CASE STUDY

Fortune 500 Global Food Manufacturer Strengthens Cyber Resilience with Picus

As a Fortune 500 global food manufacturer operating complex production, supply chain, and IT/OT environments, the organization needed to continuously validate security controls without slowing innovation. By replacing manual testing with Picus Security Control Validation, the security team automated repetitive work, focused on advanced threats, and gained measurable proof of real-world protection. Picus enabled the team to move from assumption-based security to evidence-driven resilience across a globally distributed environment.

About the Company

Industry: Manufacturing

Headquarters: United States

Number of Employees:
10,000 - 50,000

Global Presence:
Operating in 40+ Countries

Market Rank:
Fortune 500 Global and S&P 500

Products:

- Security Control Validation (SCV)

Challenges:

- Manual, time-consuming control testing delayed validation of new systems
- Frequent interruptions prevented focus on advanced threats
- Reliance on vendor claims obscured true protection levels

Solutions:

- Automated continuous security control validation
- Evidence-based reporting with reproducible proof
- Operationalized validation embedded into daily workflows

Results:

- Automated validation eliminated repetitive, manual control testing
- Analysts reclaimed time previously lost to interruptions and repetitive work
- Measurable, real-world validation confirmed actual control effectiveness
- Vendor accountability improved through detailed, reproducible evidence
- Proactive, validation-driven security strengthened long-term resilience

> ***“Cybersecurity is about determining the difference between what’s claimed and what’s true,” the Global Head of Offensive Security explained. “Picus lets us verify whether a control really protects us rather than assuming it does.”***

Business Challenge

Manual control testing drained valuable analyst time, diverting effort from higher-impact threat investigation. A constant influx of validation requests for new machines, environments, and technologies made the work repetitive and disruptive, slowing progress across the organization. Meanwhile, the team needed to move beyond vendor assurances and obtain verifiable evidence of protection effectiveness.

- **Manual, Time-Consuming Control Testing**
  Validation of new machines, environments and technologies relied on repetitive manual testing, slowing progress.
- **Frequent Interruptions to Analyst Work**
  Constant validation requests pulled analysts away from deeper, more complex security analysis.
- **Reliance on Vendor Claims**
  Without measurable proof, the team lacked clear visibility into whether controls actually worked as claimed.
- **Delayed Visibility Into Defensive Gaps**
  Limited insight made it difficult to quickly identify where controls failed and prioritize remediation.

> ***"It's important work," the security leader said. "But it's monotonous and repetitive, and it interrupts the deeper, more complex analysis we need to do. Every time we get pulled away, we lose hours getting back on track."***

Solution Overview

Instead of adding another security tool, the company implemented Picus Security Control Validation (SCV) to continuously test and validate defenses against real-world attacks. Automating repetitive validation tasks saved time and eliminated what the team described as "phantom time," the loss of focus and productivity caused by constant interruptions. Picus enabled the team to verify control effectiveness with data rather than assumptions.

- **Automated Security Control Validation**
  Picus Security Control Validation continuously tests defenses against real-world attack techniques.
- **Replacement of Manual Testing With Continuous Validation**
  Repetitive, time-consuming control tests were shifted from analysts to the platform.
- **Detailed, Reproducible Reporting**
  Reports include timestamps, log data and complete attack sequences that show exactly where and why controls succeed or fail.
- **Operational Integration Into Daily Workflows**
  Validation runs against everything new that gets deployed, without disrupting analyst focus.

> ***"Before Picus, it could take months to demonstrate the impact of our work," the security leader explained. "Now we can share results every month, show where gaps exist, and help other teams close them. Our work is visible, and our value is clear."***

picussecurity.com

Experience Picus *in Action*

GET A DEMO

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
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