Ransomware Protection

An imperative for virtualization engineers

Ransomware is an epidemic companies can't ignore. Malware attacks are becoming more pervasive and sophisticated, while ransomware as a service now targets governments and companies of every size. And the threat is growing: Globally, ransomware cost $20 billion in 2021 and is projected to cost $265 billion by 2031, according to Cybersecurity Ventures.[1]

The push for innovation has resulted in unprecedented software development. While this development has been beneficial to countless companies, it has also left those companies vulnerable to exploitation by attackers who use software to gain access to their networks, where the majority of their application workloads are deployed. As a result, IT operational security is now a standard part of a virtualization engineer's daily life. To thwart ransomware, companies must evolve malware defenses to ensure their networks are resilient against these types of threats.

By combining VMware NSX® Distributed Firewall™ and VMware vSphere®, virtualization engineers can add another layer of ransomware protection to secure vSphere workloads and gain a comprehensive view across compute, networking and security—all from within VMware vCenter®.

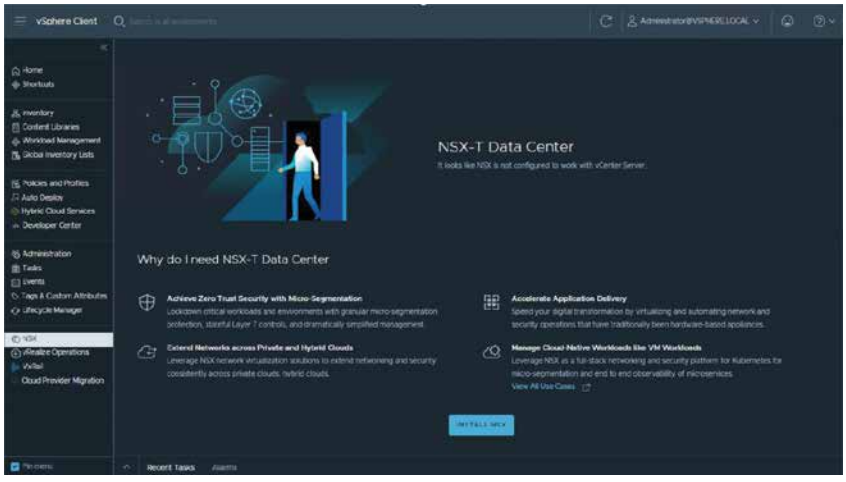

Figure 1: The NSX-T dashboard in the vSphere Client.

1. Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031." David Braue. June 3, 2021.

Top reasons to add NSX Distributed Firewall to vSphere

Built-in security

Prevent malware for distributed firewalls
NSX Distributed Firewall now has zero-day malware detection and prevention capabilities that employ advanced machine learning techniques and emulation sandboxing.

Detect and prevent advanced attacks
VMware NSX-T™ 3.2 with NSX Advanced Threat Prevention™ is uniquely positioned to detect and prevent today's sophisticated attacks by leveraging a behavioral intrusion detection and prevention system (IDPS), network traffic analysis, and full-system emulation sandboxing without agents, hairpinning or taps. With NSX Network Detection and Response™, we consolidate thousands of events from different detectors into campaigns that allow security analysts to focus on the intrusions that really matter.

Leverage a distributed firewall with vSphere networking constructs
Utilize distributed firewall capabilities for VLAN networks based on a vSphere Distributed Switch™ (VDS) without having to move virtual machines (VMs) to an NSX network. NSX Distributed Firewall supports VMs deployed on distributed port groups on a VDS.

View security metrics in an enhanced security dashboard
Get a single pane of glass view that includes identity firewall statistics for active users and active user sessions in NSX Manager™.

Implement micro-segmentation for Zero Trust
Enjoy auto-generated policy recommendations based on an intrinsic understanding of application topologies. Easily create, enforce and automatically manage granular micro-segmentation policies, and leverage an object-based policy model for automation.

Simplify operations

Simplify deployment and consumption of NSX security via vCenter
vSphere 7 Update 3 introduces a VMware vCenter Server® plug-in for NSX that makes it much easier for vSphere admins to set up and use NSX networking and security from within the vSphere Client™.

Simplify network segmentation
Configure firewall rules and security groups without the need for toggling back and forth between vCenter and NSX Manager.

Harness software-defined networking
Gain visibility into traffic, and easily create network segmentation or virtual security zones with no changes to your network by defining them entirely in software.

Drive collaboration and intelligence

Connect virtualization and network security teams with the integration of operations and management within the vCenter user interface. Virtualization engineers now have the security features they need within vSphere to counter the ransomware infiltrating the environments they are responsible for.

Network agility

Accelerate network provisioning

NSX Data Center reproduces the entire network model in software, so you can create and provision any network topology in seconds, and deliver critical apps and services faster and more easily.

Deploy new, advanced network services faster

Create virtual networks for your applications and define them entirely in software, with no network changes or traffic hairpinning.

Avoid CapEx

Forget purchasing additional hardware firewall appliances that entail expensive, vendor-specific management consoles and require upgrades and maintenance that are time-intensive. Avoid the space, heating and cooling costs of physical appliances.

Getting started

To use the vCenter Server plug-in for NSX and the deployment wizard in NSX-T, you will need both vSphere 7 Update 3 and VMware NSX-T 3.2.

Existing vSphere customers can download vSphere 7 Update 3.

Sign up for 60-day trial of NSX-T.