Network Traffic Analysis

Network Traffic behavioral analysis for VMware NSX Security

At a glance

- NTA protects East-West traffic across multi-cloud environments spanning virtualized, containerized and bare metal workloads.
- NTA is distributed to the infrastructure and virtualizes the entire security stack, empowering security teams to mitigate risk, ensure compliance and simplify the operational model at every workload.

VMware NSX® Distributed Firewall™ with Network Traffic Analysis (NTA) helps SOC teams rapidly detect anomalous activity and malicious behavior as it moves laterally across your network. NTA can uncover active threats inside the network and secures East-West traffic across multi-cloud environments—including virtualized, containerized or bare metal resources. NTA is distributed as a service to the underlying Software Defined Data Center (SDDC) infrastructure at each host, bringing authoritative context, accuracy and speed to your security teams.

Intelligent risk correlation equals better prevention, detection and response

Built into the hypervisor, NTA has unmatched visibility into network traffic with both workload and network context, providing security operations with superior detection capabilities. NTA makes it easy to quickly isolate and quarantine a compromised workload to provide application continuity to other workloads while preventing data loss. Its unique and privileged position within the hypervisor makes it harder to subvert by malware on a compromised host.

Immediately increase operational efficiency and reduce security complexity

With NTA, security controls and policy enforcement protect all distributed assets while supporting both new and legacy applications and environments.

The solution's centralized ease of deployment and management allows security teams to consistently apply policies across multiple environments with little to no additional effort, reducing the number of tools and agents you need to deploy. This provides full coverage of the environment while reducing complexity and eliminating blind spots.

Expand your 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 customers with the ability to expand their MITRE ATT&CK coverage and detect the majority of tactics and techniques including:

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

Make better security decisions with contextual authority and security intelligence

Far too often, security teams are 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. NTA uses the intelligence from security experts inside the VMware Threat Analysis Unit (TAU) as well as multiple forms of artificial intelligence (AI) and machine learning (ML) to produce proactive threat intelligence to identify both known and novel threats.

NTA also allows you to incorporate other sources of threat intelligence you may have purchased using industry standards such as STIX/TAXII and MISP33.

Key Detection Capabilities

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

Traffic Anomalies

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

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 multiple hosts
- Unusual authentication activity

Protocol Anomalies

- Misuse of protocols
- Unusual Kerberos use
- Unusual SMB commands
- DNS tunneling
- Suspicious DNS resolution
- Application-layer metadata including DNS requests, web requests and email content

NSX Security: Complete coverage for MITRE ATT&CK

	NSX Security Features				
Tactics	Firewall	Sandbox	IDS/IPS	NTA	VMware
Initial access	•	•	•		✓
Execution		•			✓
Persistence	•	•	•	•	✓
Privilege escalation		•	•	•	✓
Defense evasion	•	•	•		✓
Credential access		•	•	•	✓
Discovery	•	•	•	•	✓
Lateral movement	•	•	•	•	✓
Collection		•	•	•	✓
Command & control		•	•	•	✓
Exfiltration				•	✓
Impact		•	•		✓

Item No: vmw-sol-brief-nsx-network-traffic-analysis-uslet-v2 11/21