VMware NSX Network Detection and Response

Advanced threat detection for VMware NSX Security

At a glance

- NSX Network Detection and Response (NDR) is an AI-based threat correlation and forensics engine within NSX Distributed Firewall that helps network security and SOC teams efficiently detect malicious activity and block lateral movement of sophisticated threats.
- NSX NDR is informed by the broadest set of threat signals from network sensors distributed across network infrastructure and automatically correlates them into threat campaigns mapped to the MITRE ATT&CK Framework.

Context matters

NSX NDR gives network security and SOC teams immediate contextual information they can act on, including:

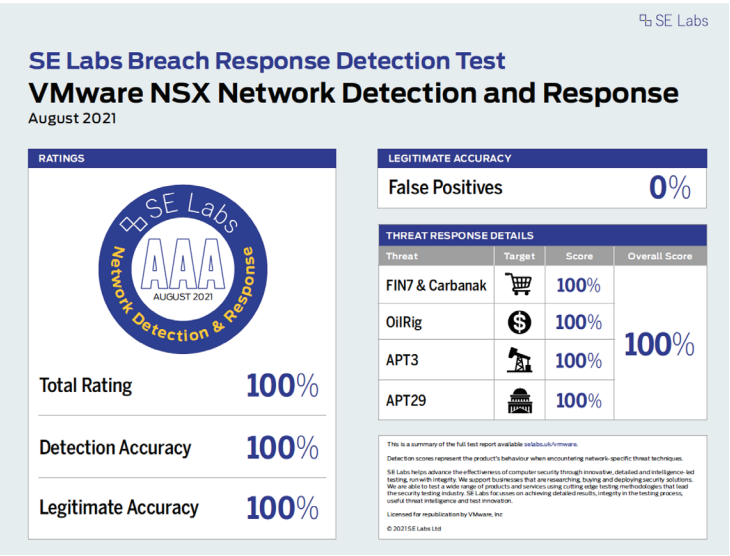
- Traffic crossing the perimeter and moving laterally across the network
- Extent and duration of every event
- Visibility into all attack stages
- Compromised systems communication between local and external systems
- Data sets accessed and harvested

VMware NSX® Distributed Firewall™ with Network Detection and Response (NDR) helps security operations teams rapidly detect malicious activity and stop the lateral movement of threats inside your network. NSX NDR ingests signals from built-in and distributed sensors located throughout your environment and is able to detect threats across the MITRE ATT&CK Framework, giving your network security and SOC teams unparalleled visibility into malicious events as they occur.

Advanced detection of sophisticated threats

Today's modern, sophisticated threats are often able to bypass detection and evade analysis by using a multitude of attack vectors and techniques to increase the chances of a successful intrusion. NSX NDR is informed by the broadest set of threat signals from network traffic analysis, intrusion detection and prevention, and network sandboxing engines to deliver the industry's most accurate threat detection capabilities.

NSX NDR received AAA rating from SE Labs after participating in the industry's first public NDR test. In the test, NSX NDR detected all network threats and payloads across four advanced persistent threats as defined by MITRE.



Broadest set of built-in detectors

NSX NDR ingests signals from detectors within NSX—spanning a full system emulation sandbox, an AI- based Network Traffic Analytics engine, a signature-based IDS/IPS engine and third-party threat intelligence feeds.

Distributed agentless network sensors

All the detectors within NSX Distributed Firewall are distributed as agentless sensors at each workload within the hypervisor, ensuring inspection of all East-West traffic while providing the most authoritative context for accurate threat detection.

Inspection of encrypted traffic and artifacts

NSX NDR detects threats in encrypted traffic with novel machine learning models that operate on JA3 hashes and network meta-data. It uniquely analyzes encrypted files at each host through guest introspection before they are written to disk.

Immediately increase SOC efficiency and reduce false positives

Your security resources are likely overwhelmed by a multitude of false positives that are constantly generated by legacy security tools that can't determine if an anomaly is malicious or not. This zaps help desk resources and impacts morale while real threats get lost in the noise.

NSX NDR solves this problem by focusing on threat campaigns rather than just isolated anomalous events. Our AI-based correlation engine generates high fidelity, highly accurate alerts that provide authoritative context to speed up forensics. This allows security operations teams to direct their attention on a small subset of relevant events instead of digging through thousands of anomalies.

Complete visibility into threats moving both into and throughout your network

Other NDR solutions require discrete network sensors that tap into traffic for inspection and analysis. This approach forces organizations to make hard decisions about where to place sensors—a strategy that leads to selective inspection of traffic and creates inspection bottlenecks inside your network.

By building network detection and response capabilities natively into the vNIC within the hypervisor, NSX NDR is able to lean on distributed sensors in every workload to eliminate the need for any network taps or discrete sensors. This enables organizations to inspect all traffic in a highly scalable and distributed manner.

Because NSX NDR provides both North-South and East-West visibility, NSX NDR is able to detect threats earlier and with much higher fidelity than other NDR solutions.

Quickly map incident actions to MITRE ATT@CK

NDR maps adversaries[1] campaigns to the tactics and techniques outlined by THE MITRE ATT&CK Framework, providing coverage and protection across 12 MITRE ATT&CK tactics through network prevention, detection and response capabilities—the broadest coverage in the industry. A NDR campaign scenario below illustrates the value of correlating MITRE ATT&CK matrix of tactics and techniques across the distributed security services:

- Initial Access & Execution: NSX NDR receives signals regarding initial access attempts by detecting phishing emails and malicious links that trick your users and evade your defenses.
- Execution, Persistence and Privilege Escalation: NSX NDR receives signals about the malicious nature of the artifact analyzed. Using industry-leading file analysis capabilities, it detects persistent advanced threats that attempt to escalate privileges and evade detection.
- Discovery and Lateral Movement: NSX NDR receives signals on detected, network anomalous activity with a deep understanding of malicious behaviors and the ability to discern between benign anomalies, malicious lateral movement, account discoveries and brute-force techniques.
- Collection, Command and Control and Exfiltration: NSX NDR receives signals on anomalous network activity that detect the staging of data and alternative protocols used to communicate and exfiltrate data.

Certified Hardware Specifications for On-Premises Deployment

Recommended hardware specifications[1]

	1G Network sensor	10G Network sensor	Data node	Manager	Detection engine
Base Model	Dell PowerEdge R440				
Processor(s)	1 Intel Xeon Silver 4114	2 Intel Xeon Silver 4114	1 Intel Xeon Silver 4116	1 Intel Xeon Silver 4114	1 Intel Xeon Silver 4114
RAM	32GB	128GB	64GB	64GB	64GB
Hard disk drive	2 x 1TB 3.5 SATA HDD (7.2K RPM)	2 x 1TB 3.5 SATA HDD (7.2K RPM)	4 x 2TB 3.5 SATA HDD (10K RPM)	4 x 2TB 3.5 SATA HDD (7.2K RPM)	2 x 1TB 3.5 SATA HDD (7.2K RPM)
Software RAID	1	1	10	10	1
Internal controller	PERC H750p				
Monitoring ports	4 x 1 GbE ports[2]	Up to 4 x 1 GbE Up to 2 x 10 GbE ports[2]			
Management port	1 GbE port				

Network performance	Up to 1GB traffic	Up to 4GB traffic			
Objects per day**	Up to 100,000 per day*				
Files analyzed					Up to 10,000 per day*
Scalability of engines				Up to 30 engines per manager	
Scalability of sensors				Up to 200 sensors per manager	
Total protected endpoints				Up to 200k endpoints per manager	

1. Only apply when NDR is deployed standalone, not when part of NSX.
2. Supported Intel NIC required for throughput of more than 200Mbps.

* Cluster N number of components to scale as needed. Performance varies by object type.

** Apply pre-filter to quickly determine maliciousness and submit unknown files for detailed analysis by Deep Content Inspection.

Note: Performance values are based on standard profile. Values may vary depending on your environment.