



PRODUCT GUIDE

Synack Security Testing Platform

One strategic platform for all your penetration testing needs

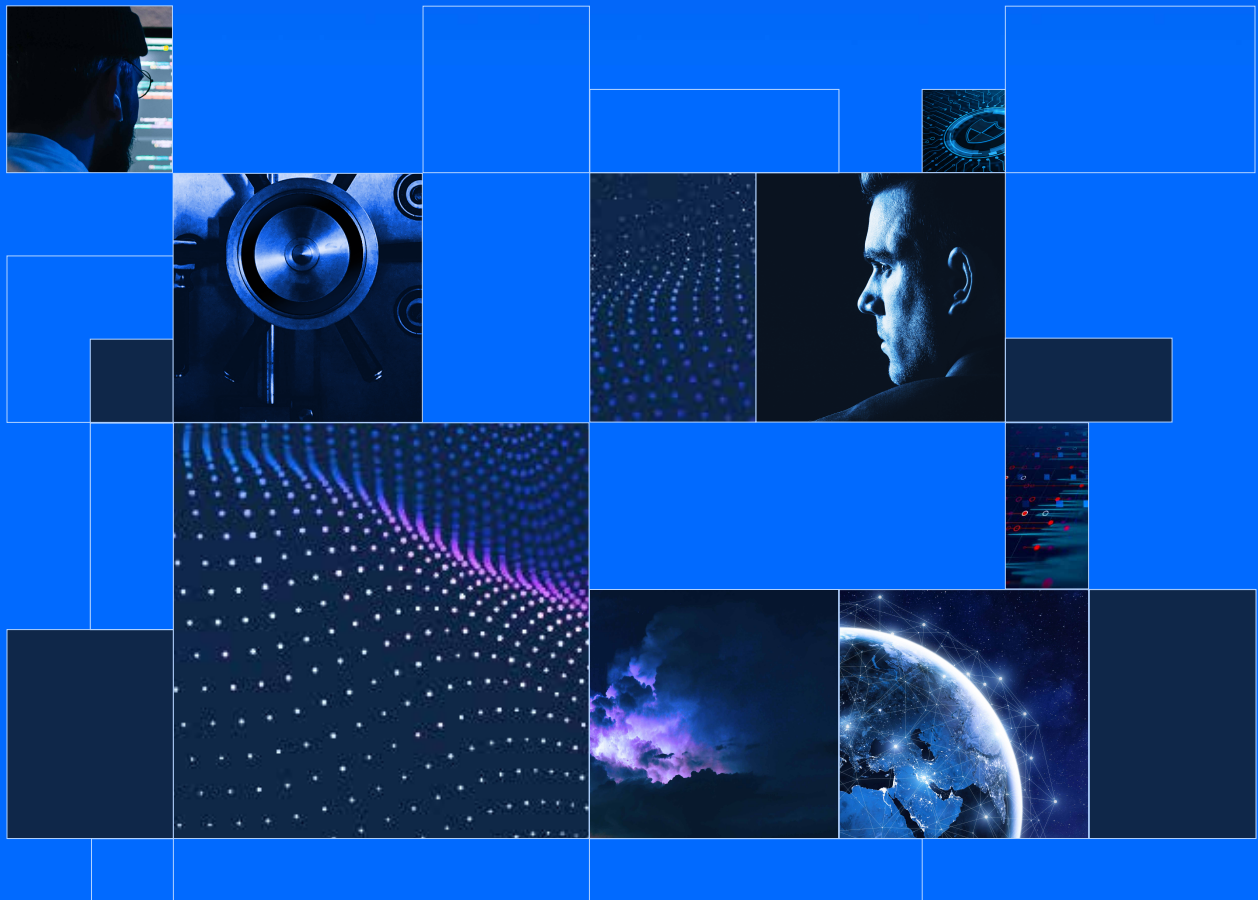


Table of Contents

Introduction	3
Benefits of the Synack Security Testing Platform	6
6 Pillars of the Synack Platform	9
Vulnerability Management	10
Operations and Support	12
API and Integrations	13
Reporting and Real-Time Analytics	14
Managed Community Access	15
Testing Controls	17
Managed Vulnerability Disclosure Program	18
Synack Catalog and Credits	20
Conclusion	22



Introduction

Imagine a world where your security testing is strategic to your security program, helping to illustrate actionable data about your attack surface and guide your security team through comprehensive remediation of exploitable vulnerabilities without adding layers to your security stack.

Traditional penetration tests for compliance is a good place to start, but they won't deliver the insights you need to improve processes that reduce vulnerabilities over the long term. As researchers discover thousands of new CVEs each year and ransomware surges in popularity, you need to be able to see the weakest points in your attack surface to proactively mitigate threats, something you can't do with compliance checklists alone. Today's security landscape requires continuous oversight of your most protected assets and the ability to identify security trends across the organization.

Synack's ability to provide continuous and strategic security testing is made possible by the six pillars of our penetration testing platform and our catalog of on-demand security testing options that gives the flexibility organizations need to meet their unique security goals.

Why security testing needs to improve

Testing once a year doesn't address a software development lifecycle that introduces new code daily, and current testing methodologies often treat all assets the same despite a varied level of risk. Finally, most firms don't take action on results because the quality, visibility and consistency of the vulnerability reports are poor.

Security leaders can no longer rely on traditional pentesting that creates noise, doesn't scale and results in only some, not all, exploitable vulnerabilities being fixed to check the compliance box. It's time to embrace a security culture that is risk-driven instead of compliance-driven.

A CISO PERSPECTIVE

Security Testing Today

"All the money we spent on security testing and remediation yesterday is gone. We don't learn anything from the process or leverage the data strategically. We claim success if the regulators are satisfied."

The evolution of security testing methodologies

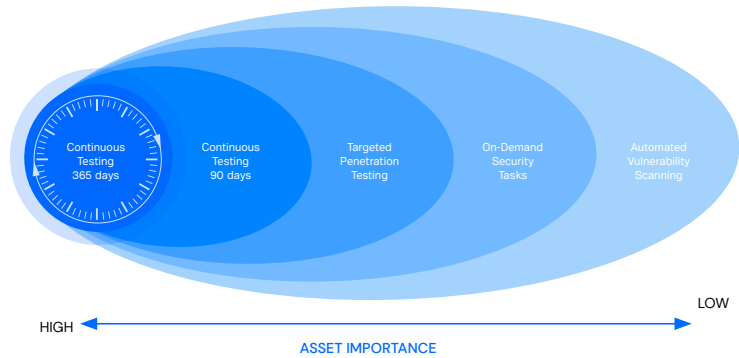
It may sound too good to be true in today's dynamic environment. Digital transformation has led to accelerated vulnerability creation as teams manage cloud sprawl and build applications faster with agile development cycles, requiring a risk-driven, instead of compliance-driven, approach.

Taking a thoughtful approach to security testing based on asset-level risk can help your organization to craft a testing strategy that will not only keep you compliant, but also help you to properly manage risk across a growing attack surface.

Learn how to craft your security testing to align with your company's business goals. Read ["A Journey to Strategic Security Testing"](#) white paper.

The spectrum of testing the Synack Platform supports includes everything from continuous pentesting for the most critical assets to automated vulnerability scanning for the least important assets. Increasingly, companies are moving away from a one-size-fits-all approach to their attack surface and want flexibility in their security testing consumption. Companies need choices and the ability to test assets when they want, where they want and how they want.

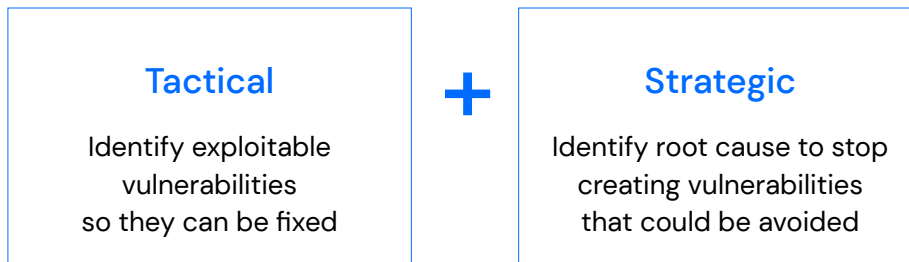
Developing an ideal security testing strategy

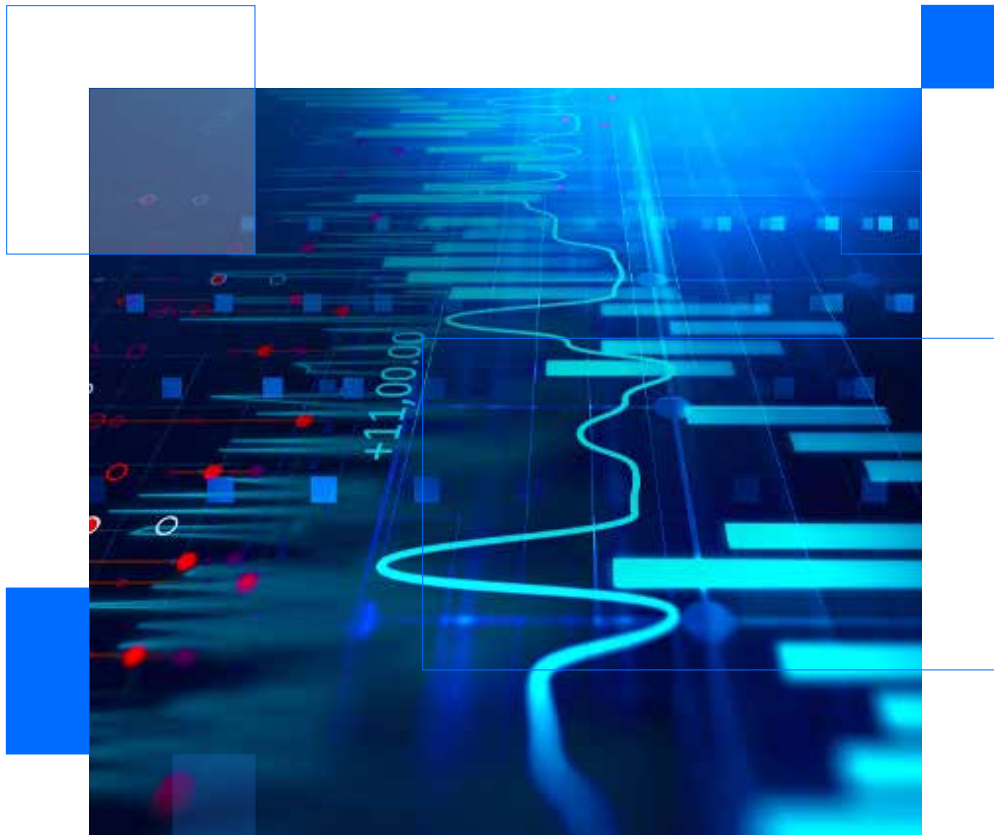


The Synack Platform: A risk-driven approach

The Synack Platform enables you to track improvements in your attack surface hardness over time, launch over 40+ types of testing on-demand and evaluate the quality of your pentesting based on researcher coverage and controls, rather than just vulnerabilities found. It also provides immediate access to actionable reports and patch verification.

When done properly, security testing can transform your vulnerability management through both tactical and strategic methods. Tactically, security teams can identify exploitable vulnerabilities to fix them and strategically, security leaders can identify root causes and trends across asset type and at scale.





Benefits of the Synack Security Testing Platform

The Synack Platform delivers a range of benefits from identifying the root cause of vulnerabilities to measuring your security performance overtime. Synack provides a best-in-class security testing platform that can launch a test in days not months, scale to meet the demands of testing a large enterprise and promote collaboration across development and security teams. Your security team can rest easy knowing that the Synack Platform meets best practice security standards for enterprise and government.

Launch a security test in days, not weeks or months

Synack offers on-demand and continuous security testing that can start and stop when you need it, leading to improved test efficacy.



CAPACITY

Synack offers access to thousands of hours of security testing on-demand.



CAPABILITY

Stay ahead of the latest threats as the best and brightest minds in security are financially incentivized to hunt for vulnerabilities in your environment.

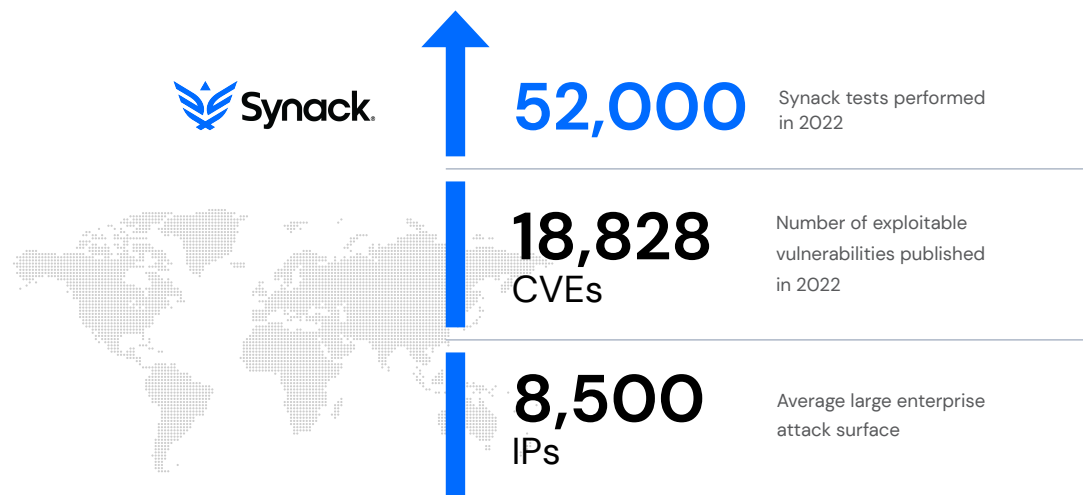


CONFIDENCE

Show your stakeholders customizable reports so no one has to worry about your security posture.

Do more testing without compromising on quality

Every year, Synack scales to meet the evolving landscape of exploitable vulnerabilities and the increasing size of enterprise attack surfaces. Synack provides a consistent and secure global experience for every test from start to finish.



Gain visibility into vulnerabilities, coverage and remediation status

Synack provides a transparent view of Synack Red Team (SRT) performance, including exploitable vulnerabilities, real-time analytics, insight, testing activity and history. Additionally, you can decide when tests start and stop at the click of a button, chat with researchers through the portal, and remediate faster with on-demand patch verification.

Work collaboratively with developers, leadership, and security teams

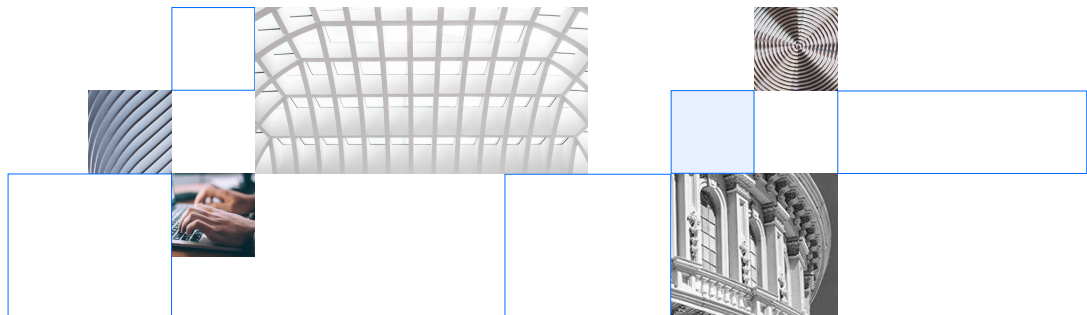
Synack allows for customized reporting, easily exportable views, integrations with ticket management, business intelligence, SIEM, Microsoft tools, and access controls that help you share information internally.

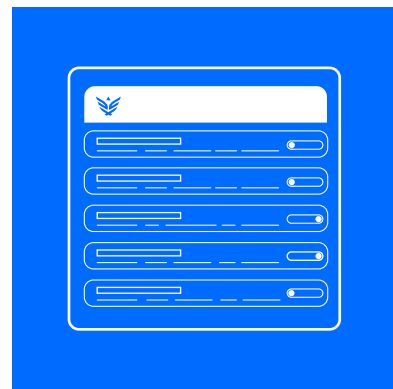
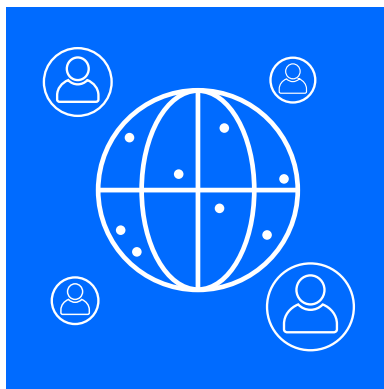
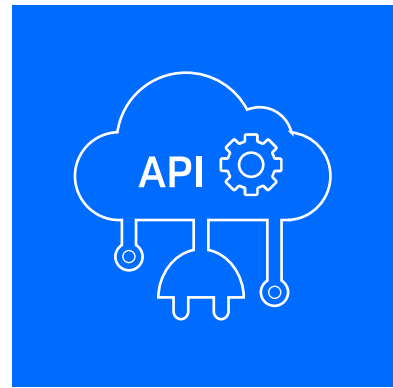
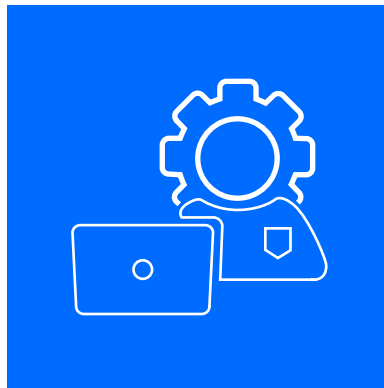
Find root causes of vulnerabilities

With the platform, you can see security trends across vulnerabilities, identify root causes, and materially improve your security posture. For example, one Synack customer learned that 80% of vulnerabilities found in applications and infrastructure were related to authentication. After they built an internal education program to retrain their teams on secure authentication, they cut their authentication vulnerability rate in half.

Government-grade security controls

Synack has achieved the FedRAMP Moderate designation, underscoring Synack's commitment to data security for all customers. FedRAMP, which stands for the Federal Risk and Authorization Management Program, is a framework that standardizes security requirements for federal information managed in the cloud. The Moderate-level designation is the highest level reached by any company in the Pentesting as a Service space.





6 Pillars of the Synack Platform

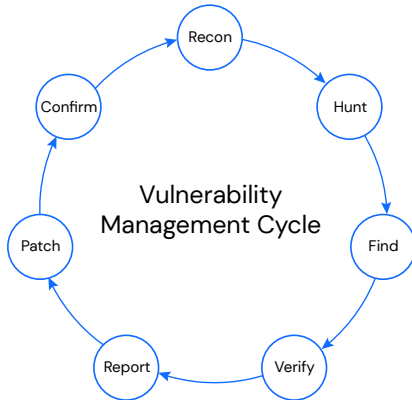
Synack provides a transformative security testing experience with you in mind. How? We'll review the core technology components of the Synack Platform and how they correlate to benefits for your team. The six pillars of the platform discussed in following sections include:

1. Vulnerability management
2. Operations and support
3. API and integrations
4. Reporting and real-time analytics
5. Managed community access
6. Testing Controls

1

Vulnerability Management

Synack manages your journey from vulnerability discovery to remediation, so your developers can address fixes earlier and you can rest assured that your vulnerabilities are thoroughly addressed.

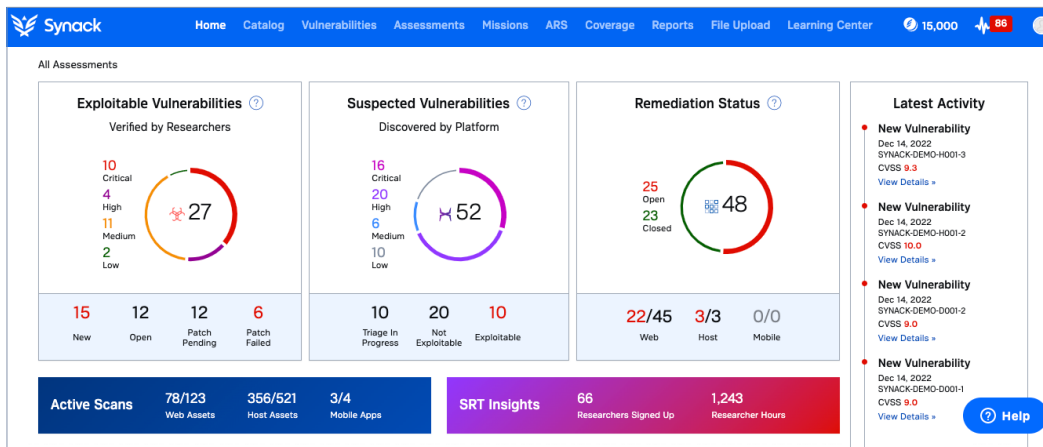


Vulnerability Management Cycle Steps

- Recon** Synack deploys SmartScan for pre-test scanning
- Hunt** SRT conduct open vulnerability discovery
- Find** SRT submit potential vulnerabilities to Synack
- Verify** Synack conducts triage of SRT findings
- Report** Synack delivers verified vulnerabilities to the customer in real time
- Patch** Customer confirms patch which creates an automated patch verification request
- Confirm** Customer requests SRT to re-test vulnerability to confirm successful remediation

Common repository for security testing

Access all testing information across teams, geographies and times, enabling trend detection and root cause analysis.



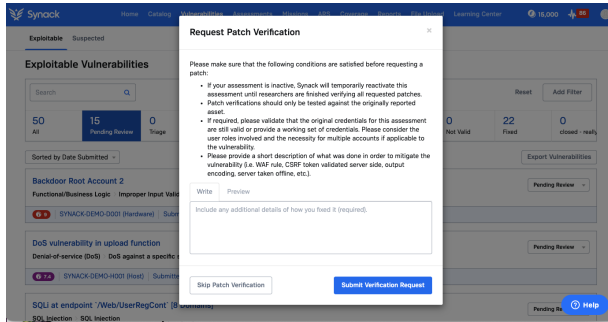
Unlimited users

No “per person” user charges to encourage secure and appropriate access to testing data. Include developers with access with role-based access control.

Key vulnerability management features

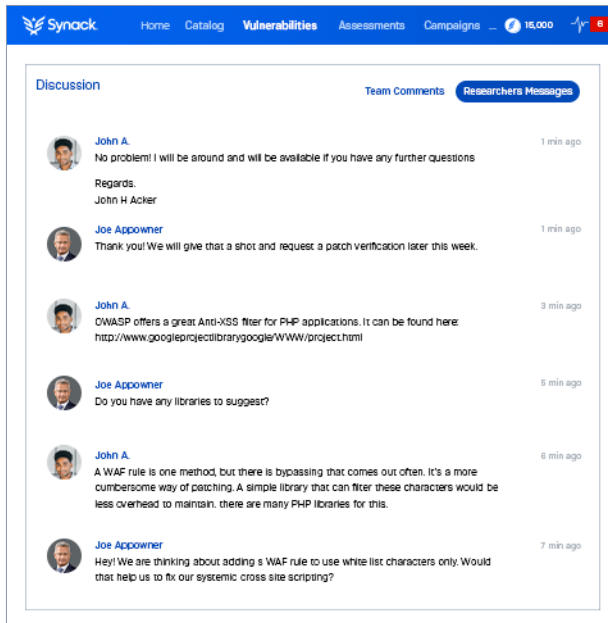
Patch verification

Researchers re-test to verify that the patch was effective.



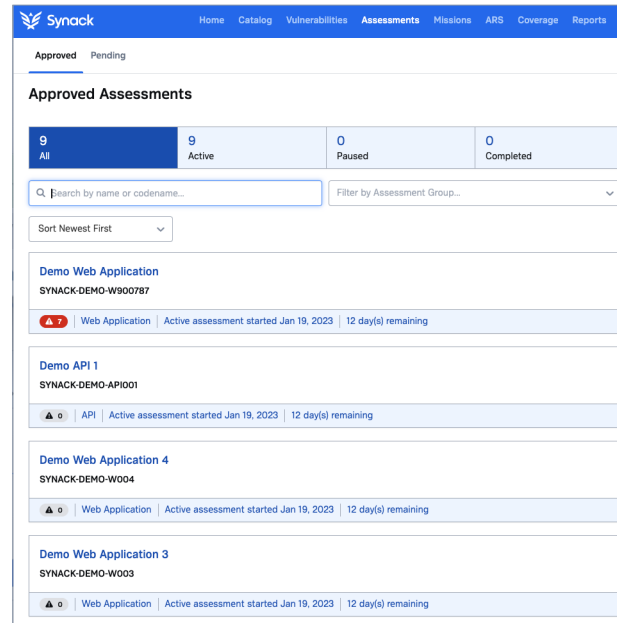
Communication with researchers on vulnerabilities

Chat directly with members of SRT through the platform.



Assessments

The Assessments tab provides a single view for all past and on going assessments.





Operations and Support

Synack ensures that vulnerabilities are high impact and truly exploitable. Triage eliminates any duplicate submissions or low quality submissions. Additionally, Synack provides customer support available 24/7 to scope and launch tests.



Customer Success

Customers are supported by trained customer success and support professionals.

Worldwide Team

Vulnerability reports reviewed by a team built to span multiple time zones, so they are reviewed in a timely manner no matter your company's global location.

Launch Assistance

Synack professionals help customers carefully prepare for each test, minimizing the chance of surprises or errors.

Professional Triage

All reports are checked for accuracy and true exploitability before being sent to customers. Duplicates are also removed.



Community Team

Dedicated Community Team at Synack advocates for, engages with, recognizes and rewards top SRT members.

Recruitment

Synack never stops enlisting great talent to help serve customers with specialized or fresh tactics, techniques and procedures.

3

API and Integrations

Integrating Synack into other security workflows and tools is important for reducing operational friction, improving responsiveness, triaging to reduce alert noise and validating security posture. Use cases for integration include process operations, security operations, incident response and security analytics.

Synack Integrations

Microsoft Synack integrates with Microsoft Sentinel, Defender for Cloud, and Azure DevOps, allowing for continuous and on-demand security testing in Microsoft Azure.

servicenow Synack-discovered vulnerabilities are triaged and remediated in ServiceNow.

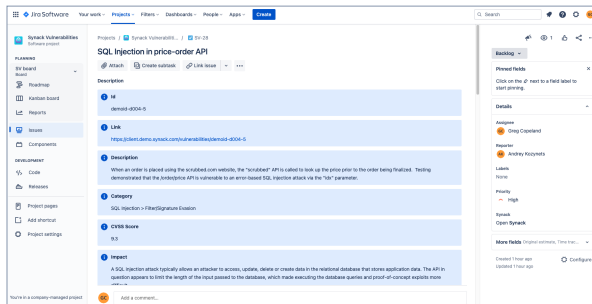
Jira Software Synack-discovered vulnerabilities and status updates are synchronized with Jira ticket handling. This enables immediate email notifications.

KENNA Security Import Synack-reported vulnerabilities into Kenna for prioritization and remediation.

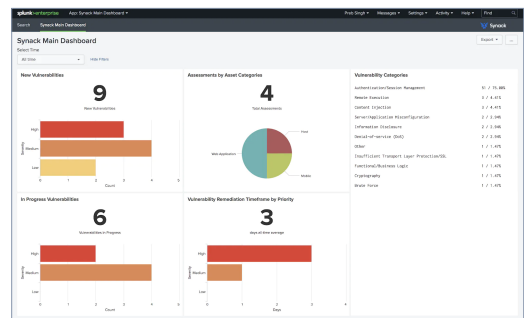
Qualys Imports Qualys vulnerability reports into Synack.

Netsparker Incorporates Netsparker vulnerability data into Synack security assessments.

splunk Integrates Synack offensive security testing results into Splunk's security operations.



Sample process operations integration between Synack and Jira



Screenshot from Splunk app of Synack integration

Build custom integrations with the Synack API

Synack's API is easy to use and designed to integrate with your team's existing security stack. Synack's API is a RESTful service to interact with Synack data, reports and test activity for full visibility across security teams. It can be used by customers to build custom integrations, and it is the basis for pre-built integration apps and modules created by Synack.

4

Reporting and Real-Time Analytics

Traditional pentest reports are descriptions of what was done during testing, what was found and what might be done about it. Those reports become a fossilized memento. Without responsive analytics and trend analysis, the report and analytics are useful for just a moment in time without context of what happened before or since.

Synack delivers a better way to communicate pentesting analytics and results. By focusing on key innovations, such as customizability, scheduling and human components, Synack creates an experience that puts customers in the driver's seat.

Real-time analytics

Dashboard

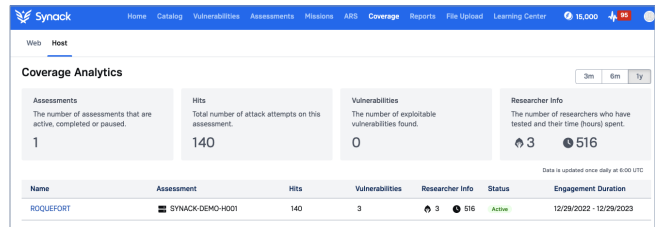
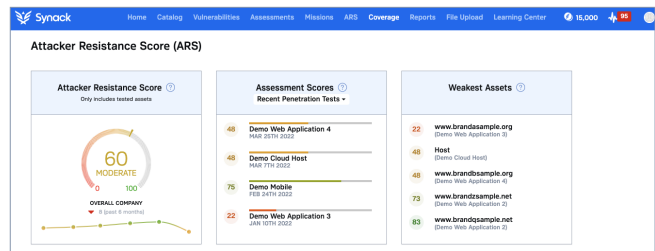
Customer portal includes testing data at a glance, including new findings, burndown charts, patch verification and historical findings.

Coverage Analytics

Provides real-time views and reporting on what (e.g. domains, subdomains, API endpoints), when and how assets are tested (e.g. number of researchers, attack types, hours of penetration testing).

Attacker Resistance Score

Quantifies and tracks attack surface resilience over time. Organizations and individual test scores change over time and are compared to key industries.



Reports

Configurable, Flexible Reporting

Synack provides customizable, compliance-ready reports suitable for business or technical audiences that encompass scope, testing information, vulnerabilities and remediation status.

Human-Written Summaries

Tests come with summaries based on a security expert analysis of the testing data.

Vulnerability Reports

Clear descriptions of found exploitable vulnerabilities, including statistics, steps to reproduce, screenshots and suggested patches.

Best Practice Reports

In addition to vulnerabilities, some Synack offerings include weakness checks that can be easily shared with developers, operations, auditors or regulators to confirm implemented best practices.

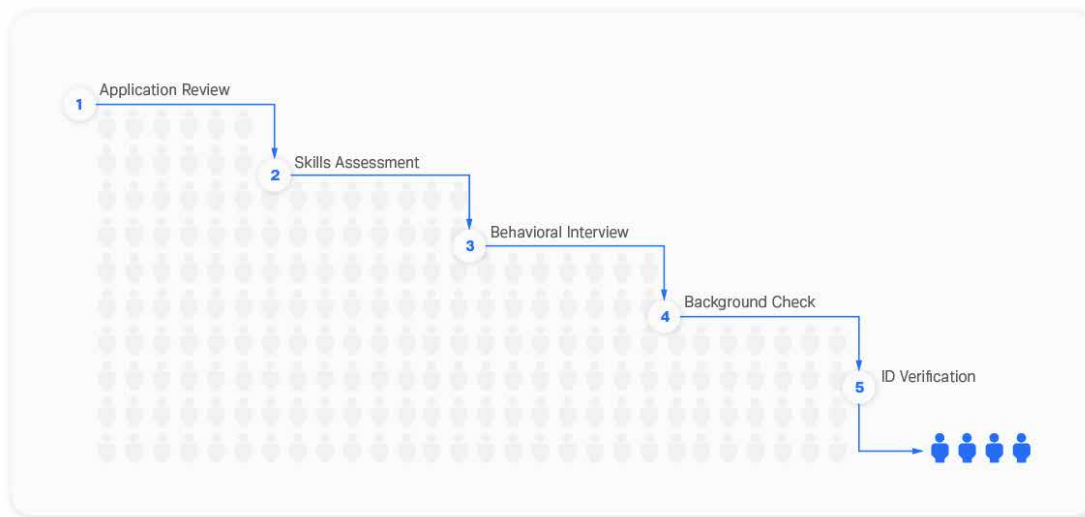
5

Managed Community Access

Access to a community of security researchers you can't hire or find. Easily launch dozens of structured security tests on-demand.

Researcher vetting

Five-step vetting process including background checks, skill assessment and video interviews.



Fully managed researcher payouts

Unlike bug bounty companies, Synack handles all payments and communications with our security researcher community.

Proactive researcher rotation

Synack rotates cohorts of researchers automatically to provide better coverage and more diverse perspectives.

Researcher skills matched to your targets


SRT members only have access to targets where they have demonstrated skill through technical assessments and proven ability to succeed.

Professional Titles	Software Developer	Penetration Tester/ Red Teamer	Security Analyst	Cryptanalysis	Network Administrator	Cyber Incident Responder
Recon Skills	Software Kill Chain	Dark Web Recon	Change Detection	Social Media Analysis	Digital Footprinting	OSINT
Technologies	PHP Environments	Docker and Containers	Kubernetes	Linux Environments	Cloud: Azure, GCP, AWS	Microsoft AD Environments
Asset Types	Web App	Cloud	API	Host/Infrastructure	Mobile	OT/ICS/SCADA
Vulnerability Expertise	SQL Injection	Remote Code Execution (RCE)	Cross Site Request Forgery (XSRF)	Session Authentication	Lateral Movement	Privilege Escalation
Offensive Security Skills	Remediation Guidance	Tools Development	Web Application Testing	Malware Analysis	Password Brute Force Testing	Reverse Engineering
Certifications	CISSP	Offensive Security Certified (OSCP)	GCIH	ECES	CCNP	eMAPT
Languages	English	Spanish	Arabic	Portuguese	German	Hindi

Nicolas Krassas
Switzerland




Reverse Engineering / System and Network Security / Virtualization / TCP/IP / CHECKPOINT/ VOIP / CISCO / Security Auditing




SYNACK RECOGNITION
Guardian of Trust

Ian Beers
United States




OSINT / Threat Modeling / Authentication Attacks / Cyber Attacker Psychology




SYNACK RECOGNITION
SRT Envoy

Mustafa Can İPEKÇİ
Turkey



SQL Injection / Remote Code Execution / Cloud Exploitation



SYNACK RECOGNITION
SRT Titan

BattleAngel
India



Web Application Pentesting / Network Vulnerabilities / Exploiting Misconfigurations



SYNACK RECOGNITION
SRT Envoy

Incentive-driven model

At Synack, security researchers are not in a race to submit first. There are multiple ways for members of the SRT to earn compensation, which results in higher quality findings for clients. They get paid out for missions, vulnerability identification, report submissions, patch verifications and community mentoring.

On-demand security tests

A comprehensive list of on-demand security tasks researchers can complete in days, including zero day response, vuln checklists, threat modeling and benchmarking against best practice frameworks like OWASP.

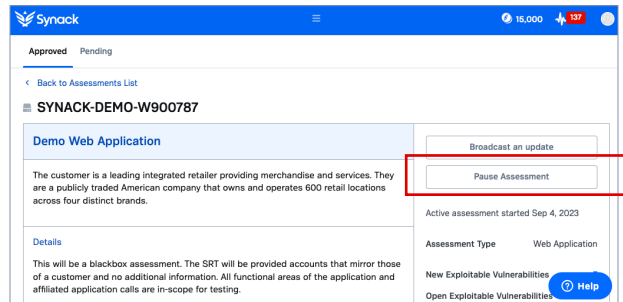
6

Testing Controls

Achieve full control and visibility over all testing traffic. Easily audit all testing traffic to spot trends, measure testing hours, and ensure coverage of your attack surface.

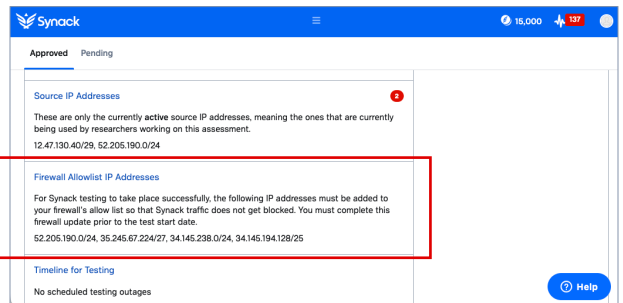
Pause Assessment

A button on each assessment page allows you to stop testing at any time.



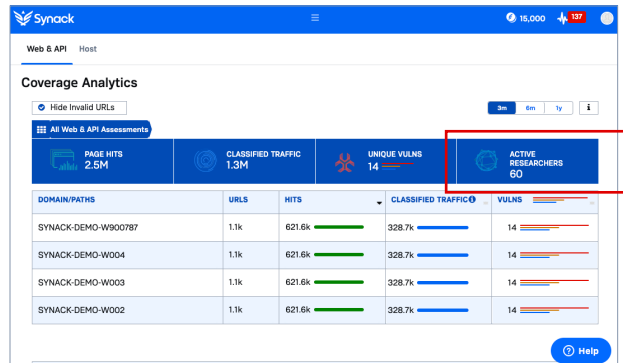
Firewall Allowable IP Addresses

This feature provides a range of IP addresses to whitelist, so researchers can get easy access to targets and you can easily identify their attack traffic.



Coverage Analytics

Synack leverages a testing traffic audit trail to provide analytics on what domains, subdomains, API endpoints, and IPs have been tested. Additionally, all researcher and scanning hours are tracked to provide a holistic view of attacker effort.



Synack Red Team Virtual Desktop Infrastructure

Testing can also cause concerns about where sensitive data and vulnerabilities are being stored. The Synack Red Team (SRT) use virtual workspaces to test as an additional security control. Customers receive data protection during the exploit process and the ability to cleanse data upon request.



Managed Vulnerability Disclosure Program

A vulnerability disclosure program (VDP) is a vital part of a strategic security testing plan. Most organizations don't have a process for external security issue reporting, which creates expensive and cumbersome internal workflows. A VDP program can help reduce noise and keep incidents from escalating.

Additionally, vulnerability disclosure programs are now a requirement for federal agencies and enterprises. Best practice standards for enterprises like ISO/IEC 27001, PCI DSS, NIST Cybersecurity Framework, and OWASP ASVS require a mechanism to receive vulnerability reports. BOD 20-01 requires federal government agencies to have a vulnerability disclosure program.

Key Features of the Synack Managed Vulnerability Disclosure Program

Synack's Managed Vulnerability Disclosure Program (MVDP) is included in the premium platform offering and provides end-to-end management of your VDP program.

Triage services and noise removal

Synack's Vuln Ops team will triage all vulnerability reports that come in, so your security team receives thorough and actionable reporting. Synack will check the vulnerability report for quality, validate the vulnerability exists, and provide actionable guidance on how to effectively address the vulnerability.

Researcher negotiation

Synack Vuln Ops will maintain consistent communication with members of the public who submit vulnerabilities. They will work with researchers to get more information about the vulnerability submitted and let them know when the vulnerability is successfully patched.

Researcher relations & expertise

Synack has 10 years of experience successfully managing relationships with security researchers. Synack has a vetted community of 1,500 security researchers called the Synack Red Team that are vital to our testing operations. Our experience navigating vulnerability disclosure programs for the Fortune 500 and for federal agencies speaks for itself.

Oversee your VDP and pentesting in Synack's integrated platform

Get real-time insight into vulnerabilities with Synack's client portal. Your security team can view all vulnerability data across your pentest and VDP program in one place. Track vulnerability details including CVSS score, remediation status, and patch efficacy.

Vulnerability management

Synack handles all stages of vulnerability management from initial discovery to patch verification.



Synack Catalog and Credits

Use our catalog of security testing offerings and platform credits model to build and execute a flexible testing program. Once you identify your security goals using Synack's risk-driven approach, you can select from offerings such as continuous testing with Synack365, OWASP and NIST vulnerability checklists, spot checks for CVEs like Log4j and more.

We designed Synack's security testing solutions to pair with your organization's security goals, keeping in mind that certain industries, like the public sector and healthcare, have specific requirements to achieve success.

The Synack Catalog: Align your security goals

We provide credits to launch on-demand security testing at any time through the Synack Catalog, featuring vulnerability checklists, NIST checklists, individual CVE/zero day tests and other targeted tasks to be performed by SRT researchers.

Available Now

- Cloud
- Compliance Checklists
- Focused Research
- Hacker's Perspective
- Microtests
- Security Benchmarks
- Vulnerability Checklists**
- Campaign Retest
- CVE Campaigns

Vulnerability Checklists

Vulnerability Checklists are a look for vulnerabilities. Most of them are based on the OWASP security frameworks and ensure that all stakeholders can see the checks were performed, regardless of the outcome. These provide in depth briefs for auditors, your internal stakeholders and as proof of having been checked in a methodical and thorough manner. This is also where the issues that may be not currently exploitable or other lower impact findings will be surfaced.

- Synack Android Basic Checklist** | 25 missions | **64 Credits**
The goal of this testing checklist is to ensure basic penetration testing coverage for Android mobile applications. It can also be deployed as a means to pr...
- Synack Android Premium Checklist** | 64 missions | **104 Credits**
The goal of this testing checklist is to ensure comprehensive penetration testing coverage for Android mobile applications. It can also be deployed as a m...
- Synack Host Basic Checklist** | 25 missions | **86 Credits**
The goal of this testing checklist is to ensure basic penetration testing coverage for host infrastructure. It can also be deployed as a means to provide au...

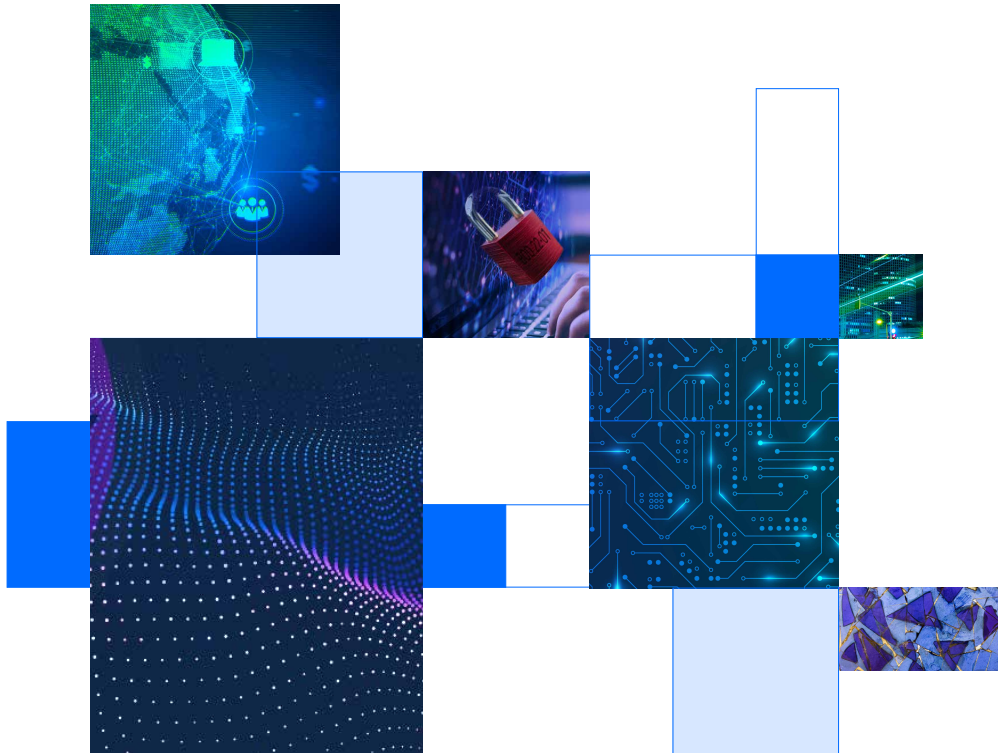
We can help you to rethink how your organization does security testing. By changing your security testing methodology, centralizing and standardizing vulnerability reports and creating a flexible security testing menu for customers, our platform can help security teams improve test efficacy and leverage vulnerability data strategically.

Synack Credits: Build a flexible testing program

Credits can be used to invest in a structured security testing program that works for you.

Examples of our credit model

400-credit plan	1000-credit plan	5000-credit plan
<p>A security team from an SME has to test a high priority web application for compliance. They also want to test for zero days that could lead to a breach if not addressed in a timely manner.</p>	<p>A new CISO of a small government agency has inherited an unknown attack surface and needs to conduct some open source intelligence work. They also want to run a more extensive pentest on some of their critical applications while testing the network for any common vulnerabilities like SolarWinds.</p>	<p>A large enterprise has an attack surface that's large, complex and potentially a target for nefarious actors. They need to develop a plan for testing their high priority external assets continuously while running an annual pentest on a few others that are less of a priority.</p>
<p>Synack14 x1 240 credits</p>	<p>Synack90 x1 600 credits</p>	<p>Synack365 x2 2480 credits 1240 credits each</p>
<p>Web Premium Checklist x1 130 credits</p>	<p>Synack14 x1 240 credits</p>	<p>Synack90 x3 1800 credits 600 credits each</p>
<p>Vuln checks x10 30 credits 3 credits each</p>	<p>Digital reconnaissance x1 150 credits</p>	<p>Synack14 x3 720 credits 240 credits each</p>
	<p>SolarWinds x1 10 credits</p>	



Conclusion

Flexibility, 24/7 Availability and Support—All in One

Capable. Confident. Synack delivers an industry-leading security testing experience for our customers. We provide a range of point-in-time and continuous options for security testing, depending on the risk of the asset. Once you've selected a testing strategy that matches your organization's security goals, you'll see improvement in your security posture with each deployed test. The Synack Platform consolidates results, so you can identify root causes of vulnerabilities and plan strategically. The Synack Catalog also extends Synack's security testing capabilities into areas like digital reconnaissance, API security, and checks for specific vulnerabilities such as SolarWinds or Log4j.

You will no longer have to guess where to focus your security testing efforts based on a point-in-time, compliance-driven pentest. Instead, you can embrace an asset-based, risk-driven approach that results in concrete improvement of your security posture, improvement that you can effectively communicate to executives and board members.

Contact us for a demo at synack.com/contact.