DATASHEET

NSFOCUS

NSFOCUS RSAS

Remote Security Assessment System

OVERVIEW

In today's dynamic cybersecurity landscape, organizations face increasing scrutiny. NSFOCUS RSAS provides comprehensive vulnerability detection, expert security analysis, and actionable remediation guidance to safeguard your critical data assets and meet compliance requirements.

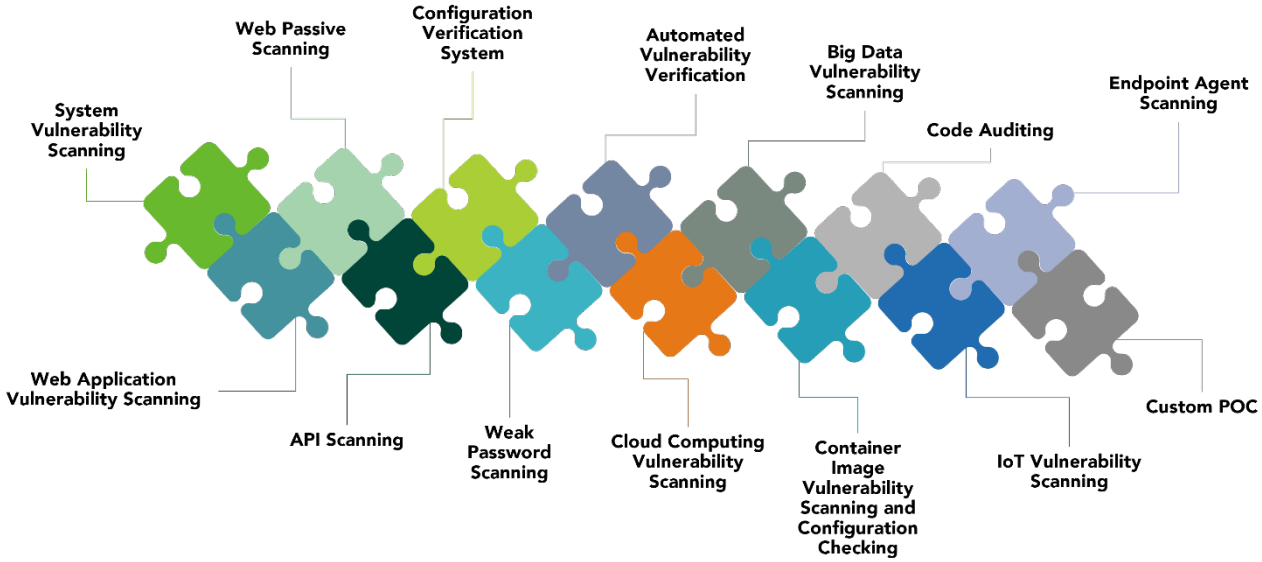
NSFOCUS RSAS integrates with NSFOCUS TVM (Threat and Vulnerability Management) platform to provide a comprehensive vulnerability management solution. By harnessing threat intelligence and continuous asset monitoring, this solution enables you to respond promptly, patch vulnerabilities in an organized manner, and consistently refine asset vulnerability management. It prioritizes and addresses key risks, minimizing their potential impact on your business operations.

NSFOCUS RSAS is available in both hardware and VM subscription formats, ensuring flexible deployment options for your needs.

RESEARCH CAPABILITIES

NSFOCUS has been instrumental in safeguarding the software products of renowned IT manufacturers, playing a pivotal role in identifying and addressing critical vulnerabilities. Our collaborations with industry leaders like Microsoft, Adobe, Google, Sun, Cisco, HP, IBM, Schneider, and Siemens have resulted in the detection and remediation of 230 critical CVE vulnerabilities.

PRODUCT FEATURES



Unparalleled Vulnerability Detection for Comprehensive Security

NSFOCUS RSAS provides comprehensive vulnerability detection capabilities, empowering you to safeguard your critical assets. With its extensive range of features, NSFOCUS RSAS can scan a wide array of systems, including operating systems, databases, middleware, communication protocols, common software, application systems, virtualization systems, big data components, network devices, security devices, IoT devices, and more. NSFOCUS RSAS also supports scanning for over 270,000 vulnerabilities and provides comprehensive vulnerability scanning for nearly 70 types of databases.

Professional Web Application Vulnerability Scanning

Leveraging a dedicated web application vulnerability scanning engine, NSFOCUS RSAS delivers comprehensive detection of all types of web application systems. Its arsenal of over a thousand methods effectively identifies website defacements and web vulnerabilities, ensuring that your web applications remain secure against evolving threats.

Powered by innovative technologies, NSFOCUS RSAS enables rapid and stable scanning of a massive number of web pages, empowering you to efficiently assess your web application security posture.

Web Passive Scanning

Web passive scanning is a dual-mode detection approach designed to enhance business security by analyzing vulnerabilities within network traffic. It operates through either a remote browser session or an HTTP proxy mode, the former enabling zero-configuration analysis, while the latter provides real-time request parsing. This method effectively covers single-page applications and dynamic interactions, enabling in-depth risk detection without disrupting business operations.

The scanning process involves task publishing, traffic capture, and detailed report generation. It supports over 3,000 web vulnerabilities, updated biweekly, and adheres to industry standards such as OWASP, WASC, and PCI DSS. This approach accurately identifies common vulnerabilities like SQL injection and cross-site scripting (XSS), delivering comprehensive security analysis and actionable remediation guidance to protect critical data assets and ensure compliance.

API Scanning

API scanning provides comprehensive security coverage from API asset discovery to vulnerability assessment, helping organizations identify sensitive data and potential risks through traffic analysis and data identification. It supports task initiation via HAR file import or remote browser sessions without configuration. The scanning engine uses specialized plugins and OWASP API Top 10-based templates to detect common vulnerabilities such as SQL injection, XSS, and sensitive data exposure. Scan results are returned in various formats including HTML, PDF, Excel, and Word. Reports include API asset lists, external links, vulnerability distribution by page and severity, and the top 5 risky APIs.

Comprehensive Configuration Verification System

NSFOCUS RSAS automates the discovery and analysis of security configuration issues across a wide range of devices and systems, effectively mitigating the risks associated with manual operations. By automating this critical task, NSFOCUS RSAS enhances the accuracy and compliance of inspection results, ensuring that your organization's security configurations adhere to industry standards and best practices.

With support for configuration checks over 140 types of systems, including operating systems, databases, applications, network devices, virtualization devices, and big data components, NSFOCUS RSAS provides comprehensive coverage for your entire IT infrastructure.

Weak Password Scanning

NSFOCUS RSAS proactively identifies and eliminates weak passwords across your IT infrastructure, safeguarding your organization from potential breaches. Its comprehensive capabilities extend to common login protocols, databases, middleware, applications, and more. Equipped with a vast repository of password dictionaries, including usernames, passwords, combinations, and external sources, NSFOCUS RSAS ensures that even the most complex and obscure weak passwords are uncovered and eradicated.

KEY BENEFITS

Streamlined Operations and Enhanced Clarity

NSFOCUS RSAS simplifies your security operations by automating complex tasks and providing clear, actionable insights.

Cost-Effective Security Procurement

NSFOCUS RSAS offers comprehensive security functionalities and streamlined assessment processes, reducing your need for additional tools and manual effort.

Elevated Security Proficiency

NSFOCUS RSAS empowers your security personnel with advanced threat detection and remediation capabilities, enhancing their overall security proficiency.

Improved Compliance Adherence

NSFOCUS RSAS helps you meet and maintain compliance with industry standards and regulatory requirements.

Automated Vulnerability Verification

NSFOCUS RSAS surpasses mere vulnerability scanning by employing exploits to verify high-risk vulnerabilities, providing you with irrefutable evidence of potential threats. Its user-friendly interface streamlines the process of combined scanning and verification, making it accessible even for non-technical users.

Cloud Computing Vulnerability Scanning

NSFOCUS RSAS extends its comprehensive vulnerability detection capabilities to the cloud, safeguarding your cloud platform components and hypervisors. It meticulously scans your cloud environment, discovering assets and assessing vulnerabilities to ensure your cloud-based infrastructure remains secure and resilient. With support for major virtualization platforms like OpenStack, XEN, KVM, VMware, FusionSphere, Docker, and Kubernetes, NSFOCUS RSAS provides comprehensive coverage for your diverse cloud environment.

Big Data Vulnerability Scanning

NSFOCUS RSAS extends its rigorous vulnerability detection capabilities to the realm of big data, ensuring that your big data platforms and components remain secure and protected. Its comprehensive support for nearly 20 types of big data components, including Ambari, Cassandra, Elasticsearch, Flume, Hadoop, Hbase, Hdfs, Hive, and more, provides unparalleled coverage for your big data infrastructure.

IoT Vulnerability Scanning

In the ever-evolving world of the Internet of Things (IoT), NSFOCUS RSAS stands as your unwavering sentinel, safeguarding your IoT devices from a vast array of vulnerabilities. Its comprehensive capabilities extend to nearly 350 IoT manufacturers, including Samsung, Lexmark, Palo Alto Networks, HP, and more, ensuring that your diverse IoT ecosystem remains secure and protected.

Container Image Vulnerability Scanning and Configuration Checking

NSFOCUS RSAS ensures your container images remain secure and free from vulnerabilities, no matter in public or private repositories, enabling thorough vulnerability scans and configuration checks before deployment.

With NSFOCUS RSAS, you can proactively identify and address potential vulnerabilities and configuration issues in your container images, mitigating the risks of cyberattacks and data breaches. Its support for nearly 90,000 container image-related vulnerabilities and coverage for common application containers, including Oracle, Weblogic, Websphere, Postgresql, MySQL, Apache, and Nginx, provides unparalleled protection for your containerized applications.

Code Auditing

NSFOCUS RSAS empowers you to safeguard your code by conducting rigorous security checks on code submitted from third-party development systems. Its comprehensive capabilities extend to lexical and syntax analysis of various programming languages, including C/C++, Python, Java, PHP, and Go, ensuring that your code remains secure and free from vulnerabilities.

Leveraging 14 commonly used defect templates and encompassing 221 defect types, including all CWE TOP 25 defects, NSFOCUS RSAS provides unparalleled coverage for identifying and addressing potential security issues in your code. NSFOCUS RSAS offers granular customization of defect templates and vulnerability rules, allowing you to tailor your security assessments to your specific needs.

Furthermore, NSFOCUS RSAS seamlessly integrates with SVN and Git, enabling you to incorporate code security checks seamlessly into your existing development workflow.

Endpoint Agent Scanning

Endpoint Agent Scanning uses an agent to gather additional asset information, resulting in more accurate scan results.

Custom POC

Custom POC enables rapid detection of 0-day and industry-specific vulnerabilities through user-defined YAML detection scripts. It supports creating, editing, and managing custom vulnerabilities, with built-in syntax checking and script uploads. Once configured, these vulnerabilities can be referenced in web or system scan tasks, triggering the custom POC execution engine via plugin scheduling. This allows for fast, targeted detection of emerging threats not yet in public databases. Custom POC is ideal for building dedicated vulnerability libraries and enhancing scanning precision, offering flexibility, speed, and adaptability in responding to evolving security challenges across diverse environments.

HARDWARE SPECIFICATIONS

Specification	RSAS NX3-E	RSAS NX3-S
Rack Mountable	2U	1U
Dimensions (W*D*H)	560 * 435 * 88mm（2U）	390 * 430 * 44mm
Power Supply	AC, Redundant	AC, Single
Network Interfaces	6 * Gigabit electrical port, 4 * Gigabit optical port, 2*expansion slot, 1*RJ45 serial, 2* USB	4 * Gigabit electrical port, 4 * Gigabit optical port, 1*expansion slot, 1*RJ45 serial, 2*USB
Weight	12.6 kg (net)	6.7 kg (net)
MTBF	> 50,000 hours	
Operating Temperature	Operating temperature: 0 to 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 or more)
Memory	4 GB	16 GB or more
Hard Disk Drive	150 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	