VMware vDefend Advanced Threat Prevention

Rapidly Respond to Ransomware and Advanced Threats

Key benefits

Efficient operation: ATP combines multiple related alerts across many different assets and hops into a single intrusion campaign view. This view enables the incident response team to quickly understand the scope of the threat and prioritize its response. Further, the information ATP provides allows security teams to proactively hunt for network threats. Finally, the solution reduces false positives.

High-fidelity detection: ATP detects not only known threats but also new, evolving threats that have never been seen before. It is engineered to detect malware specifically designed to evade standard security tools. ATP detects threats by analyzing local network traffic behavior and importing and utilizing indicators of malicious behavior from the VMware global threat intelligence network.

Deep threat visibility: ATP has complete visibility into north-south and east-west traffic. Thus, ATP provides a comprehensive overview of abnormal behavior across the network. It also extends protection to all assets in the infrastructure, including those devices that do not have endpoint protection installed, such as physical servers with legacy workloads.

Continued on page 2.

At a glance

VMware's vDefend Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats, including ransomware.

VMware vDefend ATP combines multiple detection technologies – Intrusion Detection/ Prevention System (IDS/IPS), Malware Prevention Service, and Network Traffic Analysis (NTA) – with aggregation, correlation, and context engines from Network Detection and Response (NDR).

These capabilities complement each other to provide a cohesive defensive layer. As a result, ATP increases detection fidelity, reduces false positives, and accelerates remediation while decreasing security analysts' manual work.

Advanced Threat Prevention

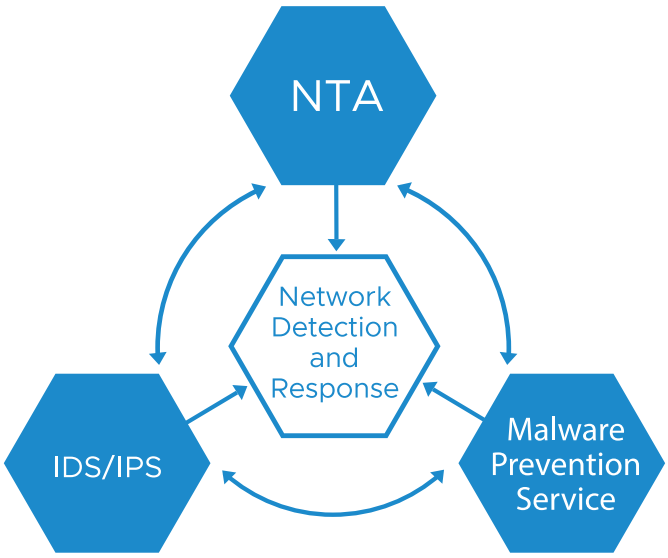

Figure 1: VMware Advanced Threat Prevention = IDS/IPS + Malware Prevention Service + NTA + Network Detection and Response

vmware by Broadcom

Key benefits (continued)

Rapid Triage and Threat Remediation: Coalesce multiple related alerts across many different assets and hops into a single intrusion campaign, enabling your SOC teams to quickly scope the threat and prioritize its remediation.

Key capabilities

IDS/IPS

This technology inspects all traffic that enters or leaves 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.

Network Traffic Analysis (NTA)

This technology looks at network traffic and traffic flow records using machine learning (ML)algorithms and advanced statistical techniques to develop a baseline of everyday activities. NTA can identify protocol, traffic, and host anomalies 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 security team's work so the team can focus on real issues.

VM-aware Malware Prevention Service (MPS)

MPS is an advanced engine designed for malware analysis and prevention, utilizing a multi-technique approach. It integrates machine learning, static and dynamic analysis, and memory analysis to safeguard organizations against highly evasive zero-day malware. MPS also features an in-house developed Guest Introspection capability, which operates on each hypervisor to deliver deep visibility into file systems, processes, and registry activities across all hosts. This enables the analysis of encrypted files, enhances threat detection and response, and strengthens overall security posture.

Multi-context Network Detection and Response (NDR)

NDR consists of aggregation, correlation, and context engines. The aggregation engine collects signals from individual detection technologies. It combines them to reach a verdict (malicious or benign) on network activities. The correlation engines combine multiple related alerts into an "intrusion campaign." The context engines collect data from various sources (including sources outside NSX) to add helpful context to the information provided to security analysts.

Use Cases

Virtual patching: Proactively protect vulnerable workloads using distributed IDS/IPS, allowing security teams time to plan and deploy patches to workloads.[5]

Compliance: Simplify audits and quickly bring environments into compliance (for PCI, HIPAA, etc) by deploying a software-based distributed IDS/IPS with minimal changes to your existing network.

Threat Investigation: Empower SOC teams to visualize attack chains by leveraging multi-context NDR, which consolidates alerts into curated threat campaigns. These campaigns are enriched with contextual information and mapped to MITRE ATT&CK techniques and TTPs, providing clear explainability and deeper insights into the attacker's behavior.

Ransomware Prevention and Recovery: Advanced Threat Prevention identifies, prevents, and detects ransomware activity. After a ransomware event, VMware Live Recovery can help to safely recover data from the last known clean backup.[6]

Anomaly detection: Provide NTA data collection points on all workloads without requiring SPAN or TAP ports. Enable real-time intelligence on anomalous activities as such activity moves laterally across the infrastructure.

5,6. Requires VMware vDefend Advanced Threat Prevention.

Deployment flexibility

ATP is available as an add-on to VMware vDefend Firewall. ATP is also available as a standalone product – VMware vDefend Network Detection and Response – that does not require the deployment of either firewall. The table below presents a view of the VMware vDefend Security portfolio and ATP's role in it.*

Capabilities	East-west Firewall	Edge Firewall	No Firewall
Access control	VMware vDefend Distributed Firewall	VMware vDefend Gateway Firewall	
IDS/IPS	VMware vDefend Distributed Firewall with ATP	VMware vDefend Gateway Firewall with ATP	VMware vDefend Network Detection and Response
Malware Prevention Service			
NTA			
NDR			

*Some use cases may require a specific ATP deployment option.

Recommended configuration for VMware vDefend Network Detection and Response

The table below summarizes the minimum resource envelope required for the successful hardware form factor of VMware vDefend Network Detection and Response (NDR).

Role	Manager[1]	Data node[2]	Engine[3]	Sensor–1G[4]	Sensor–10G[4]
Server model	Dell PowerEdge R450				
CPU type	Intel® Xeon® Silver 4314				
CPU quantity	1	1	1	1	2
RAM	96GB	96GB	128GB	64GB	192GB
RAID controller	Dell EMC PowerEdge RAID Controller (PERC) H745/H755 (with flash-backed cache)				
RAID configuration	RAID 10	RAID 10	RAID 1	RAID 1	RAID 1
Persistent storage	4 × 4 TB HDDs	4 × 2 TB HDDs	2 × 1 TB HDDs	2 × 1 TB HDDs	2 × 1 TB HDDs
Additional network card	None	None	None	Intel i350 Quad Port 1GbE	Intel X710 Dual Port 10GbE

With the configurations above, security teams can expect performance as documented in the table on the following page (performance varies with network traffic profile, server configuration, object/file type, and object/file size):

1. Manager: Correlation and Orchestration. Virtualization supported.
2. Data Node: Anomaly Detection and Data Storage. Virtualization supported.
3. Engine: Deep Content Inspection. Dedicated hardware is recommended
4. Sensor(s): IDPS, NetFlow, and Detection. Virtualization supported.

vmware® by Broadcom

Network traffic (Gbps)	Up to 1 (4), depending on the sensor type
Objects per day	Up to 100,000
Files analyzed per day	Up to 10,000
Engine scalability	Up to 30 engines/manager
Sensor scalability	Up to 100 sensors/manager
Total endpoints protected	Up to 200,000 endpoints/manager

Minimum virtual requirements for VMware vDefend Network Detection and Response

The table below summarizes the minimum resource envelope required for the successful virtual form factor of VMware vDefend Network Detection and Response (NDR):

Role	Manager	Data node	Engine**	Sensor–1G	Sensor–10G
CPU	20	20	20	20	40
RAM	96GB	96GB	128GB	64GB	192GB
Storage	4TB	4TB	1TB	1TB	1TB

*** Customers must select the following option on the VM under Hardware Virtualization: "Expose hardware-assisted virtualization to the guest OS"*

Item No: VMware vDefend Advanced Threat Prevention_JR11 11/24