TREND MICRO™

NUTANIX PARTNER NETWORK

NUTANIX READY

N

NETWORKING & SECURITY

NUTANIX AND TREND MICRO DELIVER HYPERSCALE SECURE ENTERPRISE CLOUD

The Leading Enterprise Cloud Infrastructure and Cloud Security Platform Team Up to Create Secure Hyperscale Hybrid Cloud Deployments

Customers using the Nutanix enterprise cloud platform to achieve a more agile, reliable, cost-effective IT environment need proven security that will protect all applications seamlessly. Complementing and building upon Nutanix's native security posture, Trend Micro™ Deep Security™ provides a comprehensive platform for virtualized environments and is designed to simplify security operations while accelerating the ROI of virtualization and cloud projects.

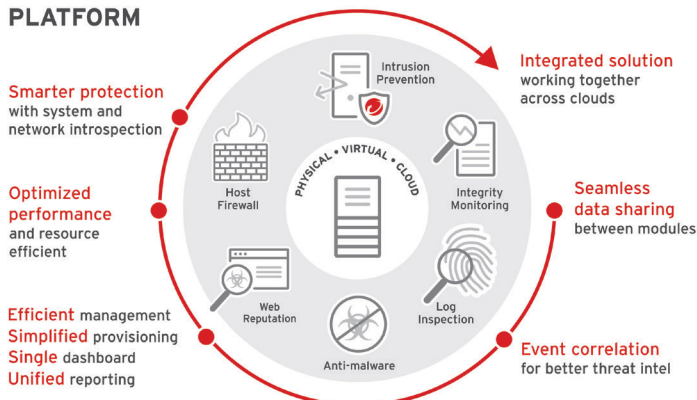## BUILDING HYPERSCALE SECURE HYBRID CLOUDS

The Nutanix enterprise cloud platform delivers invisible infrastructure for next-generation enterprise computing, elevating IT to focus on the applications and services that power its business.

Trend Micro Deep Security is a security platform that is purpose-built for cloud and virtualization and unlocks virtual machine (VM) performance for servers and virtual desktop infrastructure (VDI) environments. As a security solution with Nutanix Ready validation for all three hypervisors (vSphere, Acropolis with AHV, and Hyper-V), Deep Security helps secure workloads deployed on the Nutanix enterprise cloud platform, helping to reduce risks and meet compliance and governance requirements.

AUTOMATED, SCALABLE AND AGILE – SECURITY THAT FITS

- **Optimized for virtualized workloads** – Deep Security is purpose-built for virtualized workloads. It is architected for minimal resource consumption and improved performance, and eliminates the risk of "security storms." Automation capabilities ensure VMs are secure throughout their lifecycle, and policies and rules are applied automatically based on the context of the VM.

- **Native support for Nutanix AHV** – Fully validated on Nutanix AHV, Microsoft Hyper-V and VMware vSphere hypervisors, Deep Security enables secure mobility of workloads between hypervisors without compromising security.

- **Comprehensive security in a single centralized platform** – Deep Security includes six different security modules (anti-malware, web reputation, system integrity monitoring, intrusion prevention, bi-directional stateful firewall, and log inspection), all in one fully integrated platform. This enables Nutanix customers to apply a layered security strategy, customized to fit the security posture of the workloads.

At a glance

Traditional security is irrelevant in a hyperscale virtualized environment:

- Insufficient visibility to east-west traffic
- Security policies and provisioning lag behind workload agility
- Disparate security solutions and lack of uniform policies across platforms create security holes

Deep Security and Nutanix

- Fully validated on AHV, vSphere, and Hyper-V
- Layered security for deep protection customized for each workload
- Optimized for key enterprise workloads like VDI, SAP, and Oracle, and drive industry compliance such as PCI, HIPAA, FISMA, etc.
- Highly optimized, minimal footprint
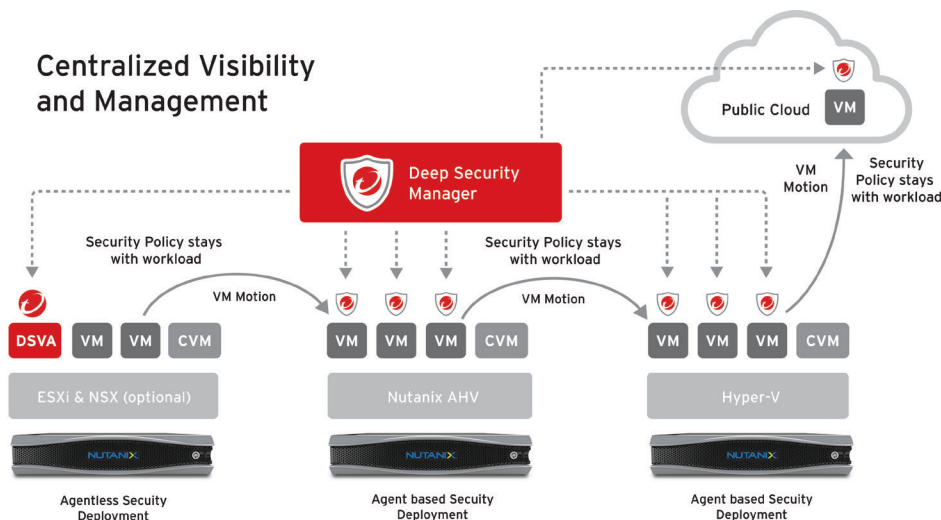
Key benefits for business and IT

- **Scale securely** without compromising on performance and efficiencies
- **Elastic protection** through automated policy and security controls
- **Consistent policies** and unified operations across hybrid cloud environments

TREND MICRO DEEP SECURITY PLATFORM

Smarter protection with system and network introspection

Optimized performance and resource efficient

Efficient management
Simplified provisioning
Single dashboard
Unified reporting

PHYSICAL • VIRTUAL • CLOUD

Intrusion Prevention
Host Firewall
Integrity Monitoring
Web Reputation
Log Inspection
Anti-malware

Integrated solution working together across clouds

Seamless data sharing between modules

Event correlation for better threat intel

HOW DOES IT WORK?

Nutanix solutions natively converge server and storage resources into a single, 100 percent software-defined appliance that comes ready to run all enterprise applications, at any scale. Built on a distributed web-scale architecture, a single Nutanix hyper-converged appliance can simultaneously run different workloads, including enterprise databases and applications, VDI, and big data workloads.

Deep Security secures workloads no matter where they reside—in a private cloud powered by the Nutanix enterprise cloud platform or on one of the public cloud platforms. Deep Security supports and is fully validated on all the hypervisors supported by Nutanix. Nutanix deployments secured by Trend Micro Deep Security function as follows:

- On vSphere hypervisor, Deep Security provides lightweight, automated capabilities leveraging VMware APIs to offload key security functions to a dedicated **Deep Security Virtual Appliance (DSVA)**, eliminating a security agent footprint on the guest VMs.

- On AHV and Hyper-V environments, Deep Security supports an agent-based architecture, where the lightweight **Deep Security Agent (DSA)** is installed on each of the guest VMs.

- All the DSAs and the DSVA are centrally managed through the **Deep Security Manager**, which helps deploy policies, rules, and security settings, and also helps automate the deployment and provisioning of the DSAs.

- As VMs are migrated from one hypervisor to another, or from private to public cloud, the security policies and rules travel with the workload, eliminating security gaps. With a single, comprehensive security solution, deployment, and management are much faster and easier as customers move workloads from one medium to another.

Practical use cases

Accelerating compliance

- Simplify security operations while enabling regulatory compliance with PCI DSS 3.1, HIPAA, FISMA/NIST, NERC, and SSAE-16, and accelerate the ROI of using Nutanix XCP for virtualization and cloud projects.

Securing VDI workloads

- Optimized for VDI workloads, Deep Security helps improve the security and performance of VDI workloads on the Nutanix enterprise cloud platform. The agentless security model on VMware vSphere hypervisor helps maximize consolidation ratios to offer 30 percent more VM density compared to agent-based security solutions. Scan cashing technology improves VDI performance with 2x faster logins and 20x faster full scans.

Elastic security for hybrid cloud deployments

- Supports all the Nutanix enterprise cloud platform hypervisors (AHV, vSphere and Hyper-V) and all major public clouds. Unified policies move with each workload as the workloads move from one hypervisor to another or from private to public cloud. Centralized management makes policy enforcement very simple.

Securing data center workloads, including SAP

- SAP-certified integration with the SAP NetWeaver platform and SAP Virus Scan Interface (VSI) helps Nutanix customers protect SAP deployments on the Nutanix enterprise cloud platform. Deep Security for SAP systems works seamlessly with SAP NetWeaver technology and the SAP HANA® platform.

Supporting multi-tenant service provider architectures

- Multi-tenant architecture enables logical separation of tenant policies and data, allows delegation and self-service for tenants, and supports elastic cloud-scaling with automated deployment and provisioning of Deep Security components. RESTful management of APIs also facilitates extensibility and integration into modern cloud infrastructure.

MORE INFORMATION

For more information on how Nutanix and Trend Micro Deep Security can help with your virtualization and cloud projects, please visit nutanix.com/resources and trendmicro.com/virtualization.

For more information about Trend Micro Deep Security and how it can be used to secure Nutanix deployments, email us at Nutanix@trendmicro.com or call 1-877-218-7363.