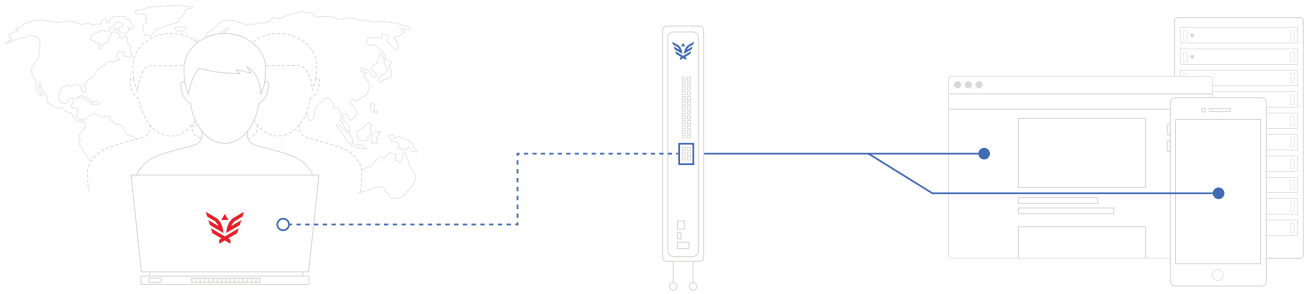
# Synack Crowd Security Intelligence™

Data Sheet

## Crowdsourced Application Security & Penetration Testing from the World's Best Ethical Hackers

Synack is pioneering a trusted, hacker-powered approach to protecting an organization's digital attack surface. Our private crowd of skilled and trusted hackers, the Synack Red Team (SRT), provides proactive application security penetration testing from a truly adversarial perspective—detecting and reporting vulnerabilities within clients' web and mobile applications, host infrastructure and networks, and connected IoT devices, that often remain undetected by traditional security solutions.

The solution combines the human ingenuity of the Synack Red Team with the scalability of Hydra, our proprietary vulnerability intelligence platform, to mimic attacks and discover the vulnerabilities that real-world hackers can leverage to gain access to IT systems. The cloud-based, crowdsourced solution allows the enterprise to initiate an engagement quickly with more time on target, and presents a controlled and continuous adversarial view of the organization's application and infrastructure security. Acting as a closely integrated extension of internal security teams, the Hydra-enabled SRT delivers exploitation intelligence that reduces windows of risk exposure and provides comprehensive testing coverage across vast, complex enterprise assets.



### SRT + Hydra Technology

Hydra technology enables the Synack Red Team to continuously discover vulnerabilities efficiently and effectively.

### LaunchPoint™

All Synack Red Team testing activity is routed through our secure gateway technology, providing our clients with full transparency and control.

### Customer Assets

Synack tests each customer asset on a continuous basis and provides real-time testing coverage results and analytics.

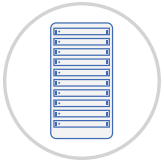
---

**Web Application Assessment**

Web applications still make up a large portion of the enterprise core product portfolio for customers. The Synack Platform performs continuous analysis of externally facing web applications for exploitable web-based vulnerabilities.

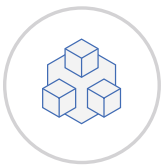
**Mobile Application Assessment**

71% of the F500 have built a home-grown native mobile application, yet only a small percentage of those companies actually test them for security vulnerabilities. The Synack Platform identifies problems with the application and underlying API/network-layer traffic that are often overlooked.



**Infrastructure**

Enterprise, host-based infrastructure is highly dynamic, requiring changes to be tracked on a regular basis. The Synack Platform monitors externally facing assets to determine if software updates or configuration changes have introduced new security vulnerabilities.



**IoT**

IoT is comprised of predominantly sensor-based products with limited computational power that renders legacy security detection measures such as AV redundant. The Synack IoT assessment consists of ongoing security testing to identify issues within firmware, APIs, business logic and physical devices.

# Features and Benefits

**The following is a list of key features in the Synack Platform:**

| | |
|---|---|
| **Web Management Platform**<br>Included | Synack's client portal offers users an easy-to-navigate web interface that gives them access to the following: internal vulnerability management, communication with the Synack Red Team members testing their assets, engagement updates, reporting options, and patch verification services. |
| **LaunchPoint™**<br>Included | Clients benefit from LaunchPoint™, Synack's proprietary secure gateway technology. All SRT testing activity is routed through LaunchPoint™, providing clients with full transparency of testing coverage, findings, insights and analytics, and the auditability and controls necessary for crowdsourced testing of an enterprise environment. |
| **Hydra Technology Platform™**<br>Included | Clients benefit from the Hydra Technology Platform™, Synack's proprietary technology that continuously probes and scans the assets and applications in scope and alerts the SRT members to newly detected findings, such as attack surface changes or suspected vulnerabilities. |
| **Mission Ops Team**<br>Included | The Synack Mission Ops team is an internal team of vulnerability experts that works closely with clients throughout their engagements to deliver the following services: asset definition and scoping, SRT communication and management, comprehensive vulnerability triaging & management, and periodic engagement outbriefs. |
| **Implementation**<br>Included | The Synack Platform is cloud-based, providing flexibility and speed for your security team. As a result, Synack can start an engagement in 24 hours, helping your team scale and respond quickly to security issues uncovered in business critical assets or the risk and compliance requirements for a security audit. |
| **Onboarding / Training**<br>Custom | At the kickoff of every engagement, the Synack Mission Ops team offers training for all internal business and technical stakeholders, educating them on the Synack model and client portal usage. In addition, Mission Ops provides ongoing customer support and comprehensive management throughout the entirety of an engagement. |
| **Integrations**<br>Custom | Synack's platform supports multiple integrations to meet enterprise requirements for internal security policies and compliance as well as optimizing security operation workflows for vulnerability management.<br>• Single Sign-On support utilizing SAML2.0 is supported for centralized user credential management.<br>• A REST API is available to retrieve and update vulnerability statuses for seamless integration with ticketing or GRC systems used for vulnerability management or compliance audits.<br>• A dedicated connector for Jira Cloud is built-in and ready to use. |
| **Production, Beta & QA Environment Testing**<br>Custom | The Synack Platform can provide security testing of production as well as Beta and QA environments. When used in conjunction with LaunchPoint™, site-to-site VPNs can be leveraged for internal network segments. This gives your organization ultimate control of testing products at the appropriate development cycle for your organization. |
| **PCI Compliance**<br>Custom | Synack's subscription models meet the PCI DSS requirements for an external penetration test, and a specific PCI-scan report required for auditing purposes can be generated at will during and/or after an engagement. |
| **Patch Verification**<br>Custom | Patch verification gives customers the ability to request an independent review of a vulnerability patch in order to ensure that the attack vector specified by the vulnerability report has been closed. All patch verifications are performed by the Synack Red Team (SRT) working in conjunction with the Synack Mission Ops team, creating a true find-to-fix model that can be managed entirely from within the Synack portal. |