DATASHEET

Unified Threat Sensor (UTS)

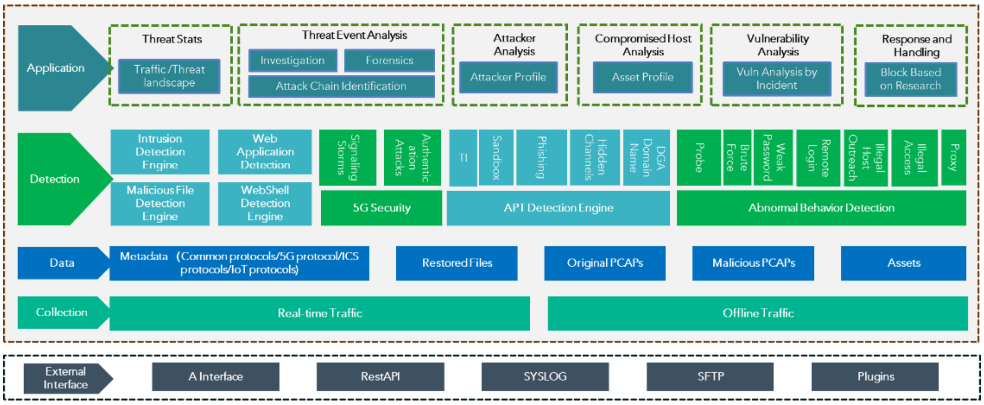
OVERVIEW

Today network traffic shows explosive growth with organizations' businesses moving to the cloud, the use of 5G technology, and the proliferation of the Internet of Things (IoT). The complex traffic carries important information, such as personal credentials and payment information. At the same time, the network boundary is blurring, making it hard to monitor the traffic. How to identify, detect and analyze threats by network traffic has become the focus of any organization's security program. That's where the NSFOCUS Unified Threat Sensor (UTS) comes in.

The UTS integrates NSFOCUS's IDS, WAF, Threat Intelligence and All-traffic logs, and supports multi-functional sensors of third-party data platforms to provide data collection, data analysis, threat detection and threat mitigation. The comprehensive threat detection capabilities, including Intrusion detection, Web application firewall, threat intelligence, malicious file and WebShell detection, allow users to locate threats and respond to critical incidents quickly.

The UTS accesses the user network for traffic collection, analysis, storage, file restoration and threat detection in out-of-the-path mirror mode. The UTS can also work with the big data analysis platform to summarize the detection results and metadata for comprehensive analysis, precise threat identification and display on a single panel.

The UTS consists of the collection, data, detection, and application layers and provides external interfaces to integrate with other products and platforms.



KEY BENEFITS

Spot all kinds of network security issues in a single system in the out-of-the-path mode

Enhanced data analysis for advanced attacks detection, including zero-day and APTs

Quick locate threats, automatically policy applying and attack blocking by one-click operation

Precise detection before an event, automatic block during an event, traceback and forensics after an event

KEY FEATURES

Complete traffic collection and analysis

Multiple detection engines for both common and advanced threat detection, including 0-day and APTs

Fully-integration with NSFOCUS products and 3rd-party SIEM

Threat Traceback and Forensics

Comprehensive Threat Detection

Leveraging dual detection engines of IDS and WAF and combined with threat intelligence, malicious file analysis, WebShell detection, sandboxing and abnormal behavior detection, the UTS levels up users' perception capabilities on threats of not only traditional intrusion and web attacks but also advanced malicious code and advanced persistent threats (APTs).

Threat Traceback and Forensics

The UTS supports complete traffic collection and storage. Users can retrieve the threat's metadata to obtain the attack's context information once a threat is detected. At the same time, it supports the extraction of relevant PCAPs as evidence for forensics. The traceback and forensics cover zero-day and APT attacks, too.

Fast and Automatic Threat Mitigation

The UTS supports threat blocking in out-of-the-path mode. Once a threat is detected, it can automatically block attacks according to pre-set security policies. It also provides an external interface for fast response by one-click operation on data analysis platforms.

Integration with Third-Party SIEM

As a fully-integrated sensor, the UTS can integrate the detection capabilities of NSFOCUS's IDS, WAF, threat intelligence, malicious file inspection system and other products, and also can integrate with the third-party SIEM platforms to meet the needs of users for multi-phase construction. Users do not need to purchase hardware equipment for single-function detection capability one by one. In addition, users can choose hardware or software form factor, which is flexible in building their security capabilities.

5GC Security

The UTS is a vital part of the 5GC security solution. When the UTS is connected to the 5G core network, it can identify protocols of the 5GC signaling plane and management plane, detect 5GC threats, including authentication attack detection, signaling storm detection, and UE anomaly detection, and support dynamic tuning of the detection cycle and detection thresholds in algorithms. The UTS provides in-depth analysis of 5G protocols, including:

- NAS (N1)
- NGAP (N2)
- PFCP (N4)
- HTTP2 (N5, N7, N8, N10, N11, N12, N14, N15, N20, N21, N22, N24, N28, N40)
- GTPv2 (N26)

Working with NSFOCUS Intelligent Security Operation Platform (ISOP) and global threat intelligence, a complete 5GC security solution is formed. This solution provides all-traffic detection, analysis, threat response, and threat traceback. Users can get comprehensive situation awareness from a single dashboard and the reporting system, and get alerts immediately when any threat is discovered.

5GC security solution can be deeply integrated with users' 5G networks to make network security status visible, meet compliance requirements, and improve the entire 5G network security posture comprehensively.

Hardware Specifications (Sandbox Included)

Model	UTSNX3-HD4201	UTSNX3-HD4501	UTSNX5-HD6101	UTSNX5-HD8100
Flow Handing	2Gbps	5Gbps	10Gbps	20Gbps
CPU Cores	4	10	12	24
Memory	16G	64G	128G	192G
Hard Disk	Up to 36T	Up to 48T	Up to 48T	Up to 48T
Extension Slot	4	2, 4 or 8	2, 4 or 8	4 or 8
Optional Extension Interface	4GE/4SFP/8GE/8SFP/2SFP+/4SFP+	4GE/4SFP/8GE/8SFP/2SFP+/4SFP+	4GE/4SFP/8GE/8SFP/2SFP+/4SFP+	4GE/4SFP/8GE/8SFP/2SFP+/4SFP+
Management Port	2GE	2GE	2GE	2GE
Console	1*RJ45	1*RJ45	1*RJ45	1*RJ45
USB Interface	2	2	2	2
Application-layer Throughput	2Gbps	5Gbps	10Gbps	20Gbps
Network-layer Throughput	2Gbps	5Gbps	10Gbps	20Gbps
Max. Number of Concurrent	12,000,000	20,000,000	28,000,000	40,000,000
TCP Connections Per Second	24,000	30,000	60000	100000
HTTP Connections Per Second	20000	24,000	50000	80000
File Processing Capability	10,000	50,000	100,000	100,000
HTTPS Performance	40Mbps	100Mbps	200Mbps	400Mbps
Full Traffic Storage Performance	500Mbps	MAX 3Gbps	MAX 3Gbps	MAX 5Gbps
Dimension (W*D*H)	430mm*390mm*44mm	560mm*435mm* 88mm	626mm*443mm*88mm	626mm*443mm*88mm
Weight	≤6.6kg	≤20kg	≤24kg	≤24kg
Power Supply	Redundant power supply，100-240V, AC, (50-60HZ), 4.5-2A,300W	Redundant power supply, 100-240v, AC, (50-60hz) , 7-3.5A, 550W	Redundant power supply, 100-240V, AC, 50-60Hz, 7.0- 3.5A, 550W	Redundant power supply, 100-240V, AC, 50-60Hz, 7.0- 3.5A, 550W
MTBF	>100,000 hrs.	>100,000 hrs.	>100,000 hrs.	>100,000 hrs.
Operating	0 - 40℃	0 - 40℃	0 - 40℃	0 - 40℃
Operating Humidity	10% - 90% RH	10% - 90% RH	10% - 90% RH	10% - 90% RH
Radiation Standard	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15	Class A, EN55022, FCC Part15

Software Performance and Recommended Configurations

Model		UTSNX1-V4100C	UTSNX1-V4200C	UTSNX1-V4500C	UTSNX1-V6100C	UTSNX1-V8100
Flow Handing Capacity		1Gbps	2Gbps	5Gbps	10Gbps	20Gbps
Resources Required (Sandbox not included)	**vCPU**	8C	12C	20C	40C	48C
	Memory	24G	32G	64G	128G	192G
	Hard Disk*	⩾1T	⩾2T	⩾4T	⩾10T	⩾20T
	# of Network Interface	⩾3	⩾3	⩾3	⩾3	⩾3
	NIC	igb (GE): 82575, 82576, 82580, I210, I211, I350, I354 ixgbe (10GE): 82598, 82599, X520, X540, X550, X710, X722				
Resources Required (Sandbox included)	vCPU	16C	20C	32C	48C	64C
	Memory	32G	48G	96G	144G	256G
	Hard Disk*	⩾1T	⩾2T	⩾4T	⩾10T	⩾20T
	# of Network Interface	⩾3	⩾3	⩾3	⩾3	⩾3
	NIC	igb (GE): 82575, 82576, 82580, I210, I211, I350, I354 ixgbe (10GE): 82598, 82599, X520, X540, X550, X710, X722				
Performance	Network-layer Throughput	1Gbps	2Gbps	5Gbps	10Gbps	20Gbps
	HTTP Throughput (21K)	1G	2G	5Gbps	9.8Gbps	20Gbps
	Max.Concurrent TCP Sessions	500,000	1,800,000	2,000,000	2,800,000	4,000,000
	New TCP Sessions per Second	18,000	25,000	30,000	60,000	100,000