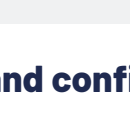
Security Validation for the Financial Industry

Know that your defenses are continuously tested and validated.

A growing digital footprint and the promise of a large payout keep the financial industry at the top of threat actors' target lists. Despite nearly one in five cyber attacks targeting a financial institution, sensitive data, and financial assets must remain accessible to prevent a loss of trust and reputational damage.

Ensure data availability and confidentiality with Automated Security Validation by Pentera.

Validate security controls continuously to protect personal and financial data



Verify proper segmentation and privileges to sensitive data

Prioritize remediation based on exploitable security gaps and improve resilience at scale

Use Cases

Security Posture and Readiness

Validate your security resilience across IT and hybrid environments to quickly identify exposure and minimize impact on your business.

- Track risk exposure trends across your complete attack surface
- Continuously validate tools and processes to ensure readiness for PCI DSS compliance

Ransomware Defense Validation

Safely emulate complete ransomware attacks to test readiness against ransomware in your live environment.

- Act before compromise by pinpointing specific security gaps in your security program
- Test the most prevalent ransomware strains to ensure data cannot be accessed without authorization or exfiltrated during cyber attacks

Credential Exposure Validation

Continuously validate stolen and compromised credentials against your complete attack surface to preempt breaches.

- Reduce manual work by correlating threat intelligence with active credentials
- Identify and remediate credential-sourced exposure based on true business impact

Mergers and acquisitions

Validate the posture of organizations you plan to merge with or have already acquired.

- Assure consistent testing across newly added controls and networks
- Remove risk assumptions by executing tests continuously and via schedule

Segmentation & Access Control

Ensure that data confidentiality and access are working as expected by testing to and from different points on the network.

- Conduct what-if user persona test scenarios to validate access control policies are applied and working correctly
- Verify micro-segmentation initiatives are configured as designed by validating ports and routes are not accessible via certain machines or identities

Testing more frequently ensures you're protecting information that's going to have a massive financial and reputational impact if it ever gets out. We sleep better knowing that our security controls are operating effectively.

Adam Fletcher
Senior Managing Director, Chief Security Officer, Blackstone

Pentera Platform Highlights

Fully Automated
Continuously validate security tools and processes with automated reconnaissance and attack propagation techniques.

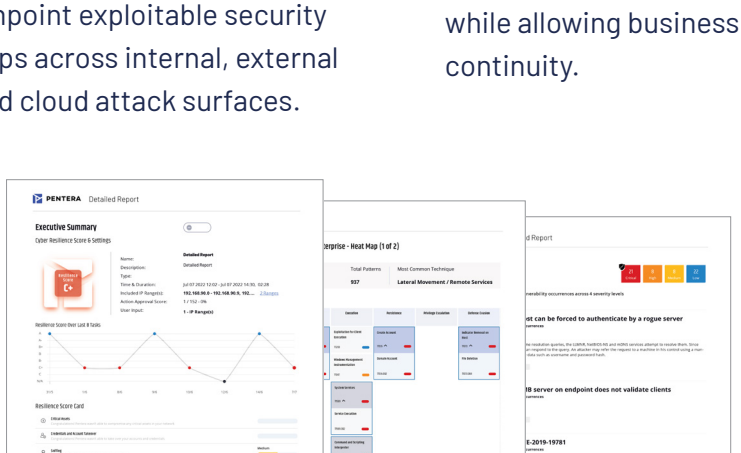
Safe by Design
Safely emulate attacks in production without impacting business continuity.

Distributed Agentless Architecture
Gain seamless enterprise-wide security validation without the need to deploy agents.

Continuous Security Control Validation
Use the latest attacks to pinpoint exploitable security gaps across internal, external and cloud attack surfaces.

Impact Focused
Get evidence-based insights to optimize security programs while allowing business continuity.

Surgical Remediation
Pinpoint the root cause of the attack for efficient remediation alongside step-by-step guidance.



Actionable reporting
Generate instant post-run reports to provide overtime posture benchmarks, executive summary reports to management, and a detailed view of exposures with prioritized remediation guidance. All reports can be easily exported and shared.

Summary

The importance of data availability and confidentiality means financial organizations can't afford to merely assume security controls will prevent the next incident - they need to be confident they will. Trusted by over 130 of the leading banks, credit unions, hedge funds, and asset management companies worldwide, Pentera's Automated Security Validation platform enables financial institutions to continuously improve their security posture through attack emulation. By testing operational resilience against thousands of real-world attack methods, your Security and Red Teams can offload tedious testing tasks and focus their time on edge scenarios. Because emulation is run safely and continuously, security gaps are revealed in real-time against your cybersecurity ecosystem providing an immediate roadmap for improvement and a way to benchmark success.

About Pentera

Pentera is the category leader for Automated Security Validation, allowing any organization to test all cybersecurity layers, over all the attack surfaces, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.