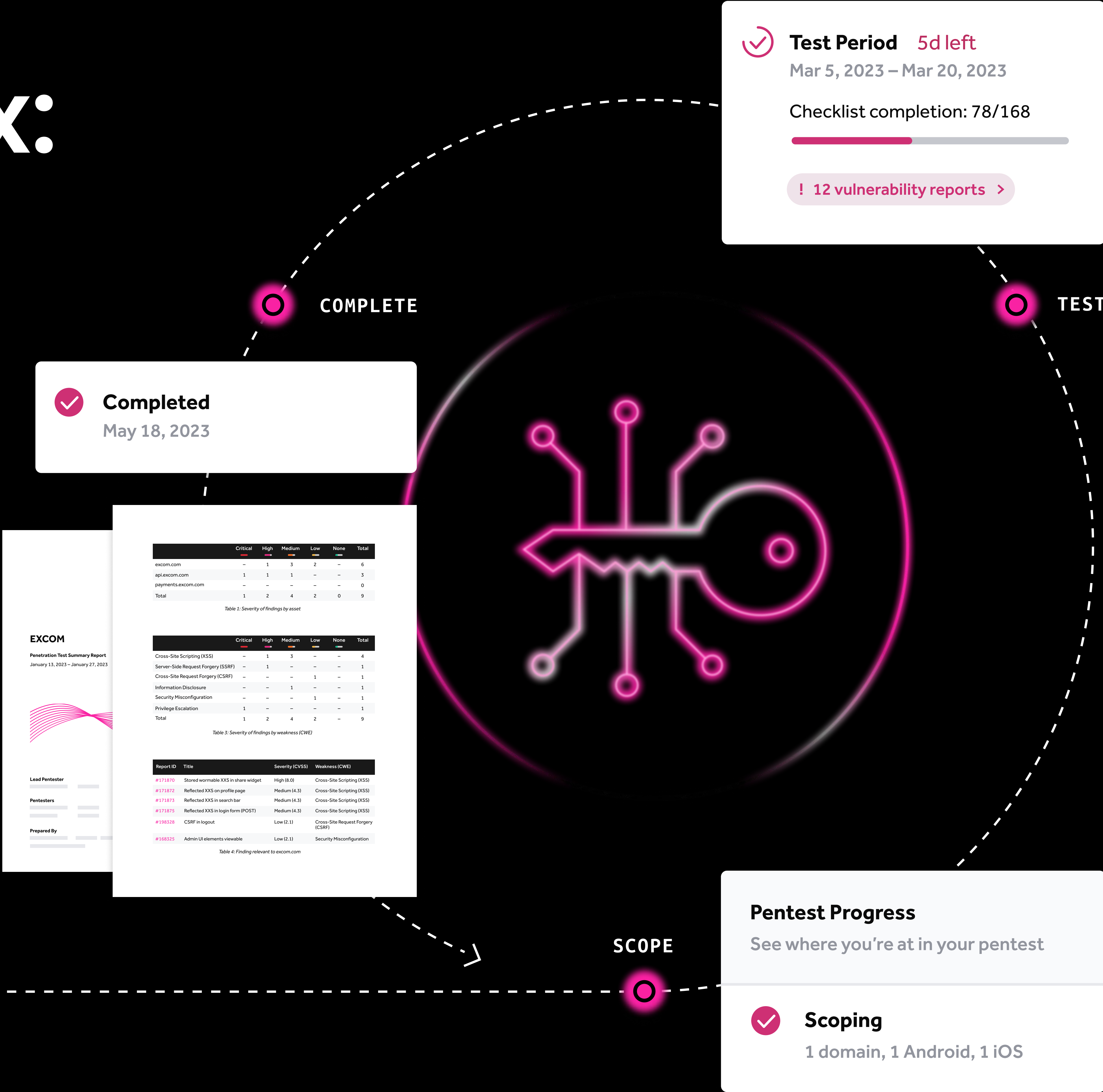
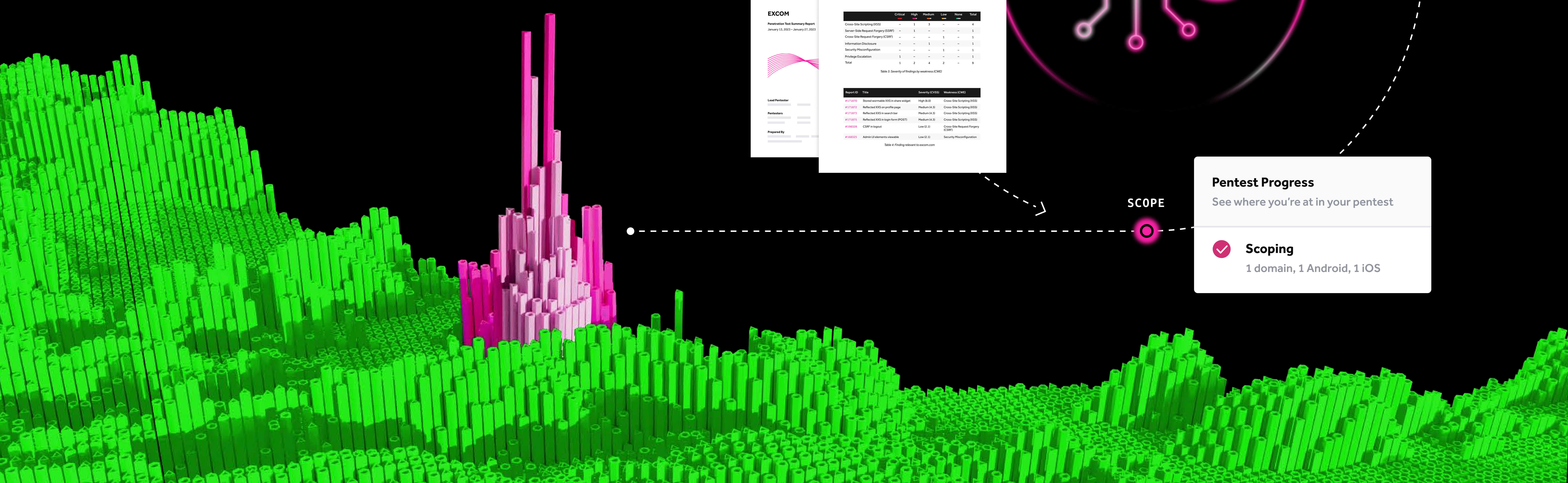
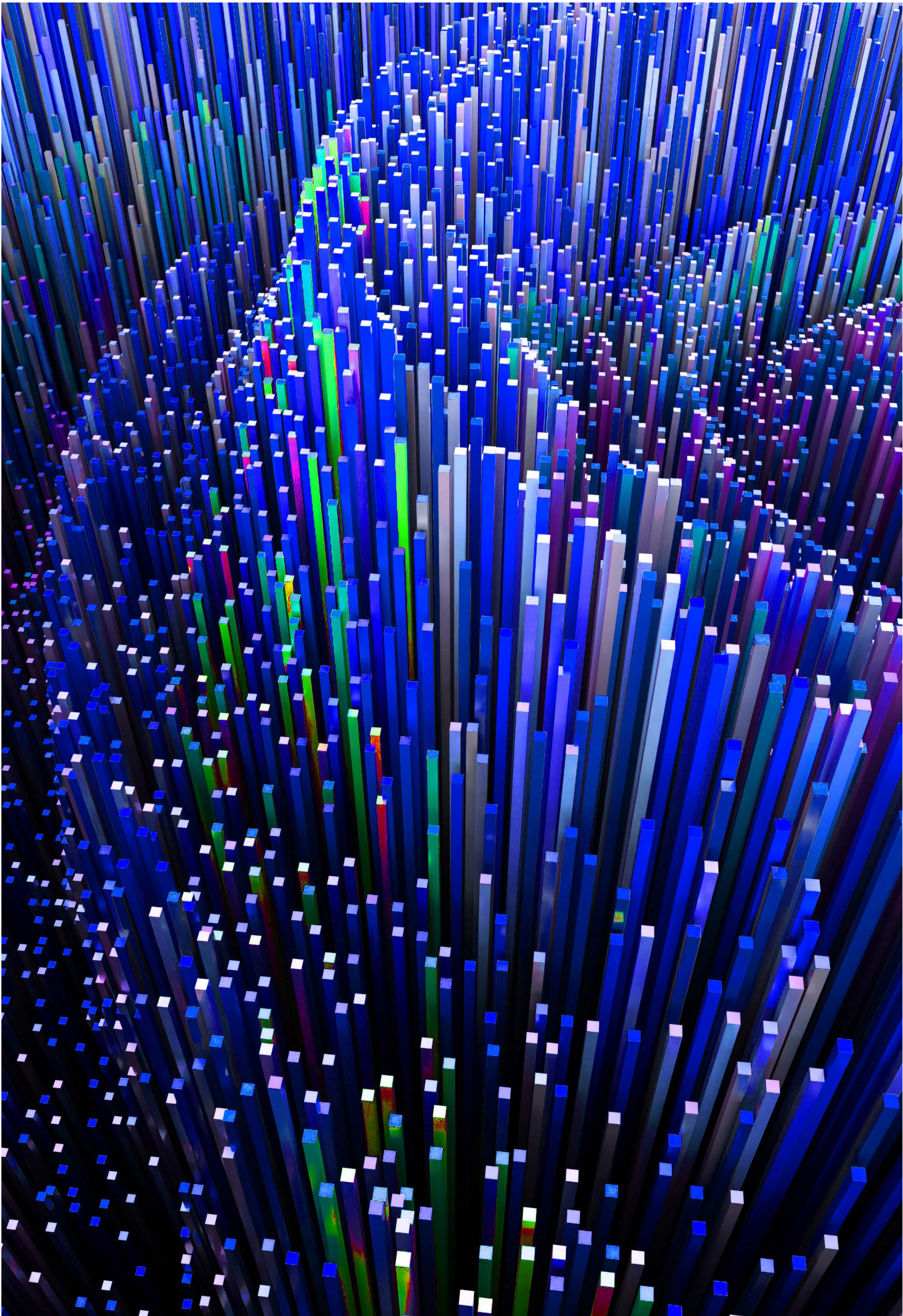


The Pentesting Matrix: Decoding Modern Security Testing Approaches





Contents

Introduction	03
Pentesting Drivers	04
Security Testing Alternatives	05
Decoding the Characteristics of Modern Pentesting	07
Quality	08
Speed	09
Value for Price	10
The Power of PTaaS	11
Conclusion: Ready to Rethink Your Traditional Pentest?	14
Appendix A: Security Testing Evaluation Matrix for Security Leaders	15
Appendix B: Unlocking PTaaS Value and More at Zebra Technologies	17

Introduction

Security leaders understand the imperative nature of pentesting in today's dynamic threat landscape. Pentesting isn't just another task on the checklist; it's a critical component of the larger security management structure, integral to proactively identifying and mitigating vulnerabilities in fast moving software environments.

As a decision-maker, aligning business and security objectives efficiently is paramount. Beyond the internal complexities, choosing the right external partner that seamlessly integrates with your workflow and resonates with your distinct goals can be challenging. With the multitude of security testing methodologies in the market, each claiming supremacy, the path to an informed decision is mired in complexity.

This eBook is tailored specifically for leaders like you, to navigate this intricate realm of security assessments. Our mission is straightforward: to enlighten and equip security professionals by unravelling the complexities of the varied alternatives in this domain. In the coming chapters, we will delve into the nuances of security testing approaches and benchmark them based on three pivotal comparison categories:



1. Quality

Does the approach offer depth, precision, and reliability in its findings?



2. Speed

How swiftly does the approach yield results, and how agile is it in adapting to ever-evolving security landscapes?



3. Value for Price

Beyond the financial implications, what's the real ROI when considering operational efficiencies, coverage, and long-term security posture improvements?

Pentesting Objectives

Organizations need pentesting that supports key business objectives. These begin with basic regulatory and compliance obligations, but ultimately encompass a wider range of security, risk reduction, and business needs.

The most common pentesting objectives include compliance, customer requirements, mergers and acquisitions, internal governance needs, and drivers for a secure software development life cycle (SDLC).

Pentest Progress

See where you're at in your pentest



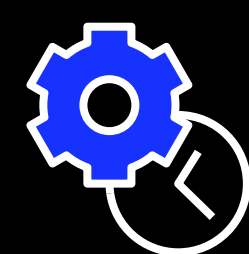
Scoping

1 domain, 1 Android, 1 iOS



Compliance

Every industry has compliance frameworks dictating security measures. Regulations like FedRAMP, NIST, and CISA mandate annual pentests. E-commerce follows PCI DSS, healthcare abides by HIPAA, while SaaS vendors use SOC 2 and ISO certifications. All of these frameworks incorporate regular security assessments.



Meeting customer requirements

Organizations often partner with entities maintaining high security standards. Even if auditors don't request pentests, customers may due to the interconnected risks of digital networks. Consequently, before finalizing deals, businesses increasingly seek recent security documentation like SOC 2 or 6-month-old pentest reports.



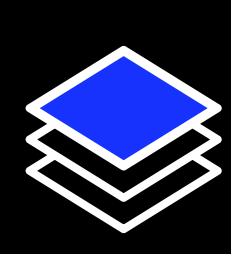
Mergers and acquisitions

Security assessments have become an integral part of the due diligence process for organizations acquiring others or being acquired. Pentests are a critical component of these audits, both as a point-in-time practice and as part of a continuous security testing program.



Internal Governance

As businesses grow and mature, their internal stakeholders demand evidence of rigorous security practices. Ensuring regular pentests not only demonstrates a proactive stance on security but also strengthens trust with the board and audit committees.




Supporting software and product development

Organizations need more frequent and thorough pentests that deliver timely information to support rapid development cycles and allow collaboration between security and development teams. Ideally, organizations choose a combination of external pentesting and internal controls that supports existing development workflows (e.g., DevOps or CI/ CD pipelines) and reliably delivers secure code to production.


Security Testing Alternatives

A variety of security testing alternatives exist, and it can be confusing to compare each of them to identify which might best align with your organization’s needs. Below, we’ve broken out four security testing alternatives, with objective descriptions indicated by ⓘ, and with our analytical opinions on the method indicated by 🔍.

Traditional Pentesting via Consultancies




- Traditional pentests generally follow a fixed schedule, spanning from one to two months, often with a preparatory phase of four to six weeks.
- Pentesters at consultancies are typically generalists, often from non-technical backgrounds, who have obtained basic pentesting certifications.
- The collaboration between the pentesters and the client's security or DevOps teams is often limited, if present at all.




- Historically, consultancy-led pentests have been the preferred choice for many organizations, particularly to satisfy compliance mandates.
- They bring a systematic approach to the table, yet can sometimes seem too routine and transactional: “engage, execute, and exit” until it’s time for the next assessment, perhaps in another six months or a year.
- The financial investment might not always reflect the comprehensiveness or granularity of the vulnerabilities unearthed.

Bug Bounties via Crowdsourced Security Testing




- A bug bounty is a structured program for ethical hackers and security researchers to safely find and report vulnerabilities to an organization in exchange for a monetary reward.
- These programs are delivered through a wider crowd of ethical hackers that offer flexible, evergreen ways for an organization to continuously test its applications and network security.
- They provide access to a community of dedicated, incentivized ethical hackers to find and report security flaws on a continuous basis.

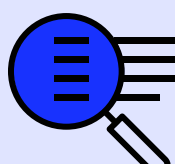


- A bug bounty program can help organizations meet certain compliance standards, but alone they are not sufficient for more prescriptive frameworks where summary reports/letters of attestation are required.
- Bounties and pentesting complement each other by striking a balance between continuous, proactive vulnerability discovery and in-depth, time-bound testing.

Modern Pentesting via Pentest as a Service (PTaaS)




- Delivered through a hybrid approach, PTaaS seamlessly integrates human security expertise with platform-driven capabilities.
- PTaaS grants access to the top tier of crowd-sourced security talent, expanding the pool of vetted and readily available skills during each assessment.
- The approach enables pentesters to deliver real-time results, allowing customers to launch tests rapidly and actively manage their pentest program(s) on a dynamic platform.

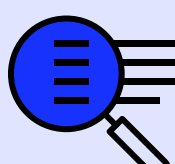


- PTaaS provides comprehensive reporting, aligning with various regulatory and compliance requirements such as PCI DSS, SOC 2 Type II, HITRUST, and FISMA.
- PTaaS alleviates previous painful scheduling delays and enables development teams to move faster and push out their applications in-line with business goals.
- The approach offers frequent and cost-effective pentesting.

Early-Stage Security Measures in the SDLC




- While this guide primarily focuses on pentesting, it's essential to acknowledge security testing measures implemented earlier in the SDLC. Early in the software lifecycle, it's customary to employ secure software design principles, conduct source code reviews, and utilize code scanners.

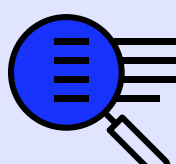


- Recognizing these early-stage practices reinforces the comprehensiveness of your approach and seamlessly complement pentesting and other methods used to test the security of deployed software.

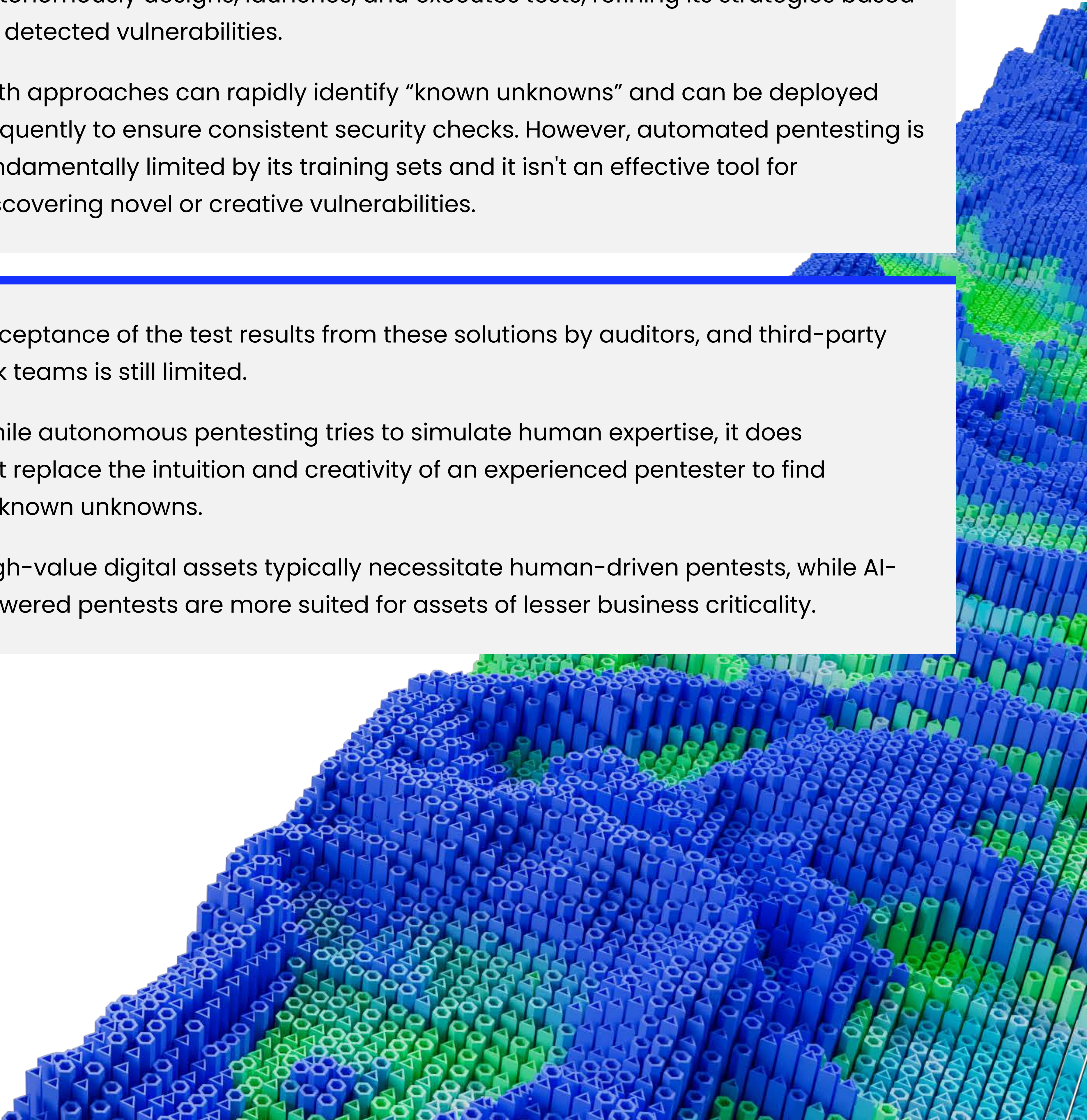
Automated and Autonomous Pentesting





- Automated pentesting is a platform-driven approach that uses predefined scripts or tools to automatically scan, probe, and assess systems for vulnerabilities based on known signatures or patterns.
- Autonomous pentesting, often driven by Generative AI algorithms and advanced machine learning models, is an emergent concept. This self-evolving approach autonomously designs, launches, and executes tests, refining its strategies based on detected vulnerabilities.
- Both approaches can rapidly identify “known unknowns” and can be deployed frequently to ensure consistent security checks. However, automated pentesting is fundamentally limited by its training sets and it isn't an effective tool for discovering novel or creative vulnerabilities.



- Acceptance of the test results from these solutions by auditors, and third-party risk teams is still limited.
- While autonomous pentesting tries to simulate human expertise, it does not replace the intuition and creativity of an experienced pentester to find unknown unknowns.
- High-value digital assets typically necessitate human-driven pentests, while AI-powered pentests are more suited for assets of lesser business criticality.



































Decoding the Characteristics of Modern Pentesting

This comparative analysis leverages the expertise of in-house subject-matter experts and HackerOne’s vast experience—having managed thousands of public and private programs and delivered hundreds of pentests to date. It focuses on the three categories outlined in the introduction—Quality, Speed, and Value for Price. These criteria empower decision-makers to align their choice of pentesting approach with their overarching business, security, and technological objectives. Our methodology evaluates different pentesting approaches against key dimensions of effective security testing, using a scale of 1  to 4 . Here, 1 denotes the lowest performance or value, and 4 represents the pinnacle of performance or value.

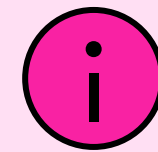


While the results do highlight a preferred method, it's essential to understand that our scoring system reflects the general attributes of each security testing type. The actual effectiveness of an approach may vary based on business priorities, technology stack, and other unique factors. As you interpret the findings, remember to prioritize which of the three categories resonate most with your specific business objectives and consider how your needs and processes might influence the outcomes of different techniques.

Categories	Characteristics	Traditional Pentesting	Bug Bounty	PTaaS	Automated Pentesting
Quality	Human-centric				
	Platform-centric				
	Quality of the Findings				
Speed	Performance & Efficiency				
	Integrations & Feedback				
Value for Price	Coverage				
	Scalability				
	Pentesting ROI				
Average Total Score		2.1	2.4	3.7	2.9


Quality

In security testing, the essence of quality is twofold. First, there's the consideration of whether the testing leans more on the expertise of individual human testers or the capabilities of platforms. Second, there's the matter of how deep the analysis goes and the quality of the findings themselves.



Human-centric vs. Platform-centric: This dimension weighs the reliance on individual expertise against the consistency and scalability of platform-driven approaches.

Quality of the Findings: This aspect evaluates how thorough the testing is and the significance of the identified vulnerabilities.

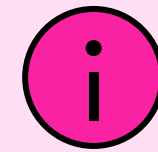


PTaaS leads the pack in the Quality category, due to its fusion of human expertise and platform efficiency. Bug bounties follow closely, benefiting from diverse testers, though depth varies with individual tester motivation. Traditional pentesting, emphasizing depth, ties with automated pentesting, which champions breadth—highlighting the ongoing tug-of-war between human intuition and automated scope in the pentesting outputs.

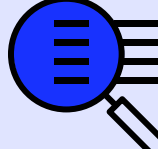
	Traditional Pentesting	Bug Bounty	PTaaS	Automated Pentesting
Human-centric	Relies on the individual skills and expertise of the pentester. There is varying availability of highly experienced or seasoned pentesters.	Draws upon a decentralized pool of testers, each bringing unique skills and methodologies.	A global community of vetted, skilled pentesters are typically complemented by in-house technical engagement managers (TEMs).	While some human oversight and customization is offered, the primary focus is on automation.
	<div></div>	<div></div>	<div></div>	<div></div>
Platform-centric	No platform. While tools are utilized, they often serve more as aids than as primary mechanisms	Platforms facilitate the process, but the primary value arises from diverse human expertise.	Advanced platforms are used to streamline and enhance the testing process, ensuring broader coverage.	Heavily relies on advanced automated tools for continuous scanning and vulnerability identification, with a predominant platform-centric approach.
	<div></div>	<div></div>	<div></div>	<div></div>
Quality of the Findings	Due to scheduling constraints and varying expertise, pentest outcomes can fluctuate in depth, quality, and comprehensiveness, depending on whether a highly skilled or less experienced pentester is assigned.	Due to the diverse range of testers and an incentive-driven model, findings can vary from surface-level tests to the discovery of significant vulnerabilities.	Methodology-driven nature and systematic depth ensure quality results on a consistent basis. A healthy blend of expert oversight and platform capabilities.	Continuously scans for known vulnerabilities with a broad scope; may miss novel or intricate issues that require human intuition.
	<div></div>	<div></div>	<div></div>	<div></div>
Average Score for Quality	2.3	2.7	3.7	2.3

Speed


When evaluating security testing options, the pace at which they deliver results and how seamlessly they integrate into existing processes are paramount. This comparison breaks down each approach, assessing the performance and the speed of the testing, as well as the feedback mechanisms.



Performance and Efficiency: This dimension assesses how quickly and efficiently each option identifies and reports vulnerabilities.




Within the Speed category, PTaaS outperforms the rest, excelling in real-time results and streamlined feedback loops. Automated pentesting follows closely, primarily driven by its rapid, automated processes. Bug bounty and traditional pentesting are tied; while bug bounty benefits from its decentralized nature and immediate alerts, its variability in feedback depth parallels the detailed but time-intensive nature of traditional pentesting—revealing a trade-off between immediacy and depth in these approaches.

	Traditional Pentesting	Bug Bounty	PTaaS	Automated Pentesting
Performance and Efficiency	Time-intensive and project-based, initiating can take weeks to months due to tester and project manager availability. Findings are shared post-testing.	Incentive-driven and decentralized, vulnerabilities are quickly reported by testers, yet the efficiency of findings varies with each tester's expertise and motivation, even with parallel testing.	Faster setup and systematic approach compared to traditional methods, due to a combination of human expertise and platform capabilities.	Very rapid and continuous; however, as an organization grows, automated pentesting tools must be regularly updated to manage increased complexity.
				
Feedback and Integrations	Without real-time integrations, detailed feedback is provided solely in the final report. Manual processes lead to extended durations for tester communication and issue resolution during the test.	Notifications are immediate upon vulnerability submissions, but feedback depth varies by tester. Platforms provide APIs or integrate with popular ticketing and security information systems.	Real-time results coupled with expert insights enhance understanding and action on findings. Modern platforms prioritize integrations with prevalent security and IT tools, promoting seamless workflows and immediate collaboration.	Provides real-time vulnerability alerts. While feedback tends to be generic (worded by generative AI) and lacks human analysis, it can effectively identify known vulnerabilities by cross-referencing with vulnerability databases.
				
Average Score for Speed	2	2.5	4	3.5

Value for Price

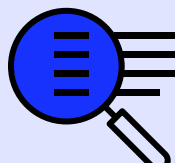
Security leaders have the essential and difficult role of justifying the value of security testing for the price tag associated with it. When evaluating the economic justification, two crucial factors stand out: the breadth and depth of the testing (coverage and scalability) and the return on investment (ROI) for the testing process. By breaking down each security testing option based on these features, security leaders can provide a much more clear picture of the value offered. When reviewing the results, it's important to note that the efficacy of each approach can vary based on the specific implementation, the expertise involved, and the exact goals of the pentesting activity.



Coverage: Measures the comprehensive scope of the testing, ensuring that various areas of potential vulnerabilities are scrutinized.

Scalability: Assesses the ability of a testing method to efficiently expand or adjust in response to an organization's growing and changing needs.

Pentesting ROI: Evaluates the cost vs. benefit equation, providing an understanding of the tangible and intangible returns for each testing option.



PTaaS tops the Value for Price category, due to its blend of manual and platform-driven capabilities. Automated pentesting stands second, with its scalable yet generic coverage. Meanwhile, bug bounty and traditional pentesting tie: while the former provides broad but unpredictable coverage at a variable cost, the latter offers depth but at potentially higher long-term costs, underscoring the importance of aligning choice with specific organizational needs and budgets.

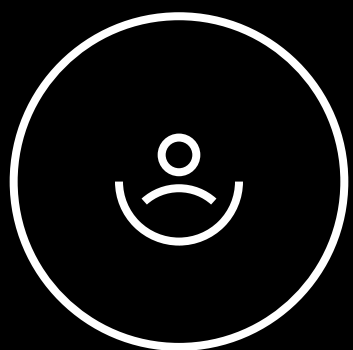
	Traditional Pentesting	Bug Bounty	PTaaS	Automated Pentesting
Coverage	Often focused on specific areas of concern; might not have the bandwidth to cover all assets.	Offers broad coverage from diverse testers, but depth varies with each tester's skill and motivation. Unlike pentests, bug bounties don't ensure directed efforts, potentially affecting consistent coverage.	A balanced approach, leveraging both manual expertise and platform capabilities checks to ensure comprehensive checks and systematic coverage.	Provides broad coverage (rather than in-depth) via automation.
	<div></div>	<div></div>	<div></div>	<div></div>
Scalability	Often involves thorough, in-depth evaluations, yet its scalability is challenged by less frequent continuous or periodic checks.	Influenced by the attractiveness of bounties, the complexity of the environment, and the clarity of program guidelines.	PTaaS can be activated on demand, providing scalable options tailored to an organization's depth requirements, ensuring flexibility and timely security assessments.	Easy to set up, scale, and automate periodic and continuous checks.
	<div></div>	<div></div>	<div></div>	<div></div>
Pentesting ROI	Long-term costs are higher because of manual efforts and limitations in repeating pentests or integrating results. While reports are given, they often lack the standardized metrics seen in platform-driven systems.	Costs fluctuate, primarily linked to vulnerability discoveries. While the platform-driven approach typically includes metrics, consistency can vary due to individual tester reporting.	Provides a balanced cost-to-value ratio through predictable SaaS pricing and continuous insights. Platforms deliver detailed metrics, trend analytics, and benchmarks, simplifying ROI tracking.	Heavily automated, these platforms shine in offering real-time metrics, KPIs, and benchmarks. However, false positives from automated systems demand manual reviews, potentially diminishing the projected ROI by consuming extra time and resources.
	<div></div>	<div></div>	<div></div>	<div></div>
Average Score for Value for Price	2	2	3.7	3

The Power of PTaaS

When scoring against Quality, Speed, and Value for Price, PTaaS stands out as a flexible approach that can adapt to an organization’s specific needs, and is priced accordingly. PTaaS is the best option when combining robust testing and deep analysis with the opportunity to quickly set up and complete an assessment.

HackerOne Pentest combines the convenience of a centralized platform with the expertise of our pentester community to excel in all three categories.

“Through 120 dedicated hours with 3 testers from HackerOne Pentest, we deepened our understanding of our attack surface and addressed 1 critical and 5 high-risk findings. This collaboration enabled us to secure our network and web applications more effectively.”



Toan Ha
Application Security Engineer
Katalon Inc.



HackerOne Pentest Quality

72%

of HackerOne Pentest customers value HackerOne pentesters’ ability to detect hard-to-spot vulnerabilities and discover unknowns within their attack surface.

18%

of HackerOne Pentest findings are high or critical severity—which is nearly double the industry standard.

HackerOne Pentest Speed

4.4
days

HackerOne Pentest customers receive their first vulnerability report within 4.4 days on average.

86%

of HackerOne Pentest customers receive their first vulnerability report in less than one week.

HackerOne Pentest Value for Price

8,500+

vulnerabilities have been found via HackerOne Pentest in three years.

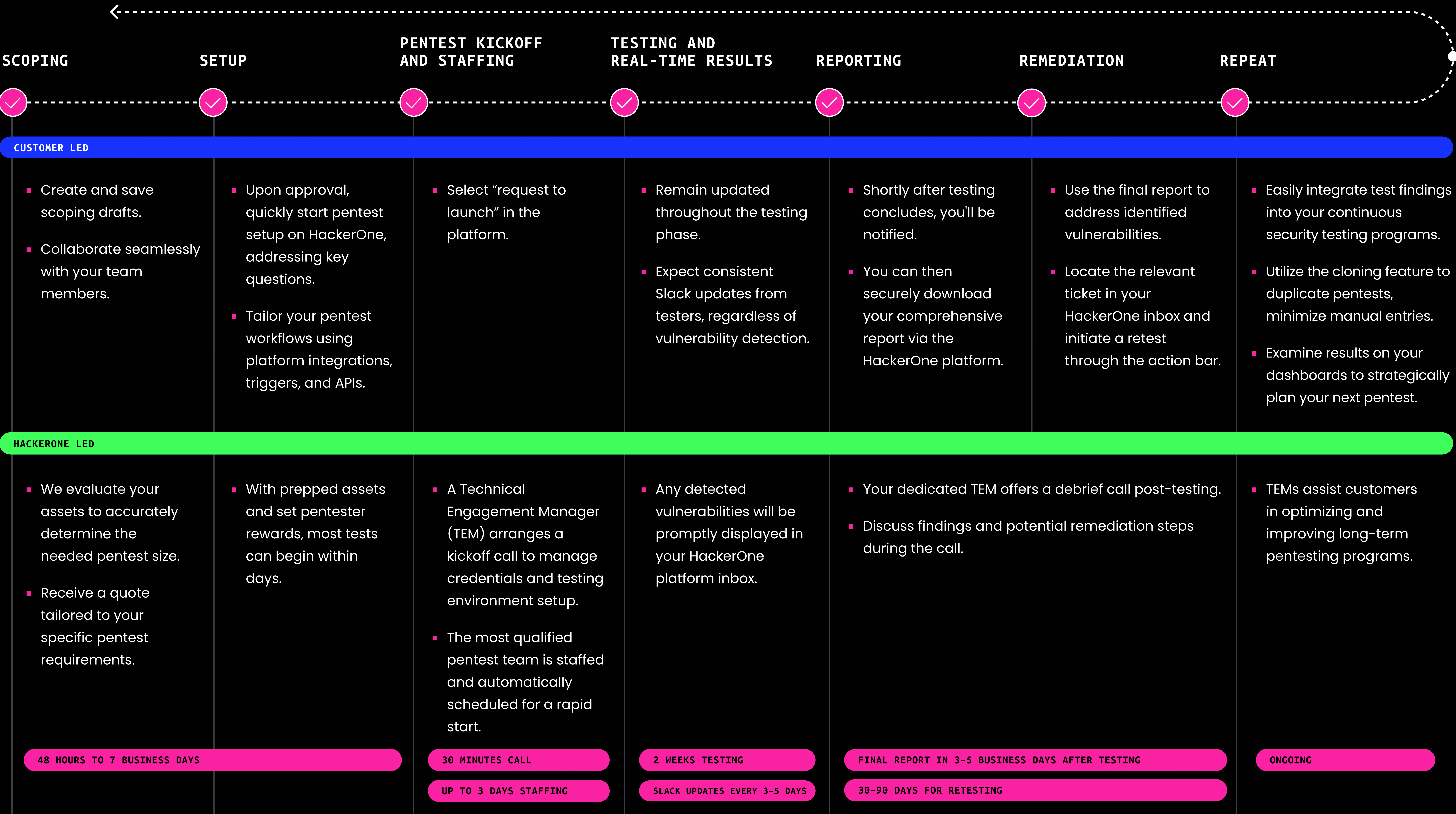
61%

of HackerOne Pentest customers identify more vulnerabilities with HackerOne than with traditional pentest vendors.

HackerOne Pentest supports many compliance frameworks, so organizations can achieve compliance for multiple frameworks through one streamlined platform.




Streamlined Pentesting Process




HackerOne's Trusted Pentester Team

HackerOne pentesters are an elite subset of the ethical hacking community that is hand-selected and professionally vetted by HackerOne. As part of the vetting process, we evaluate the pentesters' professional experience and performance on existing HackerOne security testing programs. The vetting also takes into account the pentesters' certifications and other credentials, including OSCP, OSCE, OSWE, and CREST. We maintain these high standards to deliver to our customers experienced and credentialed testers they can trust to deliver impactful results.




HackerOne's pentesters are meticulously chosen from the ethical hacking community. Only those displaying exceptional skill, outstanding productivity, and impeccable conduct move forward to levels qualified for participation in HackerOne's PTaaS programs. This elite group comprises less than 10% of those registered on the platform, representing the pinnacle of global security testing expertise.


Meet Some of Our Top Pentesters




Leandro
(none_of_the_above)




Miguel Regala
(fisher)




Trev
(SoWhatSec)



Leonel
(delisyd)



Joel
(niemand_sec)



Rodrigo
(rororodrigo)

What Sets HackerOne's Pentesters Apart

8500+

vulnerabilities uncovered by the pentesters in the last 3 years.

11 valid

vulnerabilities are reported on average, per pentest.

+50%

of our pentests unveil at least 1 vulnerability within first 3 days.

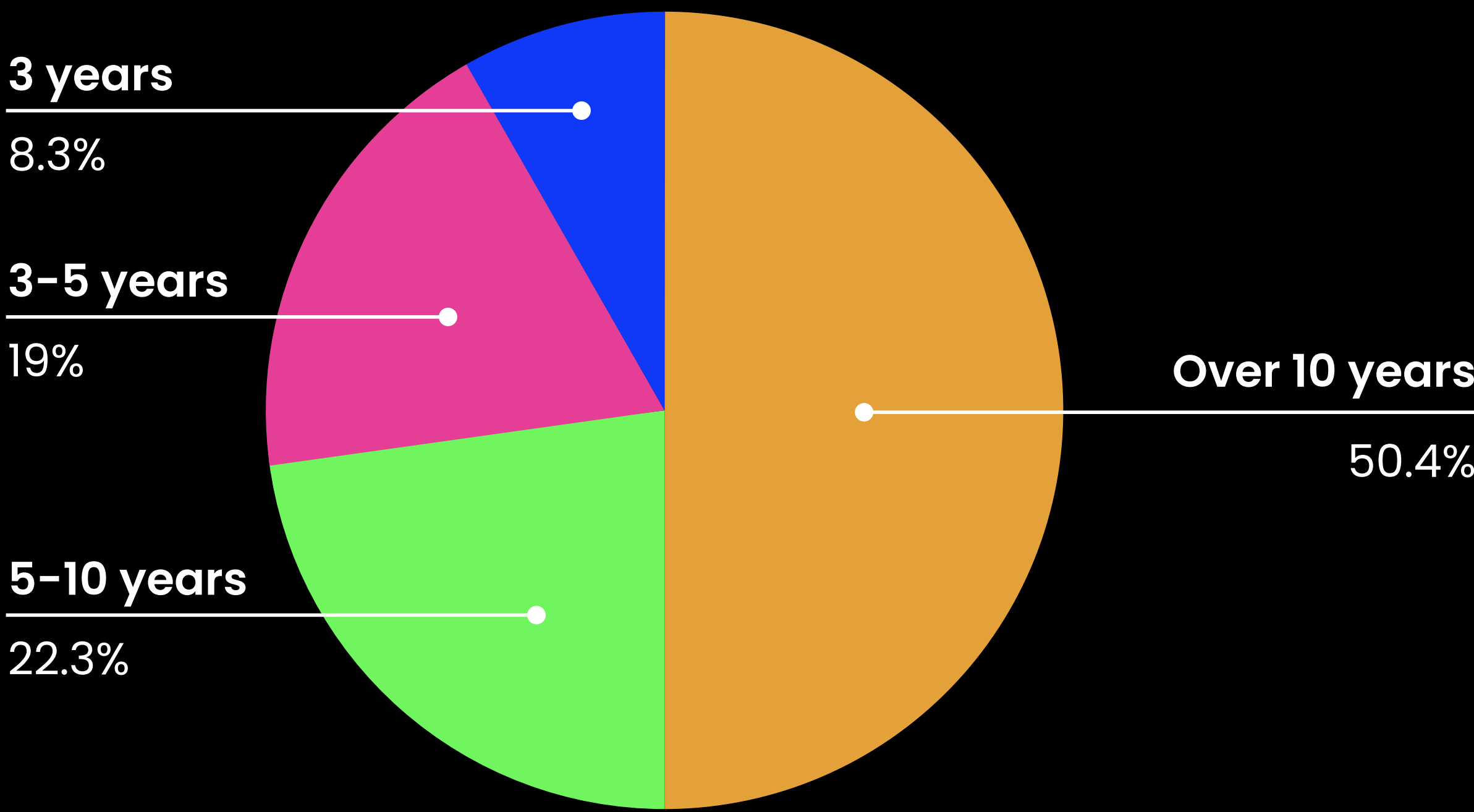
74%

possess 5+ years of industry expertise.

+70%

of our customers value pentesters' abilities in finding elusive vulnerabilities.

Pentesting and Industry Experience



*Source: Analysis of statistics captured from the HackerOne platform.

Ready to Rethink Your Traditional Pentest?

HackerOne Pentest transcends routine compliance checks, delivering in-depth insights, efficiency, and actionable results tailored to your business and security needs. **Tell us about your pentesting requirements, and one of our experts will contact you.**



Visit the [HackerOne Pentest web page](#) for more information and how to get started.

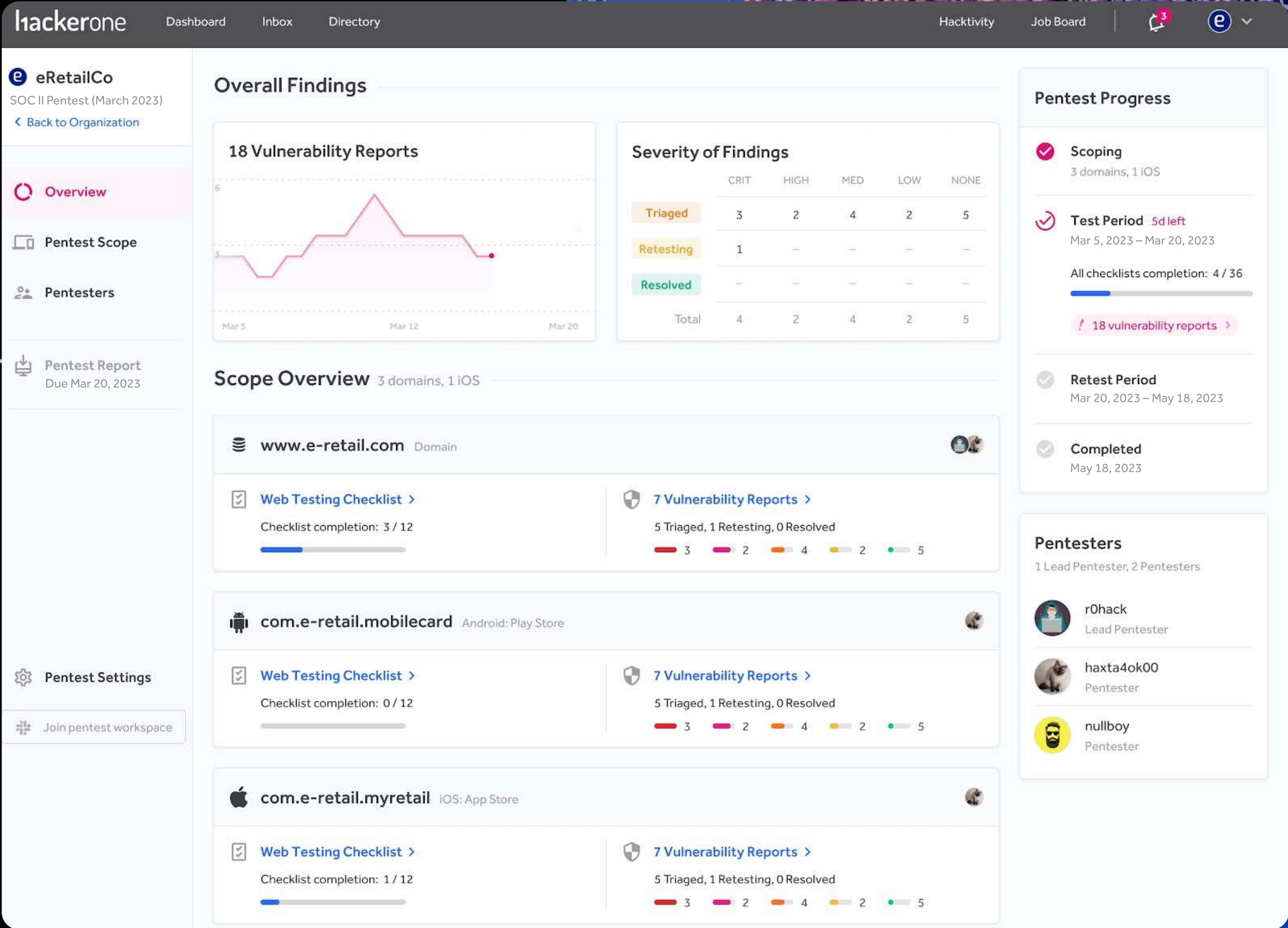


[Watch a demo](#) to see how HackerOne redefines pentesting.

“HackerOne’s pentest capability has helped us identify ways to strengthen our products by uncovering inconsistencies we may not have been alerted to previously.”



Dallan Wagner
Senior Product Security Engineer



Appendix A: Security Testing Evaluation Matrix

This checklist can be used to evaluate each of the four security testing options presented in this eBook: traditional pentesting, bug bounty, modern pentesting via Pentest as a Service (PTaaS), and automated and autonomous pentesting. Security leaders can use this checklist to determine whether their focus is on quality (depth), speed (performance and efficiency), or value for price (overall ROI), then use this as a guide to decide on the most suitable path for their organization's needs.

Quality	
Human-centric vs. Platform-centric	<div><input type="checkbox"/> How well does the approach balance human expertise and platform capabilities?</div> <div><input type="checkbox"/> How intuitive is the platform or interface for managing pentests?</div>
Depth of Analysis	<div><input type="checkbox"/> How deep does the analysis go? (Surface-level vs. deep-rooted vulnerabilities)</div> <div><input type="checkbox"/> Are the findings actionable and significant?</div> <div><input type="checkbox"/> Does the approach provide context and insights beyond the vulnerability, such as potential business impact?</div>

Speed	
Performance and Efficiency	<ul style="list-style-type: none">❑ How long does it take to scope and launch a pentest?❑ How much manual oversight or interaction is required throughout the process?❑ How quickly after initiation do you receive the first set of findings?❑ Can the testing scale up or down based on the size and complexity of the application being tested?❑ How easy is it to adjust or expand the scope of testing?
Feedback and Integrations	<ul style="list-style-type: none">❑ How easily does it integrate with existing systems, tools, and workflows?❑ Are there prebuilt integrations or APIs available?❑ Is the feedback actionable, with clear remediation steps?❑ Is there real-time collaboration and reporting between teams and pentesters?
Retesting	<ul style="list-style-type: none">❑ How easy is it to initiate a retest, especially after remediation?

Value for Price	
Coverage and Scalability	<ul style="list-style-type: none">❑ Is there a capability for continuous testing or periodic checks?❑ Can the frequency of these checks be adjusted based on organizational risk appetite and change rate?❑ Is retesting offered as part of the pentest?
Pentesting ROI	<ul style="list-style-type: none">❑ Does the cost of the service compare with the perceived value and results delivered?❑ Are metrics and benchmarks provided to quantify the impact of the pentest?❑ Is there an automated way to measure the improvement in security posture over time through repeated testing?❑ Are insights provided substantial enough to inform broader security and IT strategy, beyond just immediate vulnerabilities or compliance needs?



Appendix B: Unlocking PTaaS Value and More

As a world leader in digital products, solutions, and software, with over 10,000 partners across 100 countries, Zebra Technologies empowers its customers (including 86% of the Fortune 500) with a broad portfolio offering and regularly launches new products through organic innovation and acquisitions.

With a business transformation in full swing, Zebra needed to double down on its security approach. Each new product or acquisition increased the potential for unknown assets that could cause gaps, making them more vulnerable to breaches and security risks. Traditional pentesting provided some coverage, but the tests took time to spin up and were costly. Seeking a better solution, Zebra reached out to a leading research firm, which recommended HackerOne. A rapid proof of concept provided impressive results, fueling internal decision makers' interest and trust in the value of a vetted ethical hacker community combined with PTaaS.

[Read the full Zebra + HackerOne story.](#)

"From the workflows that make life easier to the speed of our pentests and the quality of our product development—all these benefits have lead to accolades from the executive team, developers, and customers."

Dr. Jasyn Voshell, Dir. of Product and Solution Security, Zebra



CHALLENGE:

Traditional Pentests

- Slow, traditional pentesting with insufficient reports led to gaps in testing the attack surface.
- Security was not included early enough in development, leading to developers working separately from security.
- No formal process was in place for reporting vulnerabilities, exposing the company to more risk.

SOLUTION:

HackerOne Pentest via PTaaS

- A collaborative partner that works closely with Zebra to keep its attack surface covered
- The ability to spin up rapid pentests with findings that go beyond traditional scanners
- On-demand reports and feedback that help Zebra drive root causes back into the SDLC

RESULTS:

A Scalable, Security-First Mindset

- Customer, partner, and key stakeholders trust has increased.
- Pentests give them visibility into findings in real time, allowing them to fix and retest while the test is ongoing.
- Teams can immediately plan efforts to remediate any weak spots.
- Speed and security of delivery practices support revenue and lower risk.

"HackerOne can stand up our pentests three to five times faster than traditional firms."

Dr. Jasyn Voshell, Dir. of Product and Solution Security, Zebra

hackerone

HackerOne pinpoints the most critical security flaws across an organization's attack surface with continual adversarial testing to outmatch cybercriminals. HackerOne's Attack Resistance Platform blends the security expertise of ethical hackers with asset discovery, continuous assessment, and process enhancement to reduce threat exposure and empower organizations to transform their businesses with confidence. In 2021, HackerOne was named a 'brand that matters' by Fast Company.

Trusted by



Book a meeting with a security expert
and scope your pentest today.

Contact Us