VMware NSX Network Detection and Response

AT A GLANCE

A broad set of detection capabilities comprised of the most effective prevention of lateral movement and comprehensive protection against a wide range of known and unknown advanced threats.

VMware NSX Network Detection and Response provides a tightly integrated set of network detection and response capabilities for east-west security within the data center and multi-cloud environments. VMware NSX Network Detection and Response™ has the broadest set of detection capabilities that span network IDS/IPS, behavior-based network traffic analysis, as well as VMware NSX Advanced Threat Analyzer™, a sandbox offering based on a full-system emulation technology that has visibility into every malware action.

Powered by AI, NSX Network Detection and Response correlates individual detection events across multiple assets and hops into fewer security-relevant intrusions, organizing them into a timeline for rapid threat hunting and response. Together, the detection capabilities provide the most effective prevention of lateral movement and comprehensive protection against a wide range of known and unknown advanced threats.

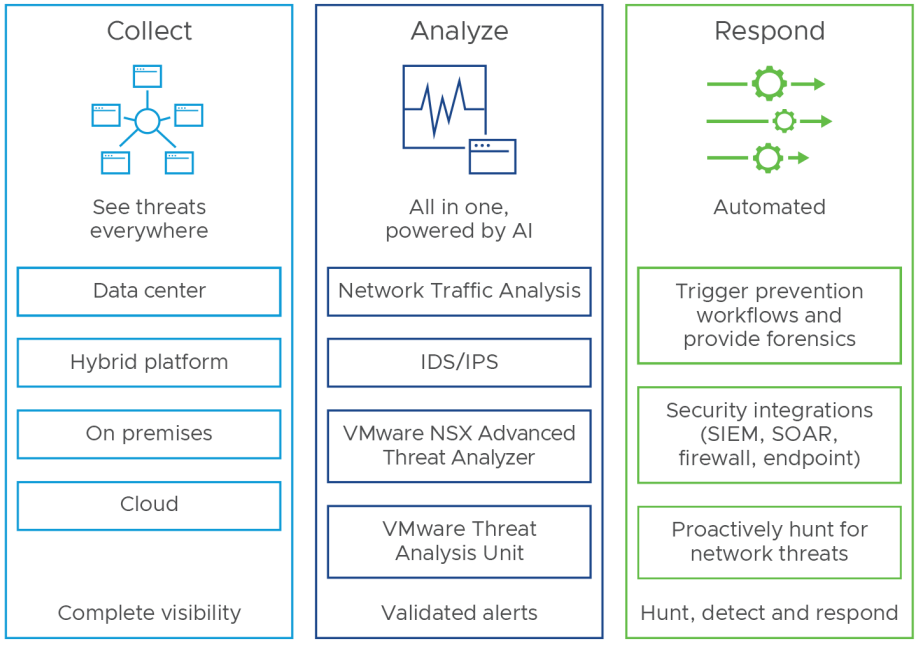

FIGURE 1: NSX Network Detection and Response.

"The VMware Threat Analysis Unit™ continuously updates NSX Network Detection and Response in real time with threat intelligence, such as active command and control (C&C) servers, objects with zero-day exploits, toxic websites and malware distribution points, and malware information useful to defend against threats specific to your organization."

Enjoy complete network visibility

NSX Network Detection and Response maps and defends against MITRE ATT&CK techniques. It protects your network, cloud and hybrid cloud traffic. NSX Network Detection and Response provides a cloud-based architecture that enables sensors to gain comprehensive visibility into traffic that crosses your network perimeter (north/south), as well as traffic that moves laterally inside your perimeter (east/west), for both your on-premises network and cloud infrastructure.

Looking ahead

Powered by AI, NSX Network Detection and Response uses a combination of four complementary technologies to detect and analyze the advanced threats that other tools miss, while dramatically reducing false positives by up to 90 percent.

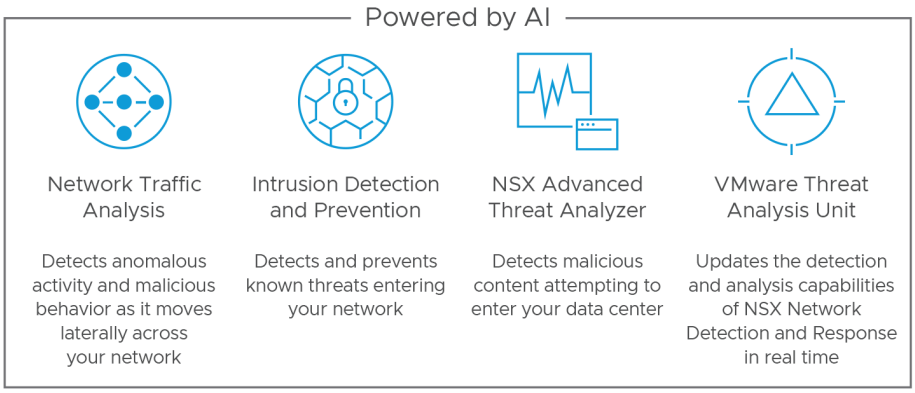

FIGURE 2: NSX Network Detection and Response uses four complementary technologies.

The industry's most accurate threat detection

Network traffic analysis (NTA) applies unsupervised machine learning (ML) to your network traffic to detect protocol and traffic anomalies. NTA also uses supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown malware.

NSX applies AI to the malicious behaviors and malware samples collected from customers and partners across our global threat intelligence network to automatically create new IDS/IPS signatures and push them out to all NSX sensors at machine scale.

The patented NSX Advanced Threat Analyzer deconstructs every behavior engineered into a file or URL to determine if it is malicious. NSX Advanced Threat Analyzer sees all instructions that a program executes, all memory content and all operating system activity.

The VMware Threat Analysis Unit™ continuously updates NSX Network Detection and Response in real time with threat intelligence, such as active command and control (C&C) servers, objects with zero-day exploits, toxic websites and malware distribution points, and malware information useful to defend against threats specific to your organization.

The industry's highest fidelity alerts

Security operations center (SOC) teams are often overwhelmed by the high volume of low-fidelity alerts generated by their security controls. The unique combination of NTA, IDS/IPS and threat analysis—all powered by AI—slashes false positives by up to 90 percent and provides unmatched visibility. The result is that NSX Network Detection and Response condenses massive amounts of network data down to just

"These visualizations give your SOC team the information it needs to quickly understand the scope of the attack and prioritize response."

a handful of intrusions (see Figure 3). That means your analysts can spend their time solving real incidents and protecting your organization rather than chasing false positives all day long.

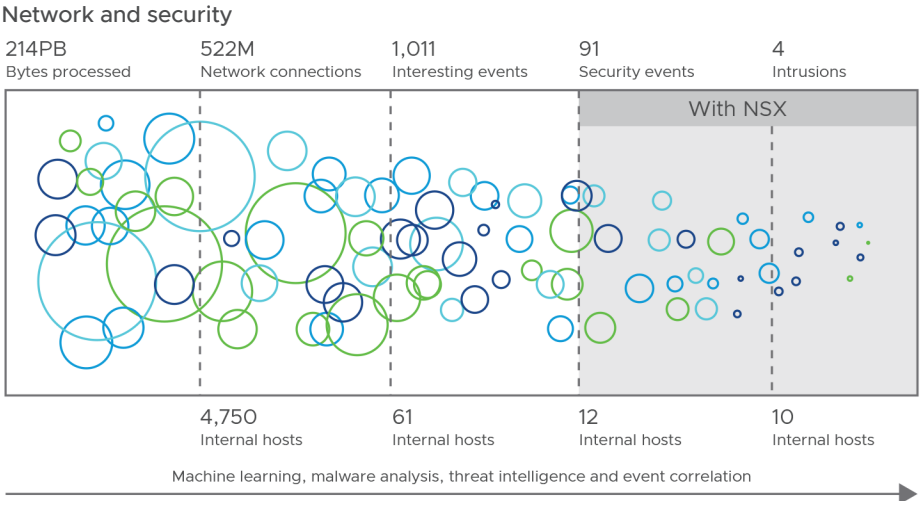

FIGURE 3: NSX Network Detection and Response reduced 214PB of data analyzed in one month in one network to only four intrusions affecting 10 hosts.

Visualize the entire attack chain

In alignment with the MITRE ATT&CK framework, NSX Network Detection and Response classifies malicious activity by attack stage (see Figure 4) to identify the risk associated with each malicious event. It also generates a dynamic intrusion blueprint (see Figure 5) and a detailed timeline of a threat as it enters and moves laterally across your on-premises and cloud network. These visualizations give your SOC team the information it needs to quickly understand the scope of the attack and prioritize response.

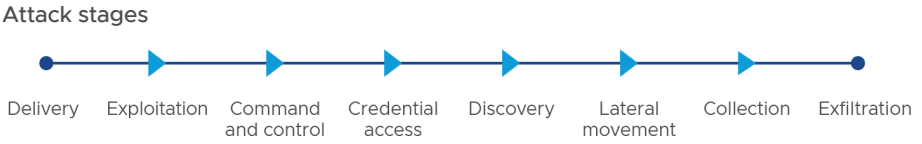

FIGURE 4: NSX Network Detection and Response helps your SOC team quickly understand the attack stage.

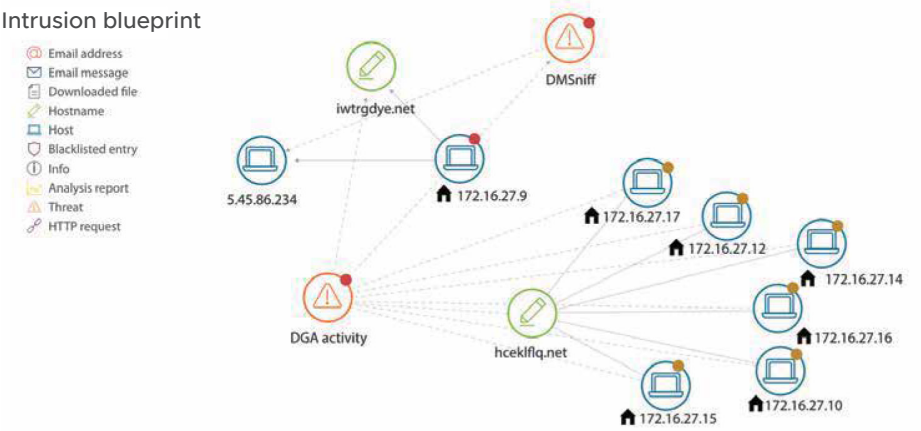

FIGURE 5: NSX Network Detection and Response shows an attack's progress in your network, including compromised systems and communication with external systems.

ADDITIONAL INFORMATION

Please consult the table on the next page for full recommended hardware specifications.

Visualize the entire attack chain

Rely on high-fidelity insights from NSX Network Detection and Response to automate your response and eliminate time-consuming manual investigations of unknown objects and anomalous activity:

- Deploy NSX Network Detection and Response in blocking mode to stop malicious content and communication at the perimeter or internally, in both on-premises and cloud environments.
- Integrate NSX Network Detection and Response with your third-party products—such as security information and event management (SIEM); security orchestration, automation and response (SOAR); endpoint protection and firewalls; custom applications; and incident response workflows—throughout your organization.

When integrating with your existing controls, you have the choice of using built-in integrations offered by our technology partners or using our robust APIs to optimize your current technologies, staff and processes. Your existing security controls can automatically send unknown objects for analysis and receive actionable threat intelligence in return—before a threat can disrupt your business.

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 H730p				
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			

[1]Only apply when NDR is deployed standalone, not when part of NSX.

[2]Supported Intel NIC required for throughput of more than 200Mbps.

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