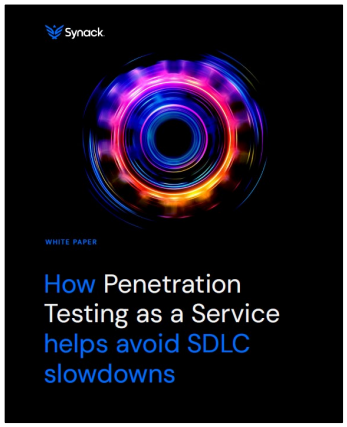


How Penetration Testing as a Service helps avoid SDLC slowdowns

Thank you for downloading this Synack Whitepaper. Carahsoft is the distributor for Synack Cybersecurity solutions available via MHEC, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Synack's solutions, please check out the following resources and information:

For additional resources:
carah.io/SynackHome

For upcoming events:
carah.io/SynackEvent

For additional Synack solutions:
carah.io/SynackSolves

For additional Cybersecurity solutions:
carah.io/CybersecuritySolution

To set up a meeting:
synack@carahsoft.com
703-871-8585

To purchase, check out the contract vehicles available for procurement:
carah.io/SynackContract

Synack

WHITE PAPER

How Penetration Testing as a Service helps avoid SDLC slowdowns

Finding and fixing security gaps sooner saves time and money

Software developers don't want to fail. But when they do, they'd like to fail quickly, getting necessary feedback to deliver pristine (and secure) code on their next commit.

Pentesters provide plenty of feedback, finding security failures they graciously present as "bugs." But when pentests are held only once or twice a year, they produce a bevy of vulnerabilities that slows down—and stresses out—developers. Or, worse, the pentesters on call don't have the skills to find software flaws that real-world adversaries will.

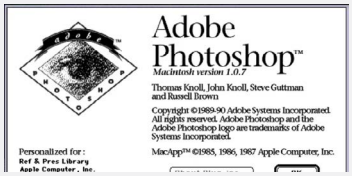
In the modern era of continuous integration/continuous deployment, agile development, and AI-enabled code releases, pentesting can feel like a painstaking manual process drawn from the medieval times of floppy disks. And yet software is easier to ship than ever before: companies no longer have to buy those floppy disks, load their product onto them, and mail these plastic-and-metal rectangles to customers to install the updated software on their devices. Instead, enterprises design software to automatically check for and install these updates as they debut.

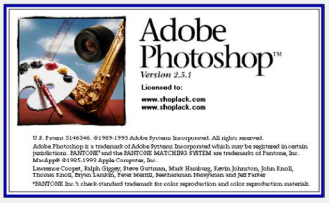
Traditional pentesting has not kept up.

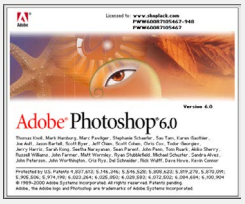
It is hampered by long lead times, lack of scalable resources, and an inability to nimbly respond to an organization's needs throughout the year. Such testing is also only useful as a snapshot in time—it won't keep applications safe from newly emerging threats or new attack vectors exposed by rapid changes to their underlying code. Traditional pentesting reports are also static and not readily visible to a broad audience of security and development operations teams.

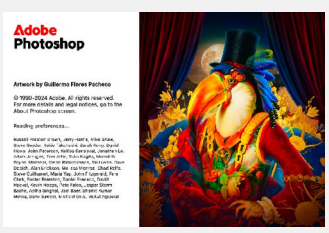
Software releases are accelerating

Adobe released Photoshop 1.0 in February 1990; version 2.0 debuted in June 1991. The company still releases major updates roughly once a year, but they are followed by monthly point updates, which are followed by even more granular updates as needed. Photoshop 26.0 arrived in October 2024—26.4 followed in February 2025, with the 26.4.1 bug fix release making its way to customers shortly after. As of June 2025, Photoshop is all the way up to version 26.8.









Penetration Testing as a Service (PTaaS) embraces the future of development

A tale of two Synack customers

PTaaS offerings are a newer breed of security testing that seek to address the limitation of traditional testing services, helping organizations implement proactive application security testing. PTaaS platforms combine the benefits of automated scanning, scalable access to on-demand security researcher expertise, and effective vulnerability management. PTaaS can also be a good way to augment and complement in-house security resources, and to bridge cybersecurity skill gaps in development teams; particularly as they rely on GenAI.

For example, one Synack enterprise customer implemented Synack PTaaS and measured a 57% reduction in the amount of time unpatched assets were exposed to potential attackers. Meanwhile, another multibillion-dollar-revenue Synack customer reduced their average time to remediate exploitable vulnerabilities by 50%. In both cases, the customers leveraged trends in Synack testing data to keep development teams in the loop about patterns of vulnerabilities, exposing areas needing more training or investment.

CISOs can use this data to prevent the same security issues from cropping up over and over again, addressing the root causes of vulnerabilities (or identifying glitches in the patching process). The first enterprise customer cited above found that patch efficacy for security issues on a key application improved to 100%, meaning they were fixed the first time. Before switching to PTaaS, that application had required up to seven patch attempts to address a vulnerability.

66% of enterprise organizations say traditional penetration testing reports are difficult to operationalize within ticketing systems, incident response playbooks, and other security operations processes.

— Enterprise Strategy Group survey, June 2024

That's a win for the team on that particular project. But patch efficacy on another important app was measured at only 10%. There's clearly room for improvment, and because the Synack platform makes this data available, the customer knows which application's development processes need more attention.

For example, one Synack enterprise customer implemented Synack PTaaS and reduced how long unpatched assets were exposed to attackers by

57%

compared to when they relied on traditional penetration testing services.

Meanwhile, another multibillion-dollar-revenue Synack customer reduced average exploitable vulnerability remediation time by

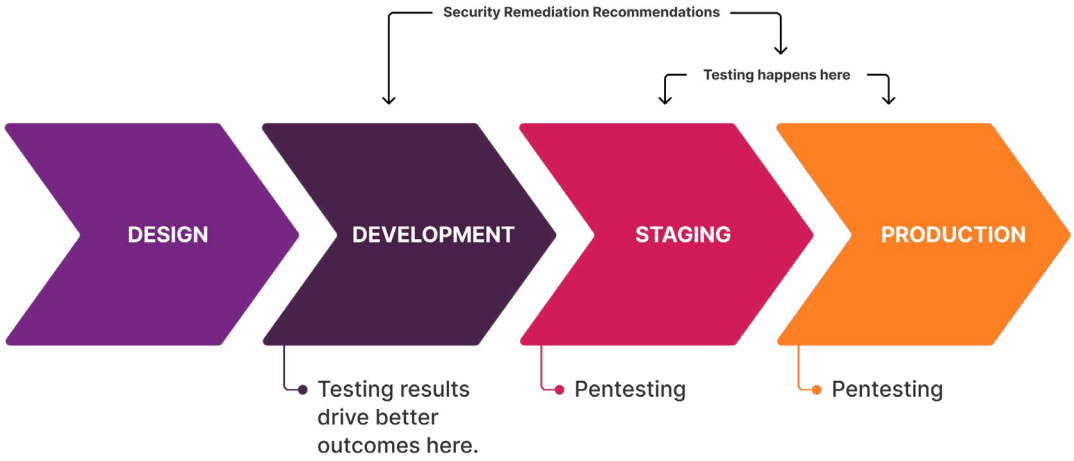
50%.

The second customer mentioned above similarly gleaned insights: Even though their total number of exploitable vulnerabilities fell 60% year-over-year, critical SQL injection vulns remained a problem, indicating work to do.

Effective PTaaS implementations need to integrate with development tools that customers already use for vulnerability remediation (e.g., Jira, ServiceNow) and security operations tools that make testing results visible to a broader audience (e.g., Splunk, Palo Alto). Synack PTaaS customers take advantage of available integrations with these DevSecOps processes and tools, giving their developers clear recommendations on how to fix security issues, plus an integrated process to verify that their patches were successful.

Synack Pentesting in the SDLC

- Faster Dev Cycles
- Reduced Dev Team Workload
- Efficient Bug (Vuln) Remediation
- Security Objectives Achieved



PTaaS rises to the GenAI challenge

GenAI technologies have further accelerated the pace of the software development life cycle (SDLC): Developers now use AI tools to generate code snippets, analyze code accuracy, write documentation, and otherwise increase their productivity.

AI helps developers produce higher-quality code more quickly than ever: GitHub said in 2022 that developers who used its Copilot tool completed a task 55% faster than developers who didn't use it, and it said in 2024 that Accenture devs saw an 8.69% increase in pull requests and a 15% increase to the pull request merge rate after they started using Copilot.

Despite these advantages, AI development tools can add security risk and introduce vulnerabilities. AI coding assistants may suggest code snippets with known vulnerabilities, use improper input handling, or utilize outdated libraries. These problems can be exacerbated if the tools use poor training data, unvetted open source repositories, insecure access controls, or otherwise introduce new threat vectors to the CI/CD pipeline. There are no silver bullets; AI is no exception.

A note on scanners

Many organizations evaluate the security of their software with a dual-pronged approach that combines automated scanning with traditional penetration testing.

Scanning is a good starting point for automated security checks. Tools such as software composition analysis (SCA), software bill of materials (SBOM), static application security testing (SAST), API testing, and others can check for known vulnerabilities and security best practices. This approach can catch common development security mistakes before they have an opportunity to progress further. Scanning is noisy, however, and prone to false positives. Techniques and tools are needed to achieve a better signal-to-noise ratio—effective vulnerability management platforms, combined with assistance from human-led analysis, can help.

A scanning tool will not find uncommon vulnerabilities or zero days or predict all the ways bad actors might interact with and exploit software once it's released to the wild. ***PTaaS leverages a network of experienced security professionals who can find vulnerabilities that are truly exploitable, suggest solutions to the problems they find, and help triage the voluminous amount of data produced by automated scanners and other data sources so organizations can focus on the vulns that matter most.*** *Effective use of security researchers, as a complement to automated scanning, is a good way to proactively fix security problems and improve overall software quality.*

PTaaS offers rapid and continuous application security testing

Organizations need ways to validate application security on a continuous basis.

They no longer have weeks, months, or years to evaluate software for vulnerabilities before a major update makes its way to their customers.

They have days.

And if they want to address security gaps without disrupting the breakneck pace at which their developers are working, they need specific recommendations for rapid remediation, as well as patch verification to confirm those gaps have indeed been closed. Traditional penetration testing isn't designed to meet those requirements.

By leveraging Synack Penetration Testing as a Service, organizations can find and fix exploitable security gaps earlier in the SDLC, saving time and money.