NetSPI

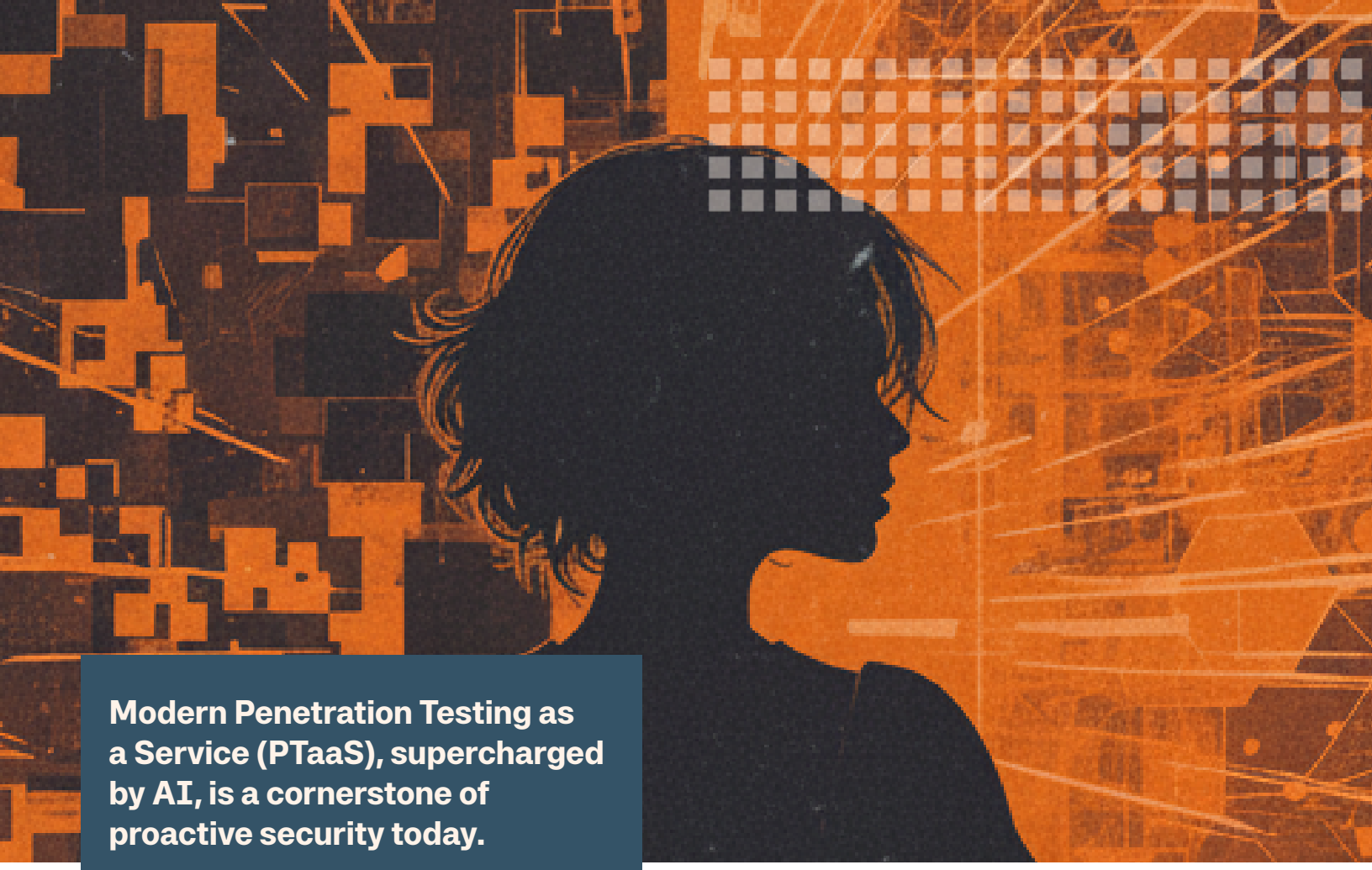
PROACTIVE PROTECTORS

THE HUNTED BECOMES THE HUNTER

The Ultimate Guide to Modern Penetration Testing as a Service (PTaaS)

NetSPI™

Table of Contents



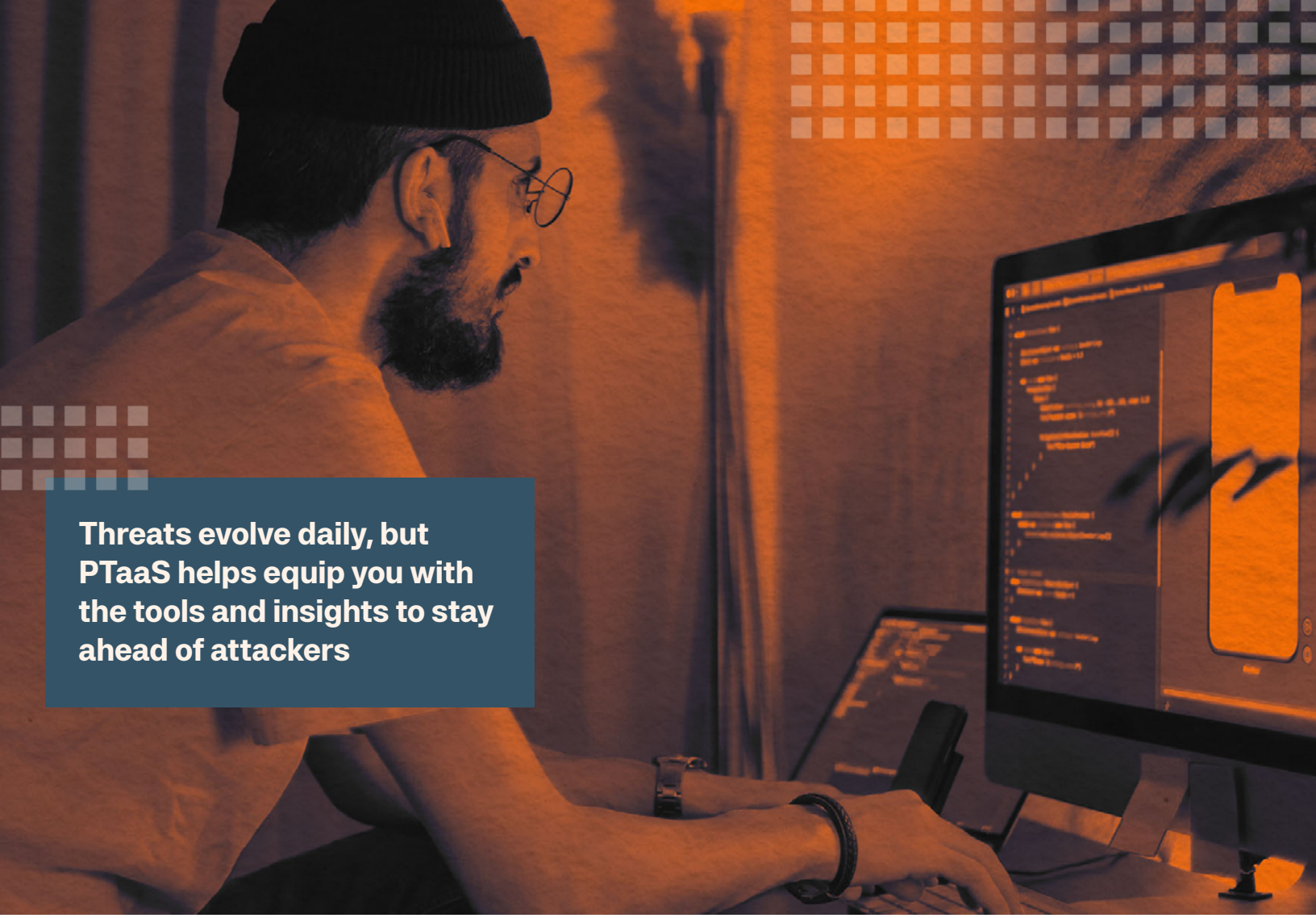
Modern Penetration Testing as a Service (PTaaS), supercharged by AI, is a cornerstone of proactive security today.

Introduction

Your mission is to stay ahead of threats. But legacy, point-in-time testing can't keep pace with today's attackers. Take the MOVEit breach in 2023: one unpatched vulnerability led to data theft across hundreds of organizations worldwide. It showed how fast adversaries exploit weaknesses, and how reactive approaches leave defenders exposed.

That's why Penetration Testing as a Service (PTaaS) has become essential. PTaaS goes beyond one-off exercises to deliver continuous validation, expert guidance, and elastic scale that internal teams alone often can't support. Security programs face peaks and valleys in pentesting demand—whether it's scoping new applications, supporting compliance audits, or responding to urgent risks. PTaaS provides the flexibility to dynamically schedule tests, align with evolving requirements, and scale up or down without slowing the business.

In this guide, you'll learn why PTaaS outperforms traditional methods, how it helps teams focus on the vulnerabilities that matter most, and how it empowers organizations to innovate safely while staying ahead of attackers.



Threats evolve daily, but PTaaS helps equip you with the tools and insights to stay ahead of attackers

What is Penetration Testing as a Service (PTaaS)?

Penetration Testing as a Service is a dynamic approach to security testing delivered through a platform that combines advanced technology with the expertise of skilled penetration testers to provide continuous, scalable, and actionable security assessments. Unlike traditional, point-in-time penetration testing, PTaaS provides teams with real-time visibility into their attack surface, allowing them to identify, prioritize, and remediate vulnerabilities more effectively. By leveraging PTaaS, organizations can proactively manage their security posture, adapt to evolving threats, and ensure compliance with industry standards, all while reducing the delays and inefficiencies associated with legacy testing methods.

Threats evolve daily, but PTaaS helps equip you with the tools and insights to stay ahead of attackers and safeguard your sensitive information. This modern approach to pentesting combines cutting-edge automation, expert human insight, and real-time reporting to give you continuous, actionable intelligence. It's not just about finding vulnerabilities. It's about becoming your organization's first line of defense.

5 Pentesting Use Cases That Are Often Overlooked

At the most basic level, the goal of a traditional penetration test is to uncover vulnerabilities that are potentially exploitable by cyber adversaries. While this is the main objective for a pentester, penetration testing has evolved over the years, and its use cases have, too. Below are five ways your penetration testing provider can add value to your vulnerability management program beyond discovering vulnerabilities.

1. Reduce time spent on vulnerability management administrative tasks
Penetration testing and automation go hand in hand. Automating mundane tasks, such as report generation, ticketing integrations, deduplication, and vulnerability correlation, will save your security team valuable time and resources. Notably, ticketing integrations with systems like Jira or ServiceNow eliminate an extra step in the remediation process.

2. Remediation recommendations and replication instructions
You've received a list of your vulnerabilities. Now what? Without guidance provided by the testers who discovered the vulnerability, assigned remediators are left in the dark. To better support your remediators, look for a penetration testing partner that provides clear guidance along with human-readable instructions on how to reproduce, verify, and remediate a vulnerability.

3. Support with communicating results to various stakeholders
Communication is a common challenge across security assessments. Communicating the results of a penetration test to an audience that may not have a deep technical understanding, the C-suite for example, has proven difficult. Pentesting companies consistently communicate with multiple stakeholders across many technical levels and should be able to help you identify the metrics that matter to each audience and educate them on the business impact of any given vulnerability if it goes un-remediated.

4. Your guide to a mature security program
A penetration testing company's role should not end after the final vulnerability report is shared. Look to your penetration testing team for guidance on how to mature your security program and improve security activities earlier in the product lifecycle.

5. Track the progress of your vulnerability management program over time
There are benefits to working with a single pentest company over time. One key benefit to seek out is the ability to track the status of your vulnerability management program over time. Benchmarking the progress of your vulnerability management efforts is a tangible, data-driven solution to communication security program ROI.

While identifying vulnerabilities remains essential, limiting pentesting engagements to discovery alone leaves significant value untapped. The most effective partnerships transform pentesters into strategic advisors who streamline operations, guide remediation, bridge communication gaps with leadership, and track long-term progress.

When it comes to protecting your company from cyber threats, NetSPI stands out as a leading PTaaS provider.

PTaaS versus Traditional Point-in-Time Testing

Approaches to PTaaS vary, but each one has clear limitations. Traditional penetration testing offers only point-in-time reports that quickly lose relevance. AI-driven autonomous testing delivers speed, but without human oversight, results are shallow, noisy, and lack real-world context. Even some PTaaS platforms that add automation and reporting often fall short, with limited coverage, little ongoing visibility, and minimal expert guidance.

Effective PTaaS must balance automation with human expertise and incorporate context from the entire attack surface. Automation provides the scale and responsiveness modern environments demand, while expert insight ensures accuracy, depth, and relevance to the business. Together, they transform pentesting into a proactive practice, delivering continuous visibility, validated findings, and actionable guidance that empowers security teams to keep pace with evolving threats.

When it comes to protecting your company from cyber threats, NetSPI stands out as a leading PTaaS provider. The table below highlights the key differences between pentesting approaches, showing why NetSPI is the best partner for modern security needs.

Comparing Pentesting Approaches: Traditional, AI Autonomous, PTaaS

Key Feature		Traditional Pentesting	AI Autonomous Pentesting	PTaaS Platforms	NetSPI
Program Management	In Platform Scoping		X	X	**X**
	In Platform Scheduling		X	X	**X**
Pentesting Coverage	Clear Scope & Methodology Transparency	X		X	**X**
	Remediation Testing	X		X	**X**
	Continuous External Network Pentesting		X		**X**
	Coverage Across Cloud, Apps, Network, Harware, etc.				**X**
Collaboration	Comments & Tagging		X	X	**X**
	Vulnerability Status Tracking		X	X	**X**
	Direct Interaction With Testers			X	**X**
Reporting	Trend Analysis And Real-Time Dashboards		X	X	**X**
	Flexible Export Engine			X	**X**
User Experience	Clean, Intuitive, Use-Case Driven Dashboards		X	X	**X**
	Asset Inventory & Contextual Groupings		X	X	**X**
	Self-Service Capabilities		X	X	**X**
	Customizable User Workflows Based On Use Cases				**X**
Vulnerability Management	Severity Scoring & Prioritization	X	X	X	**X**
	Actionable Remediation Guidance	X		X	**X**
	Access To Results In Real-Time		X	X	**X**
	Assign, Track, And Verify Fixes		X	X	**X**
Attack Surface Visibility	Weekly External Asset Discovery				**X**
	Weekly AWS Security Configuration Scans				**X**
	Continuous Domain Monitoring				**X**
	Continuous Dark Web Monitoring				**X**
Attack Simulation	Pre-built and Customizable Play Creation and Execution				**X**
	Automated Detection Validation				**X**
	Coverage Timeline & MITRE ATT&CK Heatmap Reporting				**X**
	Vendor Coverage Comparison				**X**
Integrations	Single-Sign On (SSO)		X	X	**X**
	Ticketing & Remediation		X	X	**X**
	Visibility & Discovery		X	X	**X**
	API Access		X	X	**X**
	Role Based Access Control (RBAC)			X	**X**
	Detective Controls				**X**

In a nutshell, PTaaS is the game-changer modern organizations need. Unlike traditional penetration testing, NetSPI PTaaS brings agility, real-time insights, and customizable solutions to the table. It's like having a digital bodyguard that not only spots vulnerabilities but helps you fix them before they become a problem.

Why PTaaS is Needed Today

In the battle against cyber threats, PTaaS rises as a true hero compared to traditional point-in-time testing.

Challenges with Traditional Penetration Testing

1. **Point-in-Time Testing:** You're only identifying vulnerabilities at a single moment in time, leaving your organization exposed as threats evolve.

2. **Delayed Insights:** Weeks-long reporting cycles slow down your ability to fix issues, putting your sensitive data at risk.

3. **Scalability Issues:** Traditional methods can't keep up with your expanding attack surface, making it harder to stay ahead of threats.

By embracing PTaaS, you become the proactive defender your team needs. With continuous monitoring and real-time insights, you can outpace attackers, remediate faster, and safeguard your most critical information.

Here's how PTaaS transforms you into a proactive defender:

Always-On Vigilance: With continuous testing and real-time insights, you're armed with live vulnerability data and actionable reporting at your fingertips.

Complete Visibility of Your Attack Surface: Gain a clear, all-encompassing view of your security posture by continuously discovering and monitoring internal and external assets, everything from websites to cloud workloads. You'll know where your organization is vulnerable and how to strengthen it.

Battle-Tested Defenses: Expert-led attack simulations mirror real-world tactics, helping you uncover critical weaknesses and fortify your detective controls against the very strategies attackers might use.

Strategic Decision-Making: Integrated dashboards and tailored reporting give you the clarity to track progress and make smarter, faster decisions.

Tailored to Your Mission: Every engagement is customized to align with your organization's unique needs, regulations, and environment, ensuring you're equipped to protect what matters most.

Note: *Not all PTaaS providers offer these features. NetSPI includes internal and external attack surface management as well as breach and attack simulation with PTaaS.*

How AI Enhances PTaaS

AI has significantly advanced PTaaS by offering unmatched scale, speed, and efficiency. It can rapidly process extensive datasets, identify vulnerabilities in real-time, and automate routine tasks, ensuring faster detection and response.

These capabilities empower your security team to handle increasingly complex threats and environments with greater ease. However, despite its impressive capabilities, AI-only pentesting falls short in delivering the depth of analysis and contextual understanding that reliable security testing requires.

Human expertise is irreplaceable when it comes to interpreting nuanced findings, assessing real-world attack scenarios, and providing actionable recommendations. At NetSPI, we combine the power of advanced technology with the critical insights of skilled practitioners to deliver comprehensive and trustworthy security testing.

Here's how AI can supplement PTaaS:

Task Automation & Data Classification

AI enables faster decision-making during security engagements by quickly classifying large volumes of data, allowing teams to identify key insights and act on them more effectively.

Workflow Optimization

Testing team workflows are streamlined through intelligent assistance, reducing the manual labor involved in routine tasks. This allows security experts to dedicate more time to high-value analysis and advanced problem-solving.

Verification & Validation

AI is used to verify that vulnerabilities have been properly discovered, prioritized, and remediated, ensuring that security coverage is comprehensive and no threat goes unchecked.

The Limits of AI, aka Where You Step In

AI is a tool, not a replacement for your insight. While it's great at analyzing data, it can't think critically or understand context like you can. AI models only detect what they've been trained to recognize, so relying on them alone can result in false positives or missed vulnerabilities. That's why your intelligence, intuition, and creativity are essential to uncover novel threats and ensure the picture is complete.

Practical Tips to Integrate AI into Security Testing

1. **Assess Your Needs:** Start by identifying the gaps in your current security strategy. Where can AI make the biggest impact?

2. **Start Small:** Don't try to do it all at once. Test AI tools on specific parts of projects before rolling them out across your entire process.

3. **Combine AI with Expertise:** Let AI handle routine, time-consuming tasks while you and your team focus on delivering deeper insights and critical thinking.

4. **Invest in Training:** Make sure your team knows how to interpret and fine-tune AI outputs. Equip them with the skills to maximize AI's potential.

5. **Track Results:** Keep an eye on key metrics, like how quickly issues are resolved and how many vulnerabilities you detect. Use this data to measure and refine your AI strategy.

Recap: Key Takeaways to Build a Proactive Security Strategy with PTaaS

1. **Move Beyond Traditional Testing:** Traditional pentesting is limited by periodic assessments that leave gaps in your security. PTaaS offers continuous, real-time testing to stay ahead of evolving threats.

2. **Leverage AI for Speed and Scale:** AI can automate repetitive tasks, accelerate threat detection, and analyze vast datasets, allowing you to focus on advanced threat analysis and decision-making.

3. **Combine AI with Human Expertise:** While AI enhances efficiency, human intuition is critical for validating findings, addressing context, and refining security strategies. Together, they create a proactive defense system.

4. **Tailored to Your Organization:** PTaaS adapts to your unique needs, providing comprehensive attack surface visibility, integrated workflows, and actionable insights aligned with your goals.

5. **Practical Integration Tips:** Start small, integrate AI tools into portions of your workflow and train your team to use AI's potential for more strategic vulnerability management.

6. **Proactive Defense is Essential:** PTaaS empowers you to detect and mitigate vulnerabilities before attackers exploit them, solidifying your role as the protector of your company's most sensitive assets.

By adopting PTaaS and combining the latest technology with expert human insight, your team can transition from a reactive security approach to a proactive one, building your company's resilience against today's cyber threats.

Resources to Expedite Time to Value

Ready to put PTaaS into action? Check out these helpful resources to jumpstart your journey:

- **How to Choose a Penetration Testing Company**
- **How Much Does Penetration Testing Cost?**
- **Penetration Testing RFP | Downloadable Template**
- **Web Application Penetration Testing Checklist**
- **Web Application Penetration Testing Sample Report**

About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) with its AI-powered platform supported by more than 350 in-house cybersecurity experts. Specializing in 50+ pentest types, attack surface visibility, vulnerability prioritization, and attack simulation, NetSPI delivers security testing with unprecedented clarity, speed, and scale. Trusted by 90% of the top 10 U.S. banks and many Fortune 500 companies, NetSPI sets the standard for modern AI-driven pentesting. Founded in 2001 and headquartered in Minneapolis, MN, NetSPI is available on the AWS Marketplace. Follow us on **LinkedIn** and **X**.