ZERO.
Networks

The #1 VMware NSX Alternative

Zero Networks delivers an all-in-one platform that simplifies network security through automated, agentless network segmentation and advanced identity protection solutions. Unlike VMware NSX, which is limited to protecting virtual machines (VMs), Zero Networks extends its protection to the entire virtualization stack, including hosts and the virtualization manager. This comprehensive coverage addresses a critical gap in virtualization security, as highlighted by incidents like the ESXi hack, where hackers exploited vulnerabilities to compromise multiple VMs.

Key Differentiators: Zero Networks vs. VMware NSX

Broad Coverage Beyond VMs

VMware NSX is limited to securing VMs, leaving the host and the virtualization manager vulnerable to attacks. Zero Networks, on the other hand, offers protection across the entire virtualization environment. By safeguarding the host, the virtualization manager, and all VMs, Zero Networks mitigates the risk of host-level compromises, which can have devastating effects on the entire virtualization infrastructure.

	Host Protection	Virtualization Management Protection	Virtual Machine Protection
VMware NSX	NO	NO	YES
Zero Networks	YES	YES	YES

Simplified Implementation

Implementing Zero Networks is straightforward and efficient. Our platform can be fully operational within 30 days, providing quick turnaround times and minimal disruption to business operations. This ease of implementation contrasts sharply with VMware NSX, which often requires complex, time-consuming deployment processes that can take multiple years.

Zero Networks monitors and learns all network connections over a period of up to 30 days, and then creates corresponding and highly accurate firewall rules. The rules and policies are then centrally applied to the host firewalls of all assets in the network. The policies allow only legitimate traffic and apply just-in-time MFA to privileged remote admin protocols like RDP, SSH or WinRM that are also used by attackers to move laterally.

Segmentation with Zero is this simple:

DAY 1 → **DAY 30**

DEPLOYING

A segment server (stateless VM not in line with traffic) starts monitoring

LEARNING

Zero Networks learns and creates rules for each asset and identity

SEGMENTING

Policies are centrally applied on all hosts only allowing necessary traffic/logons

- Fully automated
- Agentless
- MFA-powered

Cost-Effective and Transparent Pricing

Zero Networks prides itself on a transparent pricing model that avoids unnecessary bundling of features. Customers pay only for the services they need, which stands in stark contrast to Broadcom's strategy with VMware NSX, where bundling and inflated prices are the norm. Our approach not only reduces costs but also ensures that businesses are not forced to invest in features that do not align with their specific requirements.

Flexibility and Scalability

Zero Networks is designed to work across diverse environments, supporting any client, server, VM, and cloud workload. This flexibility is particularly beneficial for large enterprises with complex infrastructures, which may find VMware NSX's manual and complicated management challenging and restrictive. Zero Networks was built in the cloud and can scale across any number of hosts in the existing environment.

ZERO. Networks

To learn more about how Zero Networks can transform your virtualization security, please visit zeronetworks.com/nsx. Join the growing number of enterprises that have made the switch to Zero Networks and experience the difference for yourself.

Learn more