DATA SHEET

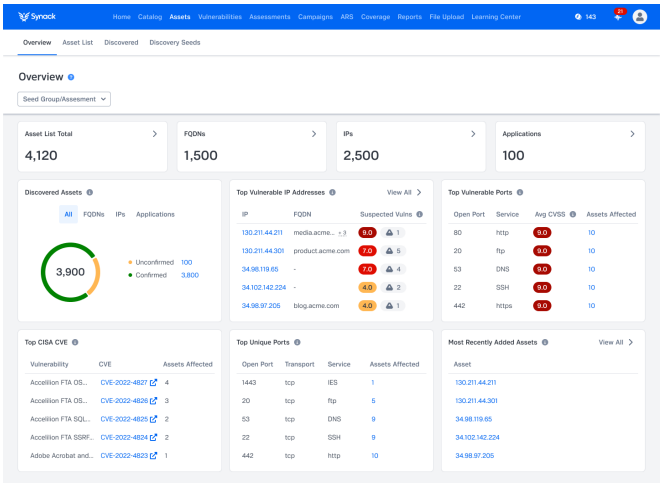
Attack Surface Discovery

Discover and manage your external attack surface with asset discovery and on-demand, continuous pentesting

Part of the Synack Platform Elite Tier

Only 9% of large organizations believe they monitor their whole external attack surface. Without an accurate inventory, unmanaged assets and risks persist while testing efficacy falls short.

Security teams using Attack Surface Discovery (ASD) will surface new IPs, applications and FQDNs previously unknown or unaccounted for, augmenting Synack's repository of tested assets. A comprehensive inventory is an important first step prior to security testing and empowers organizations with strategic, actionable intelligence.



Asset Dashboard Overview

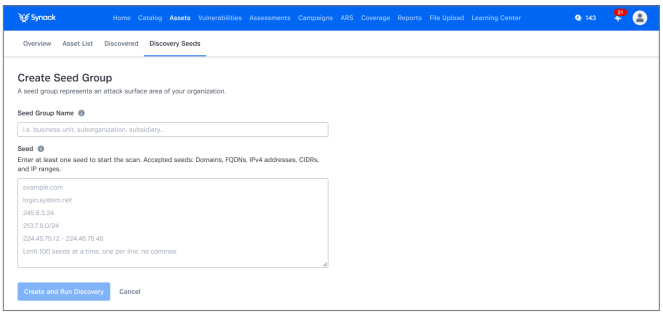
Your security team can use Attack Surface Discovery to:

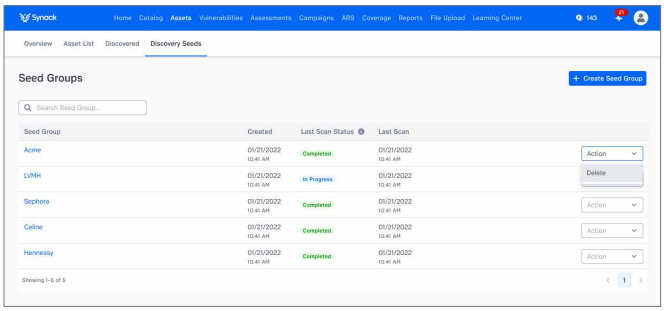
Produce an accurate inventory for pentesting	Maintaining an accurate and comprehensive inventory is vital for reducing risk and effective security testing.
Understand the scope and risk of shadow IT	Synack scans continuously to discover new assets, so your team never misses a new application or insecure system again.
Prioritize and mitigate risks with testing	Uncover assets that belong to your organization and use filters (i.e. suspected vulnerability severity, ports, software provider) to help prioritize assets for pentesting.
Stamp out third-party risk	Target discovery via passive scanning to specific parts of the infrastructure, suppliers, subsidiaries, and M&A targets by using seed groups.
Manage risks and vulnerabilities	Learn details relevant to your discovered assets, including suspected vulnerabilities, open ports, geolocation, and their testing status. Also, view Top CISA CVEs and the assets they impact.

Attack Surface Discovery Key Features

Self-Service Seed Discovery

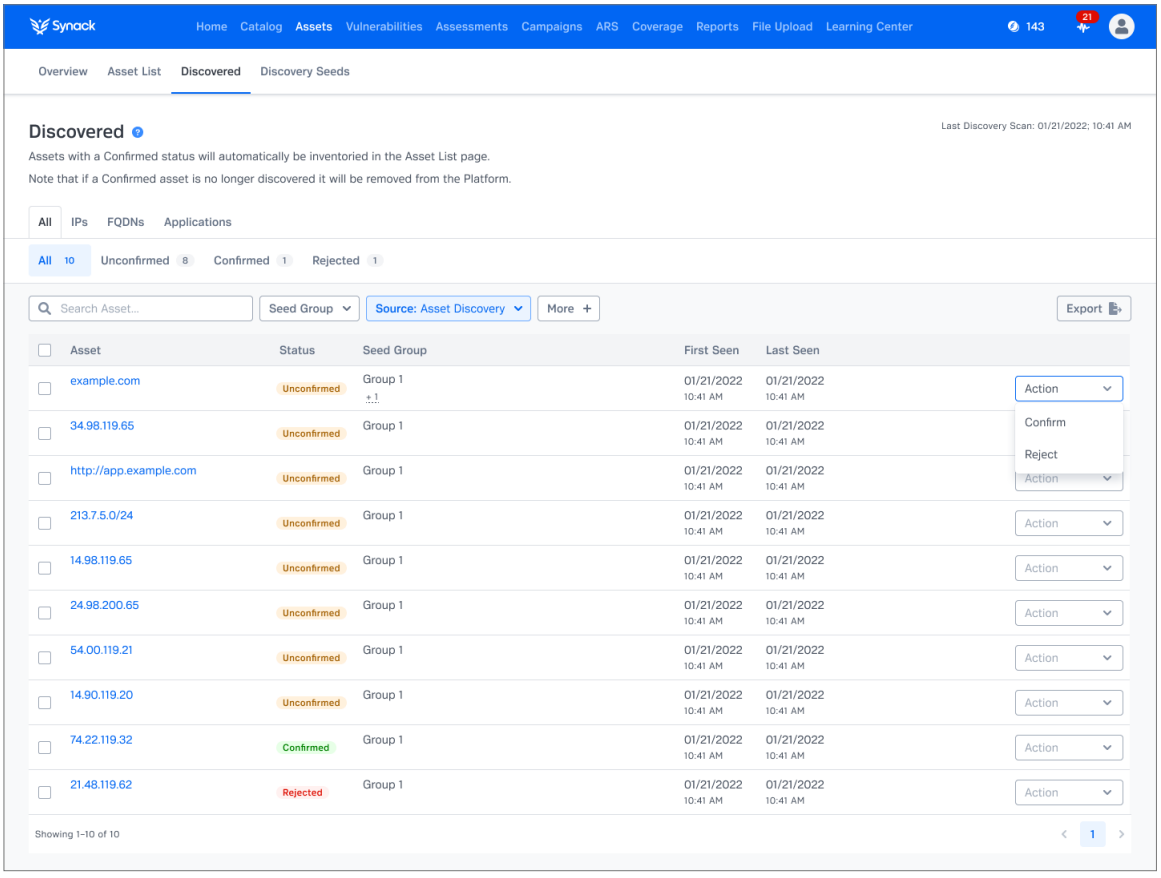
Customers can quickly add assets (i.e. domains, IPv4 addresses, CIDRs, etc.) into a seed group and launch a scan. Seed groups automatically segment assets, so you can clearly attribute assets to team divisions as well as subsidiaries, mergers or acquisitions. Security teams can control access to each group with role-based access controls.





Discovered Assets

Synack surfaces assets from past assessments and scans in a new Discovered Assets dashboard. All discovered assets are tagged with their original seed group. Security teams can easily filter for IPs, FQDNs or applications. They can also take bulk actions to confirm, unconfirm or reject discovered assets. All accepted assets appear in the Asset List alongside any assets Synack has tested in the past year.



Asset Insights

Discovered and confirmed assets receive Asset Insights, a tool to discern risk. External host assets are scanned for risks, which can then inform decisions for further testing. Assets under test show SmartScan suspected vulnerabilities and exploitable vulnerabilities found by the Synack Red Team.

Learn more about Asset Insights >

Not Just a Standalone Feature – A Fully Integrated Elite Platform Offering

Elite Platform Highlights

- **Attack surface discovery**
  Synack's ASD offering discovers and inventories untested and often unmanaged assets. Customers can easily scan for additional risks on discovered assets such as open ports, suspected vulnerabilities and old software versions.

- **Managed community access**
  Synack manages access to Synack Red Team, a community of 1,500 researchers, overseeing all vetting, payments and communication.

- **Synack engineering and customer support**
  Synack's Elite Platform includes a named support team, including a customer support engineer and a customer success manager. This team helps your organization with risk management by highlighting risky discovered assets and scoping new assets for testing.

- **On-demand pentesting**
  Security teams can add newly discovered external assets to a new assessment via the assessment creation wizard (ACW) and launch point-in-time or continuous pentesting with credits. Get more assets tested with ease.

- **Vulnerability management**
  Synack discovers, assesses and verifies remediation of vulnerabilities. Once discovered assets are confirmed, they will be scanned for suspected vulnerabilities. If assets are pentested, Synack will provide human-written reports for exploitable vulnerabilities and re-test to ensure the patch is valid.

Learn more about the Synack Platform >