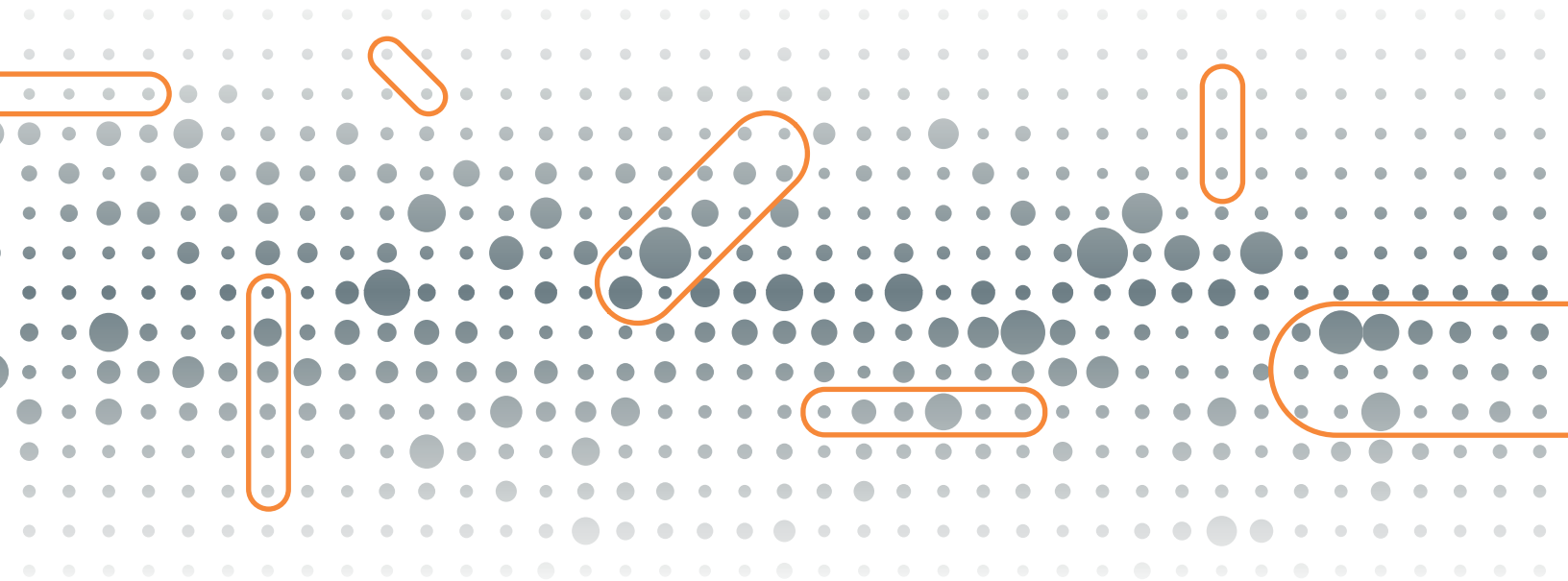




# VMware NSX vs. Illumio ASP: Comparison Guide



## About This Guide

This comparison guide outlines how VMware NSX and the Illumio Adaptive Security Platform® (ASP) solve the following security challenges:

- How do I maintain security, visibility, and micro-segmentation across environments that include bare metal servers and hypervisors from multiple vendors?
- How can I implement and maintain uniform security across private data centers and cloud environments?
- How can I create the right segmentation strategy and policies if I don't fully understand application flows and workload relationships?
- What can I do to improve efficiency and reduce/prevent errors when defining and enforcing policy?

## The Need for Micro-Segmentation

While perimeter security remains an important component of controlling inbound and outbound traffic for data center environments, it provides no real control over the lateral movement on which hacks are often predicated. As the ability to control the spread of lateral attacks (i.e., east / west movement) has increasingly become a requirement for IT teams, they have looked to micro-segmentation solutions to provide the controls needed to protect workloads and data.

Micro-segmentation offers the ability to simplify the security processes that are currently in place. Perimeter security and traditional network segmentation approaches such as VLANs, subnets, and ACLs have all proven to be cumbersome and time consuming to configure, deploy, and manage. In particular, micro-segmentation greatly reduces the number of rules managed manually by networking technologies. Organizations today demand agility that cannot be met with traditional security methods.

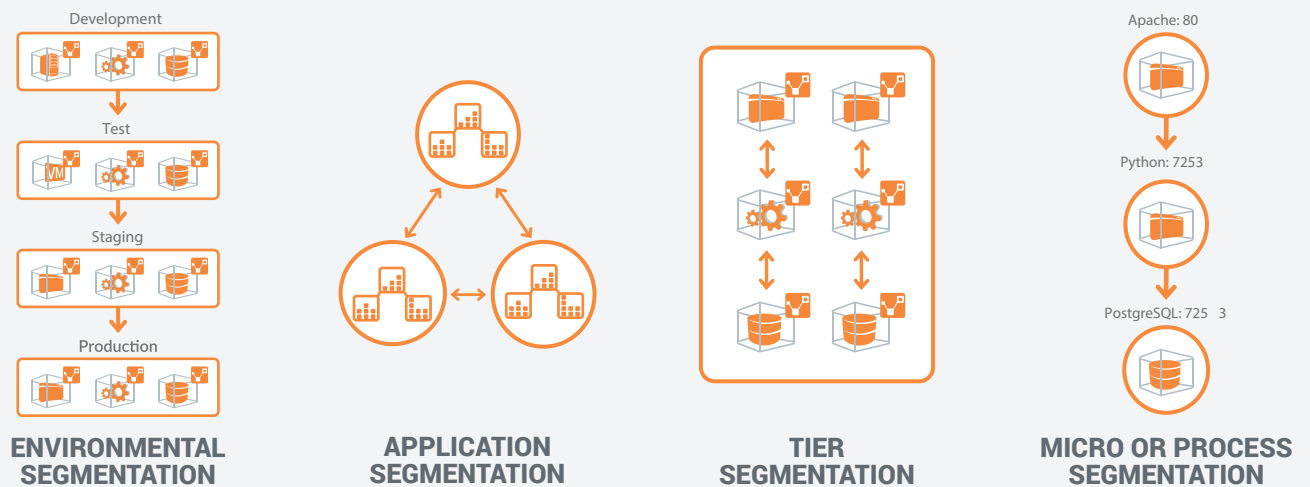
Heterogeneity and the increasingly dynamic nature of data center environments have also contributed to interest in micro-segmentation solutions. With the advent of virtualization and containers, organizations are taking advantage of dynamic application infrastructure that has the ability to move and scale applications on demand. As an increasing number of customers take advantage of the cloud, they are looking to move workloads to a hosted environment—or even to split application tiers between locations in a hybrid cloud model. Traditional security can slow down or stand in the way of realizing the true benefits of these solutions.

## The Evolution of Micro-Segmentation: Adaptive Micro-Segmentation from Illumio

How is Illumio ASP unique?

- It delivers live visibility of application dependencies, a model for IT-friendly security policies, and micro-segmentation that automatically adapts to application and workload changes—keeping security policies intact.
- It is hypervisor and operating system agnostic, and works uniformly on bare metal, virtual, or containerized infrastructure across multiple applications, environments, or locations in and across private data centers or cloud environments.
- It operates with simple, natural-language policies and offers the ability to automatically generate optimized policies and model policies before enforcing them to reduce errors and minimize disruption of application services.
- Its policies can extend across multiple applications, environments, and locations for uniform security anywhere, on anything—all applied without infrastructure or application changes.

The Illumio solution enables a wide range of segmentation granularity, including environmental, application, server-to-server, process-to-process, and user-to-application segmentation.



## Addressing Pain Points with Micro-Segmentation

Customers face a range of challenges when segmenting and securing application environments. The diversity of platforms, distributed infrastructure, lack of visibility, and complexity of policy creation can all impact the effectiveness of a solution. Not all micro-segmentation solutions are equal, and some are better equipped to address the unique and varied challenges of customers and their environments.

### Pain Point #1: Micro-Segmentation for Heterogeneous Environments

**Question:** How do I maintain security, visibility, and micro-segmentation across environments that include bare-metal servers and hypervisors from multiple vendors?









It's common to find a mix of non-virtualized (bare metal) and virtualized servers within data center environments. And, many virtualized environments include two or more hypervisors (e.g., KVM, HyperV, Xen, ESXi, Acropolis). This type of heterogeneity can make visibility and security across the application environment require coordination that increases



complexity and is likely to introduce new security vulnerabilities. A single solution to secure the entire environment—regardless of the state of virtualization or variety of hypervisors—is key to ensuring efficiency, consistency, and protection.

**VMware NSX** has limited support for bare-metal servers and 3rd party hypervisors. NSX-T can work with ESXi and KVM hypervisors but can only run many of the mapping and policy generation features on ESXi. NSX-T can support Linux on bare-metal servers but not Windows. For customers with a mix of environments, NSX can limit the ability to micro-segment the environment in a consistent way.

**Illumio ASP** has native support for diverse application environments. Since the Illumio Virtual Enforcement Node (VEN) is installed at the operating system layer, it can protect workloads running on bare metal or any variety of hypervisor. With an approach that is not dependent upon the underlying infrastructure, Illumio can improve visibility and enforce security policy for consistent protection across any infrastructure. This results in reduced complexity and potential for errors while increasing overall efficiency and security.

| Capabilities   | VMware NSX  | Illumio ASP   |
|--|---|---|
| Micro-segmentation for workloads on native bare-metal                                      | <br>works with NSX-T |  |
| Micro-segmentation for workloads on VMware hypervisors                                     |                      |  |
| Micro-segmentation works across ALL third-party hypervisors (e.g., ESX, Hyper-V, KVM, Xen) |                      |  |
| Uses native OS enforcement   |                      |  |



## Pain Point #2: Taking Micro-Segmentation to Public and Hybrid Cloud

### Question: How can I implement and maintain uniform security across private data centers and cloud environments?

Companies are increasingly moving to public cloud services like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. In many cases, this move is an evolution, with applications and infrastructure split between on-premises and cloud environments in a hybrid deployment. Some deployments even split application tiers between infrastructure to take advantage of cost or the flexibility to quickly scale application capacity.

Deploying and managing security in split or hybrid cloud environments can be extremely complex.

**VMware NSX-T** has two modes of enforcement for AWS and Azure environments. The first installs NSX Tools on the server, which configures the native security services. The second, used for unmanageable services, uses a gateway to drive native cloud security calls. Neither of these modes works with the native application mapping and policy generation in NSX Intelligence. This means that any micro-segmentation has to be managed separately and manually.

The **Illumio ASP** VEN is installed at the operating system and secures workloads consistently across all cloud environments, regardless of the environment or location—with no dependencies on the underlying infrastructure. In addition, with Illumio, security policies are automatically recalculated and applied when workloads move locations. Support for cloud environments has been an inherent capability of Illumio ASP since day one.

| Capabilities  | VMware NSX | Illumio ASP |
|---|------------|-------------|
| Single unified micro-segmentation solution works across ALL data centers and clouds | ⊗          | ✓           |
| Infrastructure agnostic   | ⊗          | ✓           |
| Security policies move with workloads between data centers in minutes               | ✓          | ✓           |



## Pain Point #3: Lack of Comprehensive Visibility

### Question: How can I create the right segmentation strategy and policies if I don't fully understand application flows and workload relationships?

Visualization is a critical first step toward understanding the application environment, creating a micro-segmentation strategy, and implementing effective policies. Proper visualization provides an application-centric view across locations with real-time details on workload dependencies and traffic flows. Integration of visualization with policy workflow makes the process of modeling, validating, and troubleshooting policy more efficient. In addition, visualization can help to identify and quickly resolve potentially risky workloads operating outside of defined policy.

The Enterprise Plus version of NSX-T includes NSX Intelligence which uses data from ESXi hypervisors and the virtual switches to build a database of information on the network. Using this information it can build a map based on VMs or NSX-T groups. It can also use the data to build a set of recommended rules for the distributed firewall. While this is useful in some limited environments it is limited to 100 workloads on ESXi hosts.

**Illumio ASP** has built-in visualization, called Illumination, to provide visibility of applications running across all data centers, clouds, hypervisor, or bare-metal servers. With Illumination, customers gain a better understanding of application relationships, workload dependencies, and flows. As a tightly integrated component, Illumination is a critical tool in policy modeling, creation, and validation, as well as the identification of potential policy violations.

| Capabilities                                | VMware NSX | Illumio ASP |
|---|------------|-------------|
| Visibility included with solution           | ⊗          | ✓           |
| Visibility integrated with policy workflows | ⊗          | ✓           |



## Pain Point #4: Improving Efficiency and Minimizing Policy Errors

### Question: What can I do to improve efficiency and reduce/prevent errors when defining and enforcing policy?

Defining security policies can be a complex process that often results in delays in application deployment or unforeseen impact to application functionality and availability. Arriving at the right policy can require coordination across multiple groups, including application, security, networking, and operations teams. It's important to have tools to aid cross-team discussions as well as tools to help model, test, and validate policy.

The Distributed Firewall is like configuring a huge firewall with all of the rule management issues of standard firewalls. While NSX Intelligence can generate some recommended rules they still need to be incorporated into the overall rule flow in the correct location. Rules are applied to NSX-T Groups which can be created using a wide variety of TAGs and properties which can create a challenge around consistency and ease of management.

**Illumio ASP** delivers a model for IT-friendly security based on natural-language policy that all teams can understand—the same declarative policy language that an application team might use to describe the way the application should work. Policy is implemented without dependency on order, and can be modeled and tested before it is enforced to ensure effectiveness. Policy behavior can be verified visually through the Illumination view of the application environment, creating a tight loop across visibility, policy creation, and policy enforcement.

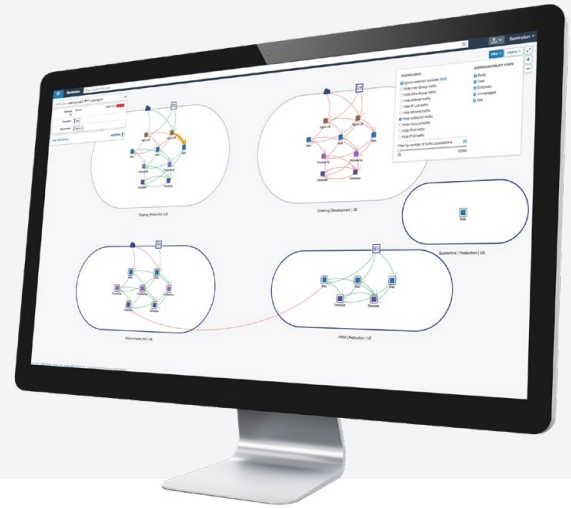
| Capabilities   | VMware NSX | Illumio ASP |
|--|------------|-------------|
| Leverages pre-configured policy templates for Microsoft Active Directory and other core services | ⊗          | ✓           |
| Auto-generates optimal micro-segmentation policies   | ✓          | ✓           |
| Model/test security policies before enforcement  | ⊗          | ✓           |



## TAKE A “TEST DRIVE”: ILLUMIO FREE TRIAL

- Visibility into live application traffic across data center and cloud environments to help assess risk and plan security policies.
- Tools to model and create the right security policies without impacting application performance, functionality, or availability.
- Adaptive micro-segmentation anywhere on anything without dependencies on the network, virtualization platform, or cloud.

Go to [illumio.com/free-trial](https://illumio.com/free-trial)



## Contact Illumio

[www.illumio.com](https://www.illumio.com)

**+1-669-800-5000**



## About Illumio

### Follow Us



Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data center or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit [www.illumio.com](http://www.illumio.com).

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 [www.illumio.com](http://www.illumio.com)

Copyright © 2018 Illumio, Inc. All rights reserved. This document is protected by U.S. and international copyright and intellectual property laws. Illumio's products and services are protected by one or more U.S. and international patents listed at <https://www.illumio.com/patents>. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. To review a list of Illumio's trademarks, go to <https://www.illumio.com/trademarks>. Third-party trademarks mentioned in this document are the property of their respective owners.