DATASHEET

NSFOCUS

NSFOCUS Threat & Vulnerability Management

RISK-BASED VULNERABILITY & ASSET VISIBILITY PLATFORM

OVERVIEW

NSFOCUS TVM is a risk-based vulnerability and asset management platform that integrates cloud threat intelligence with traditional scanning capabilities.

It provides full lifecycle vulnerability operations, including asset discovery, exposure analysis, risk prioritization, remediation guidance, and continuous monitoring. By correlating multi-source data and focusing on real-world exploitability, the platform helps organizations identify critical risks, accelerate remediation and improve operational efficiency.

Unlike traditional scan-and-report tools, TVM delivers proactive alerts, intelligent fix recommendations, and ongoing optimization across the entire vulnerability management process.

CONTINUOUS NETWORK-WIDE ASSET MONITORING

From a security operations perspective, the platform provides comprehensive asset governance by managing asset attributes, eliminating blind spots, and strengthening the security posture of all IT assets across the network. It offers efficient asset identification and classification capabilities, supporting host asset discovery, web asset discovery, and correlated multi-dimensional detection with automatic synchronization of results.

Equipped with an extensive asset fingerprint library recognizing more than 1,000,000 asset types—including a wide range of domestically developed technologies, the platform ensures accurate identification across diverse environments. Through continuous monitoring of network-wide asset dynamics, it detects additions, modifications, and removals at the attribute level, and enables streamlined, automated remediation policies to effectively close asset-related risks.

In addition to visibility and security posture enhancement, the platform provides continuous compliance validation through more than 140 built-in configuration assessment templates aligned with industry standards and regulatory frameworks.

CLOSED-LOOP VULNERABILITY LIFECYCLE MANAGEMENT

Leveraging the threat and vulnerability management platform, the entire vulnerability handling process is shifted from offline to online, enabling full-lifecycle management—from initial discovery (alerting) to final remediation verification.

- **Comprehensive Vulnerability Discovery**: The platform provides proactive vulnerability scanning and centralized management of enterprise assets. Vulnerability data from penetration tests, offline assessments, or other sources can be quickly digitized and imported through manual entry or file upload for centralized online management.
- **Lifecycle and Risk-Based Prioritization**: A vulnerability state machine tracks and marks the lifecycle of each vulnerability, with status transitions achieved through manual updates, automated verification, or re-scanning. Multi-source validation and expert analysis ensure accurate and complete verification of identified vulnerabilities. Coupled with a business-risk-aware intelligent prioritization model, the platform helps organizations focus on critical vulnerabilities, maximizing the reduction of asset risk exposure.
- **Automated Remediation Workflow**: Detected vulnerabilities can be issued as tickets at a granular level, automatically matched to asset owners or departmental leads. Notifications are delivered via messaging or email, and multiple vulnerabilities can be consolidated per recipient into a single ticket. The platform supports setting remediation deadlines, escalation, and forwarding, ensuring timely and efficient vulnerability handling.

KEY BENEFITS

Comprehensive assessment of assets and vulnerabilities

Clear visibility into enterprise risk exposure

Prioritized vulnerability remediation

Centralized management of scanning tools

Fine-grained scanning policies for complex enterprise needs

Unified standards, workflows, and knowledge bases for vulnerability handling

Continuous asset discovery and change monitoring

Threat-intelligence-driven hotspot vulnerability tracking and rapid response.

KEY FEATURES

Centralized asset discovery, classification, and monitoring

Continuous network-wide visibility across host, web, cloud, and IoT assets

Multi-dimensional vulnerability scanning and centralized task orchestration

Full-lifecycle vulnerability management from discovery to remediation verification

Multi-source vulnerability aggregation and automated ticketing

Risk-based prioritization for efficient remediation

Comprehensive knowledge base with standardized and aggregated vulnerability data

Support for custom proof-of-concept creation and flexible detection

Reporting, dashboards, and trend analytics for operational oversight

COMPREHENSIVE VULNERABILITY KNOWLEDGE BASE

The vulnerability knowledge base covers over 570,000 entries, supporting detection across operating systems, middleware, databases, services, web applications, cloud environments, and IoT devices. It supports scanning more than 90 database types and recognizes over 330,000 asset fingerprints, enabling comprehensive asset identification. The platform also allows for rapid creation of custom proof-of-concept (POC) tests, enhancing detection flexibility and coverage.

MULTI-SOURCE VULNERABILITY AGGREGATION

The platform supports the integration of vulnerability data from multiple sources, including third-party vendor advisories, penetration test results, external reports, and threat intelligence feeds. Once integrated, vulnerabilities related to the same asset can be consolidated into a single remediation ticket, allowing users to view all sources, only the latest data, or the highest-confidence information. Policy-based configuration and selection further streamline the process, minimizing manual effort while maximizing the use of multi-source data and enhancing remediation efficiency.

Leveraging a local knowledge base, the platform standardizes and aggregates heterogeneous vulnerability data, addressing inconsistencies across multiple vulnerability standards. Through automated aggregation and workflow, it unifies the vulnerability handling process and significantly reduces manual processing costs.

INTELLIGENT VULNERABILITY PRIORITIZATION

Not all vulnerabilities can be addressed immediately. The NSFOCUS TVM platform introduces a multi-dimensional Vulnerability Prioritization (VPT) model, which builds traditional vulnerability scoring by incorporating factors such as asset location, criticality, protection status, and exploitability. By integrating threat intelligence, including proof-of-concept (POC) availability and social media activity, the platform generates practical, operations-oriented priority scores. Addressing vulnerabilities based on these scores allows limited resources to focus on the highest-risk issues, maximizing risk reduction and improving remediation efficiency.

To accommodate varying organizational risk focuses, the platform provides a flexible prioritization model, allowing dynamic adjustment of factor weights and enabling or disabling specific factors. The model considers vulnerability exploitability, asset or business criticality, severity, and existing compensating controls, dynamically generating priority scores that guide effective vulnerability remediation.

PROFESSIONAL CLOUD-BASED THREAT INTELLIGENCE

In the NSFOCUS TVM solution, vulnerability intelligence is applied across all stages of vulnerability management, including rapid response, risk assessment, prioritization, and remediation. Rapid vulnerability response is the first step in effective vulnerability management. Leveraging years of operational expertise from the NSFOCUS Threat Intelligence Center (NTI), the platform integrates NTI intelligence feeds to provide real-time, up-to-date vulnerability information.

By correlating vulnerability data with product and asset fingerprints, potential asset risks can be identified, while pre-alert asset fingerprint verification improves detection accuracy through standardized fingerprints. Coupled with timely intelligence-driven alerts to operations personnel, this enables organizations to quickly initiate internal vulnerability management workflows, detect vulnerabilities promptly, and ensure timely remediation.

ONE-STOP VULNERABILITY SCANNING DEVICE OPERATIONS

The platform provides a unified, one-stop operational management solution for vulnerability scanning devices. It enables centralized device onboarding, monitoring, configuration, upgrade, and maintenance for both headquarters and branch offices. Vulnerability scanning tasks can be issued, tracked, and managed centrally, while scanning results are collected, analyzed, and remediated in a unified workflow. This approach streamlines large-scale device operations, enhances efficiency, and ensures consistent vulnerability management across the organization.

SOFTWARE SPECIFICATIONS

Vulnerability Analysis and Management

- Comprehensive scanning and analysis of system vulnerabilities, web vulnerabilities, weak passwords, and configuration non-compliance.
- Provide fingerprint-based, non-intrusive correlation analysis for emerging and regulatory vulnerabilities.
- Unified ingestion, analysis, and management of multi-source vulnerability information, including penetration testing results, Nessus vulnerabilities, and others.
- Allow custom PoC plugin integration, enabling rapid PoC-based scanning and verification of vulnerability impact.
- Risk-driven vulnerability prioritization, with flexible and customizable prioritization policies.
- Full lifecycle tracking of vulnerability remediation, including assignment, status transitions, verification, and closure.
- Streamlined operational tools, including ticket management, workflow management, and notification management, to support investigation, validation, remediation, and verification tasks

Asset Management

- Continuous asset discovery, asset change comparison, and configurable asset onboarding policies.
- Support asset import and manual entry, with asset views, attribute management, and tag management.
- Provides asset risk statistics and visualization, delivering asset risk profiling across vulnerabilities, weak passwords, and configuration compliance dimensions.

Knowledge Base Management

- Comprehensive built-in knowledge base, including over 1,000,000 asset fingerprints, 140+ configuration assessment templates, 540,000+ security vulnerabilities, and 30+ weak credential categories (e.g., accounts, passwords, default credentials)
- Management of vulnerability knowledge bases, PoC fingerprint plugin libraries, and vulnerability classification.
- Enables streamlined ingestion, entry, and early-warning analysis of vulnerability intelligence.
- Maintains remediation knowledge bases and false-positive repositories to support experience reuse.
- Asset labeling library management, including label correction to enhance asset data accuracy.

System Management

- Centralized monitoring, configuration, and upgrade of NSFOCUS RSAS devices.
- RBAC-based access control with flexible function and data permission management.
- Convenient API integration for asset and vulnerability data exchange and operations.

RESOURCE REQUIREMENTS AND PERFORMANCE

Hardware Requirements		TVM NX1-SNG		
		Basic Configuration	**Recommended Configuration**	**Advanced Configuration**
Hardware Resource Requirement	**CPU Cores**	16 Logic Cores	20 Logic Cores	40 Logic Cores
	Memory	**32 G**	64G	128G
	Storage	**1 TB hard disk.** **Available space in the root directory ≥ 300 GB.**	**2 TB hard disk.** **Available space in the root directory ≥ 300 GB.**	**4 TB hard disk.** **Available space in the root directory ≥ 300 GB.**
	NIC	**One dual-port 10-Gigabit NIC, or two quad-port Gigabit NICs.**		
	Operating System	**Supported Operating Systems:** **CentOS 7, Kylin V10, Tianyi Cloud CTYUN OS, Huawei EulerOS, BCLinux, Unity Operating System V20, Red Hat.** **Recommended Operating System:** **CentOS 7.6.**		
	BSA System	**BSA V3.0R01F06**		
Performance	**Number of Assets**	100,000	300,000	1,000,000
	Number of Devices	15	30	100