

# VULNERABILITY SCOPE



Get a hackers-eye view of your assets, and see which assets are exposed to attack.

- Scientifically measure your defense-in-depth architecture.
- See which attacks your security products can and cannot block
- Develop specific mitigation strategies to plug holes in your defenses
- Monitor vendor effectiveness and responsiveness

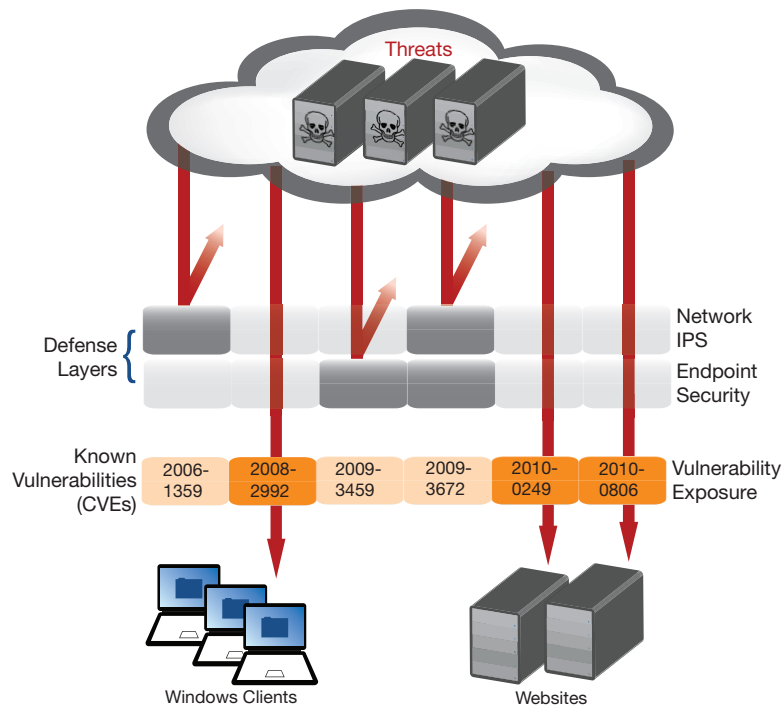
This unique service is available exclusively to NSS Labs clients. View comprehensive protection and exposure reports for critical assets and vulnerabilities in your organization (by CVE number).

## SAMPLE USE CASES

- **Improve operational security by identifying and prioritizing exposed vulnerabilities**

Identify gaps in protection immediately and prioritize remediation efforts. IT professionals can use Vulnerability SCOPE to determine whether new vulnerabilities put their organizations at risk, if they are protected, and to analyze mitigation options including patching, custom signature writing, vendor engagement, network policy changes, and others.

A comprehensive search function permits IT professionals to identify exposed vulnerabilities by Common Vulnerabilities and Exposures (CVE) number, asset type, attack vector, impact, and keyword.



The data in NSS Labs Vulnerability SCOPE is derived from recurring, scientific penetration testing of leading security products against high-impact and critical vulnerabilities – network and endpoint.

Dozens of products are tested over the course of the year, covering more than 1,200 vulnerabilities and growing. Covered products include:

- AVG
- ESET
- F-Secure
- Kaspersky
- McAfee
- Norman
- Panda
- Sophos
- Symantec
- Trend Micro
- Check Point
- Cisco
- Endace
- Fortinet
- IBM
- Juniper
- NSFOCUS
- Palo Alto Networks
- Sourcefire
- Stonesoft

- **Shortlist the best security products for the environment**

Vulnerability SCOPE can be used during the product selection process and for ongoing management efforts. The product with the highest % CVE coverage is not necessarily the best fit for your network and critical assets. This exclusive service can identify products with the most coverage for the assets you care about most. Learn which patches should be applied, and which can be 'virtually' patched with an IPS.

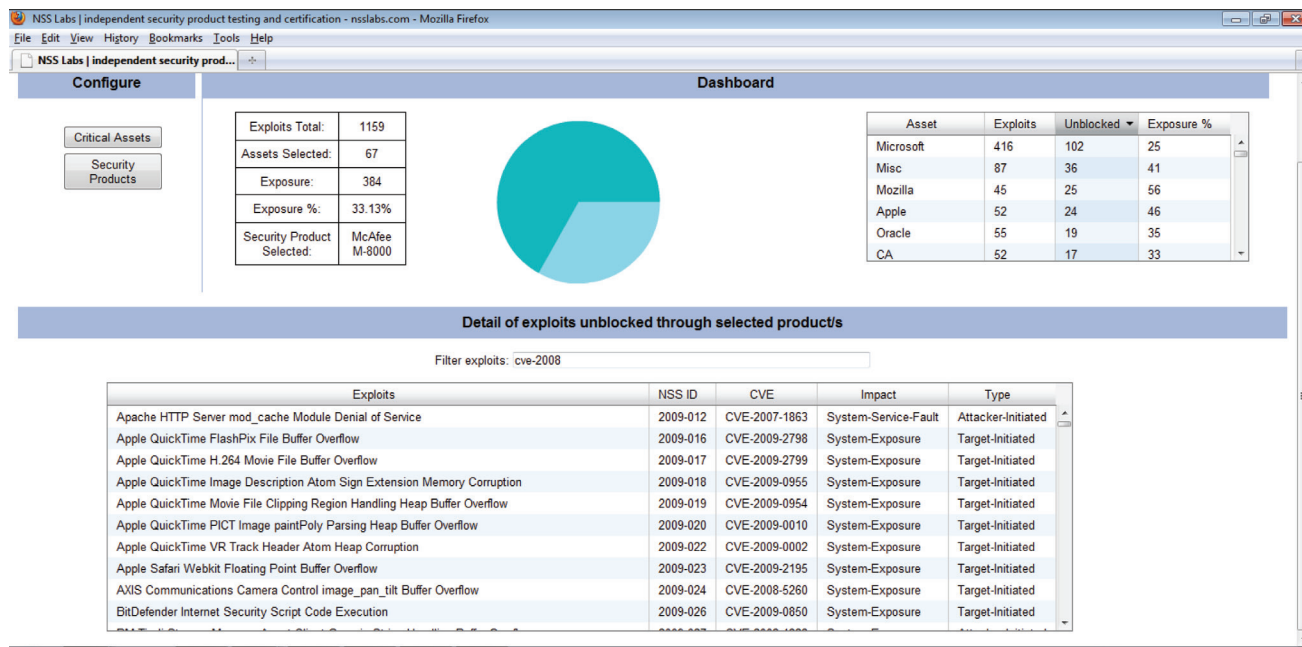
- **Model defense-in-depth scenarios**

Utilize knowledge of security product coverage and holes to model optimal combinations of security products across multiple layers. Identify the best combination of endpoint protection and network

intrusion prevention products to protect YOUR assets. Perform detailed "what if" analyses using different security product choices and configurations in order to answer questions like: "will changing from Vendor A's to Vendor B's network intrusion prevention system improve or degrade coverage?" "which specific vulnerabilities are putting our systems at risk?" and "which alternate signatures could be enabled to increase protection with existing products?"

- **Monitor and measure vendor service levels**

Updated quarterly with Live Test data, Vulnerability SCOPE allows IT professionals to analyze and monitor their vendors' progress in keeping up with current vulnerabilities. This research gives organizations the ability to monitor, benchmark, and manage vendor relationships and service levels.



Sample Vulnerability SCOPE Report

Contact us at [sales@nsslabs.com](mailto:sales@nsslabs.com) for information on delivery and pricing.