DEFENCE IN FORMATION

SECURING HYBRID AND MULTI-CLOUD ECOSYSTEMS

Benefits of the Integration

- Enterprise cloud offering with next-generation security controls
- Preventive security controls to stopthreats before they cause damage
- Consistent management of on-premises, private cloud, and public cloud security postures
- Automated, one-click deployment via the Nutanix Prism management console

The Challenge

Mobility and the cloud are transforming modern enterprises by providing employees and customers with greater access to data and services anywhere, anytime. To support these new demands, data centers are becoming increasingly virtualized, allowing for increased automation and the ability for application workloads to dynamically move across multiple on-premises data centers and multi-cloud (private, public, and hybrid) environments. The adoption of new technologies like software-defined networking (SDN) and virtualization, coupled with new trends in hyperconverged infrastructure (HCI) and hybrid cloud IT, helps organizations deliver on the demands of the business, but also introduces new risks and vulnerabilities.

As virtualized and cloud environments grow, so does an organization's attack surface, increasing the risk of attackers gaining access to the internal network. Once attackers bypass perimeter security controls, they can move laterally across the environment in search of data to steal or hold for ransom. As a result, organizations must redefine their security approach to include east-west network traffic security in addition to perimeter network security.

Preventing Lateral Movement with Microsegmentation and Nutanix Flow

Nutanix Flow delivers the ability to control east-west (VM-to-VM) traffic and reduces the risk of threats spreading laterally across the data center. This is accomplished by distributing network security controls to every Nutanix Acropolis™ Hypervisor (AHV), allowing Flow to enforce a perimeter around every individual VM—a strategy called microsegmentation. Flow's distributed architecture ensures that even when a VM moves, its security policies move with it, maintaining its security posture even in the most dynamic environments.

Augmenting Flow with Threat Prevention from Palo Alto Networks VM-Series

When integrated with Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls, Flow's ability to control traffic is augmented with industry-leading threat prevention capabilities. While microsegmentation can help reduce the attack surface of a Nutanix environ¬ment, Palo Alto Networks Threat Prevention and other services on the VM-Series detect and stop threats attempting to penetrate the perimeter, move laterally across legitimate network connections, or exfiltrate data. Realtime threat intelligence feeds arm the VM-Series with the latest signatures based on threats detected across the entire Palo Alto Networks install base, protecting Nutanix environments from the latest zero-day threats. The VM-Series tag-based policy model ensures that even as new workloads are created, they are automatically protected based on their tags.

Seamless, Consistent Security Through Automated, Single-Pane Management

Security must keep pace with the speed of business. A VM-Series deployment blueprint for Nutanix Calm allows for simple, repeatable, and automated deployment of VM-Series firewalls when and where needed, all with the click of a button. Preconfigured workflows for scale-up and scale-down in the Calm blueprint make maintenance of your environment simple.

Palo Alto Networks Panorama™ network security management provides a single pane of glass through which to manage security and policies, alleviating the need for administrators to jump between interfaces. From Panorama, administrators can consistently manage the security postures of their Nutanix environment, physical data centers, and even public clouds.

Use Case No. 1: Microsegmentation

Challenge: Virtual applications running on the same host are difficult to selectively segment without complex network design and configuration, often requiring hairpinning of traffic and negatively impacting performance. This may lead to increased threat exposure or vulnerabilities in virtualized environments.

Answer: Microsegmentation helps reduce the attack surface by preventing lateral movement across east-west traffic. This is accom¬plished by deploying VM-Series integrated with Nutanix Flow. Use the Nutanix Calm blueprint to create service chains and deploy VM-Series on every AHV host. With Nutanix Flow, specific traffic can be transparently directed to the VM-Series firewall in the service chain for deep packet inspection based on the user-defined Nutanix Flow policy.

Use Case No. 2: Virtual Desktop Infrastructure

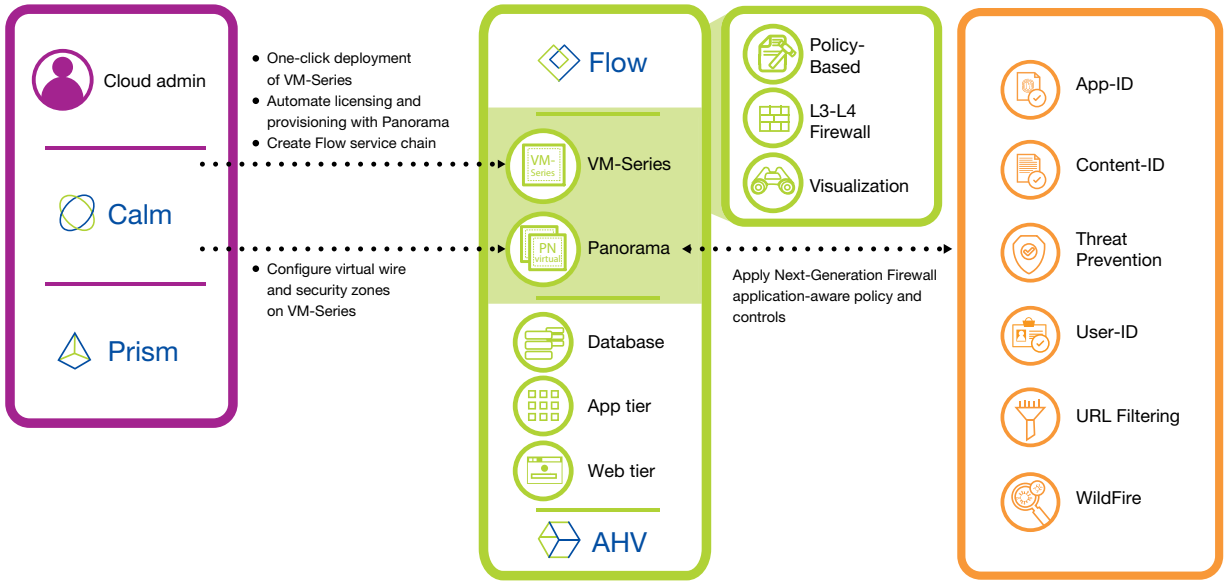
Challenge: Virtual desktops are growing in popularity, but hosting all of these desktops in your core data center without the proper protection in place dramatically increases your attack surface. The dynamic nature of these desktops can also make security management challenging.

Answer: Nutanix Flow can isolate groups of virtual desktops with a simple security policy, work with VM-Series on AHV to inspect and enforce Layer 7 controls based on application and user identity, and block threats across the virtual desktop infrastructure.

Exclusive Networks: Your Choice for Nutanix and Palo Alto Networks Solutions and Value-Added Services

Exclusive Networks is the global specialist VAD for cybersecurity and cloud solutions – the defining and interdependent technologies of the digital era. Our expertise is perfectly aligned to support the opportunities presented by integrated Nutanix/Palo Alto Networks technologies.

Our Global Services further enable partners to maximise extra service revenues and augment their existing capabilities while retaining focus on their core business – adding value throughout the customer lifecycle, accelerating time to revenue, growing overall deal margins and transforming sales relationships from transactional to transformational. Services encompass multi-vendor professional and technical services, implementation and support, asset financing and leasing, project management and logistics, and accredited training. All are available on both a global and local basis.



EXCLUSIVE NETWORKS