



Secure Your Critical Applications and Infrastructure with Guardicore Advanced Security

Guardicore delivers a simple, scalable and highly secure data center environment

Today's data center and cloud environments are transforming from highly complex to radically simple thanks to the native convergence of compute, virtualization and storage delivered by the Nutanix Enterprise Cloud Platform. But even as organizations gain agility, ease of management and reduced costs associated with a data center infrastructure based on Nutanix, they also realize that today's agile and dynamic cloud environments have outpaced traditional security technologies. And due to the dynamic nature and high traffic rates inside modern data centers, organizations face significant challenges in gaining visibility into application communications and putting proper controls in place to secure east-west traffic.

The Guardicore Centra™ Security Platform is designed specifically for today's modern data centers and clouds, applying multiple security controls in a single platform to protect critical applications in these dynamic environments. By deploying Guardicore on top of Nutanix, organizations get granular visibility into network and applications flows combined with micro-segmentation, real-time breach detection and automated response across all traffic and applications in the data center.

A Nutanix Ready AHV and ESXi validated solution, the Guardicore Centra Security Platform features a distributed architecture for Nutanix Acropolis (AHV) Environments, and VMware or Microsoft Hyper-V that easily and seamlessly distributes security across the entire data center, as well as other workloads that you might have in the public clouds or Bare Metal servers, leaving no workload or application unprotected. This distributed architecture is non-intrusive and lightweight, allowing it to apply security controls in any Nutanix environment without affecting performance.

While monitoring and visualizing all applications and network flows with process-level context, Guardicore combines micro-segmentation with multi-method breach detection capabilities including patented dynamic deception, reputation analysis, file integrity monitoring and policy-based detection. Deploying these four methods simultaneously forms a strong security net, virtually ensuring that any live breach in the data center is caught, mitigated and contained for in-depth investigation.

The Nutanix logo is the word 'NUTANIX' in a bold, white, sans-serif font, with a small trademark symbol (TM) to the right. It is set against a dark purple diamond-shaped background.

Key Benefits

- ◆ **Security Value from Day One**
Easy, non-intrusive deployment requires no configuration and delivers immediate value.
- ◆ **Total Visibility**
Get real-time and historical visibility into your entire environment, including Nutanix— all network and application flows, including process-to-process communications.
- ◆ **Reduce the Attack Surface**
Micro-segmentation done at the critical application layer applies granular controls that reduces the attack surface and prevents the spread of active breaches.
- ◆ **Accelerate Nutanix Adoption**
Guardicore's deep visibility and flexible policy engine simplifies migration to Nutanix and helps drive AHV adoption.
- ◆ **Accelerate Incident Response**
Automated real-time attack isolation and remediation of infected files and servers stops attack at initial stage, before it has caused any damage.
- ◆ **Reduce the Cost of Data Breaches**
Catch active breaches earlier in the kill chain, eliminating costs related to investigation and clean up.

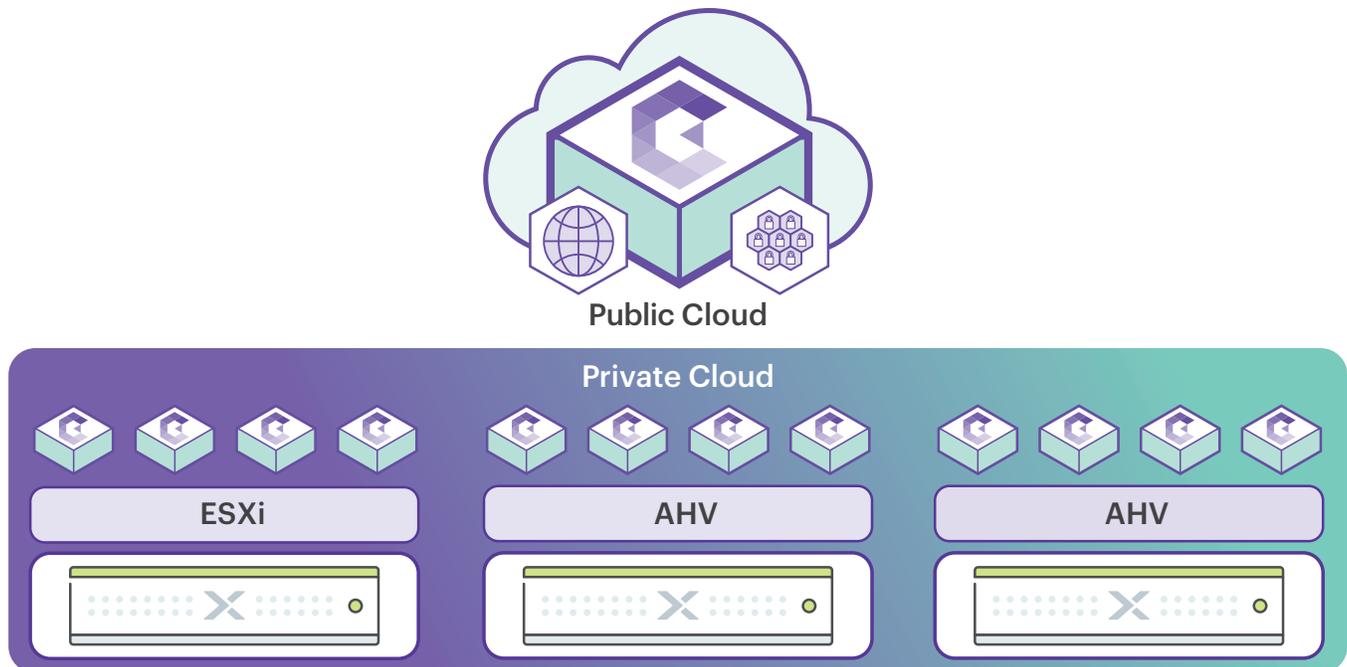
Enabling Advanced Security for Virtual Data Center Environments

Virtual machines and applications running on Nutanix are protected by the Guardicore Centra Security Platform, featuring application-layer visibility, micro-segmentation and multi-method breach detection. Deployed seamlessly, Guardicore Centra monitors all traffic, collects network and application flow data, and redirects suspicious connections for investigation by the Guardicore Analysis Engine. The Guardicore Analysis Engine provides visibility by enriching collected flow data and provides real-time breach detection, analysis and response.

VALIDATED SOLUTIONS:

- ◆ Guardicore Centra 3 Release 24 and above validated on AHV
- ◆ Guardicore Centra 4.0 Release 31 and above is validated on Nutanix AHV (AOS 5.15)
- ◆ Guardicore Centra 4.0 Release 31 and above is validated on ESXi (AOS 5.15)

Guardicore + Nutanix Architecture



Read more about technical partnerships to augment each solution:

www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.