drug or life-saving equipment (below).



Customer Goals

Alongside the security team, SafeBreach identified three customer outcomes leveraging the zero-trust principle to mitigate common attacks arising from breached third-party vendors.

To achieve these outcomes, SafeBreach offered continuous security validation powered by our breach and attack simulation (BAS) platform to help the customer gain visibility into their supply chain ecosystem and associated cybersecurity risk to their infrastructure. The SafeBreach solution would have an immediate impact in reducing their attack surface and decreasing risk associated with the supply chain.

CUSTOMER GOAL #1

Attack Simulation for Network Segmentation Weaknesses

Network Segmentation

Network segmentation is often described as the first approach to insufficient security controls. Segregating information technology (IT) assets from operational technology (OT) assets can mean the difference between a widespread catastrophic attack and a compartmentalized attack with limited damage.

Since many significant attacks to supply chains are a result of vendor mismanagement, using micro-segmentation helps organizations to implement a zero-trust architecture and leverage the principle of least privilege to protect their networks. Additionally, organizations should use automated simulation tools that can continuously validate both segmentation and security controls that effectively prevent lateral movement between network zones.

OUTCOMES

SafeBreach security segmentation validation significantly decreased the attack surface by testing and securing segmentation policies.

SafeBreach Benefits Driving Outcomes

SafeBreach executed attack scenarios that included lateral movement simulation, which identified the locations of segmentation and access control weaknesses. Performing these types of simulations at different times during production operations and across different network segments allowed the security team to gain an enterprise view of potential attack paths and to prioritize mitigation of these vulnerabilities without disruption to their business operations.

Performing these lateral movement simulations significantly decreased their attack surface and challenged the customer's internal networks against different tactics, techniques, and procedures (TTPs) as well as persistent threat methodologies used by attackers to gain access, escalate privileges, and breach additional systems on a network after the initial compromise of a single system.

CUSTOMER GOAL #2

Security Control Validation at the Network Border

Establishing Network Borders

Network borders have multiple layers, and looking at the policy for network border filtering is important to permit the flow of legitimate traffic while closing security gaps in the network perimeter without impacting business operations.

Security teams often think only to protect their private network resources from external attacks when assessing security threats. Today's threats also emanate from malware-infected endpoints, and attackers use these to collect and forward sensitive information from your network or to attack or spam other networks. Organizations are better served when network administrators are equally concerned with threats or unauthorized access associated with outbound connections.

OUTCOMES

Closing gaps at the network perimeter decreased unauthorized access by supply chain vendors.

SafeBreach Benefits Driving Outcomes

Through our BAS platform, SafeBreach conducted continuous validation of the efficacy of security controls at all layers of their network independently and at each stage of the defense process. Validating security controls and identifying gaps with firewall rules allowed the security team to address these proactively and mitigate the associated risk. Since networks are rarely static, with new devices and vendors being added, the security team now validates these controls continuously.

SafeBreach

CUSTOMER GOAL #3

Security Control Validation of Open-Source Applications

Applications Security

Modern applications are a complex mix of proprietary and open-source code, APIs and user interfaces, application behavior, and deployment workflows. Security issues at any point in this software supply chain can expose life sciences organizations to additional risk.

The abundance of open-source marks a fundamental concern when addressing supply chain security. Although open-source is no more or less risky than proprietary code, failure to adequately secure it introduces great risk to your overall organization's security.

A robust automated tool and analysis can provide critical information to keep track of the open-source you're using, the open-source dependencies your applications are built on, and any associated security or licensing risk.

OUTCOMES

Greater visibility into supply chain open-source applications reduced business risk.

SafeBreach Benefits Driving Outcomes

The SafeBreach platform offered an advanced, hybrid, multi-cloud solution to validate security controls in the organization's cloud ecosystem to provide critical information that helped the security team track the open-source dependencies their applications are built on and the associated risk. Continuous security validation provided this information, ensuring they had the most up-to-date and accurate picture of open-source risk.

Understanding the risks associated with applications security, SafeBreach tested the customer's readiness in the cloud with real adversary behaviors to train their cloud immune system.

In Summary

The future demands a different mindset for identifying early warning risk indicators for third-party security controls and new practices to ensure a more secure internal environment. Life sciences organizations today view third-party risk management as a strategic priority for future competitiveness and success in a dramatically evolving world where cyberattacks and supply chain risk remain the entry points for attackers to gain access into your internal network infrastructure.