Security Solution Brief

Security-First with Nutanix: A Defense in Depth Strategy

Security in the enterprise datacenter must begin with a robust infrastructure foundation. Maintaining security in traditional infrastructure environments, however, is challenging for a number of reasons. The three-tier infrastructure stack is 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, for example, is time-consuming and often involves error-prone manual processes that take away from innovation and productivity.

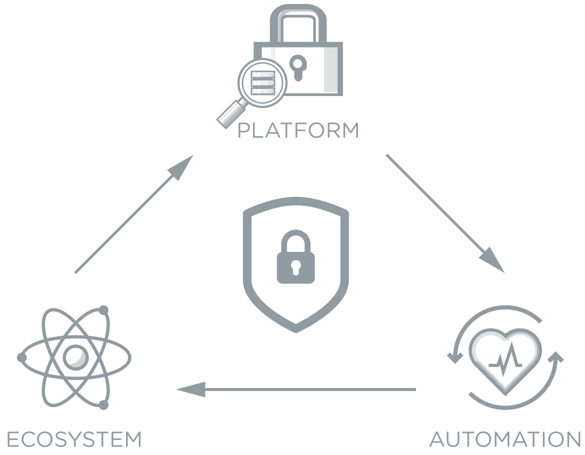
In the cloud era, security needs to become an integral and invisible attribute of enterprise infrastructure. Security must be built into the culture, and security considerations need to be an essential part of product development – from concept to conception – to meet a high bar required by federal, healthcare, and financial certifications and compliances. Enterprise clouds need to incorporate extensive automation into the process of maintaining security in the infrastructure in order to deliver seamless scalability without compromising security in a highly dynamic and agile datacenter.

Nutanix takes a holistic approach to security across three pillars:

Platform: 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.

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

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



Key Benefits

- Mitigates customer risk from code changes using Defense in Depth
- Enables faster security validation and self-healing with machine-readable STIGs and extensive automation
- Supports a broad set of certification and evaluation programs for faster and easier compliance

> “Nutanix continues to provide innovative solutions to improve IT security across federal government organizations. By publishing and testing to their own STIG incorporating DOD STIG guidelines, Nutanix has eliminated the need for time-consuming testing by customers and end-users, allowing us to bring innovative technology into government enterprises quickly.”

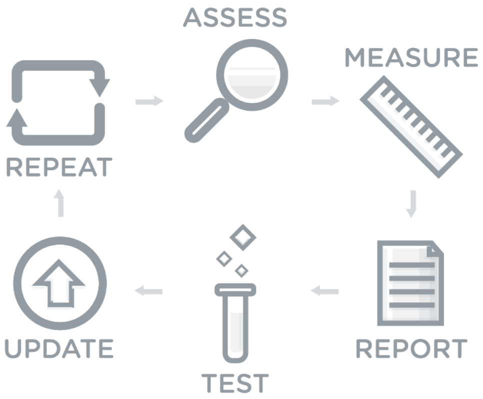
Robert Sanchious

CEO/Chief of Engineering
SHR Consulting Group

SECURE PLATFORM

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 eliminate zero-day vulnerabilities. Nutanix encompasses several key concepts in securing the platform through SecDL, two-factor authentication, cluster shield, and data at rest encryption.

Security 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.



Industry Certifications: Nutanix systems meet a broad set of certification requirements to ensure compliance with the strictest standards.

Common Criteria Certified

FIPS 140-2 Compliant

NIST-SP800-131A Compliant

NSA Suite B Support

Section 508 VPAT Compliant

TAA Compliant

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

- **Two-Factor Authentication** with a combination of a client certificate and username/password or Common Access Card (CAC)
- **Cluster Shield** that restricts access to a Nutanix cluster in security-conscious environments
- **Data at Rest Encryption** using self-encrypting drives

ROBUST AUTOMATION

Efficient one-click operations and self-healing security models help in maintaining security in an always-on solution.

Security Technical Implementation Guides (STIGs): Nutanix publishes custom security baseline documents, called security technical implementation guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployment in the field. Nutanix STIGs are based on common National Institute of Standards and Technology (NIST) standards that can be applied to multiple baseline requirements, e.g., for the DoD and PCI-DSS.

Automated Validation and Self-Healing: Nutanix STIGs 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 over 800 security entities in the Nutanix STIGs that cover both storage and built-in 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).

SECURITY-FOCUSED PARTNER ECOSYSTEM

A holistic approach to delivering comprehensive security through a broad partner ecosystem meets diverse security needs.

Network Security: Monitor, segment, and isolate data traffic in every direction, including north-south and east-west, with software-defined security solutions for dynamic datacenter environments

End-Point Security: Easily protect large numbers of end-points from viruses and malware through partners who preserve performance and consolidation ratios

Data Security: Work seamlessly with external key management system providers who offer centralized enterprise key and policy management servers, enabling compliance and ensuring tracking control

ABOUT NUTANIX

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix enterprise cloud platform leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization and storage into a resilient, software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications. Learn more at www.nutanix.com or follow us on Twitter @nutanix.