VMware Network Security Deploy and Adopt Service

At a glance

This service provides two out of five options to deploy and adopt VMware NSX®. The installation and configuration are conducted jointly with the Customer team to enhance learning during deployment.

Key benefits

- Deploy a best practice-based foundational netwok virtualization implementation
- Protect applications with micro-segmentation and advanced threat prevention at the workload level
- Enable advanced, lateral threat prevention on east-west traffic using built-in, fully distributed threat prevention
- Reduce attack surface, increase visibility, and simplify operations
- Expand security protections and capabilities within the virtual data center
- Prevent the execution and propagation of ransomware that may rely on vulnerable protocols

SKU

PS-NSX-SEC-DPY-ADPT
Delivered remotely in English

Service overview

The VMware Network Security Deploy and Adopt services provide Professional Services for VMware NSX®. This service is ideal for organizations that are new to VMware NSX and have limited exposure to implementing and managing micro-segmentation, intrusion detection and prevention, and advanced threat prevention.

Depending on the options selected, customers will be able to:

- Reduce attack surface and increase visualization
- Rapidly adopt micro-segmentation to protect applications
- Enable advanced, lateral threat prevention

For this service, customers may choose two out of five options to deploy and adopt:

- Option A: Adopt micro-segmentation with VMware NSX® Distributed Firewall™ and VMware NSX® security deployment
- Option B: Network traffic visibility with VMware NSX® Intelligence™
- Option C: Protocols hardening with VMware NSX Distributed Firewall
- Option D: Threat prevention with VMware NSX® Distributed IDS/IPS™
- Option E: Implementation of VMware NSX® Advanced Threat Prevention™

If additional options are desired, an additional purchase of this service is required.

Prerequisites and inclusions

The table below summarizes prerequisites and inclusions for each option.

	Option A Adopt Micro-segmentation with VMware NSX® Distributed Firewall™ and VMware NSX® security deployment	Option B Network traffic visibility with VMware NSX Intelligence	Option C Protocols hardening with VMware NSX Distributed Firewall	Option D Threat prevention with VMware NSX Distributed IDS/IPS	Option E Implementation of VMware NSX Advanced Threat Prevention
Prerequisites					
VMware NSX must be deployed (3.2 or above)		✓	✓	✓	✓
VMware NSX Distributed Firewall (DFW) must be enabled.				✓	
VMware NSX Intelligence for Networks or VMware Aria Operations™	✓ (may choose Option B to fulfill this prerequisite)		✓ (may choose Option B to fulfill this prerequisite)		
VMware NSX application platform (NAPP) must be deployed					✓
VMware vSphere must be deployed (V 6.7)					
Included in each option					
VMware NSX® security deployment	✓				
Micro-segmentation	✓				
NAPP deployment		✓			

VMware NSX Intelligence		✓			
VMware NSX Distributed IDS/IPS				✓	
VMware NSX® NDR™					✓
Network traffic analysis					✓
Malware prevention					✓
Protocol Hardening			✓		

Project scope

Option A – Adopt Micro-segmentation with VMware NSX® Distributed Firewall™ and VMware NSX® security deployment

Implementation of VMware NSX to support networking and security use cases.

VMware NSX® security deployment

This option is ideal for organizations who do not have VMware NSX deployed and want to adopt micro-segmentation.

Specification	Parameters	Description
VMware NSX® security deployment		
Data center location	Up to one (1)	Data center deployment of VMware NSX components
VMware NSX Manager cluster(s)	Up to one (1)	Deployment of Management cluster of three (3) VMware NSX Managers (if required) providing high availability of the user interface, API services, and central control plane function
Configure Compute Manager (vCenter) Prepare vCenter cluster (ESXi hosts)	Up to one (1) vCenter Cluster	Hypervisor hosts (ESXi) with NSX modules installed, registered to the NSX management plane and configured as transport nodes.

Logging and monitoring		Direct logging output to a pre-installed end customer-designated syslog target such as VMware Aria Operations for Logs
Role-Based Access Control		Integration of NSX-T to VMware Identity Manager and role-based access control (RBAC)
NSX Segments	Up to four (4)	Data center deployment of VMware NSX components
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop for the NSX Deployment

Adopt micro-segmentation with VMware NSX® Distributed Firewall™

Rapidly adopt micro-segmentation to protect applications using VMware NSX Distributed Firewall.

Specification	Parameters	Description
Adopt micro-segmentation with VMware NSX Distributed Firewall		
Number of infrastructure service policies	Up to five (5)	Security rules that contain mutually agreed upon widely used core and foundation services (e.g. NTP, Active Directory, DNS, etc.)
Number of environment level policies	Up to one (1)	Security policy that segments between broadly defined object groups (e.g. tenants, business units, environments)
Application(s) to be secured	Up to three (3)	Target applications identified for micro segmentation, with each application comprised of twenty (20) or less virtual machines
VMware NSX® Manager™ cluster	Up to one (1)	Target application virtual machines exist within a single VMware NSX Manager cluster
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop on micro-segmentation

Out of scope – Micro-segmentation with VMware NSX Distributed Firewall

- VMware NSX design and deployment

- VMware NSX application platform and VMware NSX Intelligence deployment
- VMware NSX® Gateway Firewall™ security (north/south)
- VMware NSX Advanced Threat Prevention deployment
- Application profiling design
- Protocol Hardening

Option B – Network traffic visibility with VMware NSX Intelligence

Deploy VMware NSX Intelligence to allow visualization of application and network security policies.

Specification	Parameters	Description
Network traffic visibility with VMware NSX Intelligence		
Data center location(s)	Up to one (1)	Data center deployment of VMware NSX-T™ components
VMware NSX Manager cluster(s)	Up to one (1)	Management cluster of three (3) VMware NSX Managers providing high availability of the user interface, API services, and central control plane function within scope
VMware NSX application platform deployment (NAPP)	Up to one (1)	Prescriptive NAPP architecture deployment with NAPP automation tool appliance with VMware vSphere® with VMware Tanzu® and VMware NSX integration
VMware NSX Intelligence	Up to one (1)	Enabled VMware NSX Intelligence instance
VMware NSX metrics	Up to one (1)	Enabled VMware NSX metrics
Security service policies	Up to five (5)	Number of security service policies.
Application(s) to be secured	Up to three (3)	Number of applications identified for micro-segmentation, with each application comprised of twenty (20) or less virtual machines
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop on NSX Intelligence

Out of scope – Network traffic visibility with VMware NSX Intelligence

- VMware NSX design and deployment
- Micro-segmentation
- VMware NSX® Gateway Firewall™ security (north/south)
- VMware NSX Advanced Threat Prevention deployment
- VMware NSX application platform custom design
- Non-VMware vSphere with VMware Tanzu® environment

Option C – Protocols hardening with VMware NSX Distributed Firewall

Rapidly secure virtualized environment using VMware NSX Distributed Firewall to limit lateral movement to spread malware and ransomware. (This option can be used twice if customer only pick this option)

Specification	Parameters	Description
Protocols hardening with VMware NSX Distributed Firewall		
VMware NSX® Manager™ cluster	Up to one (1)	Target environment within a single VMware NSX Manager cluster
Assessment: Assess VMware NSX environment security based on protocols	Up to six (6) workshops	Assess and review protocol hardening requirements and required policies in the VMware NSX Manager
Execution: Protocol Hardening implementation	Up to three (3) protocols	Create distributed firewall rules to whitelist protocols for NSX, and explicitly block up to six protocols (e.g. RDP, Telnet, FTP, TFTP, SFTP, SSH, DNS, SMB, SNMP, SMTP, POP3, IMAP, HTTP or HTTPS). Publish and Apply Firewall Rules
Validation: (Monitoring)	Up to thirty (30) h	Validation of implemented solution. Test the protocol blocking rules by attempting to initiate the blocked protocols from the specified source VMs. Verify that the traffic is indeed blocked as expected.
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop on protocols hardening.

Out of scope – Protocols hardening with VMware NSX Distributed Firewall

- VMware NSX design and deployment
- VMware NSX application platform and VMware NSX Intelligence deployment
- VMware NSX® Gateway Firewall™ security (north/south)
- VMware NSX Advanced Threat Prevention deployment
- Application profiling design
- Application Micro-segmentation
- This service option cannot exceed 150 hours.

Option D – Threat prevention with VMware NSX Distributed IDS/IPS

Rapidly activate, tune, and optimize VMware NSX Distributed IDS/IPS to secure applications.

Specification	Parameters	Description
Threat prevention with VMware NSX Distributed IDS/IPS		
Data Center Location(s)	Up to one (1)	Data center deployment of VMware NSX component(s).
VMware NSX Manager cluster(s)	Up to one (1)	Management cluster of three (3) VMware NSX Managers providing high availability of the user interface, API services, and central control plane function
VMware vSphere® cluster(s)	Up to two (1)	Number of VMware vSphere cluster(s) with IDS/IPS enabled
Application(s) to be analyzed and secured	Up to five (5)	Number of target application(s) to be secured with VMware NSX Distributed IDS/IPS, with each application comprised of twenty (20) or less virtual machines
VMware NSX Distributed IDS/IPS profiles	Up to five (5)	Number of VMware NSX Distributed IDS/IPS profile(s) to be configured and tuned
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop on VMware NSX Distributed IDS/IPS

Out of scope – Threat prevention with VMWare NSX Distributed IDS/IPS

- VMware NSX design and deployment
- Micro-segmentation
- VMware NSX Advanced Threat Prevention deployment

Option E –Implementation of VMware NSX Advanced Threat Prevention

Implementation of VMware NSX® NDR™, traffic analysis, and malware prevention.

Specification	Parameters	Description
Implementation of VMware NSX Advanced Threat Prevention		
Data center location	Up to one (1)	Data center deployment of VMware NSX components
VMware NSX Manager cluster(s)	Up to one (1)	Management cluster of three (3) VMware NSX Managers providing high availability of the user interface, API services, and central control plane function
Enablement of VMware NSX NDR, traffic analysis, and malware prevention		Implementation and enablement of VMware NSX NDR, traffic analysis, and malware prevention
Data consumption workshop		
Knowledge transfer	Up to one (1)	Conduct knowledge transfer workshop on VMware NSX NDR, traffic analysis, and malware prevention

Out of scope – VMware NSX Advanced Threat Prevention

- VMware NSX design and deployment
- Micro-segmentation
- VMware NSX Distributed IDS/IPS deployment
- VMware NSX application platform deployment
- VMware NSX Intelligence deployment
- Gateway deployments for VMware NSX Advanced Threat Prevention features

Project activities

Activities for this engagement are organized in phases as shown below.

Description	Deliverable	Primary Owner
Phase 1: Initiate		
Pre-engagement call	Kick-off agenda	VMware
Create kickoff presentation	Kick-off deck	VMware
Phase 2: Plan		
Kickoff meeting	Kickoff presentation	Joint
Basic design and solution overview workshop	Solution overview presentation Solution checklist	VMware
Phase 3: Execute		
Solution implementation	Solution specification workbook	Joint
Solution verification	Solution verification workbook	VMware
Knowledge transfer	Knowledge transfer workshop	VMware
Phase 4: Close		
Closure meeting	Engagement summary presentation	VMware

Responsibilities

All VMware and Customer responsibilities are listed in the Project Activities section. The ownership is defined as follows.

VMware: VMware is responsible for the delivery of the component, with minimal assistance from the Customer's project team.

Joint: VMware and Customer's Project Team: Both are jointly responsible for the delivery of the component.

Customer: Customer is responsible for the delivery of the component, with recommendations from VMware as needed.

Estimated schedule

This service is delivered in three to four weeks within the project scope as defined in this document.

- Total delivery time: three to four weeks
- Meetings per week: three to five
- Duration of meetings: two to four hours each

This target schedule may vary depending on availability of assigned VMware consultant. The tasks defined each week may shift based on customer readiness and availability of both the customer and VMware personnel. VMware will perform the service according to a schedule agreed to by both parties.

Service assumptions

1. Desired Add-On services must be confirmed in writing by Customer before services will begin.
2. VMware will deliver the remote services in English using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the consultant(s).
3. Procurement and installation of hardware for any components that will be installed on-premises is the responsibility of the Customer. VMware may provide recommendations.
4. Configuration of software other than VMware technology is the responsibility of the Customer.
5. Prerequisites must be completed for all installation components before any installation activities will be performed.
6. VMware and the Customer will work closely together to ensure that project scope remains consistent and issues are resolved in a timely manner. The deployments team will not provide a project manager for this service.
7. All work will only be delivered remotely via screen-share.
8. All work, documentation, and deliverables will be conducted during VMware local business hours and will be provided in English.
9. The staffing for this service assumes all work will be completed within a maximum of twelve (12) weeks after the initiation. Should the duration of the engagement be extended, or should the product scope materially change, a project change request may be issued.

Out of scope

General

- No application profiling design.
- Any feature not listed in Services Deliverables is out of scope, unless discusses and agreed to with the Product Deployment Team prior to purchase.
- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines.
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control.
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer.
- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Installation and configuration of Customer-signed certificates.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.
- Customer solution training other than the defined knowledge transfer Deploy Kubernetes session.

Service checklist

The participation of the following Customer stakeholders is required for this service to be performed.

- Network architecture team lead
- Network operations team lead
- Infrastructure architect
- Security policy team lead
- Firewall/DMZ team lead

Learn more

Visit vmware.com/services.

- VMware operations team lead
- Enterprise architect
- Security manager
- Application operations lead
- Service owner
- Infrastructure manager
- IT operations manager
- Chief Technology Officer

Terms and conditions

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware General Terms and Professional Services Exhibit on the VMware ONE Contract Center. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.