Nutanix Digital Enterprise
Solution Brief for Data Security

Security with Nutanix: A Defense in Depth Strategy

Key Benefits

- Protect data and prevent breaches
- Enable faster security validation and automated remediation
- Rich features to protect networks, applications, and data
- Simplify regulatory compliance efforts

Maintaining security in today's environments is challenging for several reasons. Many traditional infrastructure stacks are comprised of products from multiple vendors, each with a narrow and limited view of security. Validating and maintaining a security baseline through continuous software upgrades, is time-consuming and often involves error-prone manual processes that take away from innovation and productivity.

In the cloud era, security needs to become an integral and invisible attribute of enterprise infrastructure. Security must be ingrained in the culture and security considerations need to be an essential part of the organization's decision making in order to meet the high-bar of regulatory compliance as well as address the challenges of evolving security threat landscape. Enterprises should strive to incorporate automation into the process of maintaining security in the infrastructure in order to avoid human error and deliver seamless scalability without compromising security in an ever-changing datacenter environment.

Security in the enterprise datacenter must begin with a robust infrastructure foundation. This is where industry leading HCI from Nutanix AOS not only provides operational and financial value, but also aids in improving security posture and preventing data breaches by ensuring these critical areas are a product focal point:

Secure Development: The Nutanix Security Development Lifecycle (SecDL) integrates security into every step of product development and covers the entire infrastructure stack including storage, virtualization, and management.

Product Capabilities: Nutanix AOS and Xi Cloud Services contain many features and functions that can be used to secure data and support compliance goals. Features include data-at-rest encryption, local encryption key management, role based access control, and support for enterprise authentication models via SAML.

Secure Platform: Nutanix AOS delivers a hardened enterprise cloud environment leveraging recommendations from the Security Technical Implementation Guide (STIG). Management of this platform is secured through Role Based Access Control (RBAC) and support for enterprise authentication models via SAML.

NUTANIX™
YOUR ENTERPRISE CLOUD

©2019 Nutanix, Inc. All Rights Reserved

SECURITY STANDARDS AND CERTIFICATIONS

Nutanix employs multiple security standards and validation programs. It complies with the strictest international standards, including the SP800-53 guidelines, to assure governments worldwide that Nutanix products perform as expected and work with their existing technology.

Data Security: Nutanix AOS offers built-in data-at-rest encryption along with the simplicity of a native Key Manager. Organizations also have the option to use External Key Managers and Self-Encrypting Drives (SEDs).

SecOps: Automation is easily enabled through efficient one-click operations and self-healing security models to maintain security in an always-on solutions.

Networking: With Nutanix Flow, microsegmentation based application security can be quickly implemented and automated to ensure only desired traffic is allowed inside the datacenter. Microsegmentation prevents lateral spread of network based attacks and can limit the scope and impact of security breaches.

Multi-Cloud: As IT consumption expands to include public cloud and SaaS components, security controls become much harder to maintain. Xi Beam provides extensive security audits, event driven real-time security monitoring, policy based automation and one-click remediation for security controls and configurations in public cloud environments.

Ecosystem: Expanding beyond the platform into the robust set of security partners, Nutanix delivers validated joint solutions with many security solution providers.

AOS PLATFORM SECURITY

Security is a foundational aspect of product design at Nutanix. The strong pervasive culture and processes built around security harden the enterprise cloud platform and prevent zero-day vulnerabilities. Efficient one-click operations and self-healing security models help in maintaining security in an always-on solution.

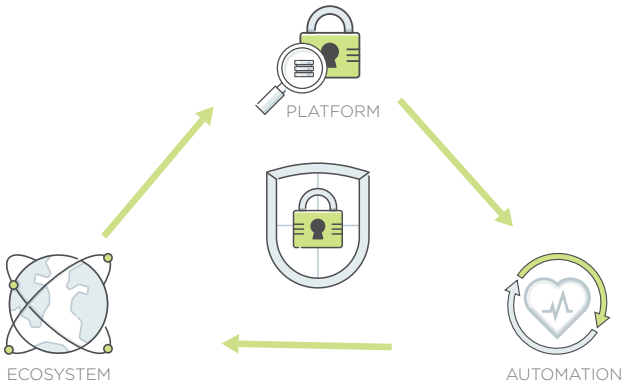
Development Lifecycle: Security is incorporated into the product development lifecycle from the start – avoiding difficult tradeoffs between security and performance or features. For example, research and development teams work together to fully understand all the code in the product, whether it is built in-house or inherited from dependencies. Strict tests for Common Vulnerabilities and Exposures (CVE) are built into the product QA process, and updates to handle known CVEs are scheduled for minor release cycles to minimize zero-day risks without slowing down product evolution.

Configuration Baselines: Nutanix publishes custom security baseline documents, based on United States Department of Defense (DoD) Security Technical Implementation Guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployment in the field. Nutanix baselines are based on common National Institute of Standards and Technology (NIST) standards that can be applied to multiple regulatory concerns, e.g., for Government, Healthcare (HIPAA), or retail and Finance (PCI-DSS).

NUTANIX™
YOUR ENTERPRISE CLOUD

©2019 Nutanix, Inc. All Rights Reserved

Automated Validation and Self-Healing: Nutanix baselines are published in a machine-readable format, allowing for automated validation and ongoing monitoring of the security baseline for compliance. Nutanix has implemented Security Configuration Management Automation (SCMA) to efficiently check security entities in the security baselines that cover both HCI and AHV virtualization. Nutanix automatically reports log inconsistencies and reverts them to the baseline. With SCMA, systems can self-heal from any deviation and remain in compliance (hourly, daily, weekly, or monthly intervals).



DATA SECURITY

Nutanix delivers a broad range of capabilities that security-conscious customers can use to meet stringent requirements, including:

Enterprise Authentication: Through support for the open SAML standard, Nutanix Prism Central provides various methods to integrate with multifactor authentication mechanisms and Common Access Card (CAC) schemes.

Role Based Access Control (RBAC): Nutanix Prism Central allows the creation of customer roles based on attributes, managed objects and permitted administrative tasks, giving administrator granular control over configuration and VM provisioning activities.

Native Data at Rest Encryption: As a native HCI option, encryption can be enabled to secure sensitive data and eliminate the risk of data loss. AOS delivers built-in FIPS compliant software-based encryption that delivers security without compromise to storage efficiency or performance. Furthermore, AOS simplifies the end-to-end solution with a built-in native Key Management Server (KMS).

Self-Encrypting Drives (SEDs): AOS also supports SEDs for organizations that require FIPS 140-2 Level 2 compliance.

Enterprise Key Management Servers (KMS): Nutanix AOS encryption supports 3rd party Enterprise KMS using KMIP for organizations that have a preference or have a regulatory compliance need.

©2019 Nutanix, Inc. All Rights Reserved

APPLICATION-CENTRIC NETWORK SECURITY

Nutanix Flow delivers advanced networking and security services that leverage the concepts of zero trust and microsegmentation to provide visibility into the virtual network, protection from network threats and automation of common networking operations. Flow covers the most common use cases including:

Environment isolation to ensure complete segmentation between application environments without the need for complex configurations

Application tier segmentation restricts communication between application tiers to ensure only necessary communication is permitted

CLOUD COMPLIANCE

Xi Beam provides continuous cloud security and compliance for multi-cloud environments with one-click remediation for cloud vulnerabilities. Beam provides insights into security vulnerabilities in real-time so that you can resolve potential threats before they turn into business challenges.

With Beam you can audit and maintain cloud security compliance for HIPAA, ISO, PCI-DSS, CIS, NiST and SOC-2, enforce custom policies and audits or leverage the 250+ built in security checks based on industry best practices.

CUSTOMER QUOTES

"We have a very secure environment, but we're always looking at ways to utilize technology to enhance that security. Flow enables us to follow an application all the way through and provide security wherever needed"

– Ken Shaffer, Assistant Vice President for Enterprise Systems, Carmax

NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix

© 2019 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all product and service names mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand names mentioned herein are for identi cation purposes only and may be the trademarks of their respective holder(s).