The network is the foundation for the connected Enterprise. With increasing application complexity, driven by distributed services and rapid growth in SaaS and cloud-based offerings, the need to easily visualize, analyze and govern network communications becomes critical.

Nutanix Flow delivers advanced networking and security services, providing visibility into the virtual network, application-centric protection from network threats, malware, and ransomware and automation of common networking operations.

Fully integrated into the Nutanix private cloud solution and Nutanix AHV virtualization, Flow allows organizations to deploy software-defined virtual networking and security without the complexity of installing and managing additional products that have separate management and independent software maintenance requirements.

**Application Visualization**
Setting the right application-centric network policies requires a complete understanding of workload behavior. Nutanix Flow provides detailed visualization of communications between VMs, making it simple and straight-forward to set the right policies for the environment.
KEY BENEFITS

- Application centric network policies for VMs
- Always-on native networking functionality with no additional software or management consoles
- Works with any network topology or architecture
- Application and network visibility
- Automated policy change management tied to VM lifecycle
- Prevent the propagation of network security threats
- Expand functionality via third-party network inspection and policy tools
- Adds Identity based security to EUC/VDI deployments

RESOURCES

- nutanix.com/products/flow
- nutanix.com/products/ahv
- nutanix.com/security

Network Isolation and Microsegmentation
Microsegmentation provides granular control and governance of all traffic into and out of a virtual machine (VM), or groups of VMs. It ensures that only permitted traffic between application tiers or other logical boundaries is allowed and protects against advanced threats propagating within the virtual environment.

Nutax Flow differs from traditional perimeter firewalls by allowing network policy to be attached to VMs and applications, rather than specific network segments (e.g., VLANS) or identifiers (IP addresses). Through centralized management from Prism, policies are auto-updated throughout the VM lifecycle, removing the burdens of change management.

Service Insertion and Chaining
Nutax Flow functionality can be extended to leverage virtualized network functions from third-party software. These services are inserted in-line or in tap-mode with VM traffic, and can be easily enabled for all traffic, or deployed only for specific network traffic. Common network functions include virtual firewalls, load balancers, threat detection, and application performance monitoring.

Network Automation
Flow provides API based notifications enabling third-party network devices to observe VM lifecycle events, such as the instantiation of a new VM into the Nutanix environment. This enables automation of typical network configuration changes, such as the provisioning of VLANs or dynamically updating firewall and load balancer policies.

PRICING AND AVAILABILITY

Nutanix Flow is built into the Nutanix software, and works seamlessly with AHV virtualization. Capabilities are delivered with AHV and are licensed separately from AOS Editions.

<table>
<thead>
<tr>
<th>Service</th>
<th>All AOS Editions</th>
<th>Flow License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Service Insertion and Chaining</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Network Automation</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application Flow Visualization</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Policy-Based Service Insertion and Chaining</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Application Security with Microsegmentation</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>