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

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.

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 virtual appliance. 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 center 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 intogranular 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**
Built on the NSX distributed firewall engine, NSX Intelligence 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 the distributed firewall within the hypervisor, making it highly efficient with minimal overhead.

**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 delivers deep NSX visibility, analytics and visualizations to the network and application security teams. vRealize Network Insight, rapidly expanding its breadth beyond NSX, provides end-to-end visibility and troubleshooting for 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 and NSX Intelligence tightly integrate bidirectionally for 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 as well as layer 7 context from NSX. Mature application modeling workflows reconcile this metadata with flow data to discover application boundaries and groups, and acts as a key input to NSX Intelligence that houses the policy repository and enforcement workflow.