# VMware NSX Sandbox

## Network sandboxing for VMware NSX Security

### AT A GLANCE

VMware NSX® Sandbox provides advanced malware analysis of artifacts traversing your data center. NSX 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.

## Unmatched malware detection with Deep Content Inspection

NSX Sandbox 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. NSX Sandbox continuously observes all the actions that a malicious object takes.

Further, NSX Sandbox interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. Finally, NSX 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 they 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

NSX Sandbox analysis of malicious artifacts provides you with the threat information you need to incorporate the results into workflows and policies. You receive high-level, actionable threat intelligence and detailed host and network indicators of compromise (IoCs).

NSX Sandbox detects advanced malware engineered to defeat advanced or next-generation enterprise security tools, such as traditional sandboxes, firewalls, and intrusion prevention systems. NSX Sandbox delivers complete visibility into malware used in advanced and targeted attacks, even when the malicious objects are hidden inside encrypted traffic. NSX Sandbox enables your security team to respond rapidly to malicious activity before it results in a damaging data breach.

## Complete malware behavior visibility

NSX Sandbox provides visibility into malware behaviors that other technologies miss.

NSX Sandbox provides a complete malware analysis system for your threat analysts and incident response teams. It safely executes malware samples, analyzes URLs, and provides complete visibility into malicious behavior. This enables your threat researchers to utilize NSX Sandbox to analyze the malicious objects used in advanced and targeted attacks safely and efficiently.

### 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

NSX Sandbox continuously updates the VMware Threat Analysis Unit in real-time with intelligence from partner and customer environments worldwide.

### FLEXIBLE DATA CENTER AND ON-PREMISES OPTIONS

You can access NSX Sandbox as part of your NSX Security deployment—NSX Distributed Firewall, NSX Gateway Firewall, or NSX Network Detection and Response—giving you maximum flexibility to meet your unique requirements. For example, if you have to meet strict data privacy laws and policies, you can deploy NSX Sandbox on-premises in your data center.

### IDENTIFY INDICATORS OF COMPROMISE

NSX Sandbox supplies your researchers with the detailed IoCs they require when investigating a piece of malware. Critical malware attributes provided by NSX Sandbox include:

- **Malware information** – Malware name and category, evasive actions, mutex activity, contents of the malware memory, applicable screenshots, 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

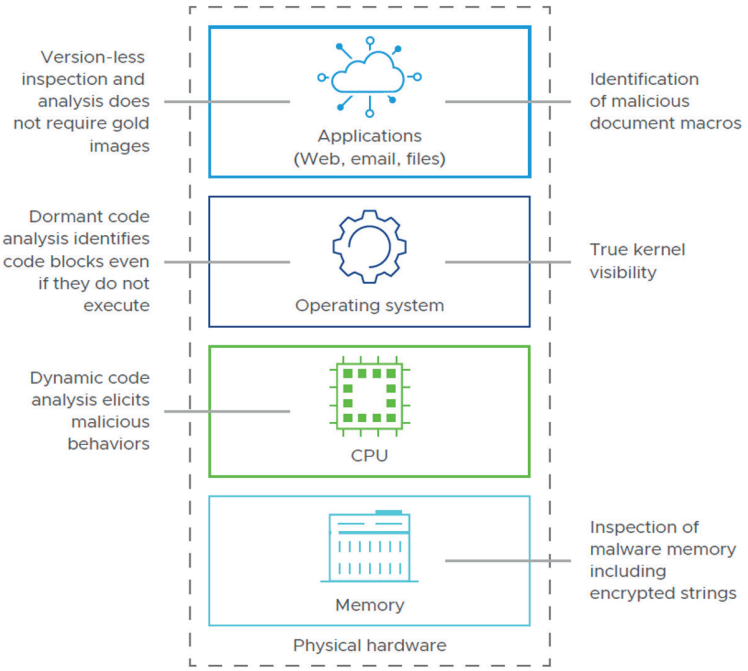


FIGURE 1: VMware Deep Content inspection delivers unmatched visibility.

## MITRE ATT&CK mapping

NSX Sandbox provides your threat analysts and incident responders with a detailed mapping of all actions taken by advanced malware against the vast majority 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 a 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.

We quickly analyze all new objects and share the results of the analysis across our entire network. This allows for faster detection and analysis of previously unseen threats and reduces the time for you to respond to malicious activity. NSX 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 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 NSX.

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com 