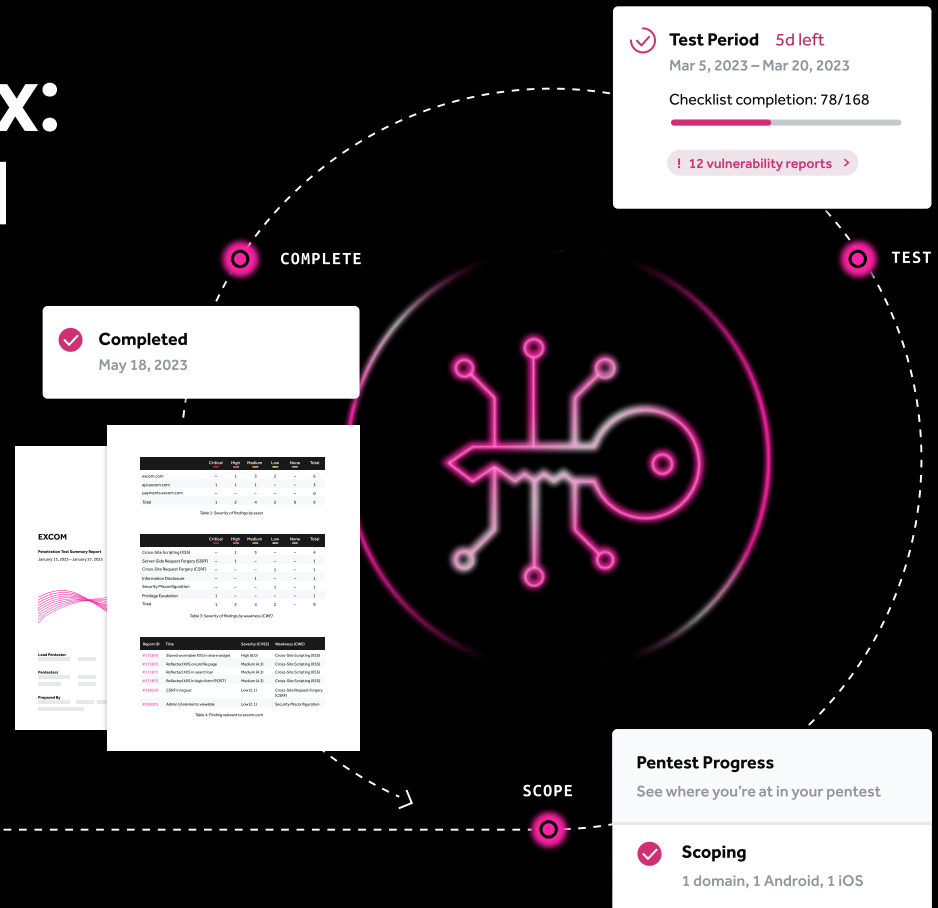
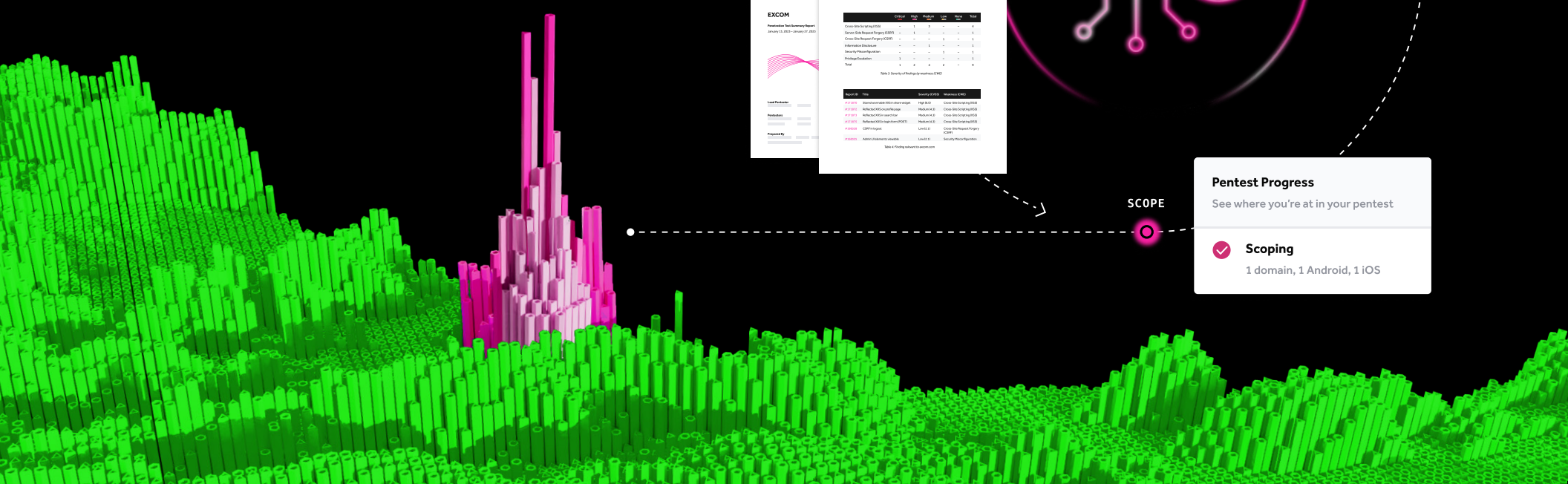
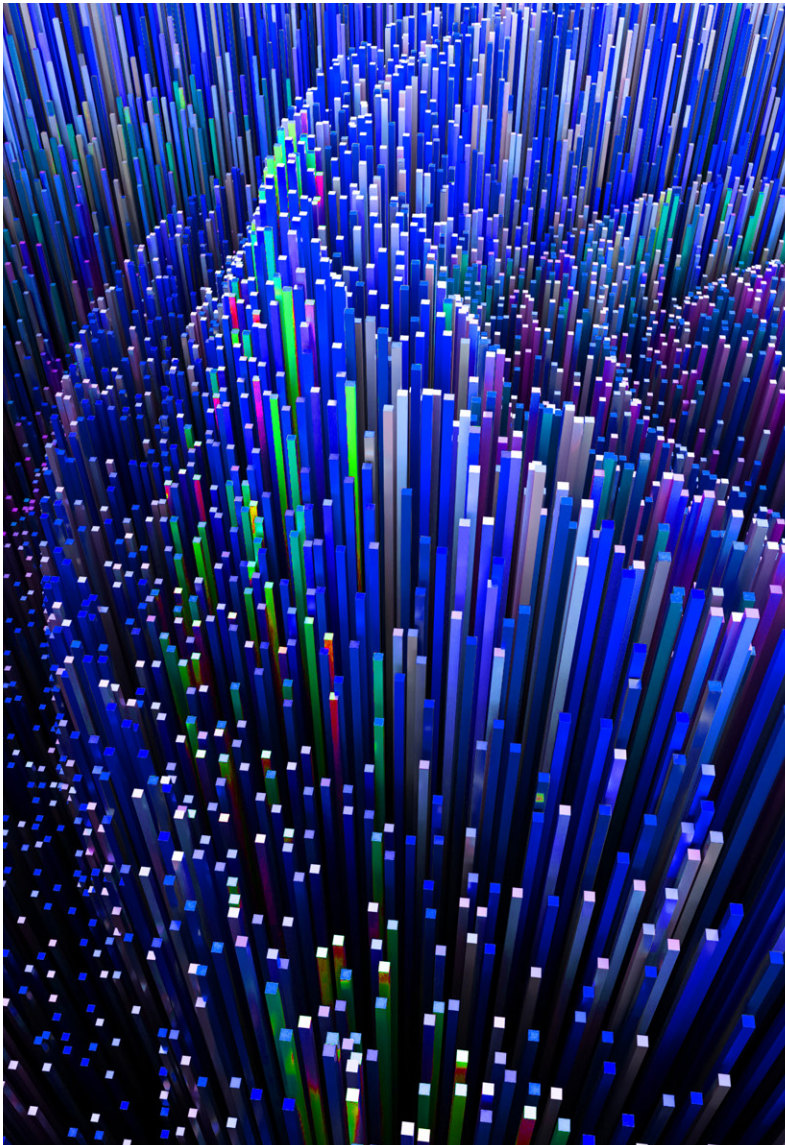


The Pentesting Matrix: Decoding Traditional and Modern Approaches





Contents

Introduction	03
<hr/>	
Pentesting Objectives	04
<hr/>	
Pentesting Options	05
<hr/>	
Decoding the Characteristics of Modern Pentesting	08
Effectiveness	09
Efficiency	10
Value	11
<hr/>	
The Power of Community-driven PTaaS	12
HackerOne Attack Resistance Platform for Best-in Class PTaaS	13
HackerOne's Trusted Pentester Team	15
<hr/>	
PTaaS or Bug Bounty?	16
<hr/>	
Ready to Rethink Your Traditional Pentest?	18
<hr/>	
Appendix A: Pentesting Evaluation Matrix	19
<hr/>	
Appendix B: Unlocking PTaaS Value at Zebra	21
<hr/>	

Introduction

Pentests are essential for software developers and deployers, ensuring compliance and verifying the security of new releases. Different pentest methodologies offer different benefits, and many of the more “traditional” methods seem redundant or are cumbersome to manage.

Modern pentesting approaches use freelance security researchers and advanced software platforms to streamline the process. However, with many vendors focusing on other core security products and services, it's important to make sure that the pentest offering you choose provides you both *the compliance and verification you need and the findings you'd expect* from skilled security researchers.

An ideal pentest not only assures security coverage but also uncovers critical vulnerabilities, assisting the engineering team in enhancing their security practices—without excessively consuming the customer's time, attention, or money.

Given the variety of models, vendors, and methodologies available, how do organizations pinpoint the ideal pentest for their needs? This eBook clarifies the diverse alternatives and guides security professionals in making informed choices to make the most of their investment and achieve the best results. We delve deep into the characteristics of various pentesting services and technologies, benchmarking them against three comparison categories:



1. Effectiveness

Effectiveness encompasses the method's ability to deliver reliable and precise findings, ensure coverage and reporting across all systems in scope, adhere to compliance standards, and use diverse tester talent for a well-rounded view.



2. Efficiency

Efficiency speaks to the operational aspects: the ease and speed of procuring the pentesting service, the real-time provision of results and analytics, continuous and clear communication throughout the process, and seamless software development life cycle (SDLC) integrations.



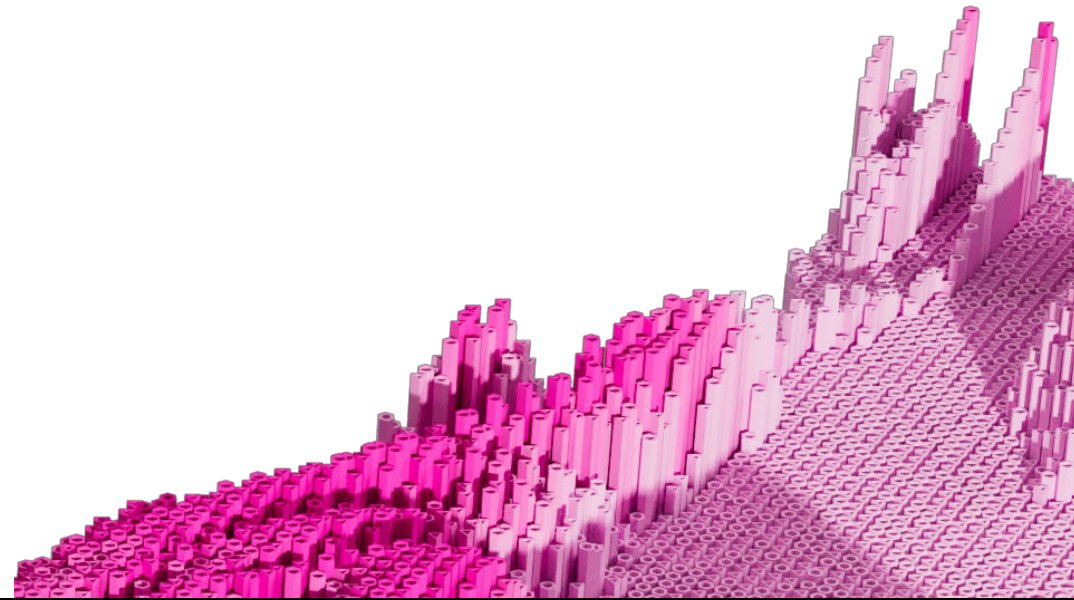
3. Value

Value dives into the return on investment (ROI), looking at the method's scalability, the tangible and intangible returns from the pentesting activities (ROI metrics), and its effectiveness in mitigating risks.

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 SDLC.



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.

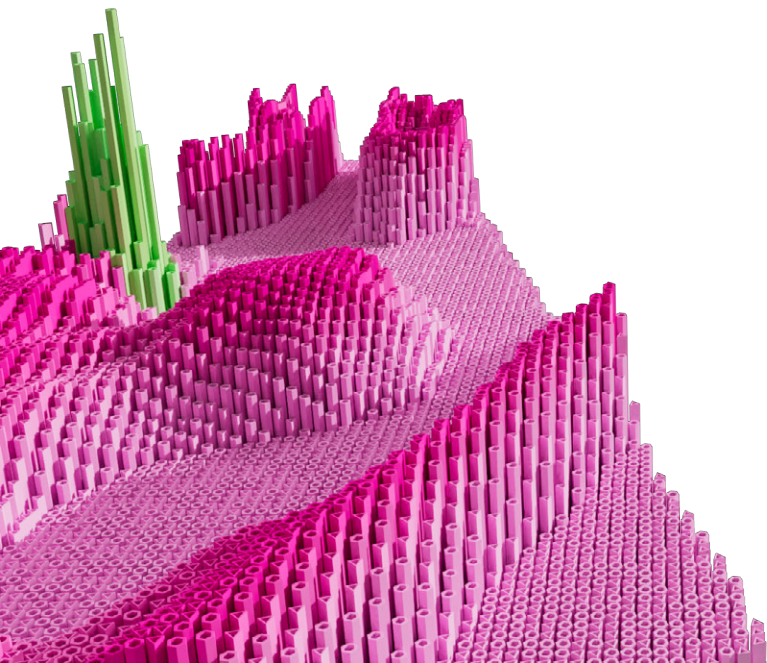


Supporting software and product development

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.

Pentesting Options

There are many ways to assess software security, especially when it's nearing production. To help you navigate these options, we've broken down four key techniques in the upcoming sections. For each, you'll find a straightforward description, followed by our insights. This section focuses on pentesting, which is tailored for production-ready software, steering clear of early SDLC practices such as code scanners, peer reviews, and traditional QA.



Traditional Pentesting via Consultancies

- **Traditional consultancy pentesting** refers to pentesting services delivered by professional service providers, primarily leveraging their in-house salaried pentesters or long-term contractors.
- This alternative encompasses both expansive consulting firms offering a wide spectrum of pentest services, as well as niche boutiques that focus on specialized pentesting domains.
- They generally follow a fixed schedule, spanning from one to two months, often with a preparatory phase of four to six weeks.

Pros:

- Helps organizations meet compliance mandates and qualify for liability insurance
- Ability to provide on-site testing
- Bundling with other services such as cyber risk advisory, offering a comprehensive security package

Cons:

- Often follows an "engage, execute, and exit" model with long gaps between assessments
- Limited collaboration between the pentesters and the customer's teams
- Findings delivered through static PDF reports, limiting real-time insights
- No dynamic platform—resulting in delays in vulnerability disclosure, extending potential exposure to threats

Traditional Pentesting as a Service (PTaaS)

- **Traditional PTaaS** refers essentially to traditional pentesting with an added user interface.
- Unlike traditional, ad-hoc pentesting, it offers continuous, on-demand testing capabilities.
- This model primarily leverages in-house salaried pentesters or long-term contractors.
- Many traditional pentesting firms will likely introduce software platforms in the near future, but this is merely a surface-level enhancement.

Pros:

- Structured methodology that aligns with certain regulatory or corporate governance requirements
- Provides a centralized platform for communication, feedback, and reporting
- Offers scalability options, as the platform can accommodate varying testing demands

Cons:

- May not be as agile or adaptive to emerging threats as community-driven models
- Reliance on a fixed team, resulting in possible missed vulnerabilities that diverse perspectives might catch
- Scheduling or resource constraints due to fixed staffing
- Potential integration challenges with newer security tools, due to potential platform rigidity

Community-driven Pentesting as a Service (PTaaS)

- **Community-driven PTaaS** represents a modern evolution of pentesting, harnessing the collective expertise of a global community of vetted security researchers.
- Using a SaaS delivery model, it provides immediate results and fosters enhanced communication, all powered by advanced platform capabilities.
- This method not only adheres to regulatory mandates but also cultivates a collaborative relationship between security teams and pentesters, leading to comprehensive security assessments.

Pros:

- Seamless access to top-tier pentester expertise
- Rapid launch and efficient management of pentesting activities
- Addresses scheduling challenges inherent to traditional methods
- Empowers development teams to accelerate workflows via platform integrations
- On-demand model promotes consistent and cost-efficient pentesting

Cons:

- Requires stringent vetting standards to ensure that the broad scope of the community doesn't introduce variability in the quality of findings
- Less equipped to provide on-site testing compared to traditional consultancies
- Depending on the specific community-driven PTaaS model, may not provide the comprehensive bundled solutions that traditional consultancies often do, such as cyber risk advisory

Automated Pentesting

- **Automated pentesting**, including autonomous approaches powered by generative AI (GenAI) algorithms and advanced machine learning models, uses predefined scripts or tools to systematically scan and assess systems for vulnerabilities based on recognized signatures or patterns.
- This method rapidly identifies “known unknowns” and can be deployed frequently to ensure consistent security checks.

Pros:

- Provides always-on coverage at a very competitive price
- Rapid detection and reporting of “known” vulnerabilities
- Efficient for routine checks and recurrent vulnerabilities

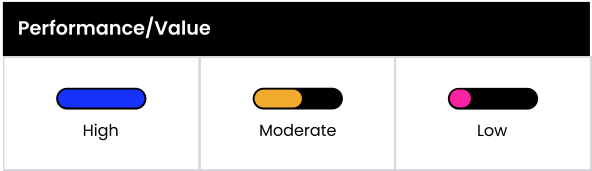
Cons:


























- Limited acceptance of test results by auditors and third-party risk teams
- Essentially revamped dynamic application security testing (DAST) with some GenAI elements—lacking the depth and intuition of a thorough human-driven pentest
- Typically more suited to assets of lesser business criticality, with high-value digital assets often requiring human-driven pentests
- High false positive rates that lead to significant hidden validation costs, negating initial savings—especially for large or complex attack surfaces

Decoding the Characteristics of Modern Pentesting

This comparative analysis includes the expertise of in-house subject-matter experts and HackerOne’s vast experience—having managed thousands of public and private security programs to date. It focuses on the three categories outlined in the introduction: Effectiveness, Efficiency, and Value.

These criteria empower decision-makers to align their choice of pentesting approach with their overarching business, security, and technological objectives. As you interpret the analysis, remember to prioritize which of the three categories resonate most with your organization’s specific objectives and consider how your preference might influence the success of your wider security strategy.



Categories	Characteristics	Traditional Pentest	Traditional PTaaS	Community-driven PTaaS	Automated Pentest
Effectiveness	Depth & Relevance				
	Report Delivery & Compliance				
	Talent Diversity				
	Coverage & Versatility				
Efficiency	Streamlined Procurement				
	Real-time Results and Analytics				
	Communication				
	Platform Integrations				
	Retesting				
Value	Scalability				
	ROI Focus				
	Risk Reduction				
	Liability Assurance				

Effectiveness

In pentesting, effectiveness measures the impact of the testing process and outcomes, guaranteeing that the tests yield meaningful, actionable, and relevant results. The elements addressed below underscore the depth, precision, and thorough nature of a modern pentesting alternative, ensuring a structured and methodology-driven assessment of an organization's security posture.

- Depth & Relevance:** Considers both the significance of vulnerabilities discovered and the potential impact, emphasizing quality over quantity
- Report Delivery & Compliance:** Focuses on the clarity and actionability of the final test report while ensuring adherence to security compliance standards and regulations
- Talent Diversity:** Reflects the diverse skills, qualifications, and testing methodologies of the pentester pool, emphasizing a mix of certifications, training, diverse testing approaches, and the capability to rotate across tests
- Coverage & Versatility:** Demonstrates the thoroughness of the pentest across all critical components while highlighting the adaptability of the approach, incorporating techniques like bug bounties or source code reviews

	Depth & Relevance	Report Delivery & Compliance	Talent Diversity	Coverage & Versatility
Traditional Pentest	<p>Due to scheduling constraints and varying expertise, pentest outcomes can fluctuate.</p> <p>Depth and relevance depend on whether a highly skilled or less experienced pentester is assigned.</p>	<p>Structured reports highlight vulnerabilities and recommend fixes.</p> <p>Ensures alignment with regulatory and governance standards.</p>	<p>Relies on the individual skills and expertise of the pentester.</p> <p>Varying availability of highly experienced or seasoned pentesters.</p> <p>Limited incentive for pentesters to stay continually up-to-date with emerging, niche threats and technologies.</p>	<p>Comprehensive security assessment through established methodologies.</p> <p>The 9-to-5 employee structure results in a slower response to emerging threats.</p> <p>Limited adaptability to diverse testing scenarios and emerging threats.</p>
	Moderate	High	Moderate	Moderate
Traditional PTaaS	<p>Due to scheduling constraints and varying expertise, pentest outcomes can fluctuate.</p> <p>Depth and relevance depend on whether a highly skilled or less experienced pentester is assigned.</p>	<p>Dynamic reports with actionable insights.</p> <p>Ensures deep analysis and up-to-date compliance adherence.</p>	<p>Relies on the individual skills and expertise of the pentester.</p> <p>Varying availability of highly experienced or seasoned pentesters.</p> <p>Limited incentive for pentesters to stay continually up-to-date with emerging, niche threats and technologies.</p>	<p>Comprehensive security assessment through established methodologies.</p> <p>The 9-to-5 employee structure results in a slower response to emerging threats.</p> <p>Limited adaptability to diverse testing scenarios and emerging threats.</p>
	Moderate	High	Moderate	Moderate
Community-driven PTaaS	<p>Methodology-driven nature and systematic depth ensure quality results on a consistent basis.</p> <p>A healthy blend of expert pentester oversight and platform capabilities.</p>	<p>Dynamic reports with actionable insights.</p> <p>Ensures deep analysis and up-to-date compliance adherence.</p>	<p>Through a rotational approach, each test uses a diverse set of vetted global pentesters and in-house technical project managers.</p>	<p>Expansive security coverage, leveraging diverse expertise for in-depth assessments.</p> <p>Diverse talent adapts swiftly to evolving threats and testing scenarios</p>
Winner	High	High	High	High
Automated Pentest	<p>Continuously scans for known vulnerabilities with a broad scope.</p> <p>Often misses novel or intricate issues that require human intuition.</p>	<p>Reporting tends to be generic (worded by GenAI) and lacks human analysis.</p> <p>Effectively identifies known vulnerabilities by cross-referencing with vulnerability databases, but struggles to meet certain compliance types.</p>	<p>While some human oversight and customization are offered, the primary focus is on automation.</p>	<p>Heavily relies on advanced automated tools for continuous scanning and vulnerability identification.</p> <p>Predominantly platform-centric.</p>
	Low	Low	Low	Moderate

Efficiency

In the context of pentesting, efficiency is not just about meeting objectives—it's about doing so through coordinated, easily repeatable processes. Together, the components listed below assess whether the pentesting process, from procurement to results delivery, is streamlined, ensuring an integrated execution that optimizes both time and resources.

- Streamlined Procurement:** Refers to the ease and speed with which pentesting services can be procured, set up, and initiated, reducing administrative overhead and delays
- Real-time Results & Analytics:** Focuses on the capability to provide immediate updates, insights, and results as the testing progresses—ensuring stakeholders are always informed and can make timely decisions
- Communication:** Ensures proactive and real-time communication with the technical project manager overseeing the test and the testers throughout the process
- Platform Integrations:** Highlights the ability of the pentesting solution to seamlessly integrate with SDLC technologies, ensuring a unified find-to-fix workflow
- Retesting:** Refers to the process of reassessing previously identified vulnerabilities for effective remediation

	Streamlined Procurement	Real-time Results and Analytics	Communication	Platform Integrations	Retesting
Traditional Pentest	Time-intensive and project-based, initiating can take weeks to months due to tester availability.	Establishing the severity of vulns can become a contentious process. Post-kickoff, pentesters go silent. The value is concentrated at the end, with reports often archived after discussions.	No collaboration or communication until the final debrief. Manual processes lead to delays in issue resolution. Follow-up on status is rare; testers usually do not see previous results.	Real-time platform integrations are often nonexistent. Detailed feedback is provided solely in the final report. Lack of dynamic insights delays remediation during the testing phase.	During initial scoping, it's challenging to predict retesting duration. There's usually no specific retesting window.
	Low	Low	Low	Low	Low
Traditional PTaaS	Faster setup and systematic approach compared to traditional methods, due to a combination of human expertise and platform capabilities.	Real-time results and analytics delivered via the dashboard. Platform capabilities and expert insights enhance understanding and taking action on findings.	Offers a structured communication flow through platform features. Direct communication with the project manager might be limited.	Offers a set of predefined integrations with SDLC tools. Might lag in accommodating newer technologies, requiring manual workarounds.	The platform facilitates the process. Tester availability results in delays.
	High	High	Moderate	Moderate	Moderate
Community-driven PTaaS	Faster setup and systematic approach compared to traditional methods, due to a combination of human expertise and platform capabilities.	Real-time results and analytics delivered via the dashboard. Platform capabilities and expert insights enhance understanding and taking action on findings.	Real-time collaboration between technical project managers, testers, security, and development teams. Supported by chat capabilities and Slack integration.	Modern platform prioritizes integrations with prevalent security and IT tools. Promotes seamless SDLC workflows to accelerate remediation.	The platform facilitates the process. Leveraging a community makes it typically faster to validate fixes.
Winner	High	High	High	High	High
Automated Pentest	Very rapid and continuous setup.	Provides real-time vulnerability alerts and analytics.	While some human oversight and customization are offered, the primary focus is on automation.	Can be integrated with existing SDLC tools. Ensures automated workflows from detection to action.	Automation allows swift re-evaluation of vulnerabilities. The process typically lacks human insights.
	High	High	Moderate	High	Moderate

Value

Security leaders are challenged to showcase the value of pentesting against its cost. In evaluating the following, keep in mind that the impact of each pentesting method varies based on its application, the caliber of expertise involved, and the precise goals underpinning the test objectives.

- Scalability:** Indicates the adaptability of the testing process to different scales, whether expanding for larger systems or being precise for specific areas
- ROI Focus:** Measures the return on investment (ROI) derived from the pentesting process, highlighting the tangible and intangible benefits against the incurred costs
- Risk Reduction:** Discerns whether the solution is geared toward meeting compliance and regulatory mandates, addressing proactive security needs, or both
- Liability Assurance:** Addresses the potential legal and financial implications of security breaches and how the pentesting solution provides a safety net against such contingencies

	Scalability	ROI Focus	Risk Reduction	Liability Assurance
Traditional Pentest	<div>Involves thorough, in-depth evaluations.</div> <div>Its scalability is challenged by less frequent continuous checks, or periodic checks.</div>	<div>Long-term costs are higher because of manual efforts and limitations in repeating pentests or integrating results.</div> <div>Reports lack the standardized metrics seen in platform-driven systems.</div>	<div>Meets compliance mandates through a structured approach.</div> <div>May not address proactive security needs.</div> <div>Incentive to find innovative bugs is often overshadowed by delivering satisfactory reports in less time.</div>	<div>In-house insured pentesters.</div> <div>Contracts often cap liability to the contract's value, with higher coverage being exceptional.</div>
	Moderate <div></div>	Low <div></div>	Moderate <div></div>	Moderate <div></div>
Traditional PTaaS	<div>Activated on demand, providing scalable options tailored to an organization's depth requirements.</div> <div>Scalability challenges due to a limited bench of talent.</div>	<div>Provides a balanced cost-to-value ratio through efficiency gained by use of a platform.</div> <div>Platform delivers detailed metrics, trend analytics, and benchmarks, simplifying ROI tracking.</div>	<div>Primarily aligns with compliance and regulatory mandates.</div> <div>A more limited scope for proactive security needs.</div>	<div>In-house insured pentesters.</div> <div>Contracts often cap liability to the contract's value, with higher coverage being exceptional.</div>
	Moderate <div></div>	High <div></div>	Moderate <div></div>	Moderate <div></div>
Community-driven PTaaS	<div>Activated on demand, providing scalable options tailored to an organization's depth requirements.</div> <div>Ensures flexibility and timely security assessments.</div>	<div>Provides a balanced cost-to-value ratio through predictable SaaS pricing and continuous insights.</div> <div>Platform delivers detailed metrics, trend analytics, and benchmarks, simplifying ROI tracking.</div>	<div>Adeptly addresses both compliance mandates and proactive security needs.</div> <div>Diverse expertise and platform capabilities for holistic risk reduction.</div>	<div>Limited liability assurance.</div> <div>Pentesters are background checked, identity-verified, and hand-selected but are not employees of the company.</div>
Winner	High <div></div>	High <div></div>	High <div></div>	Moderate <div></div>
Automated Pentest	<div>Easy to set up, scale, and automate periodic and continuous checks.</div>	<div>Heavily automated, these platforms shine in offering real-time metrics, KPIs, and benchmarks.</div> <div>False positives from automated systems demand manual reviews, diminishing ROI by consuming extra time and resources.</div>	<div>Limitations in meeting compliance mandates.</div> <div>May not comprehensively address all proactive security needs, due to reliance on predefined scripts.</div>	<div>Does not offer liability coverage for any direct, indirect, or consequential damage.</div>
	High <div></div>	Moderate <div></div>	Moderate <div></div>	Low <div></div>

The Power of Community-driven PTaaS

When evaluating based on Effectiveness, Efficiency, and Value, community-driven PTaaS emerges as a standout solution. It's a flexible approach tailored to meet an organization's unique requirements, and is competitively priced. Community-driven PTaaS is the premier choice for comprehensive testing combined with in-depth analysis, all while ensuring a swift setup and completion of the assessment.

HackerOne Pentest combines the convenience of a centralized platform with the expertise of our pentester community to excel in all three evaluation areas. HackerOne's model is superior based on two fundamental differences: the HackerOne Attack Resistance platform and the vetted and trusted pentester team.

"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 Effectiveness

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 Efficiency

4
days

New customers can initiate a new pentest in 4 business days.

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

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.



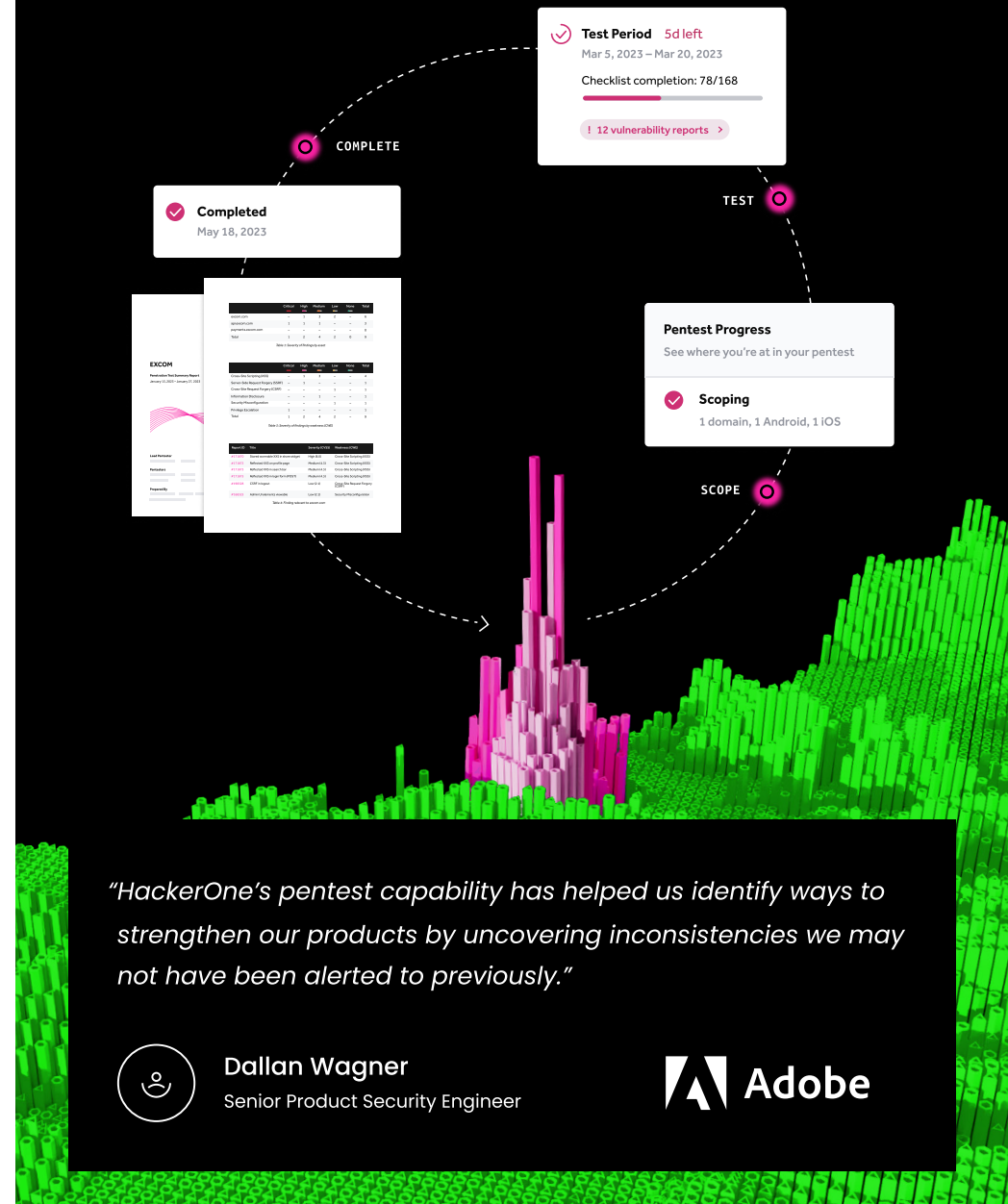
HackerOne Attack Resistance Platform for Best-in-Class PTaaS

HackerOne's Attack Resistance Platform delivers consistent results and analytics through a seamless SaaS-based solution, streamlining pentest initiation and execution. With dedicated support from experienced technical engagement managers (TEMs) and solution architects, our platform ensures compliance and coverage.

The platform's versatility is enhanced by extensive SDLC and GenAI integrations, as well as custom workflows, to identify vulnerabilities promptly and address them smartly. Customers can effortlessly transition between pentesting, bug bounty, vulnerability disclosure, and code review, fulfilling continuous, proactive security testing needs.

New customers can start a pentest within 4 business days, with returning customers enjoying a faster, tailored process. Initial reports are typically ready in under a week, and final reports follow within 3-5 business days, highlighting HackerOne's commitment to fast and effective security enhancement.

The expansive network of security experts ensures swift responsiveness to new technologies and emerging threats, such as GenAI model vulnerabilities and novel security challenges.



✓ **Test Period** 5d left
Mar 5, 2023 – Mar 20, 2023
Checklist completion: 78/168
! 12 vulnerability reports >

✓ **Completed**
May 18, 2023


EXCOM


Category	Item	Status	Priority	Severity	Impact
Application Security	SQL Injection	Not Found	High	Critical	Full system compromise
	Buffer Overflow	Not Found	High	Critical	Full system compromise
	Remote Code Execution	Not Found	High	Critical	Full system compromise
	Denial of Service	Not Found	High	Critical	Full system compromise
Network Security	Man-in-the-Middle	Not Found	High	Critical	Full system compromise
	Session Hijacking	Not Found	High	Critical	Full system compromise
	Privilege Escalation	Not Found	High	Critical	Full system compromise
	Information Disclosure	Not Found	High	Critical	Full system compromise

Pentest Progress
See where you're at in your pentest

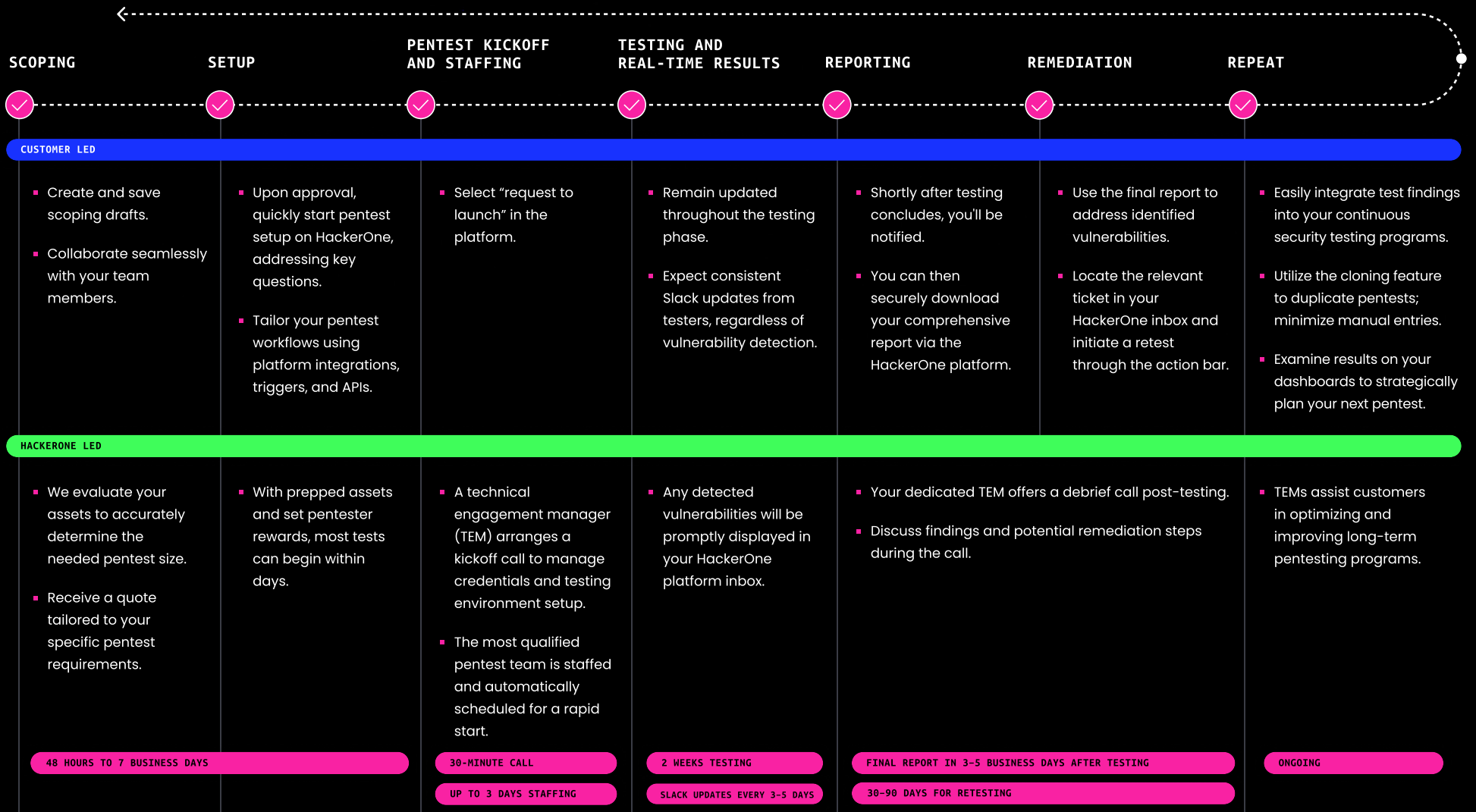
✓ **Scoping**
1 domain, 1 Android, 1 iOS

"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

 **Adobe**


Streamlined Pentesting Process



HackerOne's Trusted Pentester Team


HackerOne pentesters are an elite subset of the ethical hacking community—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, and take their certifications into account, including OSCP, OSCE, OSWE, and CREST.

HackerOne's community offers boundless capacity—skilled security researchers are available at all times and introduce a dynamic rotation of skill sets with each test. Owing to this structure, the HackerOne platform delivers insights of consistently superior quality compared to other pentesting methods and vendors.




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.

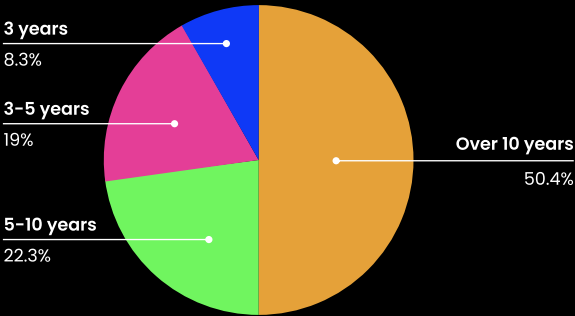
74%

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.

PTaaS or Bug Bounty?

Do community-driven pentests and bug bounties serve the same purpose or complement each other? While both approaches engage security researcher communities, their outcomes are distinct. A holistic security assessment involves a blend of both.

Bug bounty programs yield superior results over time due to a stochastic model, making them an optimal choice for organizations striving for comprehensive, ongoing testing that encompasses a diverse set of security researchers. The long-term value of this approach is evident in the lower average cost per discovered vulnerability, as well as leading global companies' commitment (like [Google](#), [Microsoft](#), and [Facebook](#)) to long-running bug bounty programs.

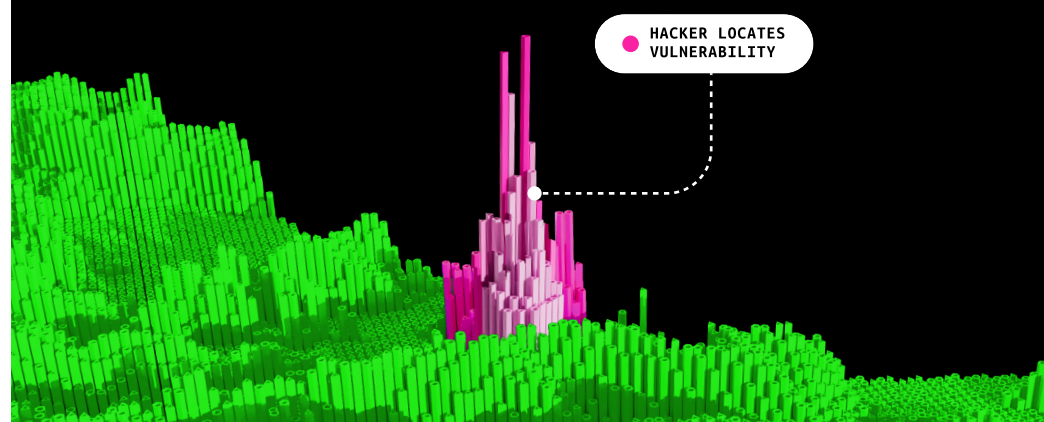
In contrast, pentests deliver immediate results through a select group of security researchers. These experts, compensated for their skill sets and backgrounds, meticulously follow specific checklists to ensure comprehensive testing. Organizations that need immediate results for compliance or commitments to stakeholders tend to gravitate toward pentests. Events like the release of a new product or a recent acquisition also catalyze the demand for such tests.

For comprehensive security testing of production applications, organizations should implement a wide-ranging bug bounty program and supplement it with targeted pentests where testing assurance is required.

What Is a Bug Bounty Program?

Bug bounty programs incentivize ethical hackers via [bug bounties](#): monetary rewards for successfully discovering and reporting vulnerabilities or bugs to the application's developer. These programs allow organizations to access the ethical hacking and security researcher community to continuously improve their systems' security posture. Bounties complement existing security controls and pentesting by exposing vulnerabilities that automated scanners might miss and incentivizing security researchers to emulate potential bad-actor exploits.

Together, bounties and pentesting strike a balance between continuous, proactive vulnerability discovery and in-depth, time-bound testing.



The Shared Benefits of Bug Bounties and PTaaS with HackerOne

Whether you start with a pentest or implement a bug bounty from HackerOne simultaneously for a more holistic coverage, certain benefits remain consistent across both program types. Both draw from a vast pool of ethical hackers, ensuring the best experts for the task. Some researchers exclusively focus on bug bounties, carefully vetted researchers focus on pentests, and the best researchers often engage in both. Both methods utilize HackerOne's Attack Resistance Platform (delivered as SaaS) , guaranteeing real-time results and advanced analytics. The vulnerabilities identified through both methods integrate seamlessly into your workflow and other systems.

For customers interested in a time-restricted bug bounty program, we offer a product called [HackerOne Challenge](#), similar to a bug bounty but limited to a duration of 2–6 weeks.

	Bug Bounty	PTaaS
Purpose	<div>✓</div> <div>Comprehensive, ongoing testing to ensure proactive security</div>	<div>✓</div> <div>Targeted, often-immediate need to ensure compliance and proactive security</div>
Approach	<div>✓</div> <div>Stochastic model, continuous</div>	<div>✓</div> <div>Methodology-driven, time-bound</div>
Results	<div>✓</div> <div>Superior over time</div>	<div>✓</div> <div>Predictable and immediate</div>
Incentives	<div>✓</div> <div>Paid for results, highly competitive among security researchers</div>	<div>✓</div> <div>Paid for effort, no competition among pentesters</div>
Duration	<div>✓</div> <div>Ongoing, continuous</div>	<div>✓</div> <div>Point in time, often repeated at regular intervals</div>

Ready to Rethink Your Traditional Pentest?

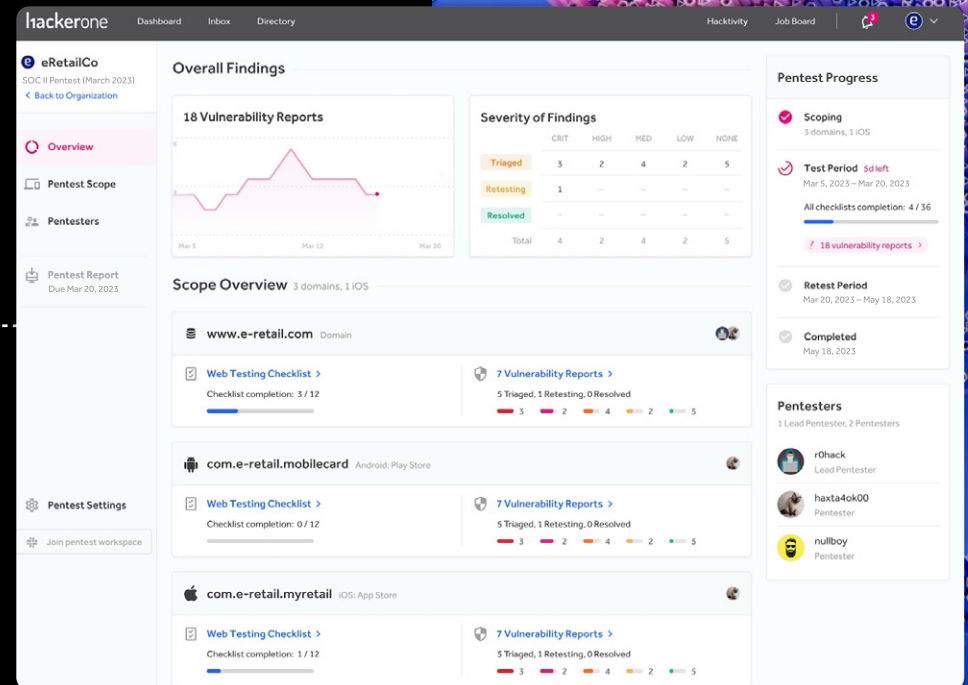
HackerOne Pentest transcends routine compliance checks, delivering in-depth insights, efficiency, and actionable results tailored to your business and security needs. **Tell us about your pentesting requirements, and one of our experts will contact you.**



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



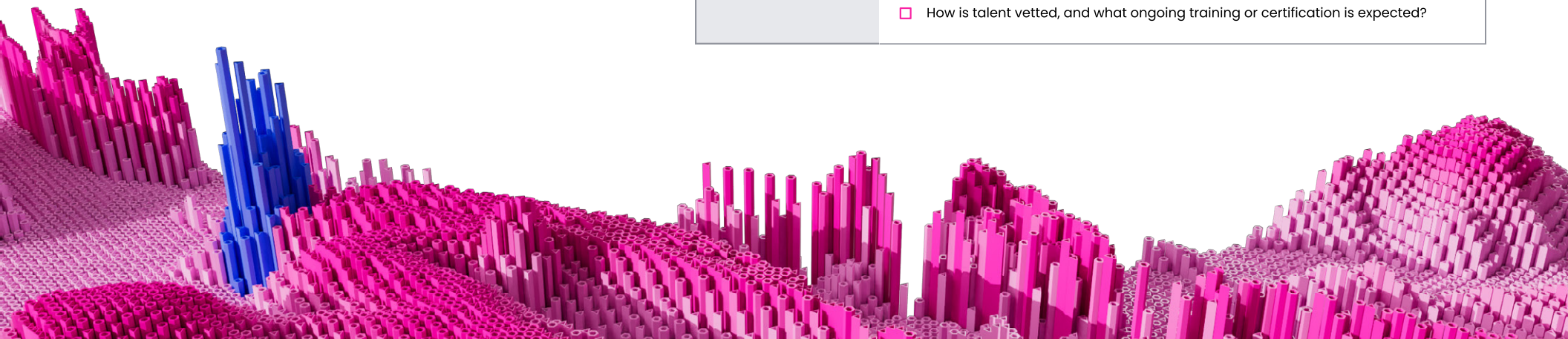
[Watch a demo](#) to see how HackerOne redefines pentesting.



Appendix A: Pentesting Evaluation Matrix

Use this checklist to evaluate each of the four security testing options presented in this eBook: traditional pentesting, traditional Pentesting as a Service (PTaaS), community-driven PTaaS, and automated pentesting. Security leaders can use this checklist to determine whether their focus is on effectiveness, efficiency, or value, then decide on the most suitable path for their organization's needs.

Effectiveness	
Quality of Findings	<ul style="list-style-type: none"><input type="checkbox"/> How deep does the analysis go? Does it uncover both surface-level and deep-rooted vulnerabilities?<input type="checkbox"/> Are the findings actionable, significant, and provided with context?<input type="checkbox"/> Beyond identifying vulnerabilities, does the approach offer insights on potential business impact?
Human-centric vs. Platform-centric	<ul style="list-style-type: none"><input type="checkbox"/> How well does the approach balance human expertise and platform capabilities?<input type="checkbox"/> How intuitive is the platform or interface for managing pentests?
Coverage Proof	<ul style="list-style-type: none"><input type="checkbox"/> Does the method demonstrate comprehensive testing across all essential components and systems?<input type="checkbox"/> Is there a capability for continuous testing or periodic checks?
Talent	<ul style="list-style-type: none"><input type="checkbox"/> How does the approach ensure the expertise and qualifications of its pentesters?<input type="checkbox"/> Are the pentesters well-versed in the latest threats and technologies?<input type="checkbox"/> Does the approach incorporate a diversified set of skills and experiences from its talent pool?<input type="checkbox"/> How is talent vetted, and what ongoing training or certification is expected?



Efficiency	
Performance	<ul style="list-style-type: none"> How long does it take to scope and launch a pentest? How quickly after initiation is the first set of findings received? Can the testing scale based on the application's size and complexity? How much manual oversight is required? Is the process streamlined? How easy is it to adjust or expand the scope of testing?
Customer Support & Expertise	<ul style="list-style-type: none"> How accessible is the customer support/success team during the pentest process? Is there a dedicated point of contact or technical engagement manager (TEM) assigned to guide you through the entire engagement? What qualifications and certifications does the TEM hold? How many years of experience does the TEM have in overseeing pentests? How quickly does the support team respond to queries or concerns? Are post-engagement support services offered, such as guidance on vulnerability remediation? What channels are available for support communication (e.g., Slack, email, chat, phone)? How experienced is the support team in handling unique or complex issues?
Feedback & Integrations	<ul style="list-style-type: none"> How seamlessly does the method integrate with existing systems, tools, and workflows? Are prebuilt integrations or APIs available? Is the feedback actionable and accompanied by 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? Is retesting included as part of the pentest?

Value	
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?
Pentesting ROI	<ul style="list-style-type: none"> How does the cost of the service compare with the perceived value and results delivered? Are metrics and benchmarks provided to quantify the pentest's impact? Is there an automated way to measure the improvement in security posture over time through repeated testing? Are the insights provided substantial enough to inform broader security and IT strategy, beyond immediate vulnerabilities or compliance needs?
Risk Reduction	<ul style="list-style-type: none"> How effectively does the solution mitigate compliance-driven risks? Is there a balance between meeting compliance mandates and proactively addressing technical vulnerabilities?
Liability Assurance	<ul style="list-style-type: none"> Does the solution offer any guarantees or assurances against breaches? How is liability distributed between the service provider and the organization?

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



<p>CHALLENGE:</p> <p>Traditional Pentests</p>	<ul style="list-style-type: none"> 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.
<p>SOLUTION:</p> <p>HackerOne Pentest via PTaaS</p>	<ul style="list-style-type: none"> 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
<p>RESULTS:</p> <p>A Scalable, Security-First Mindset</p>	<ul style="list-style-type: none"> 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