



CASE STUDY

PayPal Partners with SafeBreach to Maximize M&A Success

Learn how global online money transfer company PayPal uses continuous security validation with SafeBreach to make risk assessment decisions quickly and accurately to support its business acquisition process.



Industry Financial Technology

Challenge PayPal's security team needed to quickly, objectively, and precisely assess the risk posture of potential acquisition candidates, but manual, labor-intensive approaches were proving far too costly and time-consuming.

Solution With SafeBreach, the team at PayPal established automated testing of acquisition candidate's security architecture, using advanced breach and attack simulation (BAS) to execute attacks safely and continuously.

Results With SafeBreach, PayPal achieved:

- Reliable automation that reduces time spent on manual attacks
- More consistent, accurate testing results
- Data-driven risk assessments with actionable metrics
- More informed M&A decisions, boosting the success of each transaction
- A continuous and complete view of the company's own security posture

Overcoming the M&A Risk-Evaluation Bottleneck

Within most market segments and enterprises today, meeting growth objectives almost always means acquiring assets, technology, or entire companies before the competition. Mergers and acquisitions (M&A) represent large-dollar, high-stakes decisions—especially in the competitive, security-focused world of digital commerce that PayPal operates in. Like many fast-growing organizations, acquiring fintech assets is an important part of PayPal's growth strategy, and the last thing they want is to be surprised by security gaps and vulnerabilities after a commitment is made.

"Mergers and acquisitions come with inherent risks that can be significant, especially if you don't have the time to accurately assess an organization's cybersecurity posture," said PayPal Senior Director of Security Brian Johnson. "We've seen too often that companies are stuck with costly IT assets and a backlog of cleanup and remediation projects, simply because they have neither the time nor tools to support the M&A process. We set out to be different."

For a successful acquisition process, the security team had to move fast, working at the same pace as the acquisition team to eliminate unknowns and gain unbiased and quantifiable risk metrics. The security team needed the ability to analyze both historical and current threats, exploits, and vulnerabilities, so they could create a comprehensive picture of the entire attack surface. Further, they needed to be able to understand the mitigation costs required to bring the target organization up to their standards and risk tolerance—before the acquisition commitment was made.

"We use SafeBreach inside PayPal to gain a continuous, measurable, and complete view of our security posture. It's not only invaluable for acquisitions—it also helps keep us safe every day as a key part of our continuous testing and assurance program."

– Brian Johnson, Senior Director of Security, PayPal

Implementing Fully-Informed, Continuous Risk Assessment

In order to better facilitate security due diligence during M&A events, PayPal's security team opted to deploy SafeBreach's breach and attack simulation (BAS) solution. The SafeBreach platform automates testing of a prospective acquisition target's security architecture, using advanced, patented technology that can execute attacks safely and continuously.

SafeBreach safely executes real-world attacks in production environments to prove where security can withstand such attacks—and where it needs to be improved. While all SafeBreach activities are real attacks, all data is simulated and all methods are executed between simulators. This eliminates false positives and allows security teams to validate their people, processes, and technology, without introducing risks to critical systems or data.

“With SafeBreach, diligence teams quickly get an accurate and quantitative view of a target company’s security posture and operational readiness,” said Johnson. “They can gather risk metrics that inform accurate business valuation and potential mitigation costs.”

SafeBreach has helped PayPal boost its own defenses as well with attacks that run automatically and at scale. Findings are constantly updated and easily filtered to ensure effective remediation, delivering security value over time.

With the platform, teams can identify threats and related risks, such as inconsistent firewall signature rollouts. They can even pinpoint devices that were believed to be isolated but were instead active, vulnerable, and connected to the network—so they can quickly target them for remediation.

Ongoing Benefits & Improvements with SafeBreach

By leveraging the SafeBreach platform, PayPal has been able to realize several key benefits:

Enhanced Speed & Efficiency

With SafeBreach, the security team at PayPal doesn’t need to have multiple people spending significant time running manual tests. This frees up staff 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.

“Because SafeBreach is fast and easy to deploy, IT won’t be the bottleneck, and we’ll execute a consistent process every time,” said Johnson. “Instead of playing catch-up on acquisition projects, IT takes a proactive role in enabling the business to quickly and safely act on opportunities.”

Strengthened Safeguards

SafeBreach enables CISOs and their security teams to make data-driven and fully informed security assessments of IT risk by providing actionable metrics. Using the insights provided by the SafeBreach platform, the team at PayPal is able to identify gaps and weaknesses not only in their own environment, but in the environment of potential acquisition companies, before any acquisition is completed.

“By revealing the vulnerabilities that can actually be exploited, SafeBreach is helping us validate security investments, eliminate exposure to thousands of attacks, and focus on the most critical issues to minimize exposure,” Johnson revealed. “The solution’s complete assessment capabilities help us ensure we can reduce the chance that unknown security weaknesses might have an adverse impact on an acquisition.”

Maximized Return on Investment

With SafeBreach, decision-makers at PayPal can harness security due diligence processes that are objective, consistent, and data-driven. Ultimately, this enables leaders to make more informed M&A decisions, boosting the likelihood of the success of each transaction, and maximizing PayPal’s ability to meet its long-term growth objectives.