



Securing the Financial Frontline:

Continuous Validation for BFSI Organizations with Picus Platform

Picus Security Validation Platform validates control effectiveness across banking, financial services, and insurance environments by safely simulating real-world attacks and providing actionable remediation aligned with industry standards.

Problem:

High Stakes, Low Validation

Financial institutions face elevated risk as attackers target IT weaknesses to breach critical systems.

- **Exposures keep growing** but remain unvalidated and unprioritized across financial environments
- Tools like **IPS/IDS, EDR, DLP, and SIEM** go untested, leaving detection and prevention gaps
- Financial institutions lack **safe, scalable ways** to assess exposure to targeted malware campaigns

Solution:

Picus Security Validation Platform

Picus helps security teams validate defenses across BFSI systems, without disrupting operations.

- **Simulate APT-style behaviors** targeting BFSI to test control effectiveness across hybrid networks
- **Identify and mitigate attack paths** across endpoints, networks, and cloud-based systems
- **Demonstrate cyber resilience** through safe, automated testing aligned with industry standards

Validate Security Controls

Continuously assess defenses across core banking, payment systems, and teller networks, and fine-tune EDR, IPS/IDS, SIEM, DLP, and network segmentation.

➤ **Mitigate Security Gaps 81% Faster** ¹

Be Prepared Against Threats

Simulate ransomware, malware, and financially-motivated attack campaigns to ensure readiness against threats impacting financial systems and services.

➤ **Prevent %200 more threats in 3 months** ²

Compliance with Proof

Generate audit-ready and evidence-backed reports aligned with industrial cybersecurity standards without manual validation.

➤ **Prove Compliance with Confidence & Evidence**

Core Capabilities


- ✓ **Integrated BAS and Automated Pentesting**
Combine Breach and Attack Simulation with Automated Pentesting to continuously assess both control effectiveness and exploitability.
- ✓ **Risk Free**
Picus runs non-destructive and production-safe attack simulations to ensure business continuity.
- ✓ **Adherence to Regulations**
Validate control performance to support critical regulations, GLBA, SOX, PCI-DSS, FFIEC, and DORA, plus global privacy mandates like GDPR and POPIA.

- ✓ **Finance-Specific Threat Coverage**
Leverage the Picus Threat Library with over 26,000 unique attack actions to validate defenses against threats such as LockBit, ClOp, Akira, and Scattered Spider targeting financial systems and services.
- ✓ **Actionable Mitigation Guidance**
Receive vendor-specific detection rules, prevention signatures, and configuration fixes to close gaps quickly.
- ✓ **Rapid Emerging Threat Coverage**
Picus adds attack simulations for the latest CISA alerts and emerging threats within a 24-hour SLA.


¹ Based on analysis of 10M exposures from Early Availability Program participants, ² The Blue Report 2024, Picus Security

Picus Security Validation Platform


Integrated approach to continuous validation




Security Control Validation (SCV):
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation (BAS).




Attack Path Validation (APV):
Run automated penetration testing to eliminate high-risk attack paths.




Exposure Validation (EXV):
Distinguish between theoretical and truly exploitable exposures to prioritize remediation efforts based on real-world risk.



Detection Rule Validation (DRV):
Continuously assess SIEM rules to ensure high-fidelity alerts.



Cloud Security Validation (CSV):
Validate cloud configurations to identify exploitable misconfigurations, privilege risks, and cloud-native attack paths.



Attack Surface Validation (ASV):
Discover exposed assets across environments and gain context-aware visibility into the attack surface.

Validate Across Core Banking, Cloud, and Endpoint Layers

Picus Platform simulates real-world attacks across endpoints, networks, cloud services, and core financial systems, without disrupting operations, to validate control effectiveness across the full financial stack.

Validate Controls Across Financial Layers

Picus simulates real-world threats to test detection and prevention across financial layers.

- Validate security controls for customer-facing applications, SWIFT and ACH payment systems, and transaction databases
- Assess NGFW, WAF, IPS/IDS, EDR, DLP, and SIEM coverage across teller zones, ATM networks, data centers, and cloud banking platforms
- Simulate lateral movement from compromised identities to crown-jewel systems like core banking platforms and regulatory compliance tools (e.g., AML/KYC systems)
- Test detection pipelines across segmented financial environments, such as teller platforms, claims processing systems, and online banking infrastructure
- Validate defenses between internet-facing portals and backend financial systems
- Run simulations based on malware tactics observed in recent BFSI incidents in your region
- Design and run your own attack kill that to challenge your unique financial operations and integration points

“

In financial services, every second of disruption counts. Picus helps us safely test our defenses across environments, uncover the gaps that matter, and fix them before they impact operations.

CISO, Leading Global Financial Institution

picussecurity.com

Experience Picus *in Action*

GET A DEMO



4.8/5.0
Highest-rated vendor*

*Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

© Picus Security. All Rights Reserved.
All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.