

Network Detection and Response

Independent Testing

SE Labs has independently tested VMware's implementation of Network Detection and Response. In the test, VMware's Advanced Threat Prevention (standalone) product detected all network threats and payloads across four advanced persistent threats. As a result, NSX Advanced Threat Prevention (standalone) received an AAA rating. Check out the [test report](#).

Learn More

Check out these datasheets to learn more about Network Detection and Response deployment options in the NSX Security portfolio:

- [VMware NSX Distributed Firewall](#)
- [VMware NSX Gateway Firewall](#)
- [VMware NSX Advanced Threat Prevention](#)

At a glance

Network Detection and Response technology enables the security team to visualize attack chains by condensing massive amounts of network data into a handful of "intrusion campaigns." Network Detection and Response achieves this visualization by aggregating and correlating security events such as detected intrusions, suspicious objects, and anomalous network flows. Network Detection and Response also collects and visualizes contextual information for security events, minimizing the security team's manual work.

Network Detection and Response is a component of VMware NSX Advanced Threat Prevention along with Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis (NTA).

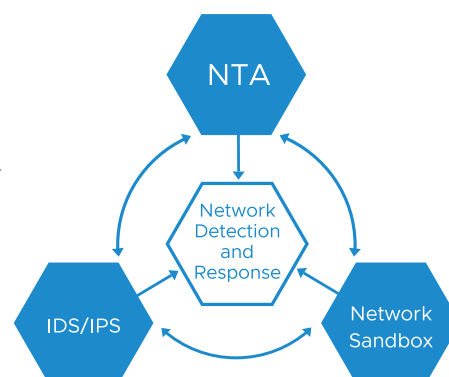


Figure 1: NSX Advanced Threat Prevention = IDS/IPS + Network Sandbox + NTA + Network Detection and Response

Quickly map incident actions to MITRE ATT&CK

Network Detection and Response maps adversaries' campaigns to the tactics and techniques described by the MITRE ATT&CK framework. The campaign scenario below provides an illustration:

- Initial Access and Execution: Network Detection and Response receives and visualizes signals regarding initial access attempts by detecting malicious links that trick an organization's users into downloading and installing malware.
- Execution, Persistence, and Privilege Escalation: Network Detection and Response receives and visualizes signals about the malicious nature of the download. Using file analysis signals, it detects advanced persistent threat actors who attempt to escalate privileges and evade detection.
- Discovery and Lateral Movement: Network Detection and Response receives and visualizes signals on anomalous network activity as the threat actor explores the organization's network and attempts to move laterally.
- Collection, Command and Control, and Exfiltration: Network Detection and Response receives and visualizes signals on anomalous network activity, indicating data staging for exfiltration.

Network Detection and Response with NSX+

The network detection and response capabilities with NSX+ are similar to those with NSX. The main difference is the deployment model. With NSX, a security administrator deploys network detection and response components in the private cloud. With NSX+, VMware delivers network detection and response capabilities as Software-as-a-Service (SaaS).

Security teams realize the following additional benefits with NSX+:

- **Easier operationalization** – Easily operationalize network detection and response as there are fewer components for a security team to install and manage. Also, scaling is simpler as resources for network detection and response are obtained and managed by VMware personnel. Finally, the NSX+ console is highly available without additional effort from the security team.
- **Multi-cloud scope** – Easily protect multi-cloud deployments as the NSX+ console supports private and public cloud out-of-the-box without additional components.

At initial availability, network detection and response with NSX+ will only ingest signals from IDS/IPS. For more information on NSX+ see www.nsx-plus.com.

Capabilities

VMware's Network Detection and Response consists of three complementary engines –

- **Aggregation Engine.** The aggregation engine collects signals from the available detection technologies – IDS/IPS, Network Sandboxing, and NTA. Then, the engine combines the signals to reach a verdict (malicious or benign) for each network activity.
- **Correlation Engine.** The correlation engine combines multiple related malicious activities into an easy-to-digest “intrusion campaign” view.
- **Context Engine.** The context engine collects data from multiple sources (including sources outside NSX) to add helpful context to the information provided to security analysts. For example, this engine provides information on who registered a particular domain and which accounts were accessed by a specific user.

Deployment Options

Network Detection and Response is available across all three products in the NSX Security portfolio –

- **NSX Distributed Firewall with Advanced Threat Prevention.** In this configuration, Network Detection and Response processes signals available across east-west network traffic and alerts security teams to potential lateral movement of threats.
- **NSX Gateway Firewall with Advanced Threat Prevention.** In this configuration, Network Detection and Response processes traffic coming into or out of an environment and alerts security teams to infiltration and exfiltration attempts. VMware's Network Detection and Response implementation processes signals across both the Distributed and Gateway Firewall when these firewalls are deployed together.
- **NSX Advanced Threat Prevention (standalone).** In this configuration, Network Detection and Response is deployed in an environment to protect non-vSphere workloads. Typically, neither the NSX Distributed Firewall nor the NSX Gateway Firewall is available in such environments. However, the Network Detection and Response functionality is similar to the other two configurations mentioned above.