

# VMware vDefend Advanced Threat Prevention

## 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 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.

**Comprehensive visibility:** ATP has complete visibility into both 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.

## At a glance

VMware's vDefend Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats. VMware vDefend ATP combines multiple detection technologies – Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, 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.

## 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.

### 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.

### Network Sandbox



This is a secure isolation environment that detects malicious artifacts. It analyzes the behavior of objects, such as files and URLs, to determine if they are benign or malicious. Because it does not rely on signatures, the sandbox can detect novel and highly targeted malware that has never been seen before.

### 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.

### Learn more

Check out these resources to learn more about protecting your ecosystem with the VMware vDefend Security portfolio. Reach out to your VMware Sales Representative for further details.

**Further reading:**

[VMware vDefend Gateway Firewall](#)

[VMware vDefend Distributed Firewall](#)

### Network security use cases<sup>1</sup>

- **Virtual patching:** Proactively protect vulnerable workloads using distributed IDS/IPS, allowing security teams time to plan and deploy patches to workloads.
- **Advanced malware detection:** Utilize a full system emulation network sandbox to detect and block sophisticated malware as it enters the infrastructure.
- **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.
- **Intrusion campaign detection:** Enable the security team to visualize attack chains by using the NDR to condense massive amounts of network data into a handful of intrusions along with contextual information. Correlate security events (suspicious objects and anomalous network flows) to automatically connect the dots for the security team.

### 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
<b>Access control<sup>2</sup></b>	VMware vDefend Distributed Firewall	VMware vDefend Gateway Firewall	
<b>IDS/IPS</b>			
<b>Network Sandboxing</b>	VMware vDefend Distributed Firewall with ATP	VMware vDefend Gateway Firewall with ATP	VMware vDefend Network Detection and Response
<b>NTA</b>			
<b>NDR</b>			

VMware vDefend Distributed Firewall with ATP and VMware vDefend Gateway Firewall with ATP are managed via the NSX Manager console. VMware vDefend Network Detection and Response has a dedicated console and is not managed via the NSX Manager.

1. Some use cases may require a specific ATP deployment option.  
 2. See “Internal Firewalls (VMware Special Edition)” for definitions of access control, traffic types, and firewall types.

## Additional capabilities of VMware vDefend Network Detection and Response

VMware vDefend Network Detection and Response is desirable when the Distributed Firewall and Gateway Firewall are not applicable. Such a situation typically arises in an IT environment with non-vSphere workloads.

- Workflows for senior security operations center (SOC) staff to hunt for threats in the network. These workflows enable both visualization-based and metadata-based threat hunting
- The ability to share low-level analysis artifacts, including malware activities, mapped to the MITRE ATT&CK framework
- The ability to submit objects manually and via an API to the Network Sandbox
- The ability to define customized analysis rules
- Robust and comprehensive integrations with third-party Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools commonly used in SOCs

## Minimum hardware configuration for VMware vDefend Network Detection and Response

The table below summarizes the minimum resource envelope required for the successful operation of VMware vDefend Network Detection & Response (NDR):

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

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

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