COHESITY & NUTANIX PRESENT

Innovations

LEARNING SERIES

Building a Ransomware Defense in the New Era with Cohesity and Nutanix

Enhance Your Cyber Resilience with Complementary Solutions

Lawrence Miller

COHESITY | NUTANIX

POWERED BY ActualTech MEDIA

Building a Ransomware Defense in the New Era with Cohesity and Nutanix

By Lawrence Miller

TABLE OF CONTENTS

www.actualtechmedia.com

Publisher's Acknowledgements

EDITORIAL DIRECTOR
Keith Ward

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

ABOUT THE AUTHOR

Lawrence Miller, CISSP, is an information security professional with more than 20 years of professional experience in various industries. He has written more than 200 books on a variety of information technology and security topics.

Introduction

Welcome to Building a Ransomware Defense in the New Era with Cohesity and Nutanix!

Whether you're a business or IT executive, IT or data protection administrator, or a security architect or engineer, protecting your organization's data from the scourge of ransomware is no doubt a top priority.

Data is a key competitive differentiator in the digital economy and has quickly become the most important asset for modern enterprises.

This guide will help you understand the scale and impact of ransomware attacks, how ransomware has evolved and become more sophisticated, and how Nutanix and Cohesity work together to help customers defend against ransomware with a comprehensive, fully integrated solution to manage, protect, secure, and store your valuable data.

Ransomware: It's a Matter of "When," Not "If"

Data is a key competitive differentiator in the digital economy and has quickly become the crown jewel for modern enterprises. As such, data is increasingly targeted by cybercriminals in ransomware attacks. Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion U.S. dollars annually by 2025 and that a business will fall victim to a ransomware attack every 2 seconds by 2031. Thus, it's practically a matter of "when," not "if" your organization will be targeted.

In February 2023, VMware ESXi hypervisors were targeted by attacks designed to deploy ransomware by taking advantage of an OpenSLP (Service Location Protocol) heap-overflow vulnerability that potentially allows remote code execution. Ransomware attacks leveraging this vulnerability were detected globally, particularly in Europe, beginning in December 2022.

Ransomware Attackers Are Getting Creative …

General awareness of digital extortion schemes is rising as ransomware has unfortunately become part of our modern cybersecurity reality. Sensational reports of ransomware crippling critical supply chain infrastructure, medical facilities, public schools, and local municipalities are all too common. But ransomware attackers are quickly adopting and evolving their tactics to successfully target an endless supply of victim organizations. Examples of these evolving methods include:

- **Ransomware as a Service (RaaS).** Practically anyone can now use ransomware to attack an organization leveraging RaaS. Like Software as a Service (SaaS), RaaS offers threat actors with little to no skill the simplicity of a turnkey ransomware campaign, complete with malware delivery, encryption, payment collection, and decryption services. The threat actor pays a nominal licensing fee or commission to the RaaS service and can even get technical support to guide the threat actor throughout the execution of the attack.
- **Double- and triple-extortion attacks.** Encrypting valuable data is a key characteristic of ransomware, but ransomware attacks themselves have diversified—and it's not only about encryption anymore. In a double extortion attack, ransomware attackers exfiltrate a copy of your data before encrypting your original data, then demand an additional ransom to not publish your data on the Dark Web. In a triple extortion attack, the attacker may demand yet another ransom payment under threat of further damage to the victim organization vis-à-vis a denial-of-service (DoS) attack. Alternatively, the attacker may directly

target individuals whose data they have compromised for smaller ransom payments in exchange for not publishing their private information on the dark web.

… And Stealthy, Too

Although it may seem that ransomware attacks "just happen," there's actually a lot of planning and execution that goes into an attack well before the victim receives the telltale ransom demand on their monitor.

While enterprises are rapidly modernizing their IT production environments, on-premises and in the public cloud, their reliance on legacy backup products puts their data at risk.

Ransomware attackers have adopted the "low-and-slow" tactics of highly organized threat actor groups and advanced persistent threats (APTs) to identify and reconnoiter targets weeks or months in advance of delivering their ransomware payload. After gaining access to the target environment, threat actors establish persistence, move laterally across the network, and identify additional targets including your last line of defense against ransomware—**your backups**.

Paying a ransom is costly, unpalatable, and in some cases, illegal, but without a secure and immutable backup of your valuable data, you may have very few options to get your data back.

The U.S. Federal Bureau of Investigation (FBI), U.S. Cybersecurity and Infrastructure Agency (CISA), and other agencies generally recommend not paying a ransom. However, the decision of whether or not to pay must be evaluated on a case-by-case basis considering factors such as the scale and scope of the attack, the value of the encrypted data, and your ability (or lack thereof) to rapidly restore your data from backups.

Sophisticated attacks increasingly target backup data and infrastructure. An attacker may simply encrypt or delete your backups, disable backup jobs, infect your backups with other malware, or render backup and recovery infrastructure inoperable.

While enterprises are rapidly modernizing their IT production environments, on-premises and in the public cloud, their reliance on legacy backup products puts their data at risk. Can your existing backup solution defend against sophisticated ransomware attacks, and if the worst happens, help reduce downtime and data loss with rapid recovery?

Complementary Solutions Enhance Cyber Resilience

Nutanix and Cohesity work together to help organizations significantly simplify primary storage, as well as backup and recovery operations, while reducing mass data fragmentation challenges by converging data silos across core, edge, and cloud locations.

With their hyperscale-inspired architectures, Nutanix and Cohesity help organizations manage, protect, secure, and store their ever-growing volumes of data, consolidating decades-old technology stacks into highly scalable cloud-first platforms.

The Nutanix and Cohesity solution helps organizations potentially reduce costs and cybersecurity exposure by reducing infrastructure and data footprints, and enabling over-extended IT teams to spend less time managing siloed infrastructure and more time focusing on other business-critical tasks. With their hyperscale-inspired architectures, Nutanix and Cohesity help organizations manage, protect, secure, and store their ever-growing volumes of data, consolidating decades-old technology stacks into highly scalable cloud-first platforms.

Nutanix AOS and AHV

The hypervisor is the foundation of modern IT. Virtual machines (VMs) and containers abstract applications from the underlying hardware so that they can be dynamically provisioned, upgraded, and managed at scale. This paradigm is central across both traditional enterprise IT as well as modern cloud-native applications, but until recently these two delivery models were siloed.

Cohesity integrations with Nutanix AOS and AHV offer a simple and more efficient backup and disaster recovery solution.

The Nutanix AOS Storage™ infrastructure is a core component of the Nutanix Cloud Platform™ solution. A key component of the Nutanix solution is the Nutanix AHV® hypervisor, an enterprise-class native virtualization solution that bridges the silos between traditional enterprise IT and modern cloud-native applications. AHV is built on an open source foundation extended with advanced enterprise features, and integrated into a hyperconverged infrastructure (HCI) framework with built-in storage and networking capabilities for a complete, seamless solution.

With simple and intuitive provisioning and management of VMs, containers, business-critical applications, and cloud-native operations and workloads, AHV enables a

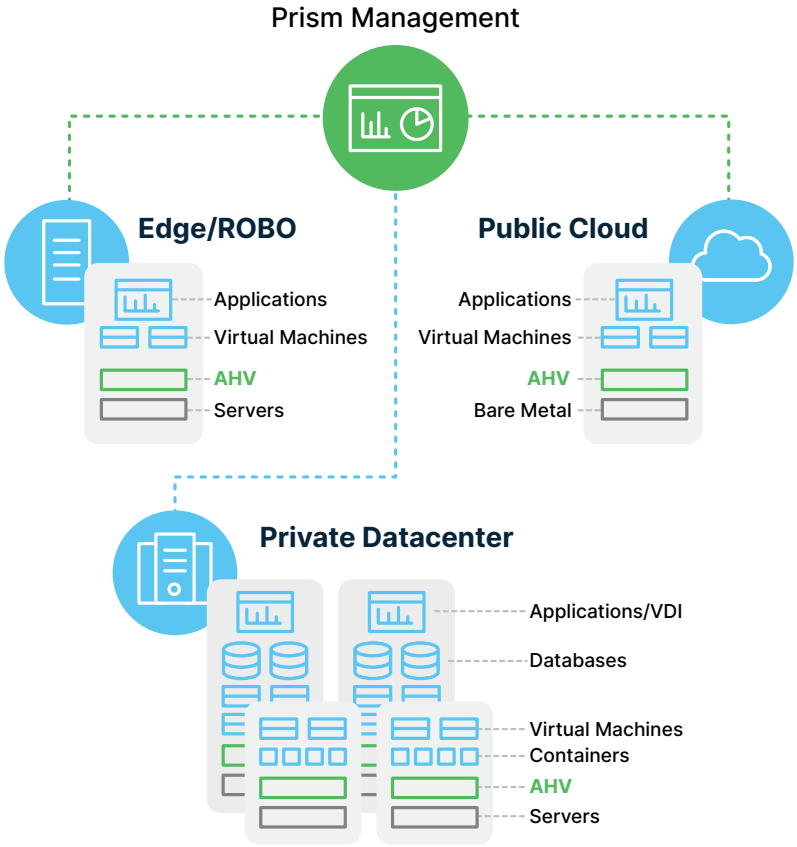

Figure 1: Nutanix AHV powers the hybrid cloud

consistent hybrid cloud operating model across datacenters, the edge, and public clouds (see **Figure 1**).

Nutanix AHV is a comprehensive enterprise virtualization solution that delivers the features required to securely run and protect enterprise applications, including:

- Combined VM operations and performance monitoring via the Nutanix Prism® control plan
- Backup, disaster recovery, host and VM high availability

- Dynamic scheduling (intelligent placement and resource contention avoidance)
- Broad ecosystem support (Certified Citrix Ready, Microsoft Validated via Server Virtualization Validation Program [SVVP])

Next-Gen Data Management and Protection

Cohesity provides a web-scale solution that simplifies and automates enterprise backup and data management—a perfect complement to the Nutanix AHV environment. It delivers a modern approach to protecting data against natural or human threats.

Cohesity effectively counters ransomware attacks and helps your organization avoid paying the ransom. Cohesity's comprehensive, next-gen data management solution features a multi-layered approach to protect backup data against ransomware, as well as detect and rapidly recover from an attack. Cohesity's Zero Trust data security architecture helps you mitigate risks from insider threats and compromised user credentials with role-based access control (RBAC), multi-factor authentication (MFA), and quorum approval to prevent unilateral administrative changes.

Cohesity's unique immutable architecture ensures that your backup data cannot be encrypted, modified, or deleted. Immutable backup snapshots and write-once read-many (WORM) DataLock capability help protect backup data from being modified or deleted. Using machine learning, it provides visibility and continuous monitoring for any anomalies in your data. And if the worst happens, Cohesity helps to locate

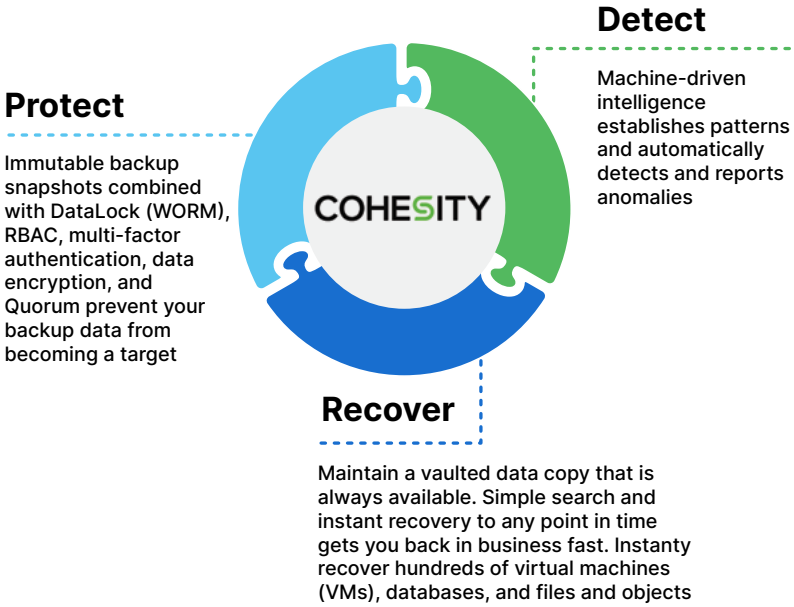

Figure 2: Cohesity delivers comprehensive capabilities to protect, detect, and recover from a ransomware attack

a clean copy of data across your global footprint, including public clouds, to instantly recover and reduce downtime (see **Figure 2**).

Cohesity's Nutanix Ready ransomware solutions deliver crucial backup security capabilities including:

- **Immutable snapshots.** Software-based, native immutable backup snapshots effectively defend against ransomware attacks because they can't be encrypted, modified, or deleted—all common tactics cybercriminals use to force a ransomware payment. This is extremely important for protecting the authenticity of data, particularly massive amounts of unstructured data, such as

audio and video files, as well as images required in certain industries such as law enforcement and healthcare. Unlike hardware-based immutability, the native read-only snapshots housed onsite or in clouds are never exposed or mounted externally to any application; they can't be tampered with, altered, or removed. That makes it hard for malware to target your backup data.

- **WORM.** Mechanisms such as WORM technology provide another layer of protection against a ransomware attack. They allow teams to create and apply a time-bound lock on data through policies and then assign them to selected jobs to enhance immutability for protected data. As this is a protection that even admins can't modify or delete, you don't have to worry as much about potential insider threats.

- **Data encryption.** There's encryption and then there's software-based Federal Information Processing Standards (FIPS)-validated, Advanced Encryption Standard (AES)-256 standard encryption for data in flight and at rest. You want the cryptographic module validated by the United States National Institute of Standards and Technology (NIST) at the FIPS 140-2 Level 1 standard. FIPS 140-2 is a U.S. government standard for cryptographic modules providing assurances that the module design and implementation of cryptographic algorithms are secure and correct, and FIPS-validated solutions must pass a rigorous set of tests to be certified.

- **Configuration audit and scanning.** Your IT team is likely now operating many different systems and tools—all

with their own setups, policies, and management interfaces. The manual processes to run them often introduce avoidable human error. An automated system with guided scanning that audits various data security and access control settings helps you avoid costly human mistakes while simplifying your data operations from setup to policies to management processes.

- **Fault tolerance.** Because data resilience should always be a guiding security principle, you also need a fault-tolerant system that helps ensure data integrity and successful backups. Look for a solution built with fault tolerance that allows backups to continue in spite of a failed component/node.

- **Modern and flexible cyber vaulting.** A companion consideration as you modernize your data management approach is updating your cyber vaulting strategy. Traditionally, organizations have relied on tapes to maintain air gapped copies, but that method can no longer keep up with today's demanding service-level agreements (SLAs) when it comes to recovery times—particularly those experienced during a widespread ransomware attack. Despite the term "air gap" protection now being widely misused to describe techniques that do not maintain an actual gap, don't be misled. Be sure your data security and management solution offer both real air gap protection as well as modern options to achieve cyber vaulting. These balance modern recovery time objective and recovery point objective (RTO/RPO) requirements with appropriate security controls by storing backup data in the cloud or at another location

with a temporary and highly secure connection. You then get a tamper-resistant environment, preventing ransomware and insider threat disruption while optimizing for meeting your organizational SLAs.

Cohesity integrations with Nutanix AOS and AHV offer a simple and more efficient backup and disaster recovery solution, which helps you achieve crash-consistent backups of your Nutanix AHV environment.

Key Benefits of Modern Backup and Recovery

Backups are your last line of defense against sophisticated and crippling ransomware attacks. Cohesity's comprehensive anti-ransomware solution is certified as Nutanix Ready™ and protects, isolates, detects, and most importantly, rapidly recovers to reduce downtime and ensure business continuity. Cohesity machine learning models proactively assess IT needs and automate infrastructure resources regularly, looking for anomalies to help identify potential ransomware attacks in progress in the IT production environment. Key benefits include:

- **Modern protection for Nutanix AHV environments.** Eliminate data silos by consolidating backup, disaster recovery, dev/test, and analytics workloads on-premises and in the public cloud into a single, multi-cloud data platform.

- **Simple backup and rapid recovery across sites.** Eliminate multiple point products and converge standalone backup software, target storage, proxy and media servers, and cloud gateways into a single, software-defined solution. Globally search VMs, files, and objects across core, edge, and cloud locations and recover to any point in time.
- **Integrated cybersecurity and protection against ransomware attacks.** Immutable backup snapshots, combined with WORM, RBAC, MFA, and data encryption (in flight and at rest), keeps backup data protected against sophisticated ransomware attacks.
- **Highly elastic and scalable, future-proof environment.** Boost agility and eliminate forklift upgrades with a web-scale architecture, enabling scale-out capacity, linear performance, and smooth data migration.
- **Deliver comprehensive cyber resilience.** Gain comprehensive data protection for a broad set of enterprise apps (traditional, cloud-native, SaaS), databases, network-attached storage (NAS), including the Nutanix Files™ software through support for Distributed File System - Referrals (DFS-R), and workloads running in virtual, physical, containerized, and cloud environments with unified management, reporting, and user experience in a single, global UI.
- **Unlock new business value.** Maximize data reuse to accelerate software development, testing, disaster recovery, analytics, and security. Minimize data movement by

running apps co-resident with data, lowering risk, and improving productivity.

Learn More

As ransomware continues to proliferate, modern businesses have no choice but to build an effective ransomware defense

Backups are your last line of defense against sophisticated and crippling ransomware attacks.

to protect their valuable data. An immutable backup is critical to your ransomware defense strategy.

To learn more about ransomware defense and get help with your ransomware defense strategy, watch the "Building a Ransomware Defense in the New Era" webinar and contact a Cohesity or Nutanix representative today.

About Nutanix + Cohesity

Nutanix, Inc. is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multi-cloud environments.

Cohesity radically simplifies data management no matter where your data lives—in multiple clouds, data centers, or at the edge. Cohesity uniquely delivers a wide-ranging set of data management capabilities, not by cobbling together tools but by fundamentally rethinking architecture.

With their hyperscale-inspired architectures, Nutanix and Cohesity have charted a new course in how organizations manage, protect, secure, and store their ever-growing volumes of data. Both companies have collapsed decades-old technology stacks into highly scalable cloud-first platforms.

About ActualTech Media

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.