DATASHEET

NSFOCUS

NSFOCUS RSAS

Remote Security Assessment System

OVERVIEW

Network vulnerabilities are increasingly a common issue in today's complex computing environments. It affects almost every organization and everybody. There are multiple scanning tools. However, they provide basic scanning with limited functionality.

Vulnerabilities to the network prove that traditional scanning tools are insufficient for today's complex environment. An increasing number of users are shifting to tools that both detect and mitigate risks. Mitigation of vulnerabilities prevents potential disasters and disruptions to business operations.

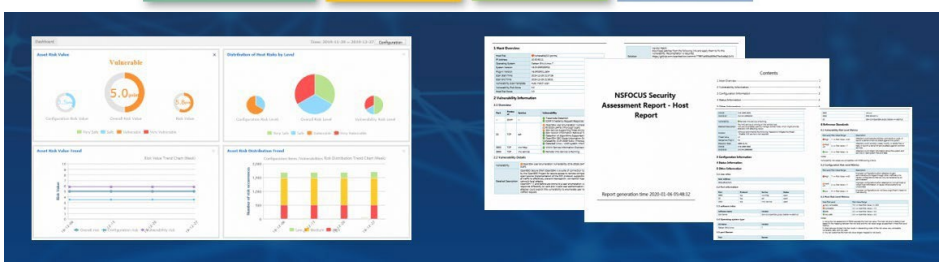
NSFOCUS RSAS provides a security assessment tool helping organizations manage risks, meet regulatory compliance, ensure secure configurations and uncover web application weak settings and vulnerabilities. The RSAS creates a platform for managing the vulnerability life cycle saving administrators time and effort from vulnerability discovery, risk prioritization, providing recommendations, hardening and revalidation.

COMPREHENSIVE SYSTEM WEAKNESS DISCOVERY

The RSAS is a market-proven vulnerability scanning tool. First launched in 2001, RSAS gains popularity and loyalty, providing cost-efficient comprehensive risk management to thousands of customers. It is constantly being upgraded based on customer requirements and up-to-date technologies.

Today's RSAS is equipped with an improved vulnerability scanner integrated with configuration verification, web-based vulnerability scanning and newer features such as cloud computing scanning, big data component scanning and IoT device scanning.

By selecting from a list of built-in templates, you can simply create a scan job. Then the RSAS will generate and present the actionable details on corresponding threat posture to you in minutes or hours through a configurable dashboard or report.



KEY BENEFITS

Comprehensive functions

Fast response to vulnerabilities
Complete view of all assets

Reduce operations burden and save time

Cost efficient

Meet regulatory compliance
Increase security posture

KEY FEATURES

Configuration assessment

Web-based vulnerability scanning

Cloud computing scanning

Big data component scanning

IoT device scanning

Closed-loop risk management

Patented risk rating technology

Dashboard demographics

Flexible deployment

Role-based asset control

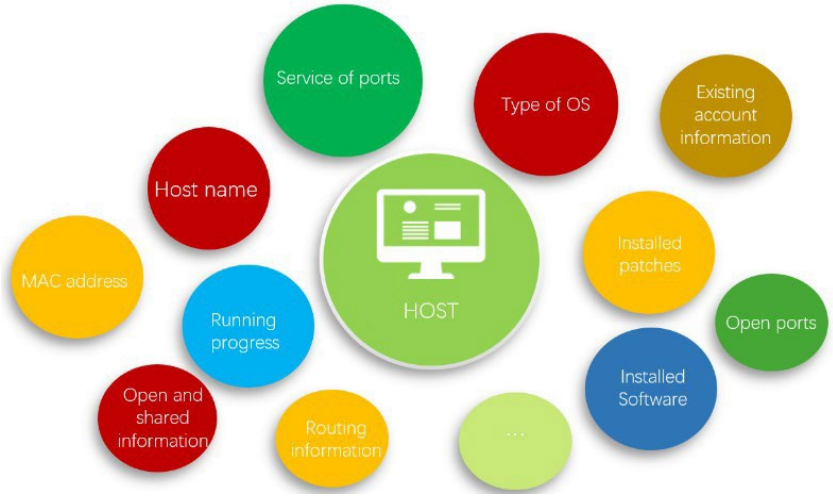
Audit logs

CLOSED-LOOP RISK MANAGEMENT

A secure and reliable network system comes with an effective risk mitigation process. NSFOCUS RSAS risk mitigation process comprises asset-centric risk management, risk prioritization and remediations that form a closed-loop risk management workflow. By proactively discovering vulnerabilities, the RSAS delivers assessment results to asset owners with revalidation to ensure remediation effectiveness.

Asset-Centric Risk Management

Protecting of IT infrastructure and assets is the foundation of network security. By building an asset tree, the RSAS facilitates prioritization of risk to assets. The RSAS can help customers quickly import and scan multiple IP addresses, and locate and remediate vulnerable assets. It also facilitates asset management with full asset visibility and informative risk assessment reports.



Intelligent Profile™ Technology

False positives hinder business operations by blocking essential applications or traffic.

NSFOCUS's Intelligent Profile™ Vulnerability Discovery Technology leverages on multiple technologies to correlate information. Profile Analysis of the results is done prior to releasing the classification.

Profiles, or "abstract information", of a target host, are built using multiple techniques to organize over 30 types of profile information, creating a validation loop with data analysis to ensure the accuracy of the results.

Patented Risk Prioritization

CVSS (Common Vulnerability Scoring System) scores are well received by penetration testers, IT operations and other industry vulnerability assessment users. However patching thousands of vulnerabilities sorted by CVSS is not practical. NSFOCUS recommends customers should find out which vulnerabilities are critical for their environment. The RSAS utilizes a market-proven network scoring criteria system that measures different weights for different factors. For system risk and asset node risk, for example, each is calculated using a unique algorithm to determine its severity.

EASE OF USE AND FLEXIBLE DEPLOYMENT

Effortless Quick Scanning

With the RSAS, customers can easily create scanning tasks with predefined templates and policies. You can start scanning a real-time scanning task or schedule a daily, weekly, monthly, quarterly or self-defined task. Setting priority allows critical tasks to be performed first to optimize network resources.

Seamless Integrations of New Plug-ins

The vulnerability filter on the RSAS automatically moves all vulnerabilities conforming to selected conditions into customized vulnerability templates. Any new Plug-in that matches a vulnerabilities template will be updated automatically, creating a worry-free solution.

Generate Reports Immediately or Scheduled

Customized templates allow users to download (or email to users directly) a report for each scanning task, alternatively create consolidated reports for several scanning tasks to know holistic trends from several task results. All reports output are available in various formats (HTML, Word, EXCEL, PDF, and XML).

Fast and Flexible Deployment

Flexible deployment methods are available for single-link (stand-alone), multi-link (multi-level) or distributed networks. The RSAS can manage network-across scans regardless of the distance. Deployment is simple and fast. NSFOCUS RSAS are available in both hardware and virtual form factors.

Whichever is your preferred deployment mode, NSFOCUS RSAS provides you with an easy-to-use security platform, flexible and efficient.

HARDWARE SPECIFICATIONS

Specification	RSAS NX3-E	RSAS NX3-S	RSAS NX3-X
Rack mountable	2U	1U	
Power supply	AC, Redundant	AC, Single	
Network interfaces	6* 10/100/1000Base-T copper ports, 1*expansion slot	6* 10/100/1000Base-T copper ports, 1*expansion slot	4* 10/100/1000Base-T copper ports, 4*GE SFP expansion
Weight	12.6 kg (net)	6.7 kg (net)	5 kg (net)
Dimensions (W*D*H)	575 * 432 * 88mm（2U）	390 * 430 * 44mm	
MTBF	> 50,000 hours		
Operating Temperature	Operating temperature: 0–40°C Ambient temperature: －20 to +75°C		
Relative humidity	10%–90%, non-condensing		

RSAS NX3-VM REQUIREMENTS

Specification	Minimal Requirements	Recommended Requirements
CPU	x86 CPU (2.4 GHz quad-core)	x86 CPU (3.2 GHz 8-core)
Memory	4 GB	8 GB or more
Hard disk drive	100 GB	500 GB or more
USB port	USB 3.0 or earlier	
Network adapter	10/100/1000 Mbps	
Running platform	VMware Workstation 9.0 or later VMware vSphere ESXi 6.0 or later FusionCompute V100R005C10SPC700 KVM 2.11.1 OpenStack 3.14.2 XenServer 7.3.0	