

CASE STUDY

Netflix DVD Continuously Validates Its Security Environment with SafeBreach

Learn how Netflix DVD moved beyond the limitations of penetration testing by implementing continuous security validation of its network and endpoint security controls with breach and attack simulation (BAS).

NETFLIX

Industry Entertainment Technology

Challenge Netflix DVD needed a more robust, consistent, and reliable way to test how well its security environment—including endpoint security controls—would stand up to attacks.

Solution Netflix DVD deployed the SafeBreach breach and attack simulation (BAS) platform, which executes thousands of proven attacks from its Hacker's Playbook automatically, continuously, and at scale across the entire cyber kill chain.

Results SafeBreach provides Netflix with a hacker's view into where their security environment stops attacks and where it needs additional tuning and configuration. With SafeBreach, Netflix DVD achieved:

- Insights into the strength and performance of network and endpoint security controls, especially from specific types of attack
- The ability to move beyond limitations of penetration testing to identify risks and achieve constant and complete attack simulations
- Actionable insights into firewall performance to block specific attack traffic, without impacting employee productivity

Moving Beyond Penetration Testing

Jimmy Sanders is in the movie business, but what he does may not be as glamorous as red carpet premieres or launching hit series and blockbuster movies. In fact, his job keeps Netflix DVD out of the spotlight. Sanders is the vice president of information security for Netflix DVD and is responsible for the company's cybersecurity.

Netflix DVD faces unique cybersecurity challenges when it comes to safeguarding the activities and access to content for hundreds of millions of its members online, not to mention thousands of employees and the company's assets.

"Cybersecurity is constantly evolving with applications and user behaviors changing and new threats emerging, all of which bring complexity," said Sanders. Netflix DVD wanted to better understand the true state of its cybersecurity and the performance of its security technologies—beyond penetration testing—to identify potential risks.

"The challenge of conducting annual penetration testing is that the tests are done by a person, so the strength of it is dependent on the consultants' knowledge," said Sanders. "You have to trust that you're getting a good team. Additionally, most of the time, pen testers take advantage of vulnerabilities, which is very different from experiencing complete attacks. Lastly, pen tests are limited because you're always going to be a little leery of giving full access to a consultant."

Like most organizations, Netflix DVD knows that simply investing in the latest security solutions isn't enough to thwart hackers. Despite an ever-increasing number of technologies deployed, modern attackers are succeeding more than ever before. In fact, the third edition of the SafeBreach Hacker's Playbook Findings Report found that over 60% of malware infiltration attempts succeed, and lateral moves are successful nearly 70% of the time. In most cases, organizations are continually implementing security controls but not a cohesive defensive strategy—and in some cases, they ignore the risks altogether.

Moreover, rather than helping to stop data breaches, the influx of new technologies adds complexity and increases maintenance costs and overhead. Without validating the configuration and implementation of security controls, there's no way to know whether attacks will actually be prevented. Security teams must emulate hacker techniques to test their own networks from every angle possible to learn if they are truly secure.

In addition to addressing the drawbacks of penetration testing, Netflix DVD sought to validate a variety of its network and endpoint security controls to see how well they stopped attacks, including specific types of hacker attempts.

Lights, Camera, Attack!

“A human pen tester can’t attack your entire system all the time, but attack simulations can be programmed to run continuously. SafeBreach helps us identify risks and issues before a breach actually occurs.”

Jimmy Sanders
VP of Information Security, Netflix DVD

The industry-pioneering breach and attack simulation (BAS) solution from SafeBreach allows enterprises to constantly test security systems to identify potential vulnerabilities. It offered Netflix the potential to achieve its objectives.

The SafeBreach platform successfully simulates hacker breach methods so that Netflix DVD’s security professionals can quantify their actual risks from breaches, validate their security controls, and empower their security red teams.

“SafeBreach augments and strengthens security and enables security teams to be proactive, which enhances cybersecurity,” said Sanders.