Professional Services for Getting Started with NSX Advanced Threat Protection

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

- Get NSX ATP up and running faster
- Minimize disruption to existing resources and operations
- Free IT staff to work on business-critical activities
- Enable network SOC teams to quickly triage advanced threats
- Provide granular application security and isolation
- Operational savings with auto-detect and policy application
- Facilitate rapid security policy definition and application

VMware NSX Advanced Threat Protection (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 protection 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 Protection 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 customer with a repeatable methodology for securing applications within the virtual infrastructure. Service includes:

- Give in-depth overview of the VMware security platform
- Gather and analyze customer security requirements
- Activate VMware NSX Intelligence. VMware NSX Network Detection & Response, Malware Prevention, Threat Discovery, and Metrics
- Complete Knowledge transfer and creation delivery

To perform this service our team will set up multiple target applications to be identified across a sample of virtual machines. During this process we will teach your team how to setup criteria for other target applications and show them how to scale the protection out across the entire network.

After deployment, our team will help create operational procedures to be sure NSX ATP is fully integrated into your company's daily operations and becomes part of your companies DNA. We also do a complete knowledge transfer to be sure your team understand all elements of what was done and can repeat the procedures as necessary going forward.

Learn more

Visit vmware.com/services.

Service Scope

The Scope of the Service is strictly defined on the table below:

Specification	Parameters	Description
NSX-T Manager Cluster(s)	Up to one (1)	Number of NSX-T Manager clusters in-scope.
Applications enabled for NSX Network Traffic Analysis, Network Detection and Response and Metrics	Up to three (3)	Number of target applications identified for NSX NTA, NSX NDR and NSX Metrics comprised of ten (10) or less virtual machines.
NSX Malware Prevention	Up to one (1)	NSX Malware Prevention enabled on mentioned applications in-scope.

Prerequisites

This service contains the following technology prerequisites:

- 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.
- Required licensing level. Defined minimum: NSX Application Platform requires at least NSX Data Center Enterprise Plus license.

This service contains the following stakeholder prerequisites:

- Security technology team leads
- Firewall/DMZ team leads
- Enterprise Architect
- VMware operations team leads

This service contains the following free form prerequisites:

- NSX Application Platform requires either a Tanzu Kubernetes cluster or upstream Kubernetes cluster for deployment.

Exclusions

This service does NOT include IDS/IPS. IDS/IPS can be implemented with our service called “Get started with 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 creating policies to integrating with your current network, we can help you quickly deploy the protection needed with minimal disruption to existing resources and operations.

vmware®

Copyright ©2022 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001
VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents. 03/22