White Paper: **September 2021**

Advanced Threat Prevention with VMware NSX Distributed Firewall

vmware®

Protecting assets against agile adversaries

Cybercrime is big business. Just how big is it? If cybercrime were a country, it would be the world's third-largest economy after the US and China [1]. It's easy to understand the allure for attackers, who see a clear path to a payoff. If they can gain access to mission-critical applications and high-value assets in the data center — such as personal information databases, intellectual property stores, and more — they can exfiltrate it and sell it to the highest bidder or threaten to disclose it unless paid a ransom.

Unfortunately, from the corporate point of view, protecting assets is more difficult than ever. The IT landscape has been transformed by a porous perimeter, personal devices on the network, pandemic-driven remote working, the ubiquitous use of mobile devices, as well as by the proliferation of applications running in the cloud and virtual desktop infrastructure in the data center. Organizations have spent many years and countless sums of money protecting the perimeter — so-called "north-south" traffic. Yet agile, adaptive adversaries have found ways to breach perimeter defenses, gaining a foothold in the data center via low value, lightly defended soft targets. Once in, they can move laterally, blending in with east-west traffic, and gain access to high-value data. Thus, the new battleground in protecting the organization is securing east-west traffic.

The nature of east-west protection

Protecting east-west traffic in an effort to avoid attacks is not a new problem, but it has been difficult to tackle because in the past it was considered too complicated, too expensive, and too time-consuming. To effectively prevent attacks requires constant inspection of all east-west traffic on the network. It's not enough to inspect only that traffic that has entered the data center from the outside. A malicious internal user, or an unsuspecting but trusted employee whose account has been compromised, could be the source of unwanted access.

Preventing east-west attacks calls for a two-pronged approach: access control and advanced threat prevention. Access control, in turn, calls for firewalls in the data center with fine-grained policies at the workload level. Advanced threat prevention involves the use of intrusion detection/prevention systems (IDS/IPS) that analyze live traffic as it passes through the network, detonating suspicious objects (such as files) in network sandboxes and performing traffic and behavior analysis to detect anomalies and determine which, if any, represent malicious behavior. All data gathered must be correlated to accurately identify intrusions and accelerate and automate remediation.

The VMware approach to preventing advanced threats

VMware has taken an automated, distributed and enterprise-wide approach to preventing advanced threats. The solution, the VMware Advanced Threat Prevention (ATP) package, is an add-on to the VMware NSX Distributed Firewall [2]. ATP provides protection against advanced threats. It increases fidelity, reduces false positives, and accelerates remediation while simultaneously reducing the amount of manual work that analysts must do.

VMware's ATP incorporates multiple detection technologies and includes logic that combines information from all these (see Figure 1):

- Detection technologies
  - Distributed IDS/IPS
  - Network sandbox
  - Network traffic analysis (NTA)
- Network detection and response (NDR)
  - Aggregation, correlation, and context engines
  - Including the ability to pull context from sources outside NSX

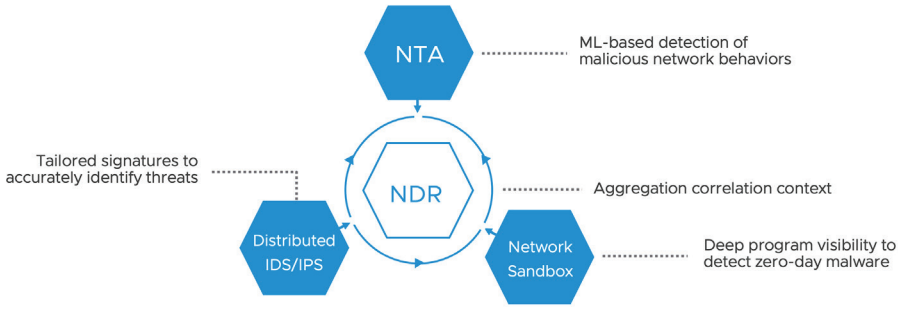

Figure 1 – ATP: Multiple detection technologies + NDR

Each technology has its individual role to play, yet they all work together to provide a cohesive defensive layer.[1] Let's examine each of the technologies and look at how they work, both independently and together.

Detection technologies

Distributed IDS/IPS is a signature-based intrusion detection/prevention system [3]. This technology inspects all traffic that enters the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns, to hunt for attacks in the traffic flow. When it finds such attacks, it generates alerts for use by security analysts. Alerts are also logged for post-incident investigation. Distributed IDS/IPS is efficient because it is co-located with the workload to optimize traffic flow and incorporates signatures tailored to the workload being protected. Because it is workload-aware, it applies only those signatures that relate to the specific workload. Using such context-based signatures not only reduces the detection effort, it also reduces the possibility of false positives.

1. NSX 3.2 integrates distributed IDS/IPS with NTA, NDR and Sandboxing technology from Lastline Inc.

Network sandbox is a secure isolation environment that is designed to detect malicious artifacts in the data center. It analyzes the behavior of objects, such as files and URLs, to determine if they are benign or malicious. Because it is not reliant on signatures, the sandbox can detect novel and highly targeted malware that has never been seen before. VMware chose the most advanced method of sandboxing available: Full-system Emulation (FUSE)-based sandboxing [4]. FUSE was chosen over virtualization and operating system (OS) emulation as both these approaches have serious shortcomings:

- Virtualization-based sandboxes [5] run on virtual machines, giving up control for a short period of time during which the malware and the OS run directly on system hardware. While this optimizes the number of files a single piece of hardware can analyze, it is not entirely effective against malware. Criminals have adapted their malware to discover if it is being run in a virtualized sandbox and alter its behavior to evade detection or wait until the sandbox operation times out. In addition, virtualization limits what the sandbox can see: it can observe calls to the OS but can't see what the malware does internally with those calls.
- OS emulation sandboxes provide greater visibility into what the malware is doing. While a good idea in theory, implementation is not practical. To be accurate, OS emulation would require duplicating Windows and every other OS in the enterprise, so developers emulate just the most common, applicable system calls in the OS. Naturally, criminals are aware of this approach, and their malware uses infrequently used system calls that can't be detected by the sandbox, leading to an inability to detect advanced malware. Again, a less-than-optimal approach.

Full system emulation (FUSE) sandboxes emulate the entire hardware: CPU, memory, and I/O devices. The advantages are clear: it allows the sandbox to interact with the malware and conduct deep content inspection. This enables the sandbox to view everything the malware is doing, and lets analysts carefully study the malware and its operation. Because it emulates everything, it is much more difficult for cybercriminals to evade the sandbox.

FUSE sandboxes, while clearly superior at detecting advanced malware, can suffer from performance issues since they introduce another layer. However, VMware's implementation of FUSE incorporates years of research and fine-tuning to eliminate the performance penalty of full system emulation architectures. The VMware FUSE sandbox can identify objects with novel exploits, malicious websites, command and control servers, and malware distribution points. This information is useful to defend against threats specific to an organization by triggering prevention workflows and providing secure alerts and data to other security tools.

Finally, VMware's implementation of sandboxing applies machine learning (ML) to malicious behavior and malware samples, automatically creating classifiers that recognize malicious network behaviors and IDS/IPS signatures that are pushed out to all NSX deployments.[2] This is an example of how the detection technologies in VMware's ATP work together to continuously increase overall efficacy.

2. This functionality became available in the NSX 3.2 release.

NTA looks at the data center network traffic and traffic flow records using ML algorithms and advanced statistical techniques, to develop a baseline of normal activities. With this foundation, NTA can identify protocol anomalies (unusual protocol activity), traffic anomalies (unusual traffic activity) and host anomalies (unusual workload behavior) as they appear.

Of course, not all anomalies represent threats; that's why VMware's NTA implements additional ML and rule-based techniques to determine if the anomaly is malicious. This analysis pipeline keeps false positives to a minimum, reducing the work of the security team so it can focus on true issues.

Finally, like Distributed IDS/IPS, VMware's NTA implementation is co-located with the workload enabling efficient but thorough analysis of east-west network traffic.

Network detection and response

The aggregation, correlation, and context engines in VMware's NDR provide powerful east-west security capabilities within the data center and in multi-cloud environments.

The aggregation engine collects signals from the individual detection technologies and combines them to reach a verdict (malicious or benign) on network activities. The correlation engines combine multiple related alerts into a single "intrusion." The context engines collect data from multiple sources (including sources outside NSX) to add useful context to the information provided to analysts. For example, these engines provide information on who registered a particular domain or which accounts were accessed by a specific user.

Collectively, the aggregation, correlation, and context engines condense massive amounts of network data down to just a handful of intrusions along with contextual information. This allows the team to visualize the attack chain, as shown in Figure 2. Such a comprehensive yet condensed overview of attacks greatly simplifies the work of security teams. Also, malicious activity is grouped by stage (based on the MITRE ATT&CK framework) to illuminate the risk associated with each malicious event.

Armed with this information, security teams can quickly understand the scope of the attack, zero in on real threats, and focus their attention on mitigation and remediation before damage can be done.

Figure 2: The attack chain as shown in NSX NDR

Benefits of the VMware ATP approach

It's clear that a comprehensive approach is essential to achieve effective prevention, detection, and remediation of advanced threats. VMware has designed its ATP package to take full advantage of the power of strong detection technologies and equally powerful aggregation, correlation, and context engines. The chief benefits are efficient operation, high fidelity detection, and comprehensive visibility. Let's unpack each of those.

- **Efficient Operation** – VMware's ATP is designed both for efficiency and to avoid unnecessary activities on the part of skilled analysts. ATP (specifically the NDR component) combines multiple related alerts, across many different assets and hops, into a single intrusion. This enables the incident response team to quickly understand the scope of the threat and prioritize its response. Further, the detailed information provided by ATP allows the security team to proactively hunt for network threats. Finally, the solution reduces false positives — often by up to 90% [6]. This frees up skilled analysts to focus on actual threats rather than spending time and resources chasing down distractions.
- **High Fidelity Detection** – VMware's ATP is highly effective at detecting not only known threats but new, evolving threats that have never been seen before. It is engineered to detect malware that has been specifically designed to evade standard security tools. ATP detects threats not only by analyzing local network traffic behavior, but also by importing and utilizing indicators of malicious behavior from the VMware global threat intelligence network.
- **Comprehensive Visibility** – VMware's ATP has full visibility into both north-south and east-west traffic. Thus, ATP provides a comprehensive overview of anomalous behavior across the network. And ATP extends its protection to all assets in the infrastructure, including those devices that do not have endpoint protection installed, such as legacy workloads.

Securing east-west network traffic — available today in NSX Distributed Firewall

Protecting the organization calls for securing east-west network traffic. With the rapid increase in clever, innovative attacks by agile adversaries, even the strongest perimeter defenses can be breached, allowing attackers to gain access to the data center. Once inside, they can carry out reconnaissance, elevate privileges, and potentially access or exfiltrate highly sensitive data. Securing east-west traffic is the only way to protect against such attacks.

While securing east-west traffic has been something of an elusive goal in the past, due to the cost and effort, the problem of enterprise security has only gotten worse as organizations move to more cloud-based applications and hybrid environments. But today the outlook is much different. Thanks to VMware's ATP package for the NSX Distributed Firewall, organizations can ensure constant vigilance over east-west traffic and finally enjoy comprehensive protection against malicious activities and traffic.

References

1. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybercrime Magazine, 2020

2. Internal Firewalls for Dummies

3. VMware NSX Distributed IDS/IPS

4. Sandbox Architectures

5. Virtualization-based Sandboxes are Vulnerable to Advanced Malware

6. VMware NSX Network Detection and Response

Item No: vmw-wp-NSX-distributed-firewall-uslet-v2 9/21