# VMware NSX Advanced Threat Analyzer

## Network sandboxing for VMware NSX Service-defined Firewall

VMware NSX® Service-defined Firewall™ with Advanced Threat Prevention provides advanced malware analysis of artifacts traversing your data center. The patented VMware NSX Advanced Threat Analyzer™ 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.

### Comprehensive analysis of advanced malware

NSX Advanced Threat Analyzer detects advanced malware engineered to defeat advanced or next-generation enterprise security tools, such as traditional sandboxes, firewalls and intrusion prevention. NSX Advanced Threat Analyzer delivers complete visibility into advanced malware, enabling your security team to respond rapidly to malicious activity before it results in a damaging data breach.

NSX Advanced Threat Analyzer 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 as well as detailed host and network indicators of compromise (IoCs).

NSX Advanced Threat Analyzer 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 Advanced Threat Analyzer to analyze the malicious objects used in advanced, targeted and zero-day attacks safely and efficiently.

### Unmatched detection with VMware Deep Content Inspection

NSX Advanced Threat Analyzer provides complete visibility into the malware behavior that other technologies miss. It 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. VMware Deep Content Inspection interacts with the malware to observe all the actions a malicious object might take.

NSX Advanced Threat Analyzer interacts with the malware to elicit every malicious behavior, including identifying dormant code and documenting all CPU instructions executed. It also 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 level. They can inspect content and identify potentially malicious code, but they can't interact with malware like NSX Advanced Threat Analyzer can. As a result, they have significantly lower detection rates and higher false positives, in addition to being easily identified and evaded by advanced malware. (Advanced threats evade other sandboxing technologies by recognizing the sandbox environment or using kernel-level exploits.)

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 malware information useful to defend against threats specific to your organization

NSX Advanced Threat Analyzer continuously updates the VMware Threat Analysis Unit in real time with intelligence from partner and customer environments around the world.

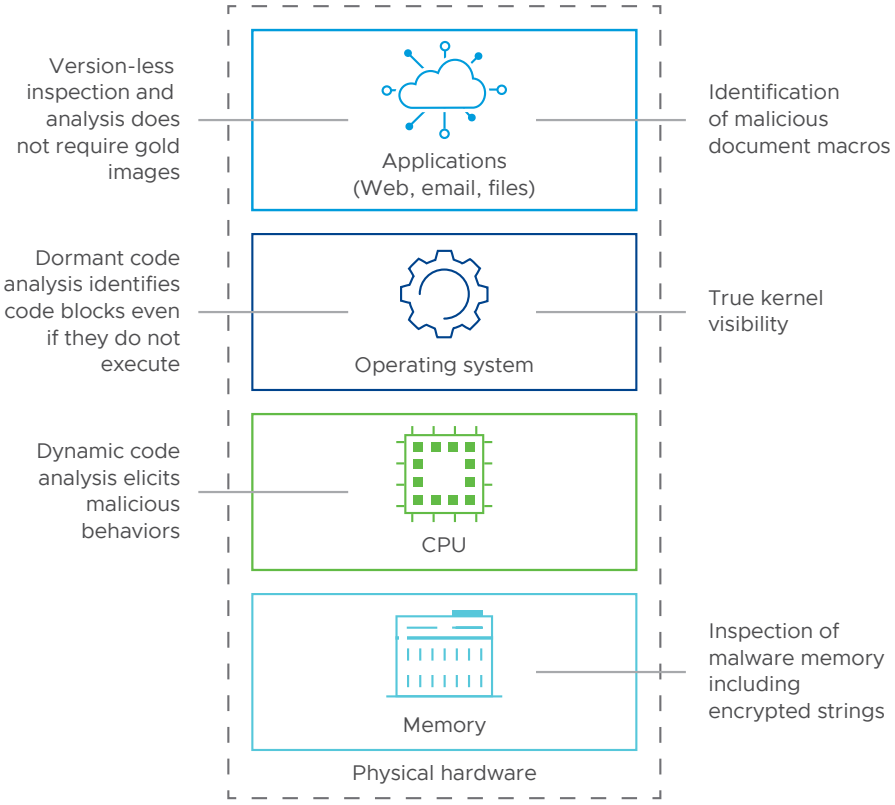


FIGURE 1: VMware Deep Content Inspection delivers unmatched visibility.

## VMware Threat Analysis Unit

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 Advanced Threat Analyzer continuously updates the VMware Threat Analysis Unit in real time with intelligence from partner and customer environments around the world.

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 unseen threats. It contains the malware characteristics, behaviors and associated IoCs of every malicious object curated and analyzed by NSX.

## Flexible data center and on-premises options

You can access NSX Advanced Threat Analyzer either through an on-premises deployment or as part of NSX Service-defined Firewall with Advanced Threat Prevention, 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 Advanced Threat Analyzer on premises in your data center.

## Identify indicators of compromise

NSX Advanced Threat Analyzer supplies your researchers with the detailed IoCs they require when investigating a piece of malware. Critical malware attributes provided by NSX Advanced Threat Analyzer 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

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