Professional Services for Design and Implementation of VMware NSX Advanced Threat Prevention

Detect and block malicious activity

At a glance

Leverage our expertise in NSX and network security to help network security and SOC teams efficiently use NSX ATP to detect malicious activity and block lateral movement of sophisticated threats.

Key benefits

- Accelerate adoption and security design leveraging best practices for VMware NSX ATP use cases
- Increase SOC efficiency to quickly triage threat activity with combined related alerts to prioritize response
- Protect assets against agile adversaries, including north-south and east-west traffic protection
- Enable a network sandbox secure isolation environment to detect new, evolving threats and targeted malware

VMware NSX Advanced Threat Prevention (ATP), available in NSX-T 3.2 or higher, helps security operations teams rapidly detect malicious activity and stop lateral movement of threats inside your network. Advanced threat prevention is no longer an optional feature of SOC teams and should be deployed and configured as quickly as possible. Many IT organizations know they need to implement ATP, but do not have the time, skill, or expertise to get it installed and deployed.

Service overview

VMware Professional Services can establish the foundation and activities for Advanced Threat Prevention to help SOC teams get ATP up and running quickly and efficiently. With this service, IT departments can start efficiently detecting malicious activity and block lateral movement of sophisticated threats.

VMware Team will establish foundational tasks and activities to provide customers with a repeatable methodology for securing applications within the virtual infrastructure. Service includes:

- Give in-depth overview of the VMware security platform
- Review current infrastructure
- Gather and analyze customer security requirements
- Create functional requiremens and use case
- Design workshop
- Create architecture design for VMware NSX Application Platform (NAPP), VMware NSX Intelligence, VMware NSX Network Detection & Response, and VMware NSX Malware Prevention
- Deploy Tanzu Basic Kubernetes Cluster (applicable only for customers who don't have Kubernetes cluster to deploy NSX Application Platform)
- Deploy VMware NSX Intelligence, VMware NSX Network Detection & Response, and Malware Prevention

- Verify events and threat discovery capabilities
- Knowledge transfer workshop

Service Scope

Design NSX Advanced Threat Prevention

The scope of this service is defined on the table below and aprameters values must be agreed upon and validated between the customer and VMware sales representative.

Specification	Parameters	Description
NSX ATP Solution	Min: 1, Max: 99	Number of sites/environments in the overall ATP solution to be designed
NSX Application Platform and NSX Intelligence	Min: 1, Max: 99	Number of instances designed with NSX Intelligence
NSX Malware Prevention	Min: 1, Max: 99	Number of instances designed with NSX Malware Prevention
NSX Network Detection & Response	Min: 1, Max: 99	Number of instances designed with NSX Network Detection & Response

Deploy NSX Advanced Threat Prevention

Specification	Parameters	Description
Tanzu Basic	Min: 1, Max: 99	Number of sites Tanzu Basic is deployed for the NSX Application Platform
NSX Intelligence	Min: 1, Max: 99	Number of sites NSX Intelligence is deployed
NSX Malware Prevention	Min: 1, Max: 99	Number of sites NSX Malware Prevention is deployed
NSX Network Detection & Response	Min: 1, Max: 99	Number of sites NSX Network Detection & Response is deployed

Learn more

Visit vmware.com/services.

Prerequisites

The following prerequisites are required to enable VMware to perform this service:

- Required licensing level – Defined minimum: NSX Application Platform requires at minimum NSX Data Center Enterprise Plus license. Tanzu Basic requires a Tanzu Basic license.
- VMware NSX-T management plane and control plane deployed and configured with VMware recommended practices. Defined minimum: must be running on NSX-T version 3.2 for Advanced Threat Prevention features.

Exclusions

This service does NOT include IDS/IPS. IDS/IPS can be implemented with the service “Get started with VMware NSX Intrusion Detection and Prevention Systems.” Please see your sales representative for support.

Benefits

VMware Professional Services has the experience, best practices, and proven methodologies to help you get ATP up and running quickly. Our broad expertise and deep knowledge of VMware technology and security best practices can help reduce complexity. From creatign policies to integrating with your current network, we can help you quickly deploy the protection needed with minimal disruption to existing resources and operations.