Network Traffic Analysis

MITRE ATT&CK Coverage

Like many technologies, security has a unique language. MITRE ATT&CK is a globally recognized "language" of adversarial tactics and techniques based on real-world observations. NTA provides NSX Distributed Firewall, Gateway Firewall, and Advanced Threat Prevention customers with the ability to expand their MITRE ATT&CK coverage and detect most tactics and techniques, including:

- Persistence
- Privilege escalation
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and control
- Exfiltration

At a Glance

Network Traffic Analysis (NTA) helps security teams rapidly detect anomalous activity and malicious behavior as such activity moves laterally across the network. NTA looks at network traffic and traffic flow records using machine learning (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.

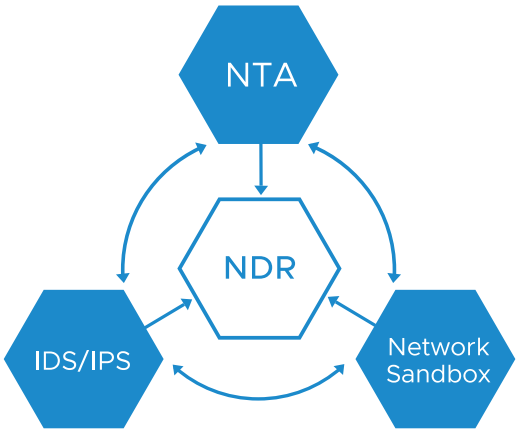

Figure 1: NSX Advanced Threat Prevention = IDS/IPS + Network Sandbox + NTA + NDR

At VMware, NTA is a component of NSX Advanced Threat Prevention along with Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Detection and Response (NDR).

Integrated Security Intelligence

Security teams are often forced to make snap decisions based on inaccurate, incomplete, or worse, incorrect data. Not having complete visibility and understanding of the network inhibits their ability to detect and stop attacks. VMware's NTA implementation uses the intelligence from security experts inside the VMware Threat Analysis Unit (TAU) and multiple forms of ML to produce proactive threat intelligence to identify known and novel threats.

Detection Capabilites

NTA identifies abnormal activity, whether it be by hosts, in protocols, or inside the network traffic itself. NTA's detection capabilities include:

Learn More

Check out these datasheets to learn more about NTA deployment options in the NSX Security portfolio:

- VMware NSX Distributed Firewall
- VMware NSX Gateway Firewall
- VMware NSX Advanced Threat Prevention

Host Anomalies

- Lateral movement of attackers from compromised hosts inside the network
- Detection of scans by an attacker looking for other workloads
- Detection of malicious content and artifacts targeting other workloads
- Use of compromised credentials
- Unusual connections between hosts
- Unusual authentication activity

Protocol Anomalies

- Misuse of protocols
- Unusual Kerberos use
- Unusual Server Message Block (SMB) commands
- Domain Name System (DNS) tunneling
- Suspicious DNS resolution
- Application-layer metadata, including DNS requests, web requests, and email content

Traffic Anomalies

- Data exfiltration of critical data outside the network
- Domain Generation Algorithm (DGA) activity
- Beaconing
- Network enumeration and reconnaissance
- Detection of unusual JA3/JA3s fingerprints
- Encrypted Traffic Analysis (ETA)
- Port scan attempts and unusual port access attempts

Deployment Options

NTA is available across all three products in the NSX Security portfolio: NSX Distributed Firewall with Advanced Threat Prevention, NSX Gateway Firewall with Advanced Threat Prevention, and NSX Advanced Threat Prevention (standalone). The distributed firewall option allows for TAP-less NTA deployment providing east-west protection against advanced threats while increasing operational simplicity.