TECH BRIEF

The Ransomware Threat

Detection, Prevention, and Recovery with Nutanix

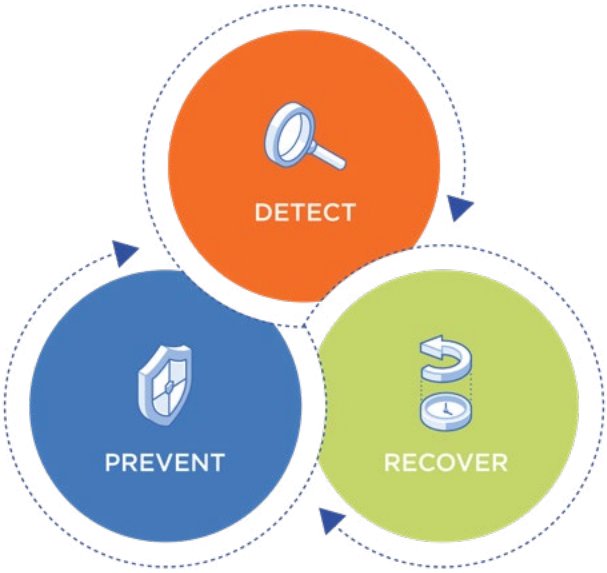
"By the end of 2021, a business will be attacked by Ransomware every 11 seconds"

– Cyber Security Ventures Oct '19

Ransomware is pervasive, pernicious, and unfortunately very popular. A combination of "ransom" and "malware," it has grown over the years to become one of the world's greatest threats to data integrity. On average, ransomware affects one in four U.S. companies, with global attacks happening every 11 seconds.

Ransomware can penetrate systems designed to identify malware because it uses advanced obfuscation techniques, such as dead-code insertion, encryption, and runtime decoding. Post infection, it is vital to detect and remediate immediately to keep the infection from completely compromising your systems. This is even more urgent in larger datacenters.

There is no single action, software solution, or security control that can completely safeguard your organization from the threat of ransomware. Much like other cyber threats, the best solution is a multi-layered approach, commonly called a "defense in depth" strategy. A comprehensive strategy should include Nutanix built-in capabilities working alongside controls and safeguards that may already exist in your datacenter. In this Nutanix Tech Brief, we outline Nutanix capabilities, industry best practices, and techniques to incorporate into your cybersecurity defense strategies for preventing and recovering from ransomware when using a private cloud built on Nutanix.



NUTANIX™

The Cybersecurity and Infrastructure Security Agency (CISA) provides extensive information on understanding Malware and ransomware and best practices in combating attacks

www.us-cert.gov/Ransomware

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

PREVENT

Stopping an attack before any damage can occur is always the best possible situation. Ransomware starts with common attack vectors, such as phishing via email or malicious web pages, or through known software vulnerabilities. Prevention is rooted in common security best practices:

- Change default passwords; enforce strong password policies
- Segment networks for operations, applications, and departments
- Block malware spread with network microsegmentation
- Use and maintain endpoint protection/antivirus to block malware
- Train your employees on cybersecurity awareness regularly!
- Restrict access to sensitive systems; authenticate and authorize people and services using role-based access control (RBAC)
- Update and patch regularly (OSs, hypervisors, firmware, BIOS)
- Follow modern guidance on passphrases and password management
- Scan regularly for Common Vulnerabilities and Exposures (CVEs)
- Leverage object storage with write once read many (WORM) features for backup images and other important data to protect their integrity and block encryption by ransomware

Some of the above recommendations, though simple in concept, can be difficult to achieve due to cost or existing architecture complexity. This is where Nutanix hyperconverged infrastructure (HCI) plays a key role. Nutanix not only simplifies storage and virtualization, it also has native features and functions that make implementing security best practices easier.

Nutanix AOS and Prism Management

Nutanix AOS, the core to our HCI, is hardened and secured using industry best practices and has built-in auditing and remediation of those configurations. Prism Central adds RBAC for HCI storage and virtualization, and supports identity and access management (IAM), which includes support for directory services and the use of multi-factor authentication. Tying this platform together is our "one-click" philosophy for full-stack management. All components of the platform are easy to patch and upgrade using Nutanix Lifecycle Manager (LCM).

Nutanix AHV and Flow Microsegmentation

Adopting AHV virtualization with Flow microsegmentation extends the above secure configuration and audits to the hypervisor layer. Flow provides network and application segmentation for virtual machines, which can limit the spread and impact of a ransomware infection.

Nutanix Objects

To ensure data cannot be locked by ransomware, Objects, an S3-compatible object storage solution, can create immutable storage buckets in WORM mode for key data and backup images.

NUTANIX

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

DETECT

Ransomware continues to be popular because it is effective. Established criminal organizations even offer ransomware as a service, while others have established malware-as-a-service derivatives for banking trojans, targeted eCrime, etc. Though the standard techniques to detect initial ransomware infection are not 100 percent effective, the activities caused by ransomware are likely to trip alarms if the right steps are taken.

Look for unusual or anomalous behavior – such as repeated failed authentications, an increase in network traffic, or a large volume of file updates and touchpoints.

- Leverage layer 7 threat detection tools like intrusion detection and prevention systems (IDS/ IPS) to identify spurious network activity.
- Use a consolidated security information and event management (SIEM) solution with real-time analysis of security events and logs and, if possible, orchestration capabilities.
- Employ network honey-pots to augment detection capability
- Leverage anomaly detection tools for resource usage and storage activity.

Nutanix AHV and Flow Service Insertion and Chaining

Traditional networking tools can have challenges operating in a virtual environment. To facilitate the use of virtual IPS/IDS or other network-based threat intelligence tools, Nutanix AHV and Flow support policy-based service insertion of network security and threat awareness tools from our ecosystem partners.

Files Analytics, Nutanix Prism Ops, and X-Play

Prism Ops provides insights and analytics that can alert on resource utilization anomalies. Nutanix Files includes an intelligent analytics engine that provides insight into file share activity and anomalies. When combined with the codeless automation of X-Play, alerts and events can trigger security operations to avoid a potential ransomware issue.

Security Information and Event Management (SIEM)

SIEM is not only a recommended best practice for early detection of malicious activity, it is also a great workload to run on Nutanix. Nutanix as a SIEM solution easily scales with your security needs, allowing you to store transactional hot data on our high-performance HCI storage, and place cold data on our S3 compliant object-store, Nutanix Objects.

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

RECOVER

Business continuity and disaster recovery (BCDR) plans are not just for natural disasters. Organizations must plan as if they will eventually be impacted by a ransomware attack with contingencies for the recovery of data and continued business operations.

Much like cyber defenses, recovery plans should be a layered approach that is based on business needs and required operations recovery times. Ideally, a clean snapshot from a time just before the ransomware infection will provide the quickest option to recover data. When snapshots are not available, restoration from the last backup cycle is the next logical option. Make sure that backups have not been corrupted.

Some general recovery best practices are:

- Create snapshot and replication plans to match your business recovery objectives
- Replicate data to one or more locations as part of a BCDR plan
- Follow the 3-2-1 rule for backup, which is to keep:
  - At least three (3) copies of your backups
  - Two (2) backup copies on different storage media
  - One (1) of those copies should be located offsite
- Use automation and frequently test recovery to ensure quick and reliable results

Resource Links

AOS Security Guide

A Security-First Approach

Data at Rest Encryption Simplified

Secure Citrix With Nutanix

Splunk on Nutanix

Nutanix Mine

Nutanix Xi Leap

Nutanix Flow

Secure Virtualization

NUTANIX FOR DISASTER RECOVERY

The Nutanix platform includes built-in disaster recovery functionality to create reliable BCDR plans.

Nutanix AOS

Starting with native snapshots for VM and file services and flexible replication options, AOS also includes comprehensive runbook automation and recovery options to meet any recovery SLA.

Xi Leap

No need to build your own recovery site. Leap is a cloud-based disaster recovery service. Easy setup and SLA configuration with failover, failback, and recovery plan testing.

Nutanix Mine for Backup

Leverage the availability and data protection of Nutanix as a target for your backup data. Mine is a turnkey secondary data backup and archiving solution powered by Nutanix platform partners. And because Mine uses the power and performance of the underlying Nutanix Distributed Storage Fabric, backup and recovery times can be minimized, which shortens downtime and required backup windows.

NUTANIX™

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 • 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) • "One-click" CVE patching, platform upgrades, and life cycle management • Firmware and BIOS upgrade management	✓		
Prism Central • Role-Based Access Control (RBAC)	✓		
Nutanix Calm • Application blueprints, automation, and life-cycle management to ensure consistent security configuration	✓		
Prism Ops with X - Play • Resource analytics and insights with anomaly detection • Codeless automation and event triggers		✓	
Nutanix Flow • Network segmentation and application microsegmentation • Integrated partner solutions for deep packet inspection and threat intelligence • Policy and event logging for SIEM integration	✓	✓	
Nutanix Files • File type blocking policies • File activity anomaly detection from Files Insights • ICAP support for antivirus integration	✓	✓	✓
Nutanix Objects • Immutable S3-compatible WORM storage for critical data and backups	✓		✓
Nutanix Mine • Turnkey archive and backup solution for secondary storage with all the benefits of Nutanix HCI			✓
Xi Leap • Simplified cloud Disaster-Recovery-as-a-Service built for Nutanix			✓

NUTANIX™
YOUR ENTERPRISE CLOUD

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