DATASHEET

NSFOCUS

NSFOCUS RSAS-SC

Remote Security Assessment System-Security Center

OVERVIEW

As organizations expand across multiple business units, geographic regions, and network security zones, vulnerability management must scale to meet increasingly complex deployment requirements. NSFOCUS RSAS-SC is a virtual appliance-based distributed vulnerability assessment platform that builds on the proven detection capabilities of NSFOCUS RSAS and extends them with a distributed scanner architecture, multi-tenant data isolation, and a built-in security policy engine. It enables large enterprises, government agencies, and service providers to deploy, manage, and scale vulnerability scanning across complex, distributed environments from a single platform.

Through the RSAS-SC Management System, distributed RSAS-SC Scanning Engines are centrally managed to deliver consistent vulnerability assessment across departments, regions, and security zones. Multi-tenant data isolation ensures that each business unit can access and manage only its own assets, while headquarters maintains centralized visibility into the organization's overall security posture and risk exposure.

UNPARALLELED VULNERABILITY DETECTION FOR COMPREHENSIVE SECURITY

NSFOCUS RSAS-SC provides comprehensive vulnerability assessment across a broad range of enterprise IT environments, including operating systems, databases, middleware, communication protocols, enterprise applications, virtualization platforms, big data components, network infrastructure, security devices, and IoT devices. Powered by continuously updated vulnerability intelligence, the platform delivers detection coverage for more than 270,000 vulnerabilities and supports comprehensive security assessment for nearly 70 database platforms, helping organizations identify and prioritize security risks across diverse environments.

DISTRIBUTED SCANNING ENGINE MANAGEMENT

The RSAS-SC Management System centrally manages distributed RSAS-SC Scanning Engines deployed across departments, geographic regions, and network security zones, enabling consistent vulnerability assessment across complex enterprise environments. Scan jobs are automatically distributed across multiple scanning engines for parallel execution and routed to the most appropriate scanning engine based on scan type. The platform maintains scanning continuity by reassigning tasks when a scanning engine becomes unavailable, supports online scanning engine upgrades without disrupting ongoing operations, and allows organizations to expand scanning capacity by adding scanning engines as their environments grow.

KEY BENEFITS

Distributed Scanning at Enterprise Scale

Centralized Scan Engine Management

Intelligent Load Balancing & Failover

Flexible Role-Based Access Control

Automated Policy Compliance Validation

Asset-Centric Vulnerability Management

Closed-Loop Remediation Verification

Simplified Security Operations

Reduced Operational Overhead

Rapid Response to Emerging Vulnerabilities

Elastic Architecture for Business Growth

Compliance-Ready Deployment

MULTI-TENANT ACCESS CONTROL AND DATA ISOLATION

NSFOCUS RSAS-SC enables centralized vulnerability management across multiple business units while maintaining strict tenant isolation and role-based administration. Headquarters gain centralized visibility into enterprise-wide security posture, while individual business units can access and manage only their own assets, vulnerabilities, and scan tasks. The platform associates security data with organizational workgroups to support accountability, auditing, and secure data separation, while its native multi-tenant architecture provides a foundation for future SaaS deployments.

SECURITY POLICY ENGINE

The built-in security policy engine automatically evaluates scan results against organization-defined security policies and generates actionable compliance events without manual analysis. By correlating detected vulnerabilities with security policies, the platform identifies affected assets, records policy violations, and provides detailed findings to help security teams prioritize remediation and enforce consistent security standards across the organization.

ADVANCED ASSET MANAGEMENT

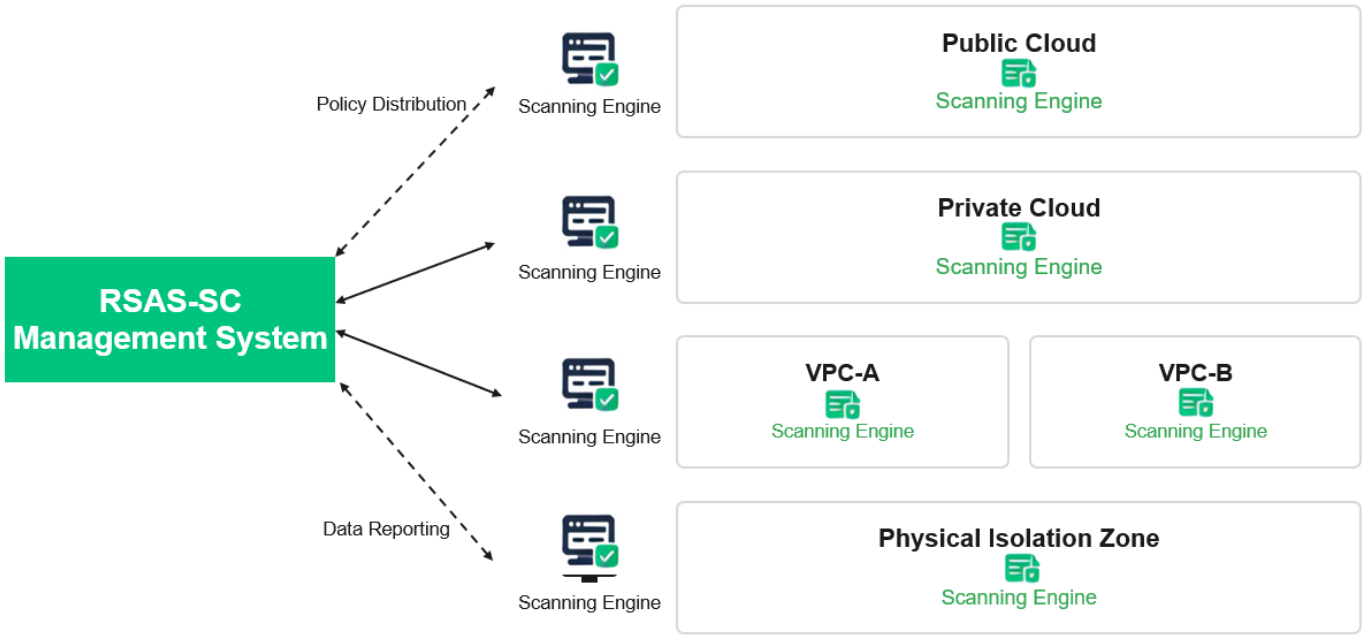
NSFOCUS RSAS-SC provides flexible asset management through multi-dimensional asset tagging based on departments, environments, regions, and business lines. Asset attributes can be automatically identified during bulk import, enabling scan tasks to be defined by asset groups rather than manually maintained IP lists. The platform also supports customized asset views for different operational roles, automated asset change detection between discovery cycles, and targeted reporting for individual business units or regions.

VULNERABILITY LIFECYCLE MANAGEMENT

The platform provides end-to-end vulnerability lifecycle management, from vulnerability assignment and remediation tracking to verification and closure. Targeted verification scans validate remediation without requiring full rescans, while complete historical records preserve assignment status, remediation feedback, verification results, and analyst annotations. Support for both version-based and proof-of-concept-based detection enables organizations to manage vulnerabilities efficiently while maintaining consistent remediation workflows.

EMERGENCY VULNERABILITY RESPONSE

NSFOCUS RSAS-SC accelerates organizational response to newly disclosed vulnerabilities by streamlining impact assessment, verification scanning, remediation prioritization, and response tracking. The platform automatically classifies assets according to exposure and scan status, supports importing vulnerability identifiers from multiple advisory formats, and provides a closed-loop workflow that helps security teams rapidly identify affected assets, validate exposure, and track remediation progress.



RSAS-SC MANAMENT SYSTEM REQUIREMENTS

Specification	Minimal Requirements	Recommended Requirements
vCPU	8 Cores	64 Cores
Memory	16 GB	128 GB
Storage	500 GB	2048 GB
Network Bandwidth	100 Mbps	100 Mbps
Operating System	Ubuntu 16.04 / CentOS 7.9 / Kylin V10	
Notes	Supports up to 150 scanners (add 4 vCPUs and 4 GB RAM per additional 10 scanners); 64 CPU cores and 128 GB RAM are recommended for deployments with 150 scanners.	

RSAS-SC SCANNING ENGINE REQUIREMENTS

Specification	Minimal Requirements	Recommended Requirements
vCPU	4 Cores	8 Cores
Memory	8 GB	16 GB
Storage	200 GB	500 GB
Operating System	Ubuntu 16.04 / CentOS 7.9 / Kylin V10	
Network Requirement	Must support communication with the management platform	