SOLUTION BRIEF

Are you prepared for Ransomware?

Harden your datacenter to beef up your defenses.

KEY BENEFITS

- Protect data and prevent breaches
- Enable faster security validation and automated remediation
- Rich features to protect networks, applications, and data
- Simplify regulatory compliance efforts

> "We were after cost governance, and we accidentally got security governance with it."

– Declan Fleming, Enterprise Architect for Cloud, UCSD (Speaking about Nutanix Beam)

ARE YOU PREPARED TO FACE A RANSOMWARE ATTACK?

"YOUR FILES HAVE BEEN ENCRYPTED." Few messages can evoke more panic to computer users and IT staff. Unfortunately, these attacks are occurring with increasing frequency and sophistication. While there are no absolute defenses against malware and ransomware, there are means by which organizations can improve their defensive posture. In this report, we'll look at three areas of focus - end user compute, shared document storage, and data center compute - and how Nutanix can help you fortify your defenses.

DEFINITIONS

Malware is shorthand for Malicious Software, and is a blanket term for software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Ransomware is a special category of malware designed to block access to a computer system until a sum of money is paid. Known for attacking consumers who may not be tech-savvy, ransomware is increasingly targeting entire businesses, agencies and institutions. Attacks are becoming more sophisticated and coordinated.

A malware/ransomware infection can be very hard to detect. Most attacks enter the environment through phishing emails or social media with weblinks or malicious code embedded in attachments that when accessed, install the malware onto then system. However, insider threats, such as the recent Capital One attack must also be considered. Typically, the code will do some reconnaissance to gather any useful information it can send back to home servers for further exploitation of other systems on the network . It will then trigger it's intended payload (i.e. encrypting connected drives), warning the user to pay a ransom to recover, then covering its tracks by deleting itself. This a criminal activity, and paying a ransom is no guarantee that the perpetrators will honor the promise to remove the harmful code and return the systems to a pre-infected state.

NUTANIX™

RESOURCES AND GETTING STARTED

- A Security-First Approach to Datacenter Modernization: http://bit.ly/2pZCUQQ
- Data at Rest Encryption Simplified: http://bit.ly/35nCqnB

The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security has extensive information on understanding malware/ransomware and best practices in combating attacks - such as keeping software versions and security patches up to date, and having established backup and disaster recovery systems. (Please refer to https://www.us-cert.gov/Ransomware).

This paper focuses on how Nutanix can help organizations harden their datacenters to mitigate these security threats.

PREVENTION

End User Systems

In keeping with CISA's guidance, virtualizing end-user computing environments is a best practice to ease keeping system and security software up-to-date. Nutanix can help with industry leading solutions for End User Computing (EUC) which include traditional Virtual Desktop Infrastructure (VDI) and Desktop-as-a-Service (DaaS). (See https://www.nutanix.com/solutions/end-user-computing)

Shared Document Storage and Server Compute

Basic concepts here are controlling access, reducing the attack surface and protecting high value data. Security in the enterprise datacenter must begin with a robust infrastructure foundation. This is where industry leading hyper-converged infrastructure (HCI) from Nutanix not only provides operational and financial value, but also aids in improving security posture and preventing data breaches. It is important that security is fundamentally ingrained in the infrastructure from design to operation.

- Secure Development: 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 – avoiding difficult tradeoffs between security and performance or features. 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.
- Operational Capabilities: The Nutanix Acropolis Operating System (AOS) and Xi Cloud Services contain many features and functions that can be used to secure datacenter infrastructure:
  - Security Configuration Baselines: Nutanix AOS delivers a hardened enterprise cloud environment with custom security baseline documents following recommendations from the United States Department of Defense (DoD) Security Technical Implementation Guides (STIGs) and based on common National Institute of Standards and Technology (NIST) standards.
  - SecOps - Automated Validation and Self-Healing: Nutanix baselines are published in a machine-readable format, allowing for automated validation and continuous monitoring of the security baseline for compliance.

Nutanix has implemented Security Configuration Management Automation (SCMA) to efficiently check security entities in the security baselines that cover both HCI and AHV 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).

- Enterprise Authentication: Through support for the open SAML standard, Nutanix Prism Central provides various methods to integrate with multi-factor authentication mechanisms and Common Access Card (CAC) schemes.

- Role Based Access Control (RBAC): Nutanix Prism Central allows the creation of customer roles based on attributes, managed objects and permitted administrative tasks, giving administrator granular control over configuration and VM provisioning activities.

- Native Data at Rest Encryption: As a native HCI option, encryption can be enabled to secure sensitive data and eliminate the risk of data loss. AOS delivers built-in FIPS compliant software-based encryption that delivers security without compromise to storage efficiency or performance. Furthermore, AOS simplifies the end-to-end solution with a built-in native Key Management Server (KMS) and supports 3rd party Enterprise KMS using KMIP for organizations that have a preference or have a regulatory compliance need.

- Self-Encrypting Drives (SEDs): AOS also supports SEDs for organizations that require FIPS 140-2 Level 2 compliance.

- Network Security: With Nutanix Flow, microsegmentation based application security can be quickly implemented and automated to ensure only desired traffic is allowed inside the datacenter. Microsegmentation prevents lateral spread of network-based attacks and can limit the scope and impact of security breaches. Flow includes environment isolation to ensure complete segmentation between application environments without the need for complex configurations, and application tier segmentation to restrict communication between applications such that only necessary communication is permitted.

- Multi-Cloud: As IT consumption expands to include public cloud and SaaS components, security controls become much harder to maintain. Xi Beam provides continuous cloud security and compliance for multi-cloud environments with one-click remediation for cloud vulnerabilities. Beam provides insights into security vulnerabilities in real-time so that you can resolve potential threats before they turn into business challenges. With Beam you can audit and maintain cloud security compliance for HIPAA, ISO, PCI-DSS, CIS, NIST and SOC-2, enforce custom policies and audits or leverage the 250+ built in security checks based on industry best practices.

DETECTION - EXAMPLE USE CASE

A standard technique to detect a malware/ransomware event in progress is to look for unusual behavior – such as an unusually high level of attempted file accesses. In addition to bespoke security tools such as Bitdefender, Nutanix Files customers can use its monitoring and analytics capabilities to identify such anomalous behavior. Upon identifying a suspected bad actor, Nutanix Flow microsegmentation can be triggered to quarantine the suspect virtual machine for isolation and further interrogation, limiting the spread of malware.

RECOVERY

Once systems are encrypted or otherwise compromised, the best recourse is to revert to a pre-infected state. This is where a Backup/Disaster Recovery (DR) plan is critical. Nutanix Mine (backup) and Xi Leap (Disaster Recovery) are simple to implement and manage, providing an offsite instance with the only connection being the management plane and the copy process, making isolation easy and secure. A proper Backup/DR plan will minimize the amount of data loss and downtime caused by a ransomware event.

CONCLUSION

Complexity is the enemy of security. By taking a holistic view of hyper-converged compute, storage, and networking infrastructure with built-in security and intelligent automation, Nutanix has simplified complex datacenter operations and protection. Our scalable systems are used by small cities and school districts, as well as the largest government agencies and commercial enterprises. Let us show you how we can modernize your IT environments, and give you peace of mind that you are well-prepared to battle security threats.

NUTANIX™
YOUR ENTERPRISE CLOUD

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