NetSPI™

Proactive Security Testing for Financial Institutions

Table of Contents

Introduction......02

Chapter 1: Comprehensive Attack Surface Management (ASM)......03

The Role of Attack Surface Visibility in the Financial Industry......03

Best Practices for Attack Surface Management......04

Chapter 2: Penetration Testing as a Service......05

Pentesting's Role in the Financial Industry......05

Pentesting Best Practices......06

Chapter 3: Self-Service Attack Simulation......08

The Role of Attack Simulation in the Financial Industry......08

Best Practices for Attack Simulations......09

Partner With the Global Leader in Proactive Security for Financial Institutions......10

Introduction

Banks, insurance companies, and organizations operating in the financial industry are known to have some of the most robust and mature security programs because of the industry's highly regulated environment, consumer expectations, and competitive pressures.

At the same time, they remain a priority target for cyberattacks, given the lucrative nature of their business. After all, adversaries go after the most valuable assets, which constantly puts financial organizations in the crosshairs of malicious actors.

To put things into perspective:

23% of cyberattacks in 2025 targeted financial services organizations making the finance and insurance industry the second most-attacked industry.

(Source: IBM Security X-Force Threat Intelligence Index, 2025)

54% of financial institutions experienced destructive attacks in 2025 a 6% increase from 2024.

(Source: VMware, Modern Bank Heists, 2025)

Financial services data breaches cost organizations an average of $5.56 million and took an average of 241 days to identify and contain.

(Source: IBM Cost of a Data Breach, 2025)

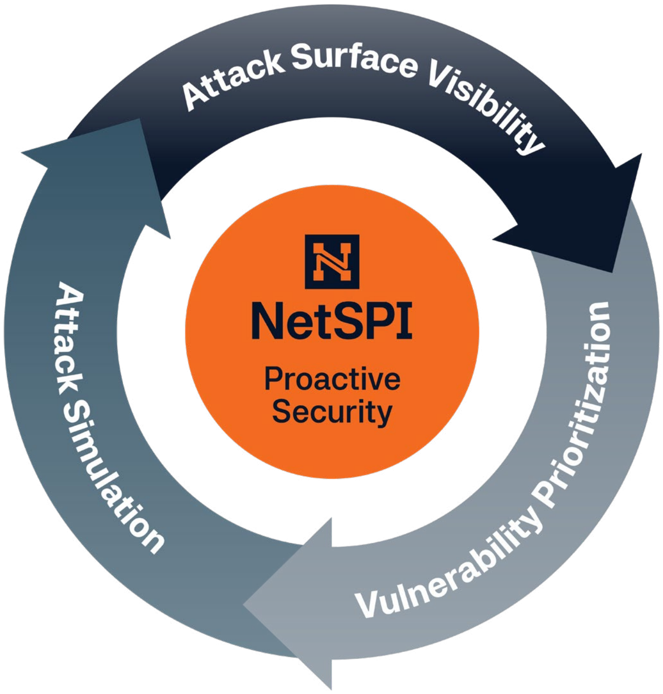
As cyberattacks increase in frequency, sophistication, and impact, it is imperative for financial institutions to reevaluate their proactive security efforts. At the foundation is a comprehensive proactive security testing and vulnerability management program.

In this guide, we break down three core categories of proactive security testing and vulnerability management: comprehensive attack surface management, ongoing penetration testing, and self-service attack simulation.

PRO TIPS

These three solutions within proactive security ultimately help financial institutions:

1. **Improve their attack surface visibility.**
2. **Find and remediate business-critical security gaps faster.**
3. **Measure and improve their detective controls.**
4. **And, most importantly, keep sensitive customer data and company assets protected.**



Overall, these three solutions complement each other as part of a multi-layered, defense-in-depth security program, which is required in most security compliance frameworks, such as Payment Card Industry Data Security Standard (PCI DSS) and Federal Risk and Authorization Management Program (FedRAMP).

CHAPTER 1

Comprehensive Attack Surface Management (ASM)

The Role of Attack Surface Visibility in the Financial Industry

What's one of the greatest challenges security leaders in the finance industry face today? Keeping up with constant change. When it comes to effective asset management and change control, even the most well-trained security teams have room for improvement.

New technologies, devices, cloud accounts, and applications pop up on your external network all the time, often without IT awareness (think Shadow IT). It's up to these security leaders to keep track of all assets and understand if they expose their organization to risk. But how?

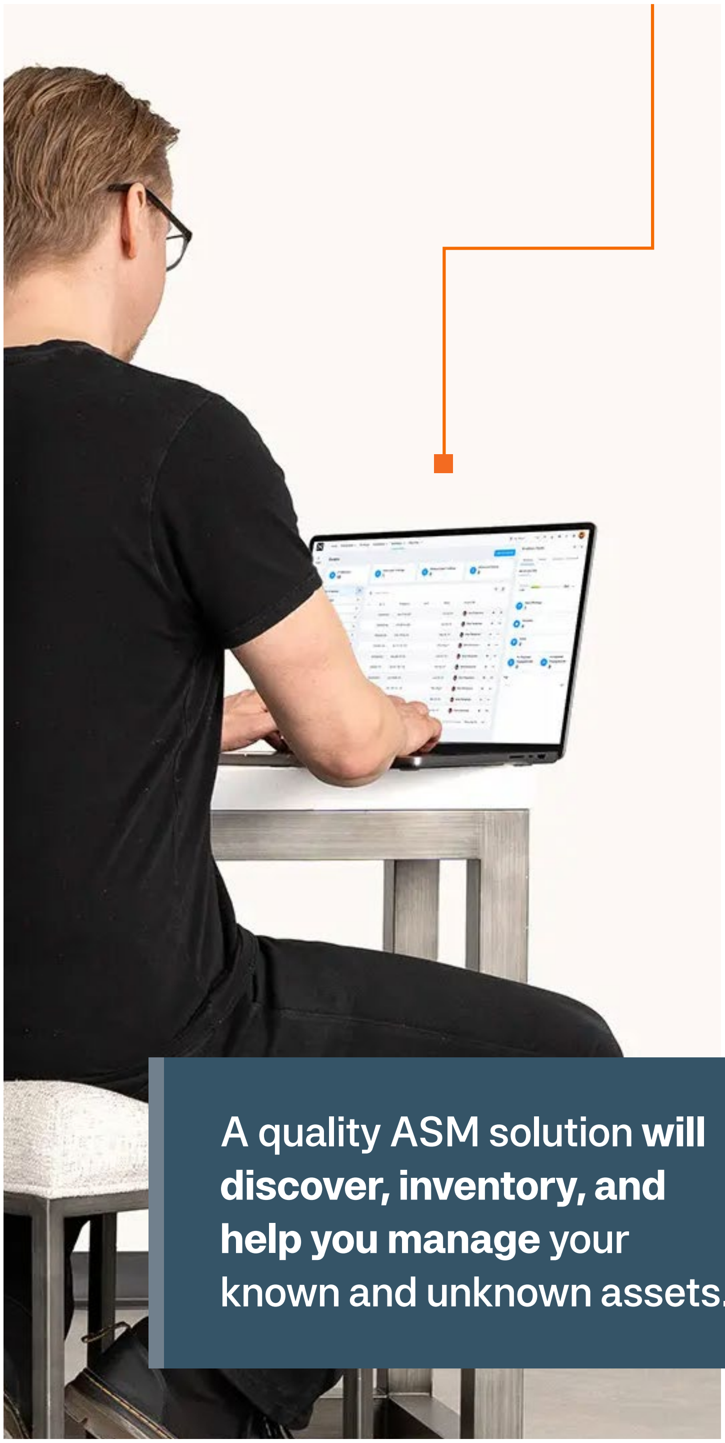
Comprehensive attack surface visibility provides continuous observability and risk assessment of your organization's entire external and internal attack surface. A quality ASM solution will discover, inventory, and help you manage your known and unknown assets.

In tandem with automated asset discovery, ASM solutions identify exposures and validate whether they are points of vulnerability that require immediate attention.

PRO TIPS

Top reasons financial institutions benefit from adding ASM to their security stack include:

1. **Assessment of M&A and subsidiary risk.**
2. **Third-party vendor risk management.**
3. **Continuous observability between periodic security testing.**
4. **Discovery of unknown assets.**



A quality ASM solution **will discover, inventory, and help you manage** your known and unknown assets.

Best Practices for Attack Surface Management

Implement Continuous Penetration Testing

Ongoing, continuous testing is key to an effective ASM program. If your current attack surface management solution is not continuously scanning and alerting, then you're giving adversaries ample time to find vulnerable public exposures before you do.

Ensure your ASM solution uses a multitude of automated penetration testing methods and relies on reputable frameworks, such as open-source intelligence (OSINT), to identify data sources such as business entities, IP addresses, domains, employee information, and sensitive company data on an ongoing basis.

Choose a Comprehensive Solution for Multi-Faceted Coverage

To truly maximize the effectiveness of your ASM strategy, it's important to select a solution that provides comprehensive coverage across all potential attack vectors. Threats can arise from various sources, including the open web, dark web, and overlooked assets like subdomains or forgotten infrastructure.

A robust ASM solution should integrate capabilities such as domain monitoring, dark web surveillance, and detection of misconfigurations to ensure no exposure goes unnoticed. By opting for a toolset that offers multi-faceted protection, you not only gain visibility into a broader range of risks but also empower your team to act proactively. This layered approach to security ensures better alignment with strategic initiatives by minimizing blind spots and reducing the likelihood of critical vulnerabilities slipping through the cracks.

Automate Attack Surface Management, but Rely on Human Expertise to Triage, Validate, and Prioritize

Most of today's ASM solutions are heavily reliant on technology. What's missing in the market are comprehensive solutions that intersect technology with human expertise. It's simple: Humans find vulnerabilities that tools miss and provide business context to each exposure. Ultimately, this approach helps security teams focus on the most relevant gaps to prioritize remediation.

Many organizations rely solely on technology, but the reports that scanners create generate noise for security teams because they contain many false positives. By adding manual exposure triaging to your ASM approach, you can limit the noise and focus on securing the exposures that matter most.

> ***"NetSPI excels for financial institutions subject to DORA regulations*** *through its intelligence-led pentesting aligned with TIBER-EU standards and CREST certification, providing comprehensive validation for stringent regulatory requirements."*
>
> **CHRIS RAY**
> GIGAOM ANALYST

CHAPTER 2

Penetration Testing as a Service

Pentesting's Role in the Financial Industry

Penetration testing is a vital component of any bank, credit union, insurance, or other financial institution's vulnerability management program. Through pentesting, or ethical hacking, you can find, manage, and fix security flaws to reduce the risk of a threat actor gaining unauthorized entry to your environment. After organizations identify exposures, it is important to understand how an attacker might exploit those security gaps. As threat actors increasingly leverage AI to scale their operations and enhance attack effectiveness, the demands on security teams grow exponentially. Combining automated tools with expert analysis helps security teams understand how attackers see your environment and prioritize the vulnerabilities that matter most.

Automation is key, but automation alone is not enough to defend against malicious entities today. Context is critical. And humans provide the context needed to advise on the most important steps for security hardening. Accurate automated actions depend on contextual awareness of systems, a.k.a. understanding what is happening, where, and why, to ensure the right decisions are made with minimal risk of false positives or wasted effort. Context-driven and streamlined remediation is a proactive security measure that connects the dots across the attack surface and internal systems to prioritize the remediation of the most important vulnerabilities.

PRO TIPS

Top reasons financial institutions invest in pentesting include:

1. **Reduce the chance of operational downtime.**
2. **Reduce the risk of ransomware.**
3. **Adhere to regulatory compliance laws and standards.**
4. **Deliver secure software and applications.**
5. **Improve vulnerability management.**
6. **Protect their companies' integrity and customer trust by avoiding data breaches.**

Take NetSPI's PTaaS Platform, for example. Its integration capabilities and API ensure that security insights are not only visible but immediately actionable within your current tech stack and workflows, with the flexibility to customize based on your organization's specific needs. Complimentary integrations span every layer of your security ecosystem, from asset management and identity providers to vulnerability scanning, detective controls, and ticketing platforms.

For decades, financial institutions have undergone compliance-based penetration testing, meaning they only audit their systems for security vulnerabilities when mandated to do so by major financial regulatory bodies such as:

1. Payment Card Industry Data Security Standard (PCI DSS)
2. Federal Deposit Insurance Corporation (FDIC)
3. Office of the Comptroller of the Currency (OCC)
4. New York Department of Financial Services (NYDFS)
5. Federal Reserve Board (also known as the Board of Governors of the Federal Reserve System) (FRB)
6. Financial Conduct Authority (UK financial regulator) (FCA)
7. Office of the Superintendent of Financial Institutions (Canadian financial regulator) (OSFI)

It's time to shift from compliance-driven testing to proactive security testing delivered in an ongoing model.

CHAPTER 2 | *Penetration Testing as a Service*

Best Practices for Pentesting

Adopt an 'as-a-Service' Model

Traditionally, organizations only pentest their environments one or two times annually to meet compliance requirements. During this engagement, a pentester performs an assessment over a specified timeframe and then provides a static report that outlines all of the validated and prioritized vulnerabilities found. While once deemed the status quo, there are many areas for inefficiencies in this traditional model that an ongoing, as-a-Service model fixes.

An as-a-Service model enables security teams to execute and address testing results in near real-time, manage the full vulnerability management lifecycle from discovery to remediation, find critical vulnerabilities that tools cannot, and more. The key to this is reducing the time to identify and fix vulnerabilities in an environment.

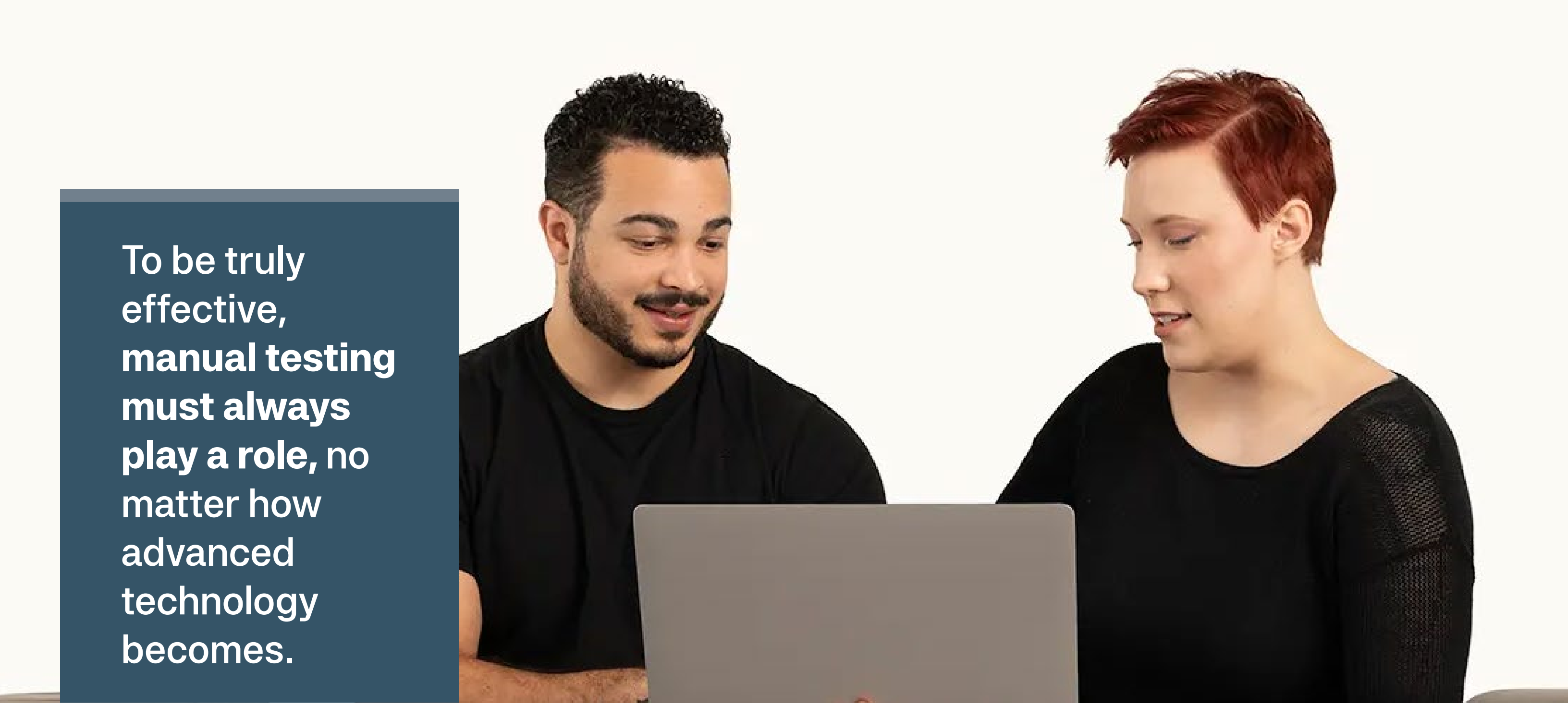
Modern pentesting should operate as a true partnership versus a transactional relationship. With a Penetration Testing as-a-Service (PTaaS) model, pentesters can help security teams become more efficient with their processes and upskill their internal testers by working as an extension of the team. We've seen this type of professional partnership strengthen our clients' skill sets and overall security posture time and time again.

Prioritize Risk Over Compliance

The best IT and security teams understand how to appropriately prioritize security activities based on the inherent risk associated with each business process. To accomplish this shift in approach, they adopt a renewed focus on risk management.

A risk-based security strategy centers on the following: differentiating assets and risks, validating the risks and then ranking them, customizing remediation due dates and SLAs based on your unique risk, pentesting assets based on what needs to be prioritized in the moment, then performing on-demand retesting of the remediation. Throughout this whole process, the ability to quickly pivot as needed is a key differentiator of a true pentesting partner.

Let's go deeper into ranking risks. Risk scoring, or the ability to score/quantify corporate assets based on the risk they pose to a business and compare the risk exposure for each asset, is a necessary step to understand how risks should be prioritized. Organizations can also leverage this type of scoring to rank their different business units or departments, determining which ones have established security measures, and which ones need improvement.



To be truly effective, **manual testing must always play a role,** no matter how advanced technology becomes.

CHAPTER 2 | *Penetration Testing as a Service*

Best Practices for Pentesting

Harness Both Automated and Manual Testing

As cybersecurity teams grapple with the talent shortage, automation has taken center stage. When it comes to pentesting, many leaders have identified automated testing as the model of the future. However, to be truly effective, manual testing must always play a role, no matter how advanced technology becomes.

While there are currently tools and scanners that test for certain vulnerabilities, scenarios, or controls, like input, validation, output, and encoding, the technology cannot automatically determine the intent, feature, or functionality of business assets.

To be successful, pentesting teams must develop a consistent and comprehensive testing methodology to uncover business logic vulnerabilities that tools simply cannot find, regardless of the latest tester assigned.

Take a Holistic Approach to Pentesting

Proactive financial cybersecurity efforts cannot be accomplished in silos. An effective PTaaS program provides coverage across all assets, systems, and business processes. While taking a holistic approach can be challenging, particularly for large organizations, it is crucial to ensure there is a proper inventory of what's being tested, what should be prioritized, and that the list remains updated as organizations add new technology and solutions.

Environments should not be tested separately; instead, they should be viewed as a cohesive ecosystem that must be maintained to continue seamless business operations. Ultimately, this visibility gives security teams a deeper understanding of the necessary pentesting strategy to deploy, which can make all the difference when preventing a data breach.

Next, take this one step further and measure how your detections and Managed Security Service Providers (MSSPs) perform against attack techniques with expert-led attack simulation.

CHAPTER 3

Self-Service Attack Simulation

The Role of Attack Simulation in the Financial Industry

Expert-supported, self-service attack simulation is an emerging proactive security activity, and one that is proving to be pivotal in the financial services industry. The purpose of attack simulation is to validate existing detective controls and help organizations improve their ability to identify and respond to common tactics, techniques, and procedures (TTPs) used in the real world.

During the engagement, attack simulation vendors work with security operations teams to perform simulated attacks against a duplicated test environment and generate security events to determine the level of visibility the target organization has for each TTP.

Financial institutions, particularly large banks, have complex environments that require a multitude of detective controls (e.g. Network IDS, EDR, SIEM) and unique configurations to ensure substantial coverage. Smaller banks and credit unions often employ MSSPs to manage their detective controls, which outsources a portion of security functions to third parties. Expert-led attack simulations are vital to help financial security leaders ensure that their controls and partners are logging, detecting, blocking, alerting, and responding to cyberattacks effectively.

PRO TIPS

Top reasons financial institutions invest in attack simulations include:

1. **Measure and improve your detective controls.**
2. **Detection and prevention of ransomware attacks.**
3. **Validate MSSP coverage and scope.**
4. **Learn from step-by-step instructions to identify and mitigate potential threats.**

Best Practices for Attack Simulations

Set Realistic Goals

One-hundred percent alert coverage is simply not realistic. Even if it were possible to achieve 100% coverage, the false alerts would overwhelm anyone receiving the info. A better approach is to evaluate your current detection coverage and set a more realistic goal. On average, 80% of attack behaviors are missed by common, out-of-the-box detective controls like EDR, SIEM, or MSSPs, according to NetSPI data. Given the coverage promises that out-of-the-box tools make, it's safe to assume that most organizations currently operate with false sense of security.

Between 60-80% alert coverage for common attacker behavior is a more realistic target to work toward. Set your expectations and goals accordingly, and it will allow you to become more focused on the real objective during attack simulation engagements: detecting the most relevant threat actors before they accomplish their goals.

Measure and Improve, Continuously

Measuring your detective controls produces metrics that help you decide where to invest in security. To measure visibility, defense teams must clearly define what attacker behaviors they want covered: What business processes present the most risk to your organization? What do your threat intelligence sources tell you?

Like penesting, attack simulations cannot be viewed as one-and-done assessments. Security teams that continuously run simulations, make adjustments, remediate security gaps, and re-run simulations ultimately work toward increasing their detection coverage in a meaningful and incremental way.

Focus on Behavior, Not Indicators of Compromise (IoCs)

IoCs alone will not provide the detection and prevention we require today. While they are defined based on another company's compromise, not all financial institutions share identical environments and security teams and tools. Furthermore, by the time we define an IoC, it may already be too late, given the speed at which attackers pivot their techniques and approaches.

To remain ahead of malicious actors, security teams must shift their gaze to threat actor-agnostic, behavior-based detections that focus on identifying artifacts, correlations, or anomalies associated with common TTPs. This adaptive approach will allow you to catch attackers earlier on in the cyber kill chain.

> ***"System Intrusion, Social Engineering and Basic Web Application Attacks Represent 74% of breaches."***
>
> VERIZON'S 2025 DATA BREACH
> 2025 DATA BREACH
> INVESTIGATIONS REPORT

Partner With the Global Leader in Proactive Security for Financial Institutions

Securing financial technology environments requires a partner with the expertise, tools, and scale to address today's complex cybersecurity challenges.

Trusted by 90% of the top 10 U.S. banks and many Fortune 500 companies, NetSPI brings more than two decades of experience working with financial institutions of all varieties, providing attack surface management, penetration testing, and attack simulations that meet compliance requirements and equip teams with a proactive approach to security hardening.

With an advanced PTaaS Platform, a team of over 350 in-house cybersecurity experts, and a specialization in more than 50 types of pentests, NetSPI delivers the clarity and precision needed to proactively manage risk today. Learn more about how NetSPI can support your security goals and enhance your program maturity by accessing our Financial Services Solution Brief.