PICUS | FORTUNE 1000

CASE STUDY

How a Fortune 1000 Financial Leader Uncovered a Security Gap, Creating Critical Detection Blind Spots

A global data and analytics company that enables organizations to make more informed decisions through trusted insights and advanced technology. It provides solutions in areas such as risk assessment, identity verification, and consumer insights, helping businesses operate with confidence while expanding access to financial and essential services. The organization is committed to innovation, data security, and responsible stewardship of information in an increasingly digital world.

About the Company

Industry: Financial Services

Headquarters: United States

Number of Employees:
10,000 - 50,000

Challenges:

- Hidden detection blind spots caused by firewall log truncation
- Inconsistent configurations broke SIEM visibility across regions
- Pentests and traditional validation missed an exploitable weakness

Products:

- Picus Security Validation Platform (SCV)
- Picus Cloud Security Validation (CSV)

Results:

- Detection coverage jumped from 33% to 100%
- Critical global blind spot identified and eliminated early
- Consistent, reliable detection restored across all regions

Executive Summary

A global S&P financial leader quickly realized value from Picus by uncovering a critical detection vulnerability: attackers could intentionally inflate web request payloads to trigger Web Application Firewall log size limits. Once the predefined threshold was reached, logs were truncated, removing the exact metadata required for SIEM detection rules to fire.

In this scenario, malicious activity executed after truncation was neither properly logged nor reliably detected. What appeared to be a blocked attack could, under specific conditions, become an undetected one.

By identifying and correcting inconsistent log truncation settings across regional firewall appliances, the organization increased detection visibility from 33% (1 of 3 attacks) to full coverage for the affected simulations before full operational rollout. The result was immediate risk reduction and restored confidence in global monitoring.

The Real Risk: How Log Truncation Can Turn "Blocked" Into "Invisible"

From a traditional security mindset, if an attack is blocked, the system has done its job. This case revealed a more dangerous reality.

An attacker who understands how a firewall handles oversized logs can intentionally craft requests that:

- Inflate metadata and URL parameters
- Force the appliance to hit its log size threshold
- Trigger truncation of critical payload components
- Execute malicious actions after truncation

If detection logic depends on full payload visibility, anything removed during truncation may prevent SIEM rules from triggering. In other words, the attack may appear blocked at the control layer, yet critical telemetry never reaches monitoring systems. In certain conditions, subsequent malicious activity may not be blocked or detected at all.

For a financial enterprise operating dozens of internet-facing application entry points across North America, Europe, Latin America, and APAC, this was not a minor logging issue. It was a systemic detection blind spot.

How the Blind Spot Was Discovered

The organization ran simulated web application attacks against its existing firewall infrastructure. The objective extended beyond prevention validation. The security team needed to confirm:

- Were attacks being blocked?
- Were they fully logged?
- Were they visible in the SIEM?
- Were detection rules triggering as expected?

Initial results varied by region. In some environments, simulations triggered alerts and complete telemetry appeared in both Picus and the SIEM. In others, simulations appeared blocked but produced incomplete or missing detection signals. Working jointly with Picus, the organization analyzed expected log artifacts using detailed log-matching criteria. This investigation shifted focus from prevention controls to logging architecture.

The root cause was that several firewall appliances were configured to truncate logs after reaching predefined size limits. When simulated payloads embedded malicious content inside long URL strings, truncation removed the exact data elements required for detection analytics to function. Some regions captured full payload data. Others silently truncated it. Detection visibility across global infrastructure was inconsistent and unreliable.

Why This Vulnerability Is Dangerous

This configuration created an exploitable condition:

1. **Craft requests that inflate metadata and exceed logging limits**
2. **Position malicious payload after the truncation point**

The result: SIEM rules never fire. The attack appears blocked. The threat goes undetected.

This is not a theoretical edge case. It is a controllable configuration issue that can be deliberately exploited, and one that traditional pentests often struggle to uncover.

Immediate Remediation and Measurable Impact

Using Picus Detection Analytics during onboarding, the organization:

- Identified regional inconsistencies in firewall logging
- Pinpointed appliances configured for truncation
- Standardized log capture settings to preserve full event data

Following the configuration update, detection visibility for previously unlogged simulated web application attacks increased from 33% to full coverage in the affected environments. This improvement occurred prior to the full operationalization of Picus.

Business Outcome

With Picus, the organization was able to:

- Uncover a critical log truncation bypass risk
- Eliminate a globally distributed detection blind spot
- Ensure blocked attacks were also fully logged and detectable
- Standardize security control behavior across regions
- Reduce the likelihood of adversaries exploiting log size thresholds

The Takeaway

Blocking an attack is not enough. Security leaders must validate that attacks are:

- Logged completely
- Forwarded correctly
- Detectable by monitoring systems
- Consistently visible across all regions

Picus does not simply test prevention. It exposes whether detection can be intentionally bypassed, even in environments where controls appear to be working. In this case, a single configuration issue had the potential to turn a blocked attack into an invisible one. Identifying it early prevented a serious detection failure before it could be exploited.