VMware NSX Intelligence

Built-in security policy management, analytics and compliance with data center–wide visibility

At a glance

VMware NSX® Intelligence™ is a distributed analytics engine that leverages granular workload and network context unique to NSX to deliver converged security policy management, analytics and compliance with data center–wide visibility.

Key highlights

- Data center–wide visibility – Visualize and gain deep insights into every flow across the entire data center with stateful layer 7 inspection and complete context of related workloads.
- Converged security operations – Reduce tool sprawl and improve collaboration between infrastructure and security teams by embedding multiple security operations consoles, firewall policy recommendation, and management within the NSX UI.
- Easy to operationalize – Radically simplify operations with single-click deployment of a lightweight virtual appliance. Eliminate the overhead of duplicating packets and large centralized appliances with analytics distributed and built into the hypervisor.

No need to trade off between insight and operational simplicity

Traditional security analytics products provide insight at the cost of operational complexity and overhead. They rely on agents or sensors deployed on each workload or on network taps to gather the necessary data for security and network analysis. They duplicate and transmit all this data to discrete, centralized appliances that each perform expensive packet analysis to reconstruct state and layer 7 context. This architectural model places a heavy burden on your network, is expensive, and results in large management overhead on operations teams.

Distributed analytics built natively within NSX

At its foundation, VMware NSX Intelligence is a distributed analytics engine built and managed natively within NSX. It empowers network and application security teams to deliver a more granular security posture, simplify compliance analysis, and enable proactive security.

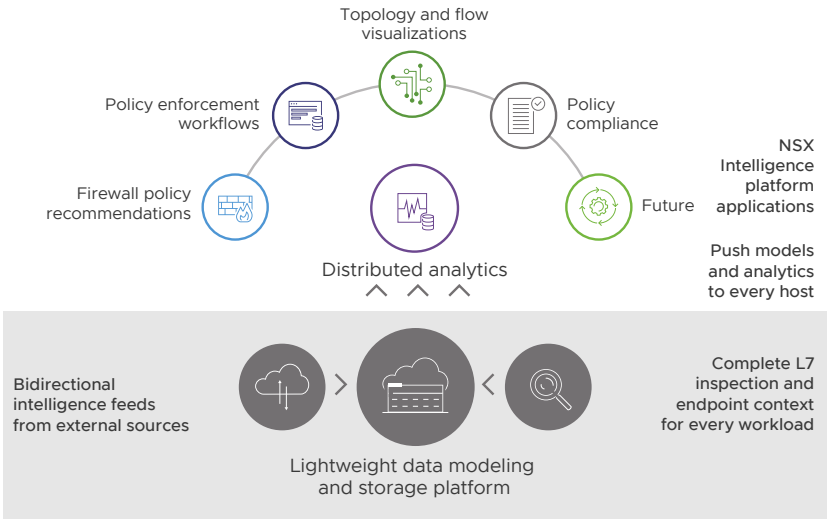


Figure 1: Built natively within NSX, NSX Intelligence provides distributed analytics that empower network and application security teams.

Use cases

- Automate micro-segmentation at scale – NSX Intelligence automatically recommends application groups and security policies, and updates application topology visualizations in real time to simplify implementation of micro-segmentation and firewall rules.
- Demonstrate and maintain policy compliance – A complete historical record of every flow in and out of every workload, detailed flow visualization, and an audit trail for security policies allow operators to compare policy against actual flows, and identify exceptions and non-compliant flows at every point in time.
- Simplify security incident troubleshooting – A complete inventory of workloads and continuous layer 7 analysis and visualization of every flow between workloads within a converged NSX console enable rapid troubleshooting of policy misconfigurations and security incidents.

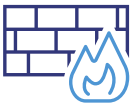
By distributing analysis processing to each hypervisor, NSX Intelligence eliminates the need for large, complex, centralized appliances required by most security analytics products. NSX Intelligence only sends relevant metadata to a lightweight central repository for building machine learning models and further analysis. It doesn't require any agents or network taps; NSX Intelligence processes packets in-line as they traverse within the hypervisor. This single-pass approach enables computationally efficient processing of multiple analytics functions.

Multiple analytics applications can be built on this foundational platform, spanning intelligent policy formulation, security analytics, and network analytics. The first set of applications available centers around intelligent policy formulation, including application dependency mapping and hierarchical topology visualization; detailed workload inventory and continuous flow monitoring; firewall policy recommendations and repository; and policy compliance.

Key capabilities

Contextual application topology maps
NSX Intelligence inventories all endpoints and traffic flows, and consolidates metadata and configuration data from NSX, VMware vSphere® and more to provide complete workload context. Workloads get automatically clustered into granular groups in a hierarchical application map that scales to tens of thousands of endpoints and enables drilling down from high-level applications to a detailed context of each workload.

Micro-segmentation and firewall policy recommendation
NSX Intelligence automatically generates rules to micro-segment applications and, with the click of a button, provisions them in the NSX Distributed Firewall™. Topology visualization gets updated based on recommended rules to enable iterative micro-segmentation planning with a seamless user experience. It is the primary security policy repository.



Stateful layer 7 processing
Leveraging the NSX Distributed Firewall, the engine processes every packet with a complete understanding of state and layer 7 context, including protocol analysis and application ID.

Comprehensive packet inspection
NSX Intelligence continually monitors every packet between every workload in the environment, without any sampling, to enable visualization of every flow with complete workload context for rapid security troubleshooting and analysis.

Efficient and distributed in-line processing
Packet processing and workload analysis are distributed to each hypervisor. The processing is done in-line with NSX Distributed Firewall within the hypervisor, making it highly efficient with minimal overhead.

Learn more

For more information about VMware NSX Intelligence, reach out to your VMware sales representative or check out the following resources:

- Learn about security with *VMware NSX*.
- Read about the *NSX Distributed Firewall*.
- Visit the *VMware NSX product page*.

VMware NSX Intelligence and VMware vRealize Network Insight

VMware NSX Intelligence and VMware vRealize® Network Insight™ together deliver a comprehensive security and network operations lifecycle. NSX Intelligence serves the network and application security teams with deep visibility, analytics and visualizations. vRealize Network Insight is rapidly expanding its breadth beyond NSX to provide end-to-end operations visibility and troubleshooting. This includes virtual and public cloud workloads, physical underlays, and SD-WAN in heterogeneous on-premises and hybrid cloud environments, including third-party network and firewall devices.

vRealize Network Insight integrates bidirectionally with NSX Intelligence to enhance micro-segmentation planning. vRealize Network Insight integrates with a rich set of sources of application metadata, including configuration management databases, virtual machine names, VMware vCenter® tags, physical servers, and network constructs from NSX. Its mature application modeling workflows reconcile this metadata with flow data to discover application boundaries and groups, and act as a key input to NSX Intelligence, which houses the policy repository and enforcement workflow.

Item No: 1356650aq-so-nsx-intlgnc-a4 3/22