SOLUTION BRIEF

HYTRUST®
Cloud Under Control

# HyTrust CloudControl for VMware NSX

Software defined data centers (SDDC) are being widely adopted as a way to make data centers more agile, operationally scalable and secure. SDDC is defined by compute, storage and network virtualization and VMware NSX provides the network virtualization component. Virtual networks enable network isolation by default and NSX native security capabilities provide in-kernel, scale-out firewalling with line-rate performance distributed to every hypervisor, automated provisioning of security services, automated workload moves/adds/deletes, and granular policy enforcement at the virtual level.

Distributed applications have significantly increased traffic inside the data center. East-West or server-to-server traffic represents 80% of overall data center traffic and is where recent breaches have occurred, but this traffic is currently not inspected. Modern day attacks exploit this gap, propagating threats inside the data center through lateral movement.

Forcing East-West traffic to be inspected by perimeter defenses causes performance chokepoints that can impact network performance throughout the data center. Moving security controls inside the data center is architecturally complex and traditional approaches to micro-segmentation are costly and unscalable, but NSX makes micro-segmentation feasible and scalable. NSX micro-segmentation is based on inherent isolation of virtual networks, segmentation through distributed firewalling and granular security controls at the individual workload level. For advanced traffic inspection NSX provides dynamic insertion and orchestration of best-of-breed partner services.

VMware and HyTrust have partnered on an integrated solution to enable fine-grained administrative access to configure, control and monitor security policies for micro-segments to reduce operational and security risks. Separation of duties and monitoring access to security configurations and policies for administrators is analogous to the separation and protection of network segments with NSX micro-segmentation.

The VMware NSX platform offers operationally feasible micro-segmentation inside the data center perimeter without compromising performance of data

## Benefits:

- Save time on compliance and audit reporting and speed time to resolution for trouble shooting with advanced reporting on NSX admin access and changes

- Strengthen security posture with granular control over security configuration and policy that is aligned with NSX micro-segmentation

- Prevent downtime and service disruption by protecting the virtualized network from process failure or configuration administrative error with change controls

- Achieve authorization and authentication requirements for two-factor authentication,
- tokens, smart cards and AAA servers for VMware NSX deployments

center traffic or increasing the cost and complexity of security infrastructure. The powerful segmentation that NSX delivers for the virtualized network must be matched with similar segmentation and control for virtual administrator access to prevent unlimited access and control of virtual routers, switches, and firewalls. HyTrust has partnered with VMware to deliver enterprise-class administrator controls for NSX.

HyTrust CloudControl helps ensure that VMware NSX deployments have the required administrative controls and monitoring to fundamentally strengthen security and risk posture. Organizations can realize the full benefits of micro-segmentation in the SDDC and also be assured that they can meet their security requirements with granular role based access control and monitoring, speed the time to trouble resolution and enable compliance monitoring.

HyTrust CloudControl deployed with VMware NSX provides advanced administrative controls and monitoring, enabling networking teams to implement and enforce privileged user separation of duties and strong authentication for the NSX network virtualization platform, protecting network resources from process failure or administrative configuration errors.

## Granular access control to support NSX micro-segmentation

HyTrust Cloud Control can contain and prevent damage to network resources due to process failure or privileged administrator error with a granular, role-based access control for NSX deployments, as well as provide separation of duties within networking teams and between networking and infrastructure virtualization groups.

## Strong authentication for NSX administrators

When HyTrust Cloud Control is deployed with NSX, organizations are able to control who gets access to NSX resources with strong authentication and authorization including two-factor authentication using tokens, smart cards and AAA servers.

## Powerful NSX logging and reporting

HyTrust CloudControl provides event logging of privileged user-level approved and denied operations on NSX resources. This provides organizations with detailed information beyond the standard logging provided by NSX for faster trouble resolution and compliance reporting.

- **Role-Based Access Control (RBAC)**
  - Limit admin actions for separation of duties and least privilege access
  - Pre-defined & customizable roles specific to NSX
- **Strong Administrator Authentication**
  - Two-Factor: RSA SecurID, CA Authminder
  - RADIUS, TACACS+
- **Enhanced Administrator Logging**
  - Event logging based on HyTrust CloudControl configured and managed roles for faster trouble resolution and easier compliance reporting

SDDC enables data center operators to deliver for the first time, operationally feasible micro-segmentation inside the data center perimeter without compromising performance of the data center traffic or increasing costs and complexity of security infrastructure. The HyTrust CloudControl with VMware NSX strengthens network security posture and reduces operational risks by applying granular role-base access controls and monitoring for administrators of NSX deployments.

**For More Information** visit www.hytrust.com
or call us at 650-681-8100.