DATASHEET

TAS

Threat Analysis System

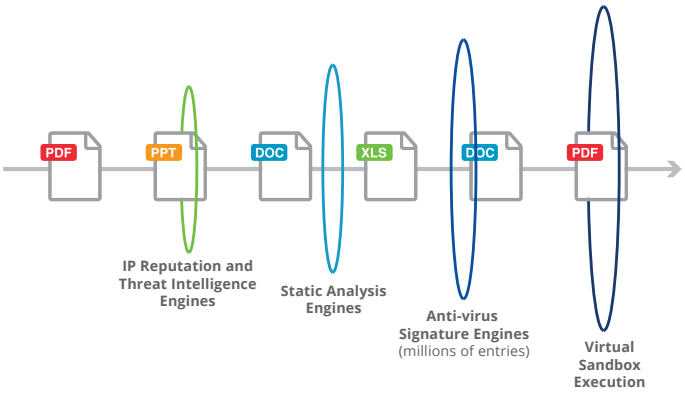
NSFOCUS Threat Analysis (TA) identifies known and unknown malware, including zero-day threats entering the enterprise network via web pages, emails, or other file sharing methods. NSFOCUS TA uses several detection engines to identify known and zero-day threats, including an IP reputation engine, anti-virus engine, static analysis engine, and virtual sandbox execution. NSFOCUS TA can optionally be added to the NSFOCUS Next-Gen IPS to provide sandboxing capabilities.

ADVANCED PERSISTENT THREAT PROTECTION

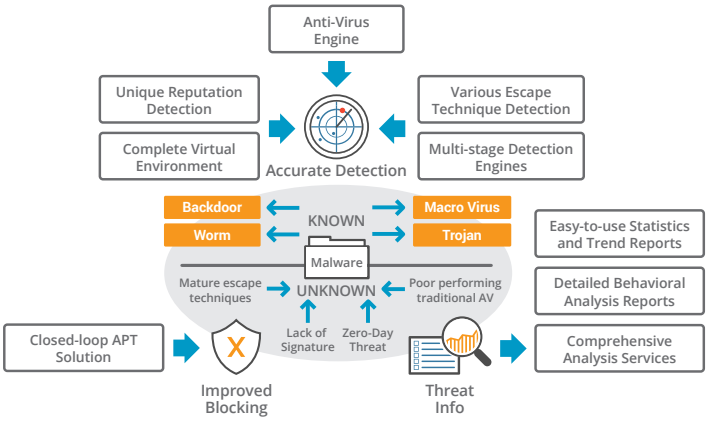
NSFOCUS TA provides virtual sandboxing capabilities capable of detecting, analyzing, and mitigating known, zero-day, and advanced persistent threats (APTs). The TA appliance monitors CPU, network activity, memory utilization, and system driver behavior in a virtual environment. It enables organizations to identify malicious activity and harmful executables before they reach critical servers and desktops.

ACCURATE THREAT DETECTION

NSFOCUS TA utilizes a multi-stage detection engine to identify malicious activity. This approach combines signature detection, heuristic analysis, threat intelligence and virtual execution techniques to protect any network against today's cyber threats.



The functionality of the NSFOCUS TA are highlighted in the diagram below. The various engines, detection techniques, malware databases, and reputation detection capabilities work in unison to address known and unknown threats. Easy-to-use statistics and trend reports, behavioral analysis reports, and comprehensive analysis services are also available.



Accurate detection of unknown malware helps reduce the risk of Advanced Persistent Threats

KEY FEATURES

Flexible configuration interface

Comprehensive object library

Custom service and policy definition

Threat visualization

Statistics based on the attack chain

Multiple views for threat information: locations, users, and assets

Simplified Threat Management

Top 5 high-level threats

Latest threat events

24-hour threat trends

Daily, weekly, monthly, or annual reporting options

MULTI-PROTOCOL, APPLICATION, CODE, AND OS SUPPORT

NSFOCUS TA has broad protocol support, supports multiple file types, performs extensive static code analysis and virtual OS support.

Protocols | File Types | Static Code Analysis | OS

INTEGRATED THREAT INTELLIGENCE

The most dangerous known threats are the ones that can't be seen or detected until it is too late. The NSFOCUS Threat Analysis integrates global threat intelligence from the NSFOCUS Threat Intelligence Subscription Service to provide up-to-date protection from botnets, malicious sites, viruses and other discovered exploits.

MULTIPLE FORM FACTORS

The NSFOCUS TA is cost and performance optimized to meet the needs of any size organization.

		TA-NX3-1000D	TA-NX3-2000D
Service Interface	Board interface	None	None
	Slot	4	4
	Expansion interface	4 x GE interface or 4 x SFP interface	4 x GE interface or 4 x SFP interface
Management Interface	Management interface	2 x GE interface	2 x GE interface
	Console port	1 x RJ-45 port	1 x RJ-45 port
	USB port	2	2
Performance	Throughput	1 Gbps	2 Gbps
	File processing (per day)	100,000	200,000
Physical Index	Size	432 x 575 x 88 mm (2U)	432 x 575 x 88 mm (2U)
	Power supply	100-240 V AC (50-60 HZ), 5-8 A, 350 W	100-240 V AC (50-60 HZ), 5-8 A, 350 W
	Mean Time Between Failures (MTBF)	Over 100,000 hours	Over 100,000 hours
	Operating temperature	0–40 °C	0–40 °C
	Radiation standard	FCC Part 15	FCC Part 15