Network Sandbox

Learn More

Check out these datasheets to learn more about sandbox deployment options in the NSX Security portfolio:

- VMware NSX Distributed Firewall
- VMware NSX Gateway Firewall
- VMware NSX Advanced Threat Prevention

At a Glance

VMware's Network Sandbox provides advanced malware analysis of artifacts traversing your cloud environment. The sandbox deconstructs every behavior engineered into a file or URL and sees all instructions that a program executes, all memory content, and all operating system activity.

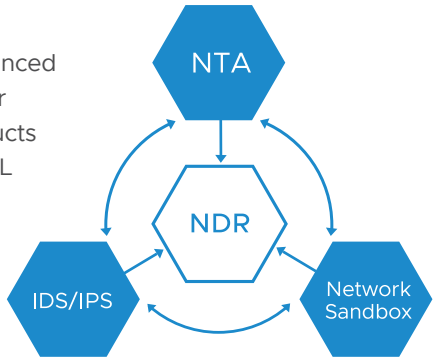

Figure 1: NSX Advanced Threat Prevention = IDS/IPS + Network Sandbox + NTA + NDR

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

How it Works

VMware's sandbox implementation uses VMware Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices), to analyze malware. The sandbox continuously observes all the actions that a malicious object takes.

Further, the sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, the sandbox identifies the memory (RAM) locations accessed by the artifact being analyzed.

Other malware detection technologies, such as traditional sandboxes, only have visibility down to the operating system. These sandboxes can inspect content and identify potentially malicious code but can't interact with the malware. As a result, such sandboxes have significantly lower detection rates and higher false positives. They can also be easily evaded by advanced malware.

Comprehensive Threat Analysis

The sandbox's analysis of malicious artifacts provides you with the threat information you need for security workflows and policies. You receive both high-level, actionable threat intelligence and detailed host and network indicators of compromise (IoCs).

The VMware Threat Analysis Unit NSX Knowledge Base Includes:

- Active command and control (C&C) servers
- Objects with zero-day exploits
- Toxic websites and malware distribution points
- Other helpful information to defend against threats specific to your organization

Identify Indicators of Compromise

VMware's sandbox supplies your researchers with the detailed IoCs they require when investigating malware. Critical malware attributes provided by the sandbox include:

- Malware information – Malware name and category, evasive actions, mutex activity, contents of malware memory, applicable screenshots, and files and registry keys that the malware accesses
- System IoCs – Process dumps, files and registry keys that the malware writes, malware filename, command line, and hash information
- Network IoCs – IP addresses and domains to which the malware connects, TCP/UDP port activity, DNS requests, and network packet capture

Complete Malware Behavior Visibility

VMware's sandbox provides visibility into malware behaviors that other technologies miss. The sandbox provides a complete malware analysis system for your threat analysts and incident response teams. It safely executes malware samples, analyzes URLs, and provides visibility into malicious behavior, even when the malicious objects are hidden inside encrypted traffic. This enables your threat researchers to safely and efficiently analyze the malicious objects used in advanced and targeted attacks.

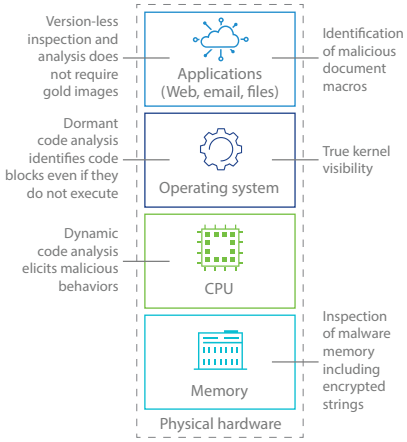

Figure 2: VMware Deep Content Inspection delivers unmatched visibility

MITRE ATT&CK Mapping

VMware's sandbox provides your threat analysts and incident responders with a detailed mapping of all actions taken by advanced malware to most of the hundreds of techniques listed in the MITRE ATT&CK framework. This allows you to quickly illuminate and assess the risk of a malicious event. Mapping malware incidents to MITRE ATT&CK brings new depth and a standardized industry vocabulary to your security operations.

VMware Threat Analysis Unit Access

The VMware Threat Analysis Unit™ automatically shares the malware characteristics, behaviors, and associated IoCs of every malicious object curated and analyzed by VMware with all VMware customers and partners.

This allows for faster detection and analysis of previously unseen threats and reduces the time for you to respond to malicious activity. The sandbox also continuously updates the VMware Threat Analysis Unit in real time with intelligence from partner and customer environments worldwide.

In addition, your threat analysts and incident response team can also subscribe to the VMware Threat Analysis Unit NSX knowledge base for faster response to previously known threats. The knowledge base contains the malware characteristics, behaviors, and associated IoCs of every malicious object curated and analyzed by the NSX team.

Deployment Options

Network sandboxing is available across all three products in the NSX Security portfolio: NSX Distributed Firewall with Advanced Threat Prevention, NSX Gateway Firewall with Advanced Threat Prevention, and NSX Advanced Threat Prevention (standalone).