PICUS | FORTUNE 1000

CASE STUDY

How a Fortune 1000 Financial Leader Automated Security Validation and Strengthened Cyber Resilience with Picus

Proving Control Effectiveness Continuously for a Rapidly Growing Leader

To support rapid growth, this financial leader replaced slow periodic audits with Picus to measure control effectiveness continuously. By running targeted simulations, they now see exactly which control layers block or miss attacks in real-time. This high-quality intelligence provides a scalable way to ensure protection across their complex global environment.

About the Company

Industry: Financial Services

Headquarters: United States

Number of Employees:
10,000 - 50,000

Global Presence:
Operating in 20+ Countries

Market Rank:
Fortune 1000 Global and S&P 500

Products:

- Security Control Validation (SCV)
- Cloud Security Validation (CSV)

Challenges:

- Rapid growth through acquisitions requiring continuous control validation
- Inability to measure control effectiveness beyond periodic audits
- Limited visibility into which control layers block or miss attacks

Solutions:

- Continuous security control validation replaces outdated, periodic audit cycles
- Targeted simulations show which control layer blocked or missed an attack
- Fast-to-deploy, intuitive platform integrated with enterprise tools

Results:

- Proved control effectiveness in real time versus assuming it
- Enhanced visibility into control performance across complex environments
- Partner-level support with a team that acts quickly on user feedback.
- Clear evidence of security effectiveness for standards like NIST and PCI-DSS.

> ***"With Picus, we can prove control effectiveness in near real time versus just assuming it," the security architect noted. "The intelligence behind Picus is consistently high quality. That's a game-changer for large, complex environments."***
>
> ***"The Picus team is genuinely invested in our success. They act quickly on feedback, continuously innovate, and approach customer relationships like true partners."***

Business Challenge

As a major financial leader growing rapidly through acquisitions, the organization faced an increasingly complex security landscape. Their existing security teams were hampered by fragmented testing methods and a lack of consistent visibility across their global environment.

- **Unsustainable Manual Processes**
  Security validation relied on manual testing and internal audits, which were slow and delayed results.

- **Legacy Tool Limitations**
  While red and blue teams utilized an open-source simulation tools, the process was very limited and failed to provide unified, actionable reporting.

- **Hidden Blind Spots**
  The organization faced hidden defensive gaps that could go undetected between periodic audits.

- **Operational Silos**
  Different security teams worked in silos, making it difficult to assess how effectively controls were operating across the entire infrastructure.

> ***“Our organization grows rapidly through acquisition,” said a security architect at the company. “Every time we bring in new applications and capabilities, we have to ensure the right controls are in place and functioning as expected. We needed a way to measure control effectiveness continuously rather than relying on periodic audits.”***

Solution Overview

To address these complexities, the organization selected the **Picus Security Validation Platform**. The selection followed an extensive evaluation by offensive security, defensive security, architecture, and engineering teams.

- **Automated Security Validation**
  Picus automates the process, reducing validation time from weeks to hours, and offering continuous security validation across a global environment.

- **Seamless Integration**
  Picus was chosen for its intuitive interface and integration with existing enterprise tools.

- **Instant Visibility with Real-Time Insights**
  By using automated simulations, Picus helps uncover defensive gaps, providing the organization with immediate visibility to remediate exposures.

- **Unified Security Teams and Collaboration**
  Picus breaks down silos by enabling effective collaboration between red and blue teams.

> ***“Our evaluation focused on ease of use, clarity of data, and the ability to run targeted simulations that show exactly which control layer blocked or missed an attack,” said the security architect. “Picus stood out because it was intuitive, fast to deploy, and integrated well with our enterprise tools.”***

Gartner Peer Insights Customers' Choice 2025™

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 30 October 2025

WINTER 2026 G2 Leader

4.9/5.0

#1 Solution Provider*

Breach and Attack Simulation

*G2, Breach and Attack Simulation (BAS) Solutions, Winter Grid Report, 3 December 2025