SYNOPSYS®

Managed Network Security Testing (NST)

Reduce your risk of a breach by identifying security vulnerabilities in your network with on-demand network security testing expertise

Overview

Protecting your network is vital in today's connected world. But what if your team lacks the resources or skills to apply network security testing effectively across your infrastructure? Synopsys Managed NST enables you to implement network vulnerability analysis quickly so you can systematically find and eliminate security weaknesses in your external network.

Key benefits

- **Flexibility.** Our on-demand, easy-to-use portal empowers you to manage your assessments. Schedule tests and make modifications as business requirements change and threats evolve.
- **Coverage.** Test networks and systems you might miss owing to resource constraints.
- **Consistency.** Get the same high-quality NST results all the time for any network.
- **Enablement.** We walk you through your test results and help you develop a remediation plan best suited to your needs.
- **Scalability.** We provide scalable NST delivery through our Assessment Centers without compromising manual reviews.
- **Comprehensiveness.** Our blended manual and tool-based assessment approach includes a thorough analysis of results, detailed reporting, and actionable remediation guidance.

Get access to the resources you need to scale at speed

Our Managed NST assessments give you the testing flexibility, scalability, and cost-effectiveness to deliver the network testing coverage required to achieve your risk management goals. Through our Assessment Centers, you'll have continuous access to teams of network security testing experts with the skills, tools, and discipline to analyze your network and systems anytime. You can close testing gaps and quickly scale to manage high-demand testing periods.

Focus on actionable solutions

We'll never leave you with a laundry list of issues. At the end of each assessment, our experts will conduct a read-out call with the appropriate IT infrastructure/security team to review each vulnerability we identified during the assessment, answer your team's questions, and discuss actionable mitigation and remediation strategies.

Our testers search for vulnerabilities in:

- Access management
- Authentication controls
- Firewall filtering
- Information disclosure that may aid an attacker
- Known configuration errors
- Operating system software flaws
- Router filtering
- Server application software flaws
- Visible network services

We attack the targeted external network to uncover hidden vulnerabilities.

Managed NST assessment

Managed NST–Standard helps you identify common to critical security vulnerabilities in your external network and systems. We employ automated scanning with manual triage of the vulnerabilities we identify. Our manual testing checklist includes test cases for encrypted transport protocols, SSL certificate scoping issues, use of administrative services, and others.

6 reasons you need Managed NST

If you're facing one of these six challenges, it's time to turn to Synopsys to develop a network security testing plan.

1. **You're deploying new infrastructure.** Make sure servers, routers, load balancers, and other network devices that run software are sufficiently hardened to prevent access to critical data.
2. **You're changing network design or infrastructure.** Any major configuration changes or upgrades should require a retest of all network security.
3. **You're moving to a hosted environment.** Moving your network infrastructure to cloud environments such as Amazon Web Services (AWS) introduces a new attack surface that must be evaluated for proper configuration to ensure sensitive data isn't exposed to unauthorized users.
4. **You're deploying new or updated applications.** In addition to testing the applications themselves, you'll want to consider how they access your network resources.
5. **You're adding new locations for your business.** Use Managed NST to understand which resources are available and identify the types of traffic passing between sites.
6. **You're implementing a regular security plan.** Performing regular network security assessments can help you identify changes that may have slipped through the cracks and ensure you are using the most up-to-date security strategies.

Ready to get started?

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

12/17/18.ds-managed-nst.