NUTANIX PRIVATE CLOUD DESIGN GUIDE:

Enhance Security with a Nutanix Private Cloud

Secure your private cloud with a **hardened platform** that offers superior **visibility and control**

To deliver on business needs and accelerate digital transformation, enterprises need private cloud infrastructure that offers the simplicity and scalability of public clouds and the security and control of on-premises datacenters. However, many private cloud deployments on traditional IT infrastructure have deficiencies in key areas, resulting in:

- Unexpected high costs and lack of cost control
- Insufficient business continuity
- Cumbersome or brittle automation
- Complex, siloed storage infrastructure
- A patchwork approach to security

Built on the industry's leading hyperconverged infrastructure (HCI) software, Nutanix private cloud solutions address these limitations and extends easily to encompass hybrid cloud deployments.

Cybersecurity Challenges

Today’s cyberattacks are more refined and harder to detect, meaning sensitive data is more vulnerable than ever. Because the private cloud environment is more dynamic—with workloads changing more quickly—and because you may not have full visibility and control over all the workloads running in your environment, safeguarding data and ensuring security in a private cloud is different than in traditional IT operations.

Your security tactics must evolve to address a growing number of security challenges:

- Datacenter complexity is the enemy of information security
- Cyberattacks are growing in frequency and sophistication and data breaches are costly
- Reliance on manual security controls impacts the agility of operations and increases risk
- As enterprises progress from private cloud to hybrid and multicloud operations, perimeters become more and more difficult to define

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 reduce productivity and take time away from innovation.

Security must be ingrained in your IT culture and security considerations need to be part of your organization’s decision making to meet the high-bar of regulatory compliance and address the challenges of evolving security threat landscape. You should strive to incorporate automation into the process of maintaining infrastructure security to avoid human error and deliver seamless scalability without compromising security.

A Nutanix private cloud makes it easier to:

Protect Data and Prevent Breaches

- Encrypt data-at-rest
- Control and restrict access to sensitive data
- Analyze and audit security configurations
- Secure your public and private clouds

Segment and Secure Networks

- Deploy microsegmentation and network inspection in minutes
- Separate regulated environments with automated software controls

Simplify Regulatory and Compliance Efforts

- Automate platform security baseline configurations
- Validate compliance with regulatory policies (HIPAA, PCI, NIST, etc)

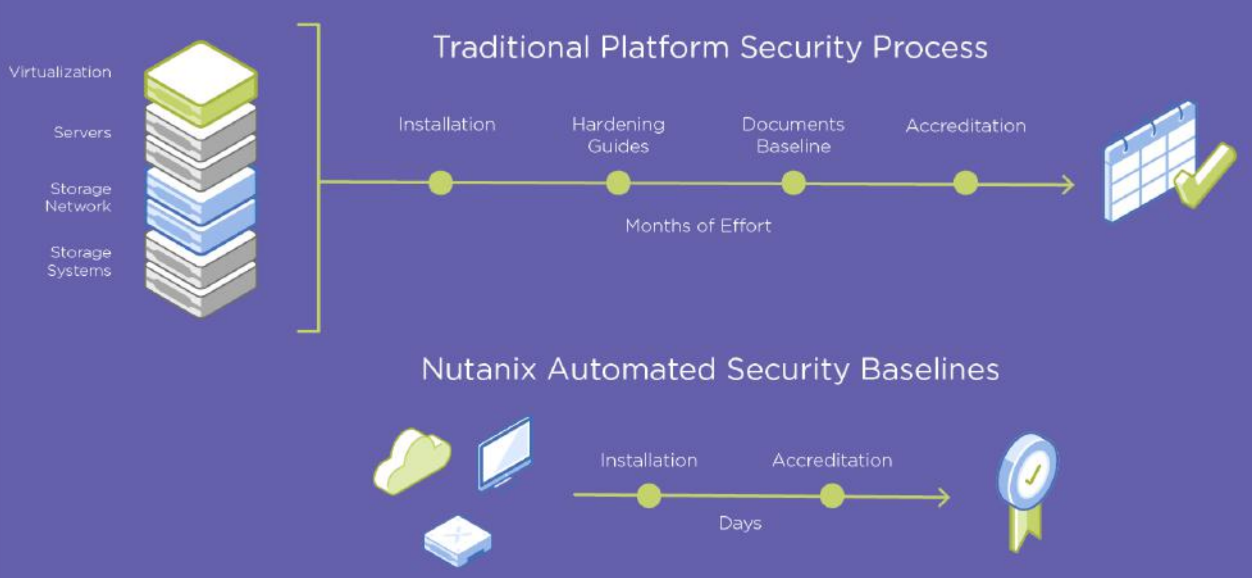
Built-In Security

Your infrastructure impacts your ability to protect your business from cyber threats. A Nutanix private cloud improves your security posture and protects your business with built-in security:

- **Platform Security.** Security is a foundational aspect of product design at Nutanix starting with built-in security hardening practices. Industry best practices and government standards are incorporated into an automated configuration monitoring and self-healing process that helps you achieve your security and compliance goals more easily.

- **Security Development Lifecycle.** Nutanix uses a unique security development lifecycle (SecDL) that incorporates security into every aspect of our software development process, from design and development to testing and hardening.

- **Security Technical Implementation Guide.** Nutanix has developed its own STIG to enable secure installation and maintenance of Nutanix systems, including fast baseline checks and validation.



Three capabilities that are particularly valuable in private cloud environments are data encryption, microsegmentation, and network visualization. Nutanix adds capabilities in all three areas to address diverse needs:

Data Encryption. Nutanix provides flexible methods for encrypting data at rest for compliance and security, including:

- Software-based encryption with local key management
- Self-encrypting drives with external key management

Network Security. Nutanix Flow protects individual applications—and groups of applications—from internal and external security threats with fine-grained microsegmentation rules controlling east-west traffic between VMs, applications, and users. Policy definition is made simple with Nutanix's ability to visualize traffic flows and categorize applications.

Security Planning, Monitoring, and Operations. Nutanix provides advanced insights into security configuration, posture, and infrastructure security compliance to help identify and fix security issues across cloud operations.

This guide describes how Nutanix private cloud protects you with built-in security and gives your organization the flexible security tools it needs to address a broad range of requirements.

A Nutanix private cloud makes it easier to:

- Reduces risk from both internal and external sources.
- Protects brand image by keeping your business out of the headlines.
- Keeps data secure and builds customer confidence.
- Protects sensitive data from leaks.
- Improves trust from crucial investors and lenders.

Find Out More:

- Nutanix Private Cloud webpage
- Nutanix Trust webpage
- Private Cloud demo
- Nutanix Security webpage
- Nutanix Security eBook

Platform Hardening

Nutanix includes native capabilities for security and governance that greatly simplify infrastructure security. A Nutanix private cloud enables you to maintain a continuous security baseline across your infrastructure and satisfy regulatory requirements more easily. Powerful security automation monitors configurations for security best practices, automatically healing any deviations from the baseline.

Secure by Design

With Nutanix, security begins with a robust software foundation built for private, hybrid, and multi-cloud operations. Nutanix starts with AOS, a hardened software platform for HCI, and builds on that foundation with features and functions to improve security posture, detect and prevent security threats, prevent data loss, and ensure continuous business operations.

Nutanix HCI and AOS are inherently more secure than traditional IT architectures; fewer disparate components means a smaller attack surface and less configuration complexity.

The Nutanix Security Development Lifecycle (SecDL) uses a security-first approach from product definition, through design, development, and implementation, with continued monitoring through the entire product lifecycle.

Nutanix has also developed security hardening guides—based on the US Department of Defense (DOD) Security Technical Implementation Guide (STIG) frameworks—that are easy to maintain and formatted so that our software automatically configures itself to a hardened standard. Regular health-checks of the applied STIG are automated. If a system is found noncompliant, the baseline settings are reapplied, so that a hardened system remains compliant after deployment, reducing the risk from manual misconfigurations.

One-click nondisruptive upgrades take the pain out of patching infrastructure software, making it far easier to stay up to date, reducing risk.

Identity and Access Management (IAM)

The ability to limit what each operator can do, and access help ensures that a lost or stolen credential doesn't create too much risk of exposure. Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) are key parts of the Nutanix security model.

AOS

AOS is hardened to be much more secure than traditional IT architectures

You can create policies to ensure that your staff has least-privilege access for the tasks they need to accomplish. Need-based access policies can ensure employees get access to specific resources only for a limited time and access expires after a certain duration. Regular audits, on a quarterly or yearly basis according to your business requirements, ensure only valid users retain access.

Role-Based Access Control (RBAC) Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network.

Prism empowers your team by enabling access control for infrastructure resources. RBAC enables granular control on which users can perform what actions on entities such as VMs, applications, reports, and clusters.

Administrators can group end users together from AD/LDAP for easy role assignment. Administrators can use tagging to group entities, making it easy to manage VM, storage, and network resources.

Multi-Factor Authentication (MFA) Multi-factor authentication provides additional security for cloud services by requiring users to submit a unique code or sequence that is received as a text message or provided by an authenticator app.

By enabling MFA, building policies to ensure that users have least-privilege access to the set of resources they need, using need-based access policies so employees get access to specific resources only for a limited time, and performing regular audits you can greatly increase security in a Nutanix environment by reducing the risks from credentials stolen via phishing or other attacks.

Stringent Security Standards

Nutanix employs multiple security standards and validation programs. It complies with the strictest international standards, including numerous ISO, SOC, and FIPS standards, to assure governments and enterprises worldwide that Nutanix products perform as expected and work with their existing technology.

For the latest information visit our compliance and certifications page.

Find Out More:

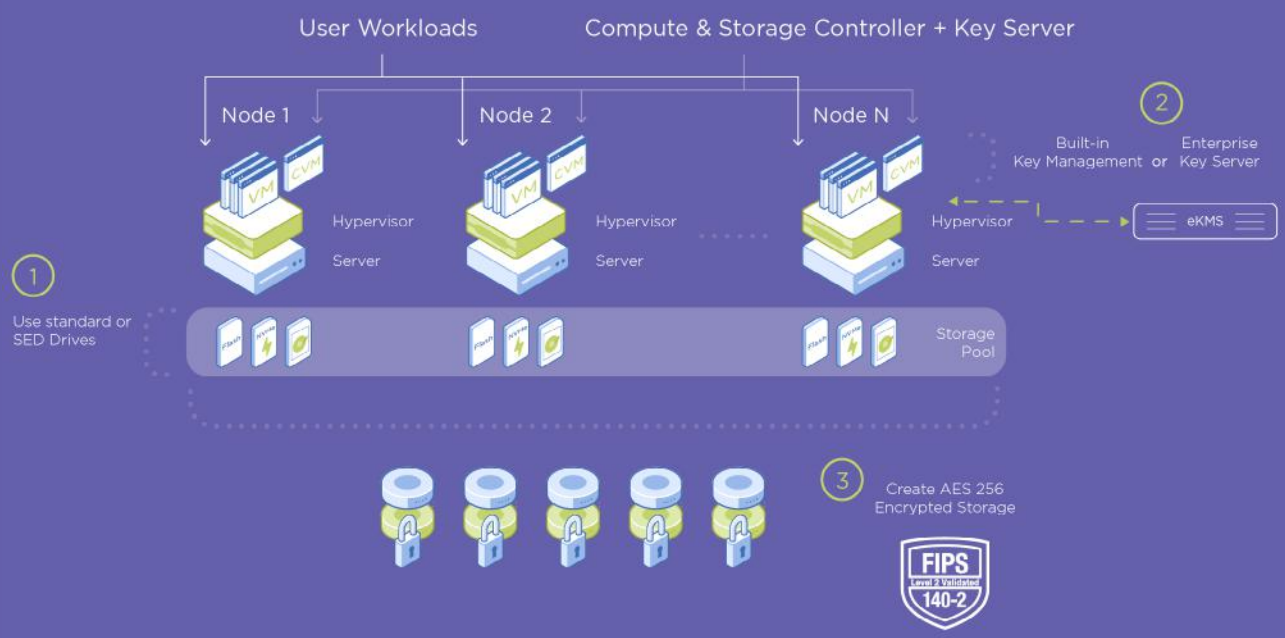
- AOS
- Nutanix Prism
- Trust Compliance

Data-at-Rest Encryption

As a company with a security-first mindset, Nutanix provides flexible support for FIPS 140-2 validated data encryption, satisfying security and regulatory requirements such as PCI-DSS and HIPAA while protecting your data from loss via theft, security breach, during repair, or as part of disposal.

Nutanix AOS offers software-based data-at-rest encryption with built-in key management services and additionally supports the use of self-encrypting drives (SEDs) and external enterprise key management.

Flexible data-at-rest en- cryption options ensure your data is protected to address your security and regulatory requirements



The software option provides data-at-rest encryption with greater flexibility and simplicity. Nutanix AOS uses the same AES-256 encryption standard that is used in SEDs to securely encrypt data.

Once enabled, data-at-rest encryption cannot be turned off. This guards against accidental data leaks (due to user errors) and helps keep the auditing process extremely simple.

Nutanix AOS also offers native key management with a one-click Nutanix-native solution, providing turnkey encryption for Nutanix environments. When configuring encryption, you simply choose native KMS as your key manager. The Nutanix KMS provides options to backup keys and rotate keys to comply with your IT Security policy.

You can also choose to leverage an existing External KMS solution for greater choice.

Find Out More:

- Data at Rest Encryption website
- Data at Rest whitepaper Encryption Simplified

Microsegmentation and Network Security

A "zero trust" philosophy is becoming an essential element of application and data security. Security policy based on the zero-trust concept shifts the focus to the application and user. It eliminates "us versus them" and "inside versus outside" thinking—assuming that an attack can originate from anywhere. Thus, the best defense is to limit datacenter communications and authorization to what's required for an application to function versus reliance on trust based solely on location or source.

Nutanix Flow makes network security simple. It allows you to discover applications and network traffic through intuitive visualizations so you can segment applications and virtual networks and effectively secure workloads.

Discover
Segment
Secure

Nutanix Flow is built into the Nutanix AHV hypervisor and managed through Nutanix Prism Central, so there's nothing extra to install.

Flow can provide:

- **Network segmentation.** Software-defined security policies enable you to segment networks, operating environments, or workloads to meet regulatory or other requirements.
- **Application microsegmentation.** Only necessary network communications reach your applications, limiting the attack surface and preventing malware or ransomware spread.
- **Threat intelligence and detection.** Nutanix allows you to further enhance network security by inserting partner security functions into the virtual network environment.
- **Identity-based security.** Utilize a user's identity to control network access to applications and services in end-user-computing (EUC) environments.

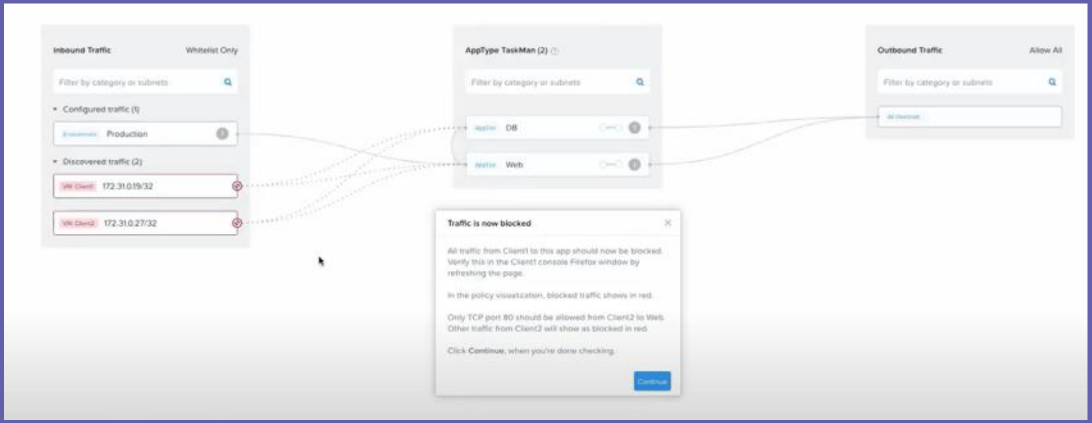
Flow

Nutanix Flow delivers advanced networking, application-centric visibility, and enterprise-grade microsegmentation for protection from network threats

Network microsegmentation provides a discovery, visualization, and policy enforcement model that simplifies and automates the application of granular network policy between VMs. You can easily create security policies to secure applications or VDI groups by controlling access to specific sets of application/user VMs or you can isolate sets of VMs from one another by blocking communication between them.

Flow isolation policies make it possible to isolate environments from one another with a few clicks. For example, you can isolate development from production or isolate tenants in a multi-tenant environment.

Using Flow monitoring, you can quickly discover and visualize traffic flows in a multi-tier app and make adjustments when needed.



Traffic is now blocked

All traffic from Client1 to this app should now be blocked. Verify this in the Client1 console Firefox window by refreshing the page.

In the policy visualization, blocked traffic shows in red.

Only TCP port 80 should be allowed from Client2 to Web. Other traffic from Client2 will show as blocked in red.

Click **Continue**, when you're done checking.

VMs that have been infected with malware or are otherwise misbehaving can be quarantined to prevent problems from spreading.

Flow Networking

Flow Networking brings virtual private cloud (VPC) and other advanced virtual networking constructs together to bridge traditional and cloud-native network models. The use of a software-defined approach simplifies the infrastructure and removes the need for costly hardware segmentation solutions or more complex and static physical network architectures. Flow Networking takes the pain out of creating, managing, and connecting virtual networks between multiple Nutanix environments.

Flow Networking makes overlay networking simple by automating deployment and simplifying configurations to ensure proper network connectivity is maintained and does not require time-consuming manual configuration of networks, routing, or IP address assignment. You will be able to quickly create new VPCs and subnets, and define DHCP, NAT, routing, and security policy right from the Prism Central interface.

Use cases include software lifecycle management and automation, self-service for developers and app owners, automated DR failover and testing, and multi-tenant networking.

At the time of this writing, Flow Networking is available as part of a technology preview with general availability expected in early 2021.

WHAT IS ZERO TRUST?

Traditional perimeter-based security is becoming inadequate to meet modern IT needs, and many are adopting a zero-trust approach in which a user or system only has access to the resources that are required to perform a specific task.

Zero trust grants least-privilege access to resources based on who is requesting access, the context of the request, and the associated risk. It relies on multi-factor authentication, analytics, microsegmentation for fine-grained access control, and encryption to protect against unauthorized data access. Zero trust minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity, and costs for private cloud.

Find Out More:

- App Centric Security eBook
- App-Centric Security with Flow tech note
- Advanced Networking with Nutanix Flow blog
- One Click App Security video
- Nutanix Flow Product Center

Security Planning, Operations, and Compliance

Success with a zero-trust approach comes not just from defining appropriate security controls, but also from the ability to monitor and maintain those controls. Nutanix helps businesses create and manage network security policies, establish and maintain a security and compliance baseline, audit in real-time, and easily remediate security vulnerabilities.

Security Central provides a hub for Nutanix security operations, so your team can easily assess the overall security posture of Nutanix deployments and gain the context required to implement a zero-trust security strategy.

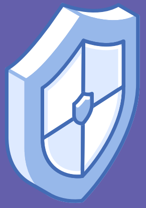
Included with Nutanix Flow microsegmentation, the solution provides:

Security Posture Monitoring with dashboards and reports offering at-a-glance information about current security compliance goals, network utilization, general security health of Nutanix clusters, and a comprehensive multicloud inventory.

Security Audit and Remediation with security configuration scanning, reporting, and automated suggestions for configuration remediation which includes Nutanix US DoD STIG-based security baselines.

Flow Microsegmentation Security Planning to facilitate granular VM-to-VM microsegmentation, application, or network segmentation policies. The visualization provided by Security Central allows you to understand network traffic and use that information to manage groups/categories and policies.

Cloud Security Compliance for those managing both on-premises HCI infrastructure, Nutanix Clusters™, or other workloads running in public clouds. This single solution provides a cohesive view of security posture across multicloud environments at an additional cost.



Flow Security Central provides advanced capa- bilities for managing security across multiple Nutanix environments, Nutanix Clusters, and public clouds

Find Out More:

- Security Central
- One Place for Nutanix Security Planning, Operations, and Compliance

Getting Started with Security on Nutanix

The Nutanix platform is uniquely suited to meet your Private Cloud security needs. Because Nutanix takes a security-first approach your private cloud is more secure right out of the box. That security will scale as your infrastructure grows, and you can add advanced capabilities as to keep pace with your security needs.

To begin designing a Nutanix private cloud that meets your security requirements, start by answering a few simple questions:

- Is your company in a regulated industry like financial services or healthcare, or does it have other unique security requirements?
- Will your private cloud be multi-tenant? Many big enterprises now operate internally using a multi-tenant structure to segment business units or departments.
- Who will be the primary consumers of services in your private cloud? Developers, application owners, business teams?
- Will you enable data encryption? If so, does your industry require the use of SEDs, or can you take advantage of software-based encryption?
- Do you need to or intend to implement network segmentation or application microsegmentation?
- How many Nutanix environments are you responsible for? Do you also manage resources in the public cloud?

Using the information discussed in this guide, you can begin thinking about and planning a private cloud that meets these needs. Use the links provided in each section to dig deeper into specific topics.

To learn more about how Nutanix can help you transform your private cloud visit nutanix.com/private-cloud. You can contact Nutanix at info@nutanix.com, follow us on Twitter @nutanix, or send us a request at www.nutanix.com/demo to set up your own customized briefing.

Take a Test Drive

You can take a test drive of Nutanix infrastructure with no hardware, setup, or cost. Experience the simplicity and agility of public cloud combined with on premises performance, security, and control via an easy-to-follow guided tour.

Test Drive

Private Cloud Design Guides in this Series:

- Automation
- Business Continuity
- Cost Control
- Storage Consolidation

NUTANIX™