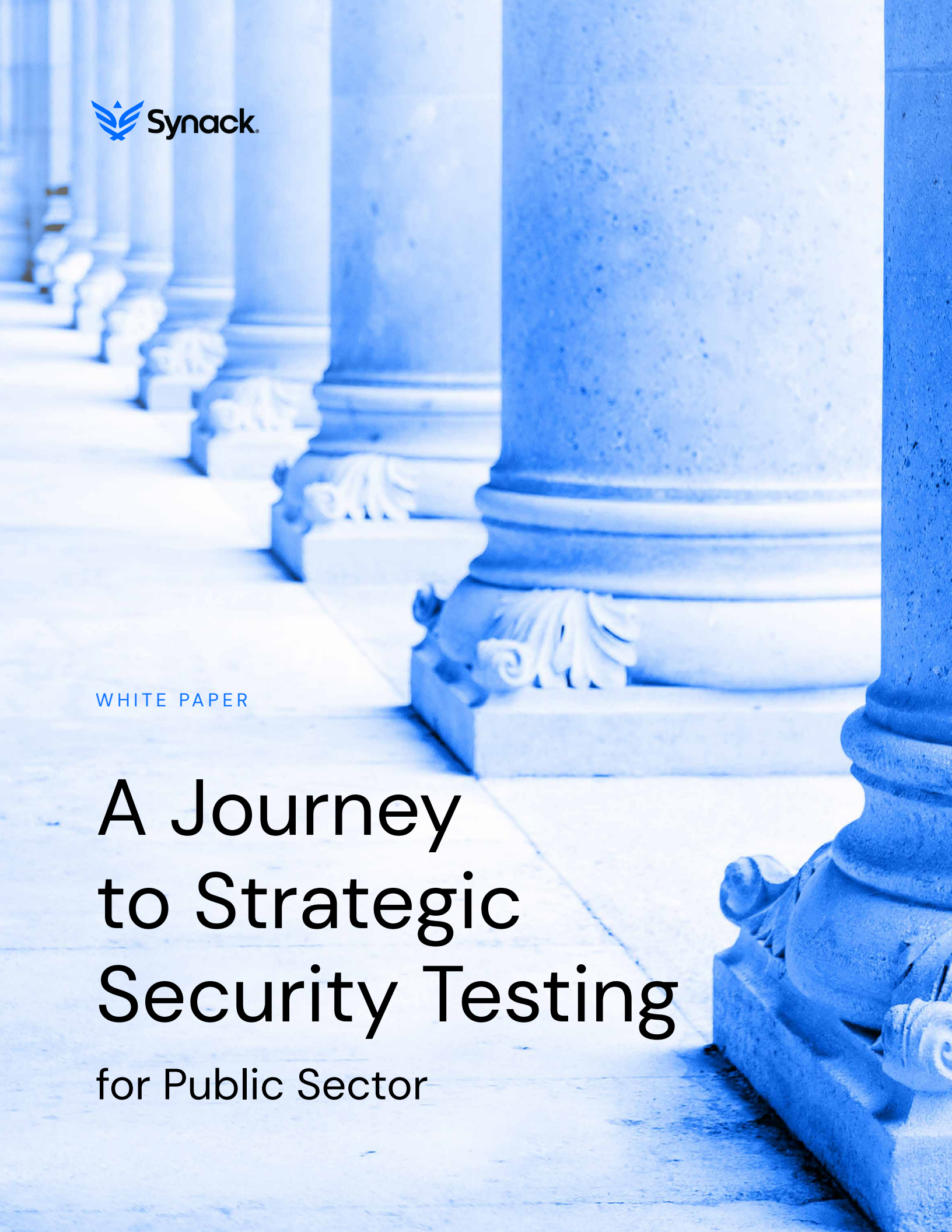


Synack

WHITE PAPER

A Journey to Strategic Security Testing

for Public Sector

Security Testing Today

Most security testing programs, particularly penetration testing, are compliance driven and performed once or twice a year. While this satisfies the regulators, the effort, investment, and results don't sufficiently inspect your applications and infrastructure for vulnerabilities or provide information enabling continuous improvement to your organization's security posture.

A CISO PERSPECTIVE

"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."

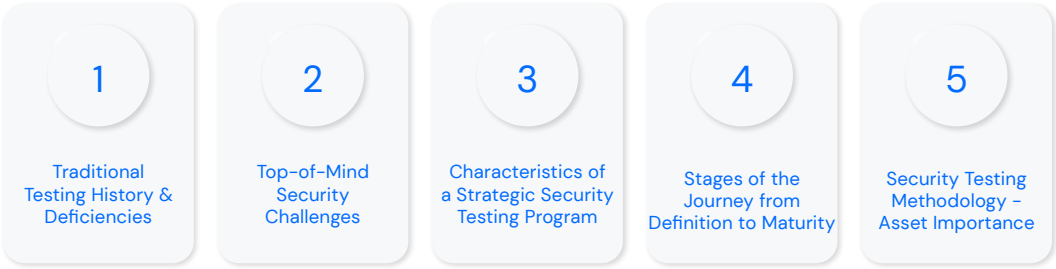
In an era of scarce security resources, fierce competition for top cybersecurity talent, conflicting priorities and limited budgets, government organizations can't afford anything that doesn't have a measurable impact on security posture. Standalone pentest reports don't compare results across organizations/regions/applications, assess whether there's improvement over time, or understand the root causes of systemic compliance deficiencies. They can ironically include all of the tactical work while failing to capture any strategic benefits.

Synack offers a better way: a strategic testing program that demonstrates you're leveraging security testing for more than compliance. We provide insight into gaps in your security program that both improve your security posture and allow you to confidently accelerate your software and cloud migration initiatives, reducing your inheritance risk as you consolidate and move to the public cloud.

Digital transformation has become increasingly important because it helps organizations modernize. Modernizing not only helps organizations better serve their constituencies, it also makes it easier for them to attract quality computer-savvy talent in an increasingly tight market. And to drive digital transformation, organizations are moving compute processing to the cloud for its efficiencies, scalability and resource savings. Digital transformation can lead to significant productivity and performance benefits, but it does bring additional risks that need to be identified and mitigated.

A true strategic testing program can meet your compliance obligations while significantly improving your testing program efficacy by providing insights into resiliency trends (across organizations, regions, applications, etc.) and identifying root causes of vulnerabilities so you can stop creating them. Deploying testing early, in the development phase rather than waiting to test after deployment can help make applications secure by design. Imagine a world where security testing is a productivity enabler aligned with organization risk—not just compliance. And for cloud-first environments, Synack empowers government agencies to procure continuous penetration testing, having been awarded FedRAMP Moderate Authorized status, the highest designation realized by any continuous security testing provider in the Pentesting as a Service space.

Transforming your security testing program is a journey, not a destination, and we'll discuss a methodology that allows you to align your transformation journey with the realities of your organization, budget and priorities. In this document, we'll explore:



Traditional Testing

Traditional penetration testing—typically driven by compliance and performed annually—was designed for a different era. Periodic testing may have been appropriate for highly structured waterfall software development models, but it fails to keep pace with today's dynamic continuous development and deployment processes. This fundamental misalignment between the traditional testing methodology and today's security challenges is not the only barrier to improved test efficacy.

Traditional testing deficiencies include:

1. Infrequent testing of continuously developed and deployed applications
2. Unlikely that one or two testers has sufficient diversity of skills and experience to assess flaws in today's complex application architectures and infrastructure
3. Significant testing lead time leaves application updates exposed to new vulnerabilities
4. Slow to assess the impact of new critical vulnerabilities like Log4j
5. Standalone reports do not provide insight into resiliency and security posture over time, across departments or across regions
6. Testing results and requests can't be integrated into security operations processes

For most organizations, traditional security testing is a siloed process required to satisfy compliance requirements such as PCI DSS, NIST SP 800-53, SWIFT and FINRA. They rarely consider how security testing can address challenges like supply chain hygiene, third-party risk and hardening mission critical assets. The capacity and effort needed to spin up occasional penetration tests can be a burden to overworked security teams.

Top-of-Mind Security Challenges

With a strategic security testing program, these risks can be better understood and mitigated:

Hardening Mission Critical Assets	Enterprise had 130 security breaches/year, a 27.4% increase. (PurpleSec 2022)
Ensure Supply Chain Hygiene	In 66% of supply chain attacks, suppliers did not know how they were compromised. (Forbes 2022)
Close Infrastructure Gaps To Reduce Unstructured Attack Risk	93% of networks can be penetrated. (Forbes 2022)
Secure Cloud Migration	79% of companies have had at least one cloud data breach. (IDC 2022)
Assess Third-Party Risk	More than 600 third parties are known to have been affected by the MoveIt vulnerability. (WSJ 2023)
API Security	67% of development teams found API-related security issues and vulnerabilities during the testing phase. (Google 2022)
Scale Security Testing Program	There were an estimated 3.5 million open cybersecurity jobs by the end of 2022. (Comptia 2022)
Reduce Security Testing Latency	The industry average lead time for "non-platform" pentesting ranges 4-8 weeks.
Report On Cyber Risk	88% of boards of directors view cybersecurity as a business risk. (Gartner 2022)

For example, in the case of third party risk, there's often a mismatch between your acceptable risk levels and those of a partner technology. When a third party has an undisclosed vulnerability in their ecosystem, it can later become your vulnerability. Synack's security testing program can provide a unique perspective on the risk of a partner's external attack surface before connecting their environment to yours.

Characteristics of a Strategic Security Testing Program

A strategic security testing initiative serves two important functions in any security program:

1. Maximize security testing efficacy with identification of exploitable vulnerabilities so they can be fixed.
2. Maximize security posture improvements by analyzing testing data to identify root causes so they can be addressed.

In order to maximize test efficacy, we have established a testing methodology that enables more comprehensive infrastructure coverage that spans applications, APIs, infrastructure, cloud and mobile. Tester diversity must match attacker diversity and ensure the speed and depth of test coverage, keeping pace with rapid development processes and increasingly sophisticated adversaries.

Tactical

Test Operations
Maximize Test Efficacy

Critical infrastructure coverage

- Applications
- API
- Infrastructure
- Cloud
- Mobile

1,500 of the world's best security researchers

- Testing diversity that's difficult to match with internal testers

Speed and depth of testing coverage

- Keeps pace with continuous development cycles

Flexibility to test on-demand and continuously

Platform for real time visibility and control of testing process and results

Strategic

Test Analytics
Maximize Security Posture

Enables organizations to understand vulnerability root causes

- Consistent vulnerabilities on disparate platforms
- Team/process functional inconsistencies
- Inconsistent spend and posture

Insight into test coverage

- Applications, Hosts

Measures resilience

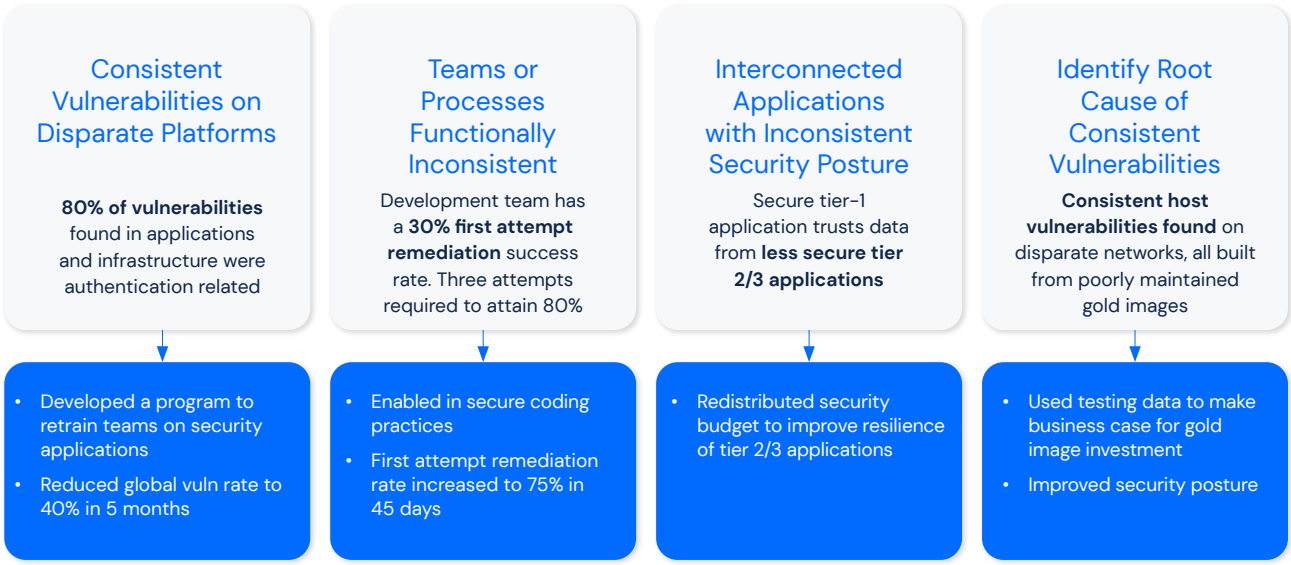
- Trending and comparison to previous results and peers

Reveals patterns and deficiencies in your security program

- Applications, Organizations, Geographies

Results available to leadership and board

A successful strategic testing program doesn't trade efficacy for strategic value. Rather, test efficacy is the foundation for a strategic testing program. If you employ the Synack Platform for test execution, all the data can be retained and analyzed to enable you to take action to stop vulnerabilities from being introduced in the first place. Here are some examples of vulnerability root causes found from the Synack testing process:

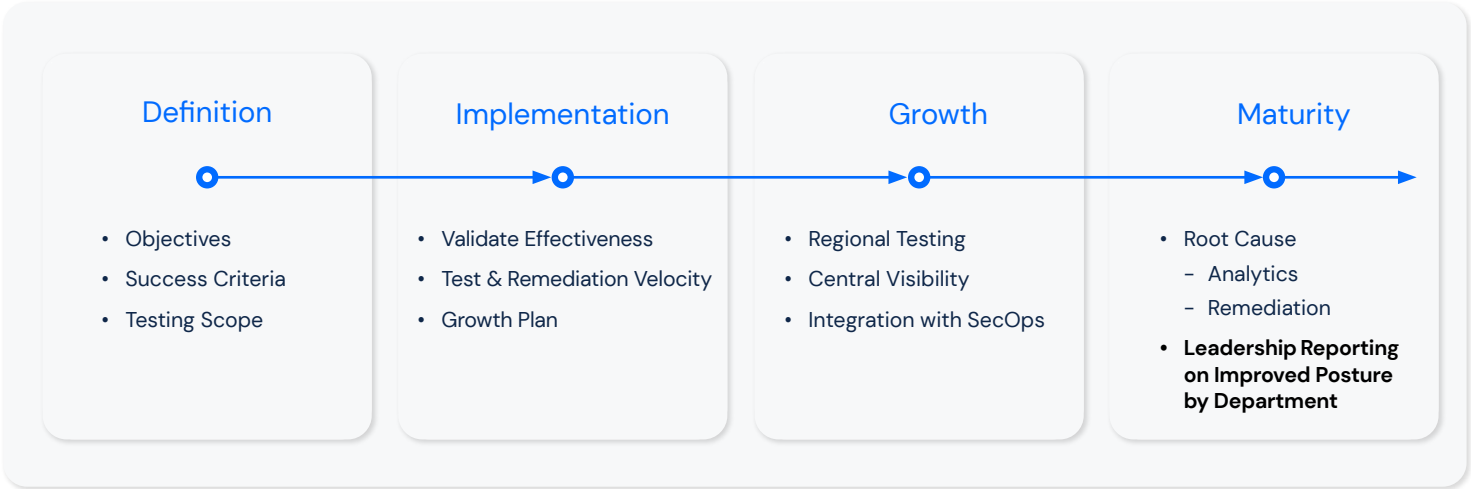


If you're like most security leaders, you:

- Like the concept of a strategic testing program but don't know how you'll transition away from your present compliance-driven tactical testing.
- Don't have the necessary internal expertise and capacity to mature your security testing program for your growing and increasingly complex attack surface.
- Need to navigate budget limitations.

Stages of Journey from Definition to Maturity

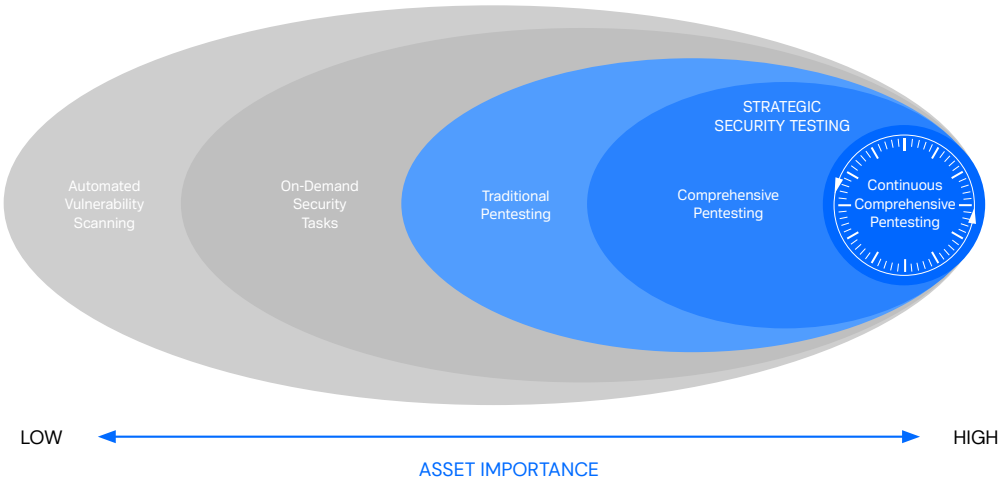
Achieving a mature security testing program is a process not an event. As you embark on your journey, it's important to define your desired outcomes for each stage, from definition through maturity. In the diagram below, we have outlined common outcomes for each phase. Your specific business objectives, budgetary constraints and processes may dictate adjustments to your outcomes.



Security Testing Methodology: Asset Importance

One of the critical initial steps in achieving strategic security testing is to define an asset's importance to business operations. More critical assets should receive more rigorous and continuous testing, whereas less critical assets should at least receive regular automated vulnerability scanning.

1. Criteria for ranking the importance/risk of attack surface assets (Application, Infrastructure, API, ...) from low to high
    - Importance of an application/service to the business
    - Risk of an asset
        - Is security testing a component of an asset's compliance requirements?
        - Does this application or asset contain sensitive data?
        - Is a critical release or update to this application expected this year?
        - Is the application business critical?
        - If the application was hacked, would it cause PR damage?
        - If the application was hacked, would it expose PII or PHI, or endanger citizens?
        - If the application was hacked, would the exposed data have a high recovery cost?
        - Rate this application's code complexity as "high," "medium" or "low."
        - Rate this application's usage as "high," "medium" or "low."
        - Rate the fault proneness of this application as "high," "medium" or "low."
    - An asset's proximity to critical app/service
        - Lateral movement risk — while an asset might not directly support an important business application, its proximity to a critical asset might dictate that it's tested as an important asset. If an attacker can establish a beachhead on the asset that's in close proximity to important applications, it's easier to circumvent existing security controls to gain access to a critical service.

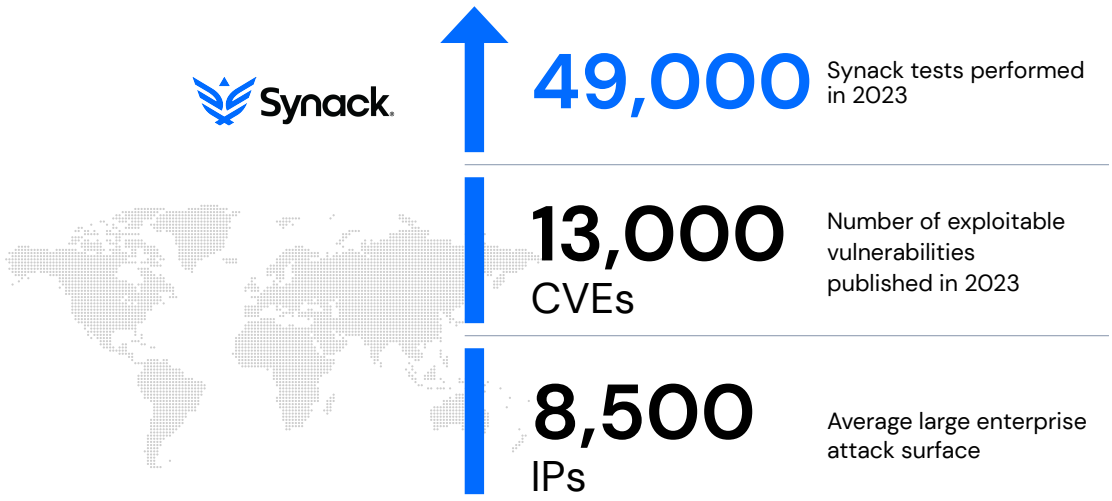


2. Identify the required level of security testing for each asset

SECURITY TESTING OPTIONS	TARGETS
Continuous Testing — 365 Days	Business-critical applications/services
Continuous Testing — 90 Days	Seasonal applications, recently merged systems/data
Targeted Penetration Testing	Important applications that don't frequently change, required for compliance
On-Demand Security Tasks	Activate researchers to test for zero days and CVEs like Log4j
Automated Vulnerability Scanning	Scan for known vulnerabilities on web applications and hosts

3. Synack Security Testing Platform

The results of asset importance analysis and desired testing options come together for test execution and root cause analysis in the Synack Platform.



By embarking on the journey to mature your strategic testing program, security can take the role of business enabler. Instead of adding friction to initiatives like digital transformation, security testing can proactively ensure there aren't any exploitable vulnerabilities. According to a recent survey, 82% believe their organization experienced at least one data breach as the result of digital transformation. Strategic security testing will increase confidence in infrastructure resilience so you can accelerate your digital transformation to drive business efficiencies, widening your competitive advantage.

So forget about the challenging level of effort to spin up traditional pentests over and over; with a Continuous/Comprehensive model, security leads set it up and the activity now becomes a Mission Process. It's time to transcend the "no news is good news" security posture of defensive security controls and leverage the Synack strategic security testing program to confidently accelerate initiatives that improve outcomes for public sector agencies.