

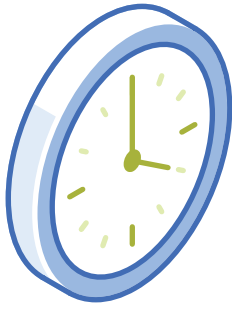


Prevent Cyber Threats: Nutanix's Advanced Security Capabilities

Prevent Cyber Threats: Nutanix's Advanced Security Capabilities

Protecting critical data and applications is crucial for businesses in today's digital age. Nutanix provides a comprehensive solution simplifying security management in hybrid and multi-cloud environments. With layers of security and data protection, network micro-segmentation, and advanced threat prevention capabilities, Nutanix ensures that critical applications and data remain safe. Nutanix's platform provides businesses with a secure and resilient cloud infrastructure that safeguards against cyber threats. With Nutanix, organizations benefit from a security solution that is agile, scalable, and cost-effective, reducing the total cost of ownership and accelerating the time-to-value.





“By the end of 2021, a business will be attacked by Ransomware every 11 seconds.”

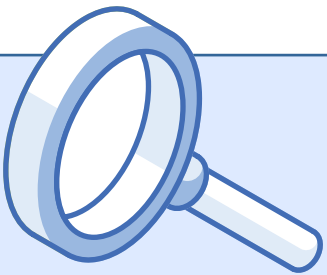
– Cyber Security Ventures Oct '19

Benefits of HCI for Cybersecurity

Nutanix’s Hyper-Converged Infrastructure (HCI) is a revolutionary solution simplifying cybersecurity. By integrating storage, computing, and networking into one platform, Nutanix reduces complexity and lowers the total cost of ownership while providing native security features and services to protect critical applications and data. Nutanix’s HCI includes secure configurations, data-at-rest encryption, network segmentation, and detection and remediation capabilities to safeguard your valuable assets. There are also audit and reporting tools to help businesses comply with regulations. Nutanix’s HCI offers a secure, scalable, and cost-effective solution for protecting critical applications and data. Trust Nutanix’s HCI to simplify your cybersecurity strategy and keep your business safe.

Nutanix’s Approach to Hybrid Cloud Security

Nutanix offers a security solution for hybrid and multi-cloud environments. It includes automated secure configurations, native data-at-rest encryption, and network segmentation to protect critical applications and data from cyber threats. Nutanix also provides audit and reporting tools for regulatory compliance, simplifying security, and reducing resource requirements.

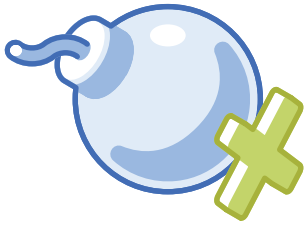


Nutanix Detect Tips

- Use service insertion from AHV and Flow to add layer 7 network threat detection
- Use Prism Ops and X-Play for anomaly detection, alerts, and event triggers
- Export Flow policy hit logs and security events to a SIEM (security incident and event management) tool for broader event correlation and detection

Security from Design and Lifecycle

Nutanix prioritizes security in its software development process, integrating best practices to ensure a secure platform from deployment. Nutanix provides automated security baselines, hardening, and centralized SIEM integration for continuous monitoring. With Nutanix, businesses can enjoy platform security from AOS, which provides a foundation for protecting critical applications and data. Nutanix’s native platform features, and network and audit capabilities establish a security baseline and protect data. Nutanix offers codified security best practices with automated healing and encryption to ensure governance and audit compliance.



Config Errors are a Top Risk

Miscellaneous errors were the second most cited reason for a data breach, after web applications.

Source: "2018 Data Breach Investigations Report," Verizon.



Nutanix Prevent Tips

- Implement RBAC and authentication through directory services
- Change all Nutanix default passwords
- Restrict file types in Nutanix Files
- Use microsegmentation from Nutanix Flow
- Segment Nutanix data and control planes

Nutanix AOS Platform Features

Nutanix AOS provides native security features to protect critical applications and data, including identity and access features like multi-factor authentication, role-based access controls, audit logging, and data protection features such as native data-at-rest encryption with key management and replication planning. Nutanix's network security features include AHV and Flow, providing application-centric visibility and protection from network threats, automation of security baselines, and data loss prevention. Additionally, Nutanix offers micro-segmentation for granular policy between application tiers, isolation groups, or user personas.

Micro-segmentation

Micro-segmentation is an effective approach that limits users and applications to necessary networks and services. Nutanix's micro-segmentation involves understanding network traffic patterns, categorizing application tiers, and providing granular policies between them. By implementing the zero-trust model, Nutanix's solution can prevent breaches and protect from data loss while also preventing malware spread.

Advanced Threat Prevention

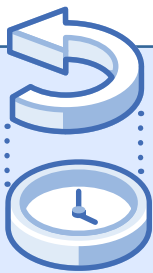
Nutanix's advanced threat prevention delivers defense in depth, using threat intelligence and detection, and Nutanix Flow for application-level visibility and network micro-segmentation. Nutanix Flow provides visualization of application dependencies and policy-based protection against unauthorized traffic. With Nutanix's multiple layers of defense, businesses can quickly respond to threats and prevent damage. Nutanix simplifies managing security in hybrid cloud environments, making it scalable and agile.



Save 82% of the Costs

Cybersecurity Prevention Efforts Can Save Businesses Up to \$1.4 Million Per Attack.

Source: "The Economic Value of Prevention in the Cybersecurity Lifecycle," Ponemon Institute, 2020.



Nutanix Recover Tips

- Include security in your BCDR planning
- Use Nutanix protection domains to replicate data to secondary sites
- Automate your replication and recovery with native data protection and run books and Xi Leap in the cloud
- Create, store, and test your backups with Nutanix Mine

Insights and Monitoring with Security Central

Nutanix Security Central simplifies security planning with real-time security audits, posture monitoring, and detailed traffic visualization. It offers audit and reporting tools to support regulatory compliance and centralized SIEM integration for continuous monitoring. With Nutanix Security Central, businesses can gain insights into their security posture and make informed decisions about their security strategy.

A Solution for Ransomware

Nutanix's solution for ransomware attacks provides businesses with a reliable way to protect their data and applications. Nutanix's network micro-segmentation with Nutanix Flow, Prism RBAC with IAM integrations, and Life Cycle Manager make it easy to protect against ransomware attacks. Nutanix's integrated backup with Nutanix Mine ensures businesses can quickly recover from any damage caused by ransomware. With Nutanix, businesses can stay protected and keep their critical data and applications safe from ransomware threats.















Protect your business with Nutanix

With hyper-converged infrastructure, native security features, micro-segmentation, and advanced threat prevention, Nutanix simplifies security and provides the tools you need to stay secure. Security Central provides insights and monitoring, and Nutanix's solution protects against ransomware attacks. Improve your security posture, prevent breaches and data loss, and accelerate time-to-value with Nutanix's secure, scalable, and agile solution — trust Nutanix to protect your critical applications and data.

TRUST NUTANIX AS PART OF YOUR RANSOMWARE STRATEGY

Nutanix can drastically simplify the process of protecting infrastructure and implementing a recovery solution which will, in turn, lower operational cost and time of resuming business operations without having to pay a costly ransom. Nutanix is focused both on being intrinsically secure and providing solutions that help prevent malware spread and create a path to quick remediation.

To learn more about how these capabilities can be part of your ransomware prevention strategy, visit us at www.nutanix.com/security.

	Prevent	Detect	Recover
Nutanix AOS <ul style="list-style-type: none">• Security hardened with self-healing security configuration• Native storage snapshots• Built-in data protection, replication, and runbook automation• Native data-at-rest encryption with FIPS 140-2 validated modules• Data plane & Control plane segmentation• Native AHV virtualization - built for security			
Nutanix Life Cycle Manager (LCM) <ul style="list-style-type: none">• "One-click" CVE patching, platform upgrades, and life cycle management• Firmware and BIOS upgrade management			
Prism Central <ul style="list-style-type: none">• Role-Based Access Control (RBAC)			
Nutanix Calm <ul style="list-style-type: none">• Application blueprints, automation, and life-cycle management to ensure consistent security configuration			
Prism Ops with X - Play <ul style="list-style-type: none">• Resource analytics and insights with anomaly detection• Codeless automation and event triggers			
Nutanix Flow <ul style="list-style-type: none">• Network segmentation and application microsegmentation• Integrated partner solutions for deep packet inspection and threat intelligence• Policy and event logging for SIEM integration			
Nutanix Files <ul style="list-style-type: none">• File type blocking policies• File activity anomaly detection from Files Insights• ICAP support for antivirus integration			
Nutanix Objects <ul style="list-style-type: none">• Immutable S3-compatible WORM storage for critical data and backups			
Nutanix Mine <ul style="list-style-type: none">• Turnkey archive and backup solution for secondary storage with all the benefits of Nutanix HCI			
Xi Leap <ul style="list-style-type: none">• Simplified cloud Disaster-Recovery-as-a-Service built for Nutanix			