FlexPod and Security

FlexPod

NetApp
March 25, 2024

Table of Contents

FlexPod and Security

FlexPod, The Solution to Ransomware

TR-4802: FlexPod, The Solution to Ransomware

Arvind Ramakrishnan, NetApp

In partnership with:

To understand ransomware, it is necessary to first understand a few key points about cryptography. Cryptographical methods enable the encryption of data with a shared secret key (symmetric key encryption) or a pair of keys (asymmetric key encryption). One of these keys is a widely available public key and the other is an undisclosed private key.

Ransomware is a type of malware that is based on cryptovirology, which is the use of cryptography to build malicious software. This malware can make use of both symmetric and asymmetric key encryption to lock a victim's data and demand a ransom to provide the key to decrypt the victim's data.

How does ransomware work?

The following steps describe how ransomware uses cryptography to encrypt the victim's data without any scope for decryption or recovery by the victim:

1. The attacker generates a key pair as in asymmetric key encryption. The public key that is generated is placed within the malware, and the malware is then released.
2. After the malware has entered the victim's computer or system, it generates a random symmetric key by using a pseudorandom number generator (PRNG) or any other viable random number- generating algorithm.
3. The malware uses this symmetric key to encrypt the victim's data. It eventually encrypts the symmetric key by using the attacker's public key that was embedded in the malware. The output of this step is an asymmetric ciphertext of the encrypted symmetric key and the symmetric ciphertext of the victim's data.
4. The malware zeroizes (erases) the victim's data and the symmetric key that was used to encrypt the data, thus leaving no scope for recovery.
5. The victim is now shown the asymmetric ciphertext of the symmetric key and a ransom value that must be paid in order to obtain the symmetric key that was used to encrypt the data.
6. The victim pays the ransom and shares the asymmetric ciphertext with the attacker. The attacker decrypts the ciphertext with his or her private key, which results in the symmetric key.
7. The attacker shares this symmetric key with the victim, which can be used to decrypt all the data and thus recover from the attack.

Challenges

Individuals and organizations face the following challenges when they are attacked by ransomware:

- The most important challenge is that it takes an immediate toll on the productivity of the organization or the individual. It takes time to return to a state of normalcy, because all the important files must be regained, and the systems must be secured.
- It could lead to a data breach that contains sensitive and confidential information that belongs to clients or customers and leads to a crisis situation that an organization would clearly want to avoid.
- There is a very good chance of data getting into the wrong hands or being erased completely, which leads to a point of no return that could be disastrous for organizations and individuals.
- After paying the ransom, there is no guarantee that the attacker will provide the key to restore the data.
- There is no assurance that the attacker will refrain from broadcasting the sensitive data in spite of paying the ransom.
- In large enterprises, identifying the loophole that led to a ransomware attack is a tedious task, and securing all the systems involves a lot of effort.

Who is at risk?

Anyone can be attacked by ransomware, including individuals and large organizations. Organizations that do not implement well- defined security measures and practices are even more vulnerable to such attacks. The effect of the attack on a large organization can be several times larger than what an individual might endure.

Ransomware accounts for approximately 28% of all malware attacks. In other words, more than one in four malware incidents is a ransomware attack. Ransomware can spread automatically and indiscriminately through the internet, and, when there is a security lapse, it can enter into the victim's systems and continue to spread to other connected systems. Attackers tend to target people or organizations that perform a lot of file sharing, have a lot of sensitive and critical data, or maintain inadequate protection against attacks.

Attackers tend to focus on the following potential targets:

- Universities and student communities
- Government offices and agencies
- Hospitals
- Banks

This is not an exhaustive list of targets. You cannot consider yourself safe from attacks if you fall outside of one of these categories.

How does ransomware enter a system or spread?

There are several ways in which ransomware can enter a system or spread to other systems. In today's world, almost all systems are connected to one another other through the internet, LANs, WANs, and so on. The amount of data that is being generated and exchanged between these systems is only increasing.

Some of the most common ways by which ransomware can spread include methods that we use on a daily basis to share or access data:

- Email
- P2P networks
- File downloads
- Social networking
- Mobile devices

- Connecting to insecure public networks
- Accessing web URLs

Consequences of data loss

The consequences or effects of data loss can reach more widely than organizations might anticipate. The effects can vary depending on the duration of downtime or the time period during which an organization doesn't have access to its data. The longer the attack endures, the bigger the effect on the organization's revenue, brand, and reputation. An organization can also face legal issues and a steep decline in productivity.

As these issues continue to persist over time, they begin to magnify and might end up changing an organization's culture, depending on how it responds to the attack. In today's world, information spreads at a rapid rate and negative news about an organization could cause permanent damage to its reputation. An organization could face huge penalties for data loss, which could eventually lead to the closure of a business.

Financial effects

According to a recent McAfee report, the global costs incurred due to cybercrime are roughly $600 billion, which is approximately 0.8% of global GDP. When this amount is compared against the growing worldwide internet economy of $4.2 trillion, it equates to a 14% tax on growth.

Ransomware takes a significant share of this financial cost. In 2018, the costs incurred due to ransomware attacks were approximately $8 billion—an amount predicted to reach $11.5 billion in 2019.

What is the solution?

Recovering from a ransomware attack with minimal downtime is only possible by implementing a proactive disaster recovery plan. Having the ability to recover from an attack is good, but preventing an attack altogether is ideal.

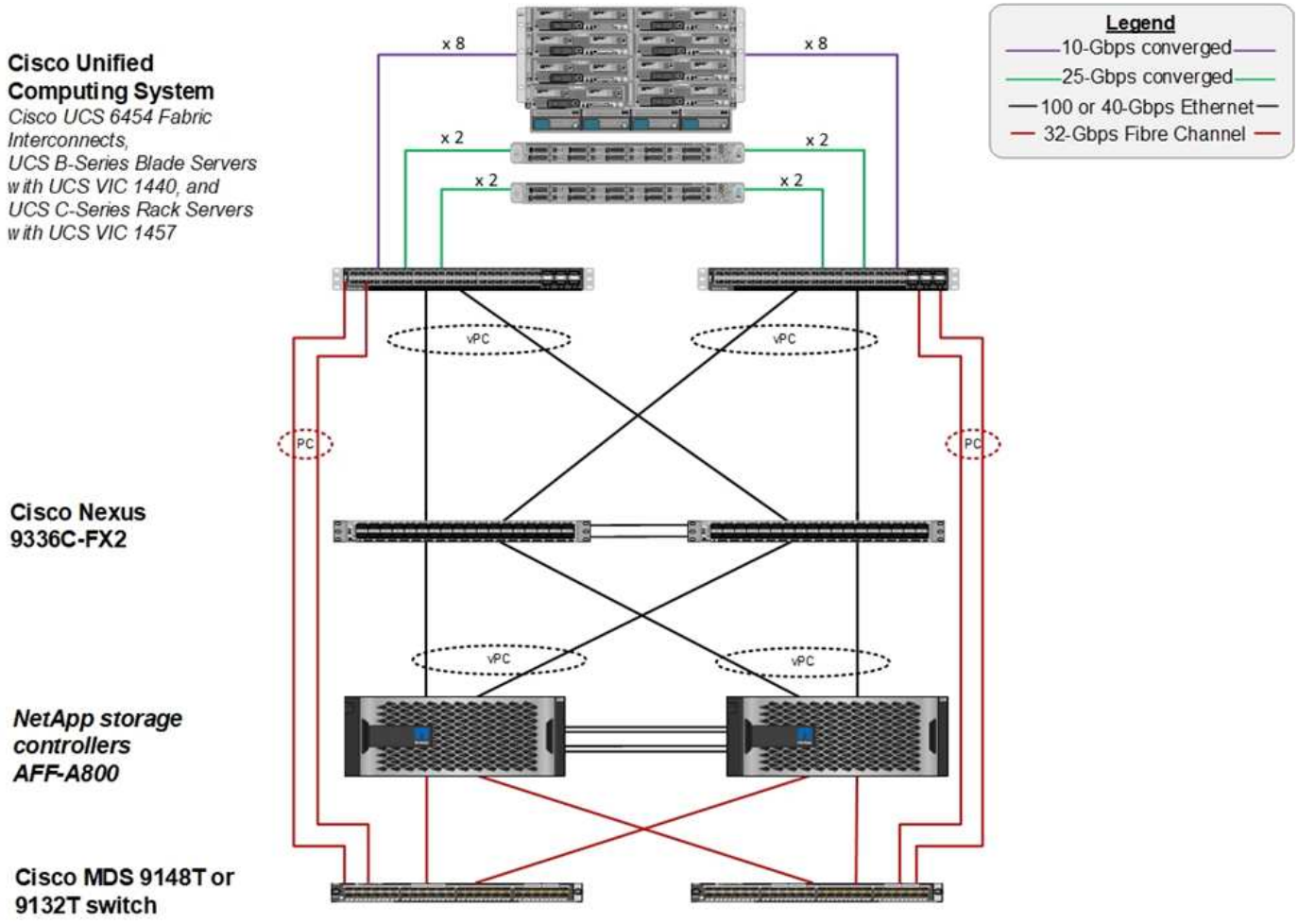
Although there are several fronts that you must review and fix to prevent an attack, the core component that allows you to prevent or recover from an attack is the data center.

The data center design and the features it provides to secure the network, compute, and storage end-points play a critical role in building a secure environment for day-to-day operations. This document shows how the features of a FlexPod hybrid cloud infrastructure can help in quick data recovery in the event of an attack and can also help to prevent attacks altogether.

FlexPod Overview

FlexPod is a predesigned, integrated, and validated architecture that combines Cisco Unified Computing System (Cisco UCS) servers, the Cisco Nexus family of switches, Cisco MDS fabric switches, and NetApp storage arrays into a single, flexible architecture. FlexPod solutions are designed for high availability with no single points of failure, while maintaining cost-effectiveness and design flexibility to support a wide variety of workloads. A FlexPod design can support different hypervisors and bare metal servers and can also be sized and optimized based on customer workload requirements.

The figure below illustrates the FlexPod architecture and clearly highlights the high availability across all the layers of the stack. The infrastructure components of storage, network, and compute are configured in such a way that the operations can instantaneously fail over to the surviving partner in case one of the components fail.



A major advantage for a FlexPod system is that it is predesigned, integrated, and validated for several workloads. Detailed design and deployment guides are published for every solution validation. These documents include the best practices that you must employ for workloads to run seamlessly on FlexPod. These solutions are built with the best- in-class compute, network, and storage products and a host of features that focus on security and hardening of the entire infrastructure.

IBM's X-Force Threat Intelligence Index states, "Human error responsible for two-thirds of compromised records including historic 424% jump in misconfigured cloud infrastructure."

With a FlexPod system, you can avoid misconfiguring your infrastructure by using automation through Ansible playbooks that perform an end-to-end setup of the infrastructure according to the best practices described in Cisco Validated Designs (CVDs) and NetApp Verified Architectures (NVAs).

Ransomware protection measures

This section discusses the key features of NetApp ONTAP data management software and the tools for Cisco UCS and Cisco Nexus that you can use to effectively protect and recover from ransomware attacks.

Storage: NetApp ONTAP

ONTAP software provides many features useful for data protection, most of which are free of charge to customers who have an ONTAP system. You can use the following features at all times to safeguard data from attacks:

- **NetApp Snapshot technology.** A Snapshot copy is a read-only image of a volume that captures the state of a file system at a point in time. These copies help protect data with no effect on system performance and, at the same time, do not occupy a lot of storage space. NetApp recommends that you create a schedule for the creation of Snapshot copies. You should also maintain a long retention time because some malware can go dormant and then reactivate weeks or months after an infection. In the event of an attack, the volume can be rolled back using a Snapshot copy that was taken before the infection.
- **NetApp SnapRestore technology.** SnapRestore data recovery software is extremely useful to recover from data corruption or to revert only the file contents. SnapRestore does not revert the attributes of a volume; it is much faster than what an administrator can achieve by copying files from the Snapshot copy to the active file system. The speed at which data can be recovered is helpful when many files must be recovered as quickly as possible. In the event of an attack, this highly efficient recovery process helps to get business back online quickly.
- **NetApp SnapCenter technology.** SnapCenter software uses NetApp storage-based backup and replication functions to provide application- consistent data protection. This software integrates with enterprise applications and provides application- specific and database- specific workflows to meet the needs of application, database, and virtual infrastructure administrators. SnapCenter provides an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. Its ability to provide application- consistent data protection is critical during data recovery because it makes it easy to restore applications to a consistent state more quickly.
- **NetApp SnapLock technology.** SnapLock provides a special purpose volume in which files can be stored and committed to a nonerasable, nonrewritable state. The user's production data residing in a FlexVol volume can be mirrored or vaulted to a SnapLock volume through NetApp SnapMirror or SnapVault technology, respectively. The files in the SnapLock volume, the volume itself, and its hosting aggregate cannot be deleted until the end of the retention period.
- **NetApp FPolicy technology.** Use FPolicy software to prevent attacks by disallowing operations on files with specific extensions. An FPolicy event can be triggered for specific file operations. The event is tied to a policy, which calls out the engine it needs to use. You might configure a policy with a set of file extensions that could potentially contain ransomware. When a file with a disallowed extension tries to perform an unauthorized operation, FPolicy prevents that operation from executing.

Network: Cisco Nexus

Cisco NX OS software supports the NetFlow feature that enables enhanced detection of network anomalies and security. NetFlow captures the metadata of every conversation on the network, the parties involved in the communication, the protocol being used, and the duration of the transaction. After the information is aggregated and analyzed, it can provide insight into normal behavior.

The collected data also allows identification of questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed.

NetFlow uses flows to provide statistics for network monitoring. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow. You can export the data that NetFlow gathers for your flows by using a flow exporter to a remote NetFlow collector, such as Cisco Stealthwatch. Stealthwatch uses this information for continuous monitoring of the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Compute: Cisco UCS

Cisco UCS is the compute endpoint in a FlexPod architecture. You can use several Cisco products that can help to secure this layer of the stack at the operating system level.

You can implement the following key products in the compute or application layer:

- **Cisco Advanced Malware Protection (AMP) for Endpoints.** Supported on Microsoft Windows and Linux operating systems, this solution integrates prevention, detection, and response capabilities. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

  The Malicious Activity Protection (MAP) component of AMP continually monitors all endpoint activity and provides run-time detection and blocking of abnormal behavior of a running program on the endpoint. For example, when endpoint behavior indicates ransomware, the offending processes are terminated, preventing endpoint encryption and stopping the attack.

- **Cisco Advanced Malware Protection for Email Security.** Emails have become the prime vehicle to spread malware and to carry out cyber-attacks. On average, approximately 100 billion emails are exchanged in a single day, which provides attackers with an excellent penetration vector into user's systems. Therefore, it is absolutely essential to defend against this line of attack.

  AMP analyzes emails for threats such as zero-day exploits and stealthy malware hidden in malicious attachments. It also uses industry-leading URL intelligence to combat malicious links. It gives users advanced protection against spear phishing, ransomware, and other sophisticated attacks.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS can be deployed as a physical appliance in the datacenter or as a virtual appliance on VMware (NGIPSv for VMware). This highly effective intrusion prevention system provides reliable performance and a low total cost of ownership. Threat protection can be expanded with optional subscription licenses to provide AMP, application visibility and control, and URL filtering capabilities. Virtualized NGIPS inspects traffic between virtual machines (VMs) and make it easier to deploy and manage NGIPS solutions at sites with limited resources, increasing protection for both physical and virtual assets.

Protect and recover data on FlexPod

This section describes how an end user's data can be recovered in the event of an attack and how attacks can be prevented by using a FlexPod system.

Testbed overview

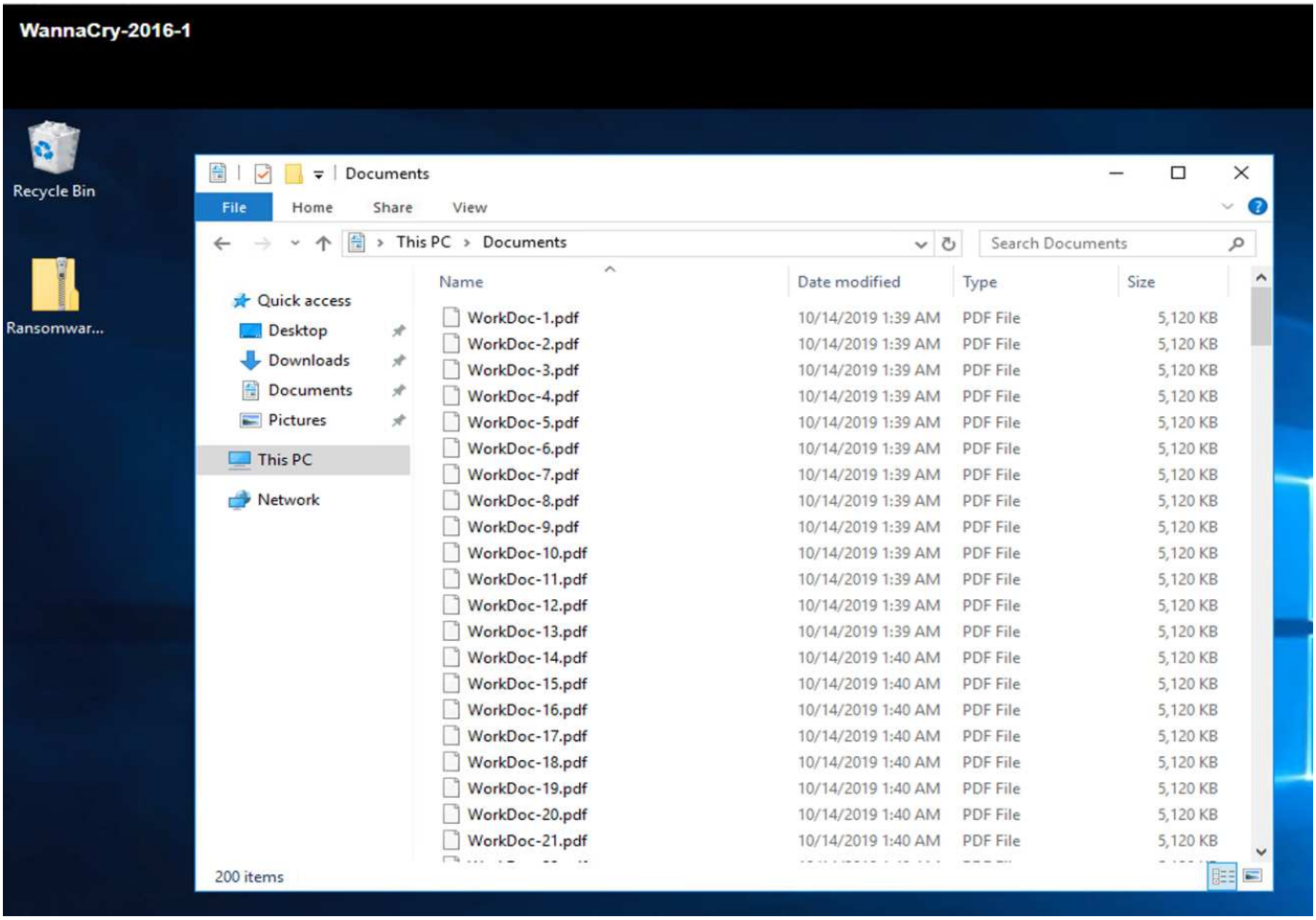
To showcase FlexPod detection, remediation, and prevention, a testbed was built based on the guidelines that are specified in the latest platform CVD available at the time this document was authored: FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS 4th Generation, and NetApp AFF A-Series CVD.

A Windows 2016 VM, which provided a CIFS share from NetApp ONTAP software, was deployed in the VMware vSphere infrastructure. Then NetApp FPolicy was configured on the CIFS share to prevent the execution of files with certain extension types. NetApp SnapCenter software was also deployed to manage the Snapshot copies of the VMs in the infrastructure to provide application- consistent Snapshot copies.

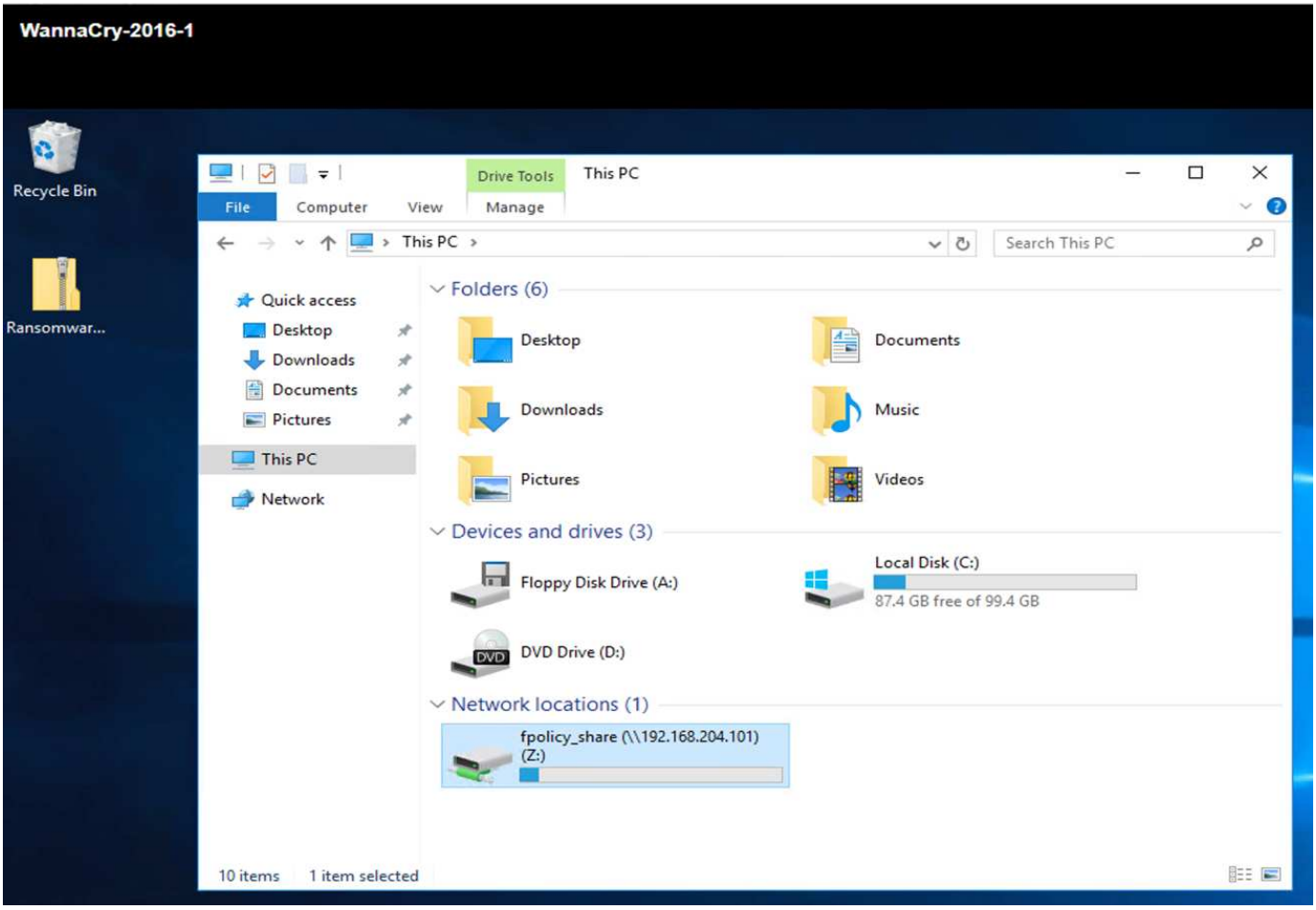
State of VM and its files prior to an attack

This section provides shows the state of the files prior to an attack on the VM and the CIFS share that was mapped to it.

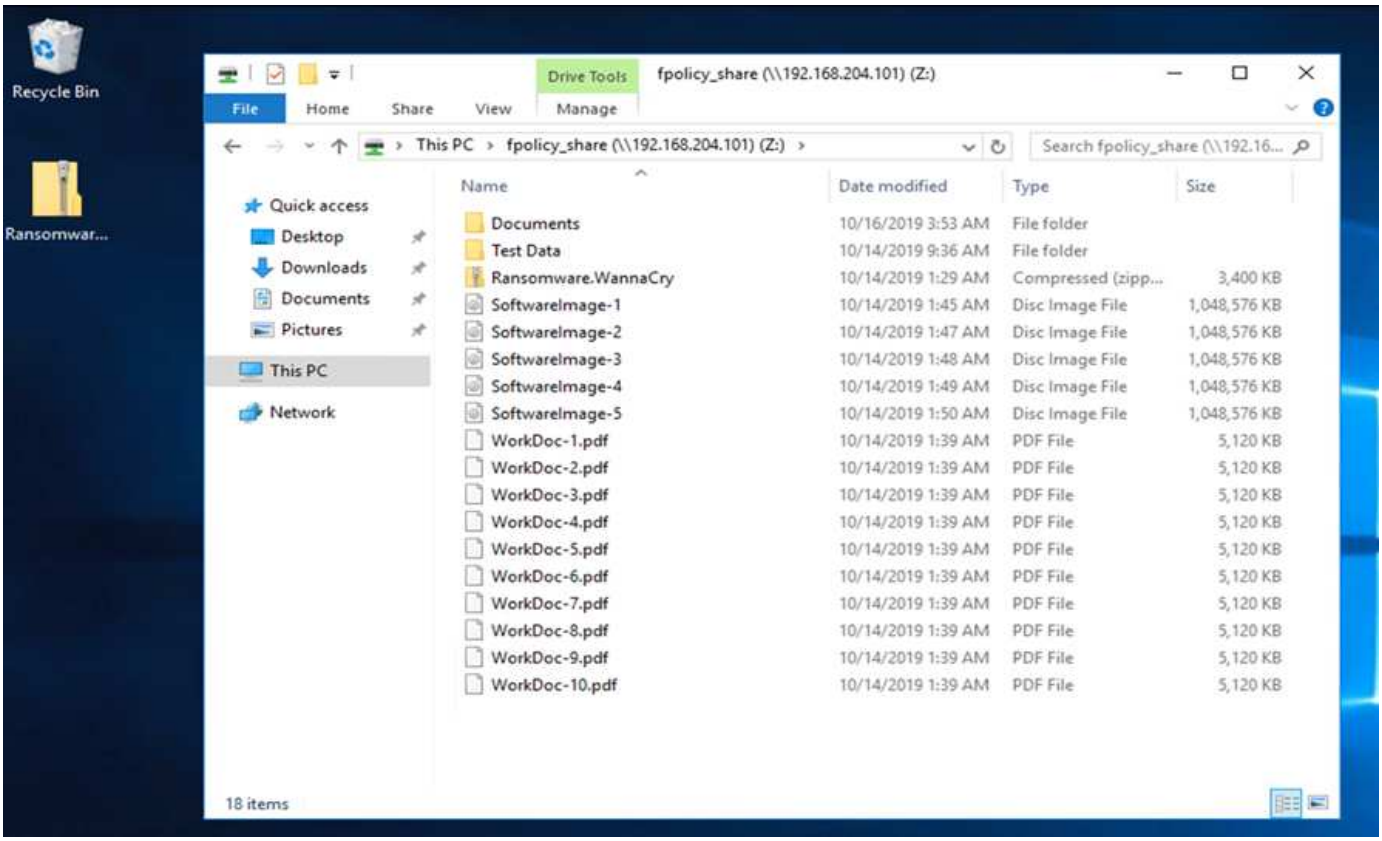
The Documents folder of the VM had a set of PDF files that have not yet been encrypted by the WannaCry malware.



The following screenshot shows the CIFS share that was mapped to the VM.



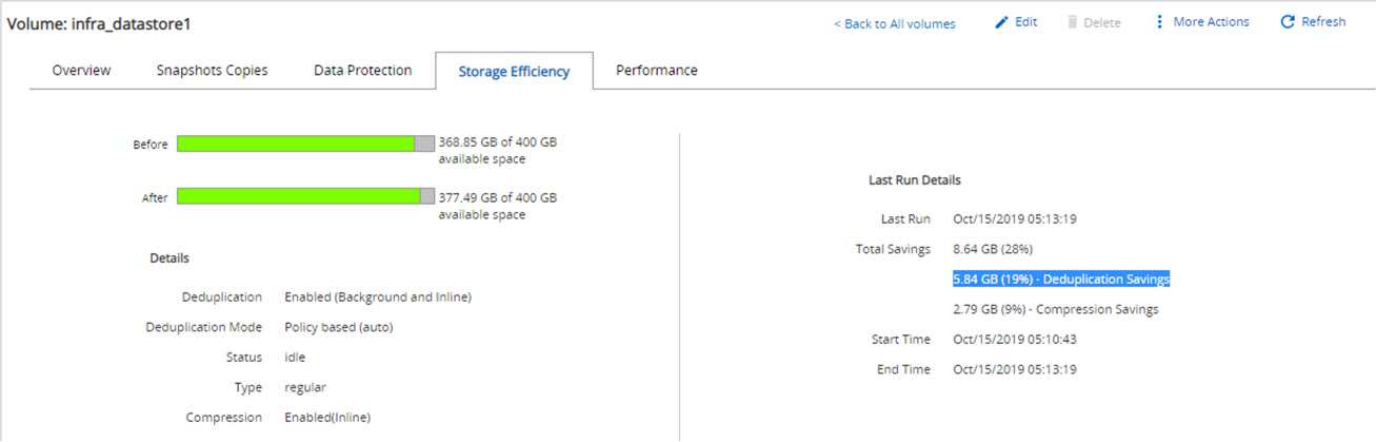
The following screenshot shows the files on the CIFS share `fpolicy_share` that have not yet been encrypted by the WannaCry malware.



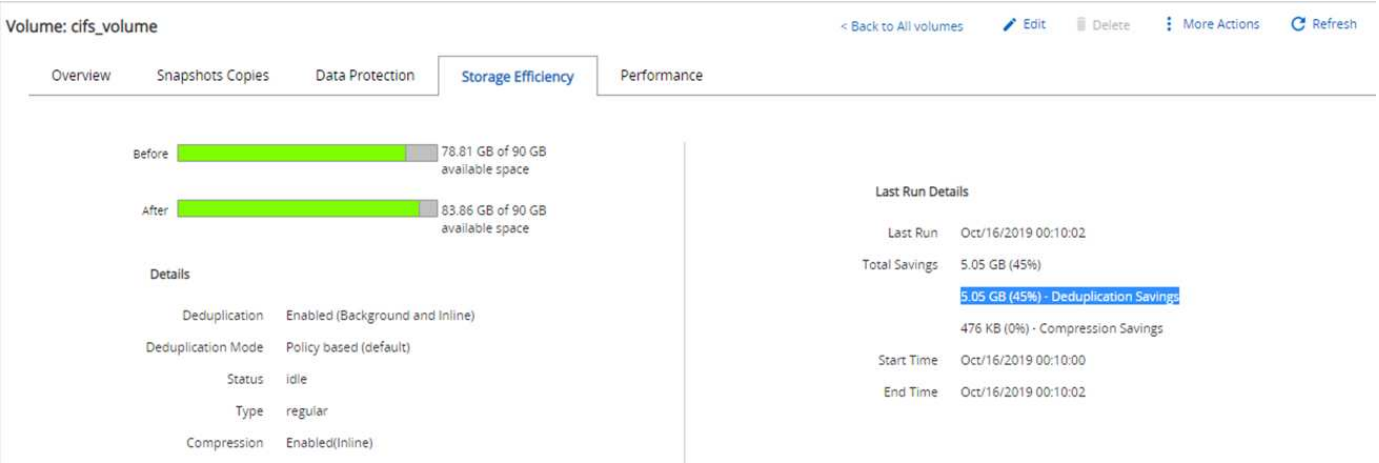
Deduplication and Snapshot information before an attack

The storage efficiency details and size of the Snapshot copy prior to an attack are indicated and used as a reference during the detection phase.

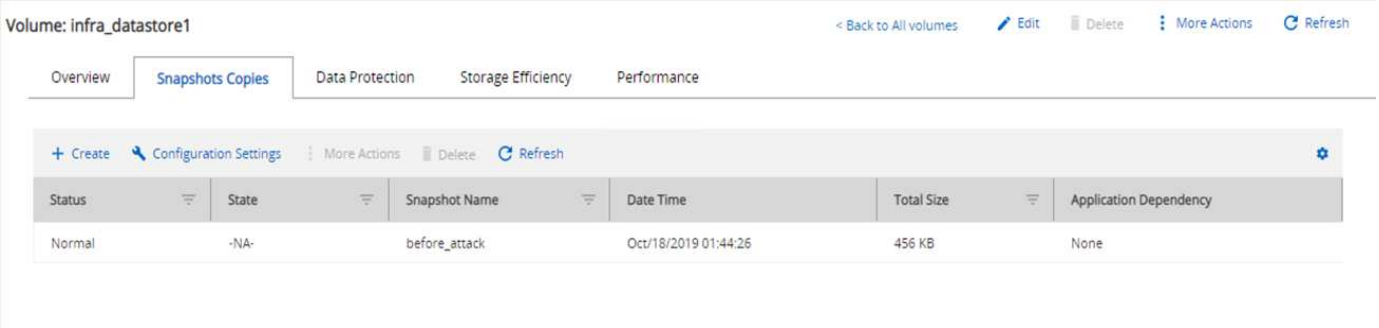
Storage savings of 19% were achieved with deduplication on the volume hosting the VM.



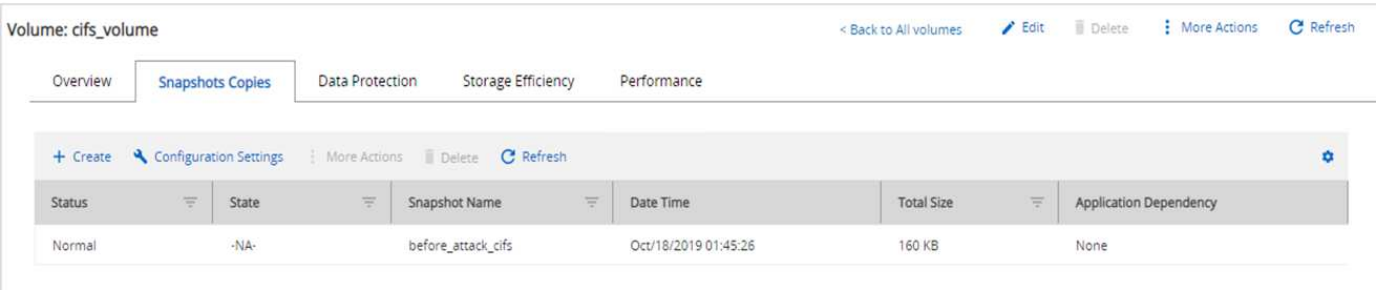
Storage savings of 45% were achieved with deduplication on the CIFS share `fpolicy_share`.



A Snapshot copy size of 456KB was observed for the volume hosting the VM.



A Snapshot copy size of 160KB was observed for the CIFS share `fpolicy_share`.



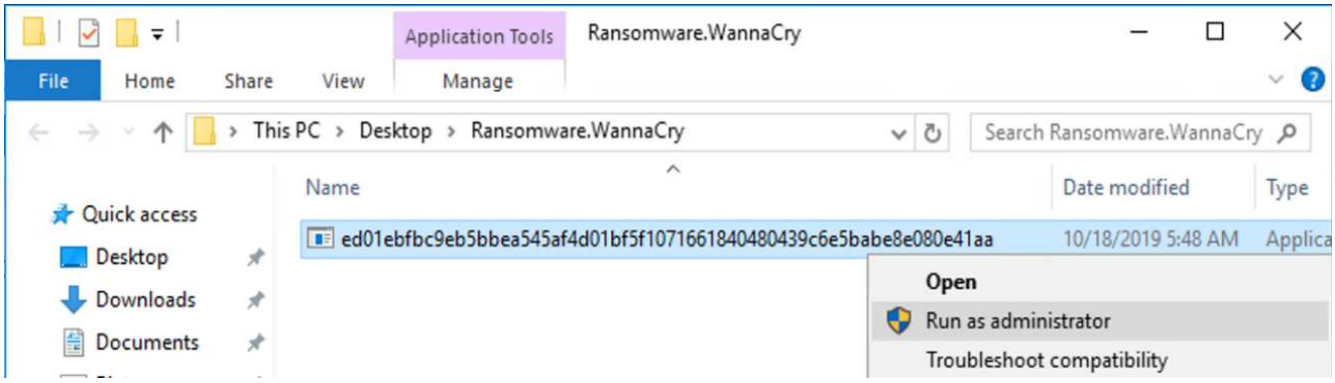
WannaCry infection on VM and CIFS share

In this section, we show how the WannaCry malware was introduced into the FlexPod environment and the subsequent changes to the system that were observed.

The following steps demonstrate how the WannaCry malware binary was introduced into the VM:

1. The secured malware was extracted.

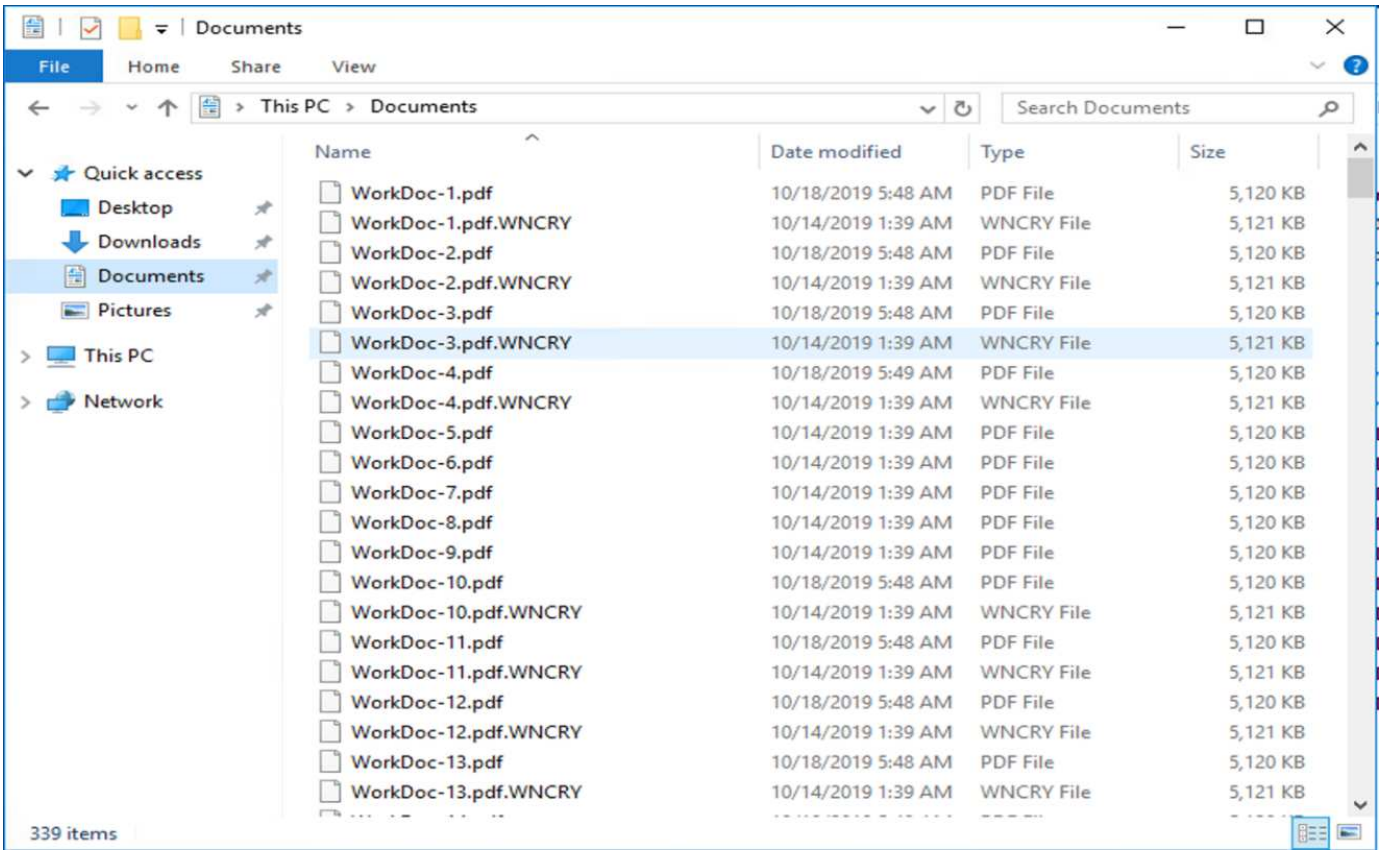
2. The binary was executed.



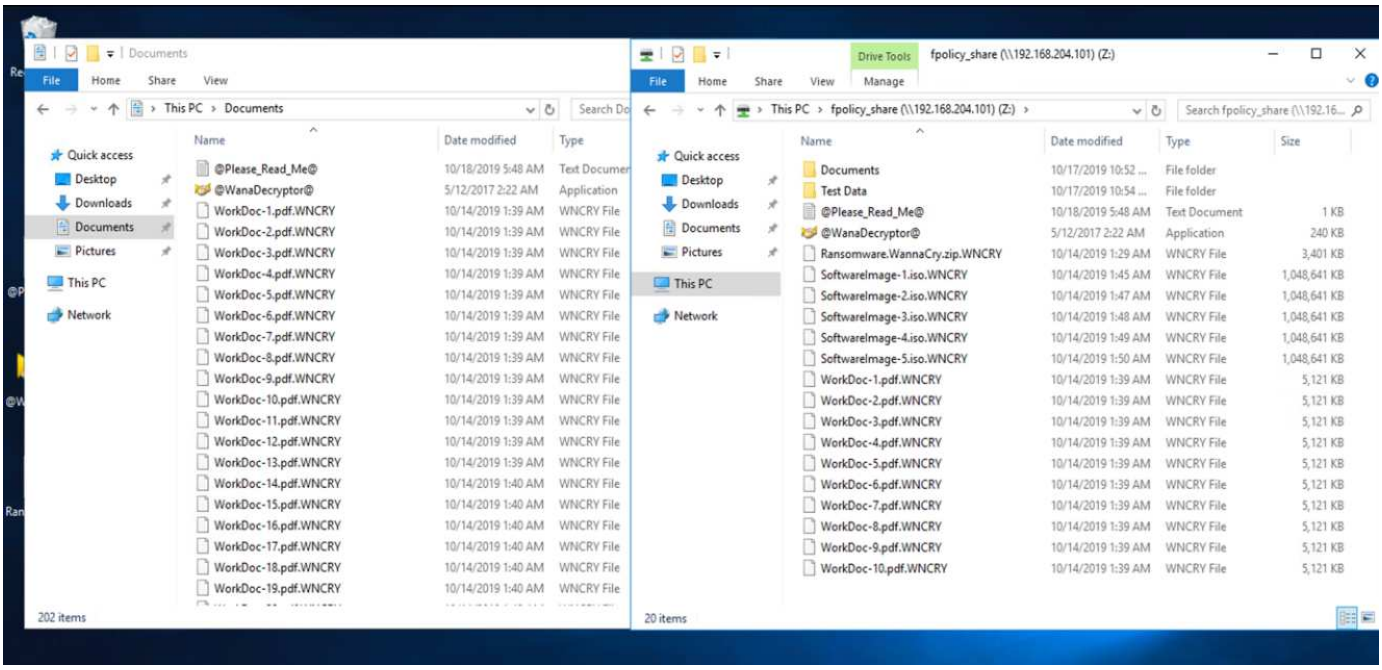
Case 1: WannaCry encrypts the file system within the VM and mapped CIFS share

The local file system and the mapped CIFS share were encrypted by the WannaCry malware.

Malware starts to encrypt files with WNCRY extensions.



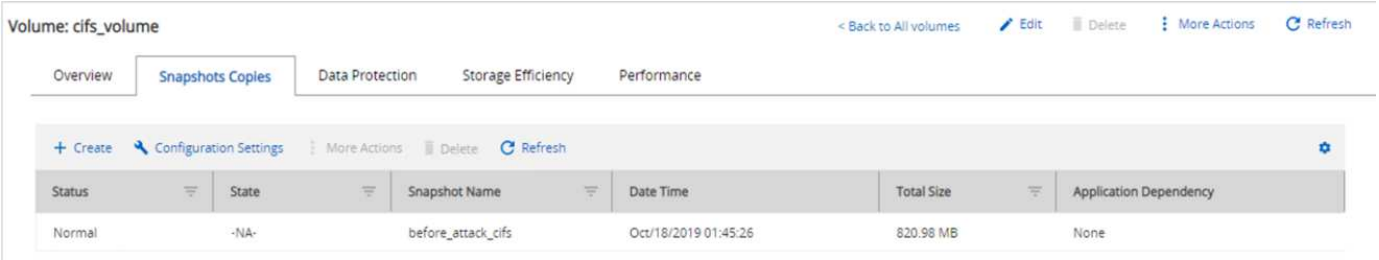
The malware encrypts all the files in the local VM and the mapped share.



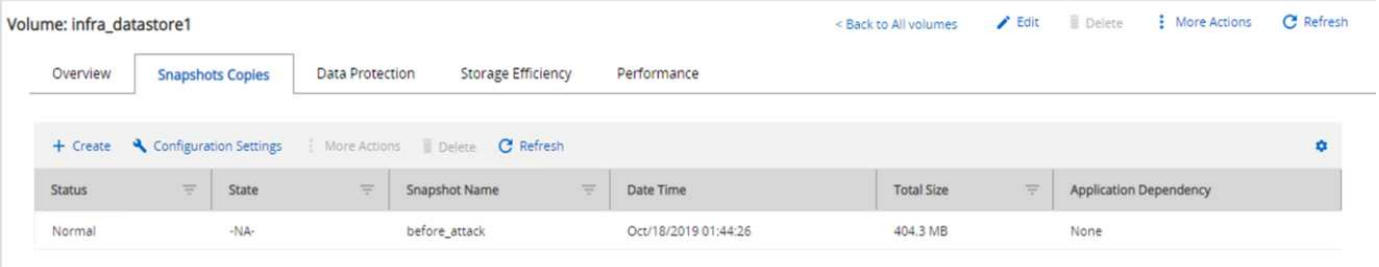
Detection

From the moment the malware started to encrypt the files, it triggered an exponential increase in the size of the Snapshot copies and an exponential decrease in the storage efficiency percentage.

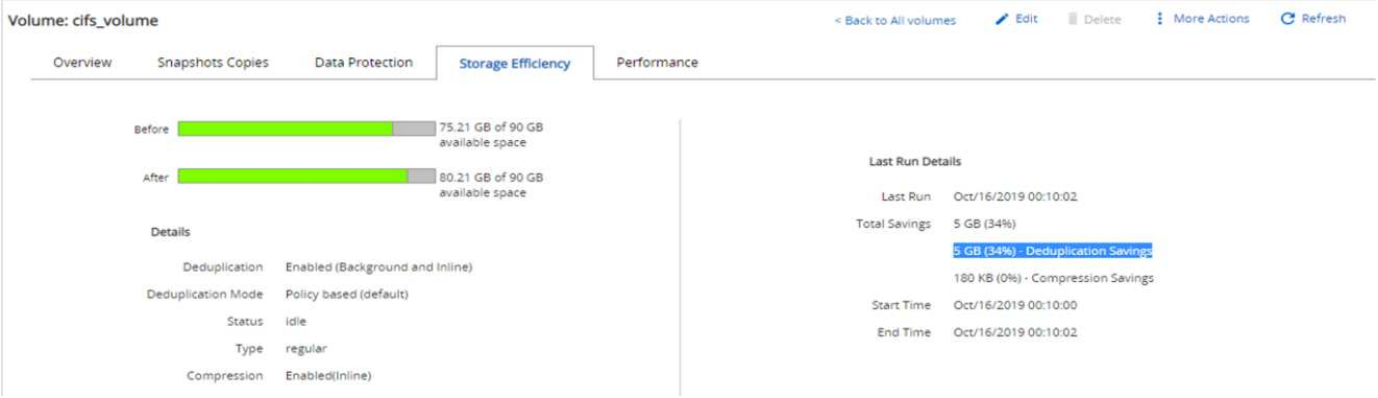
We detected a dramatic increase in the Snapshot size to 820.98MB for the volume hosting the CIFS share during the attack.



We detected an increase in the Snapshot copy size to 404.3MB for the volume hosting the VM.



The storage efficiency for the volume hosting the CIFS share decreased to 34%.



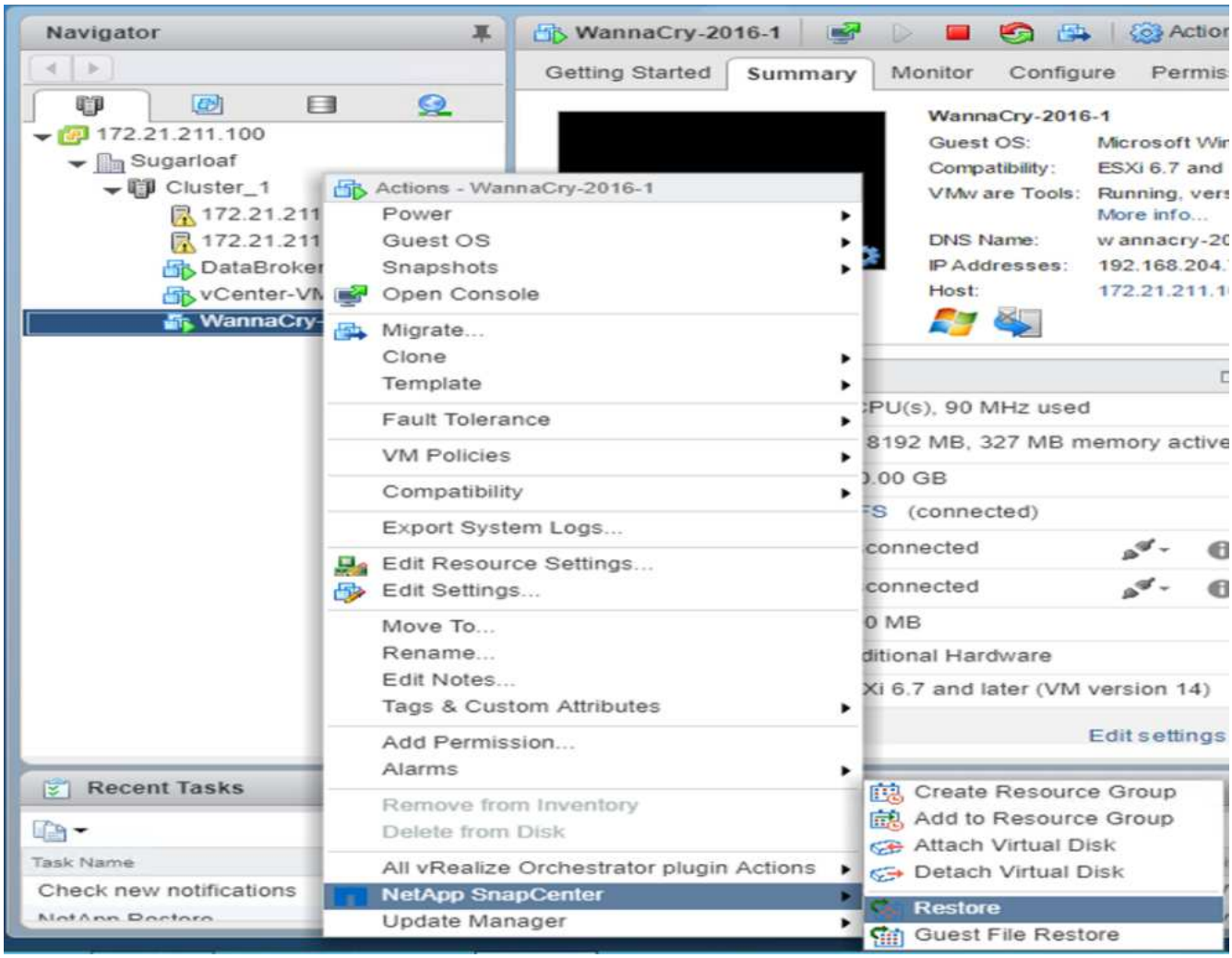
Remediation

Restore the VM and mapped CIFS share by using a clean Snapshot copy create prior to the attack.

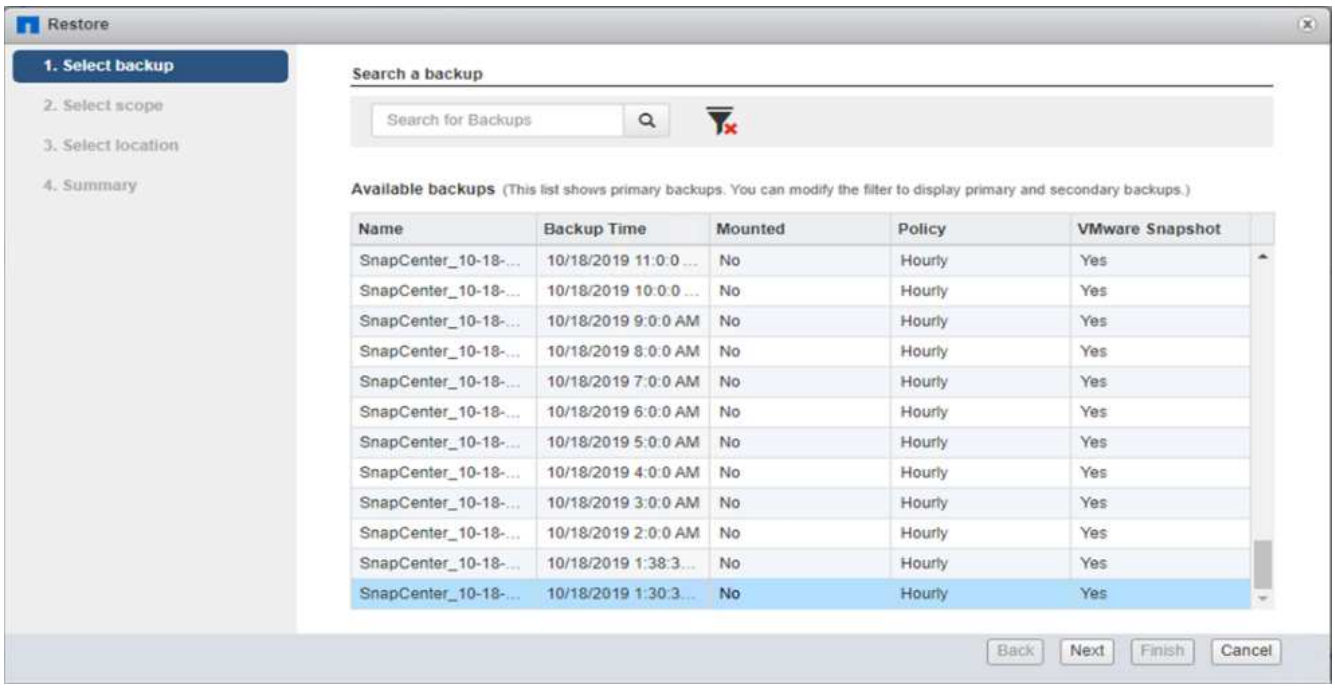
Restore VM

To restore the VM, complete the following steps:

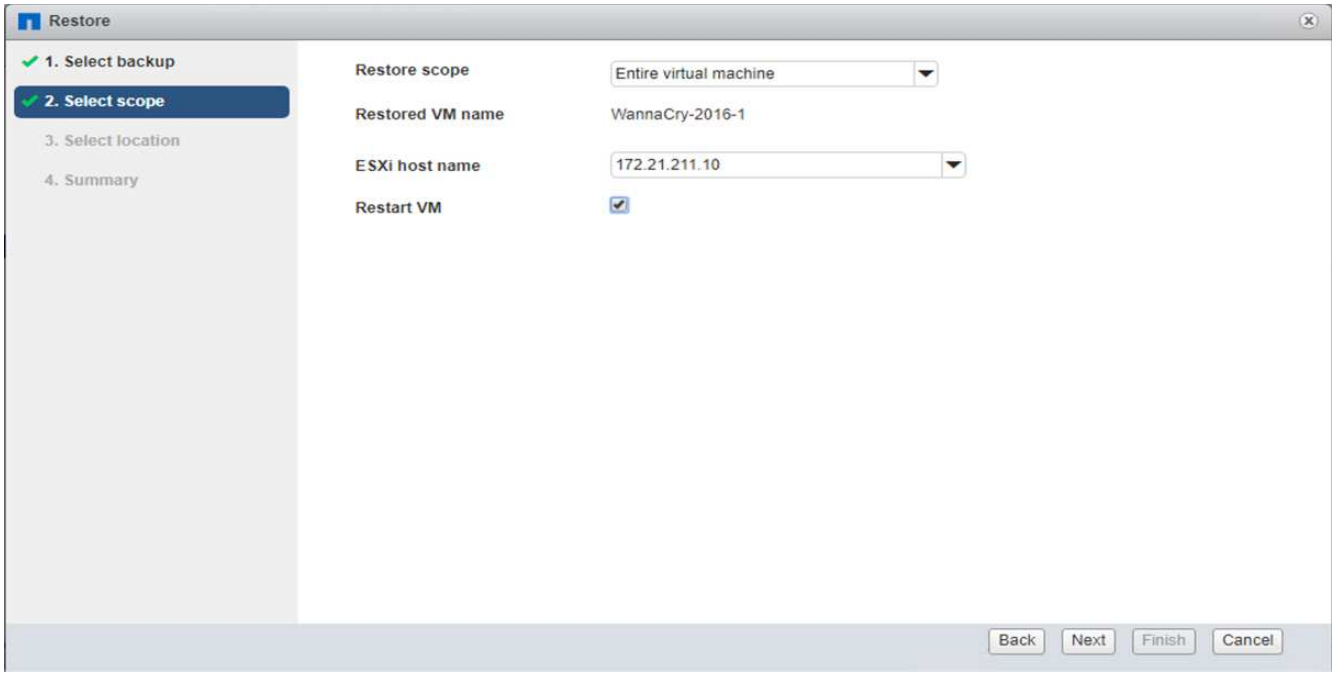
1. Use the Snapshot copy you created with SnapCenter to restore the VM.



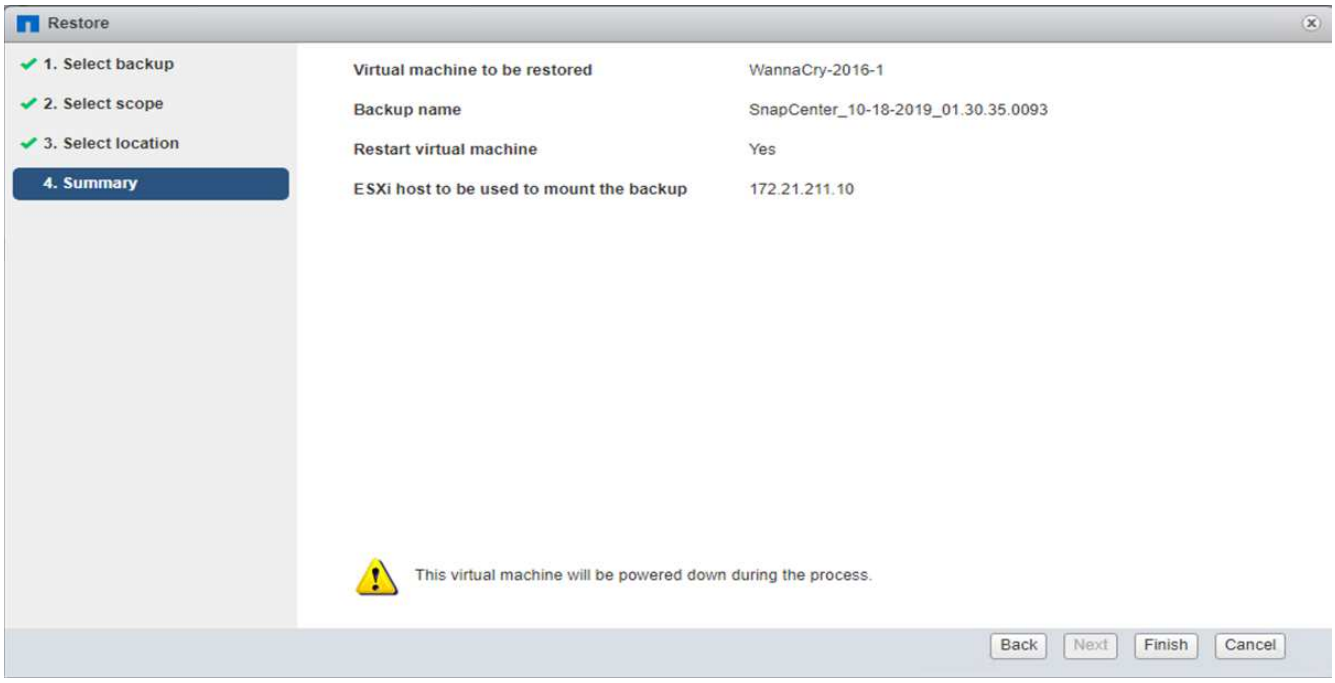
2. Select the desired VMware- consistent Snapshot copy for restore.



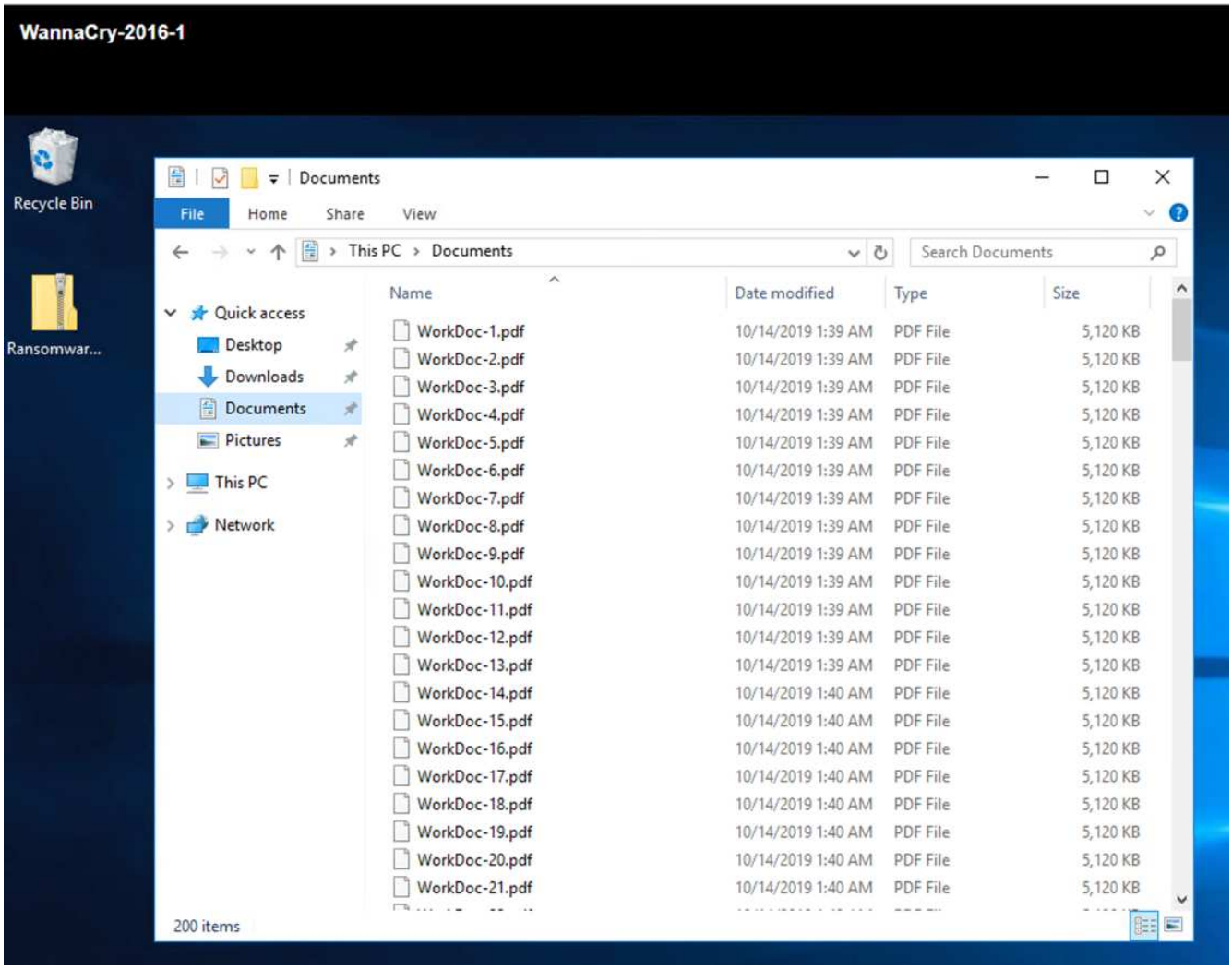
3. The entire VM is restored and restarted.



4. Click Finish to start the restore process.



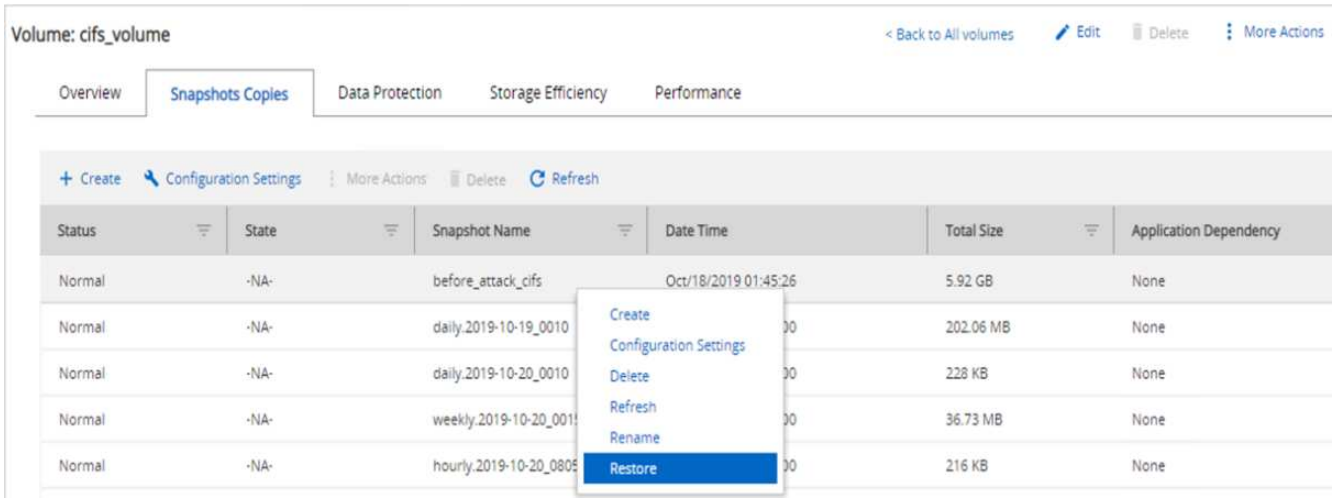
5. The VM and its files are restored.



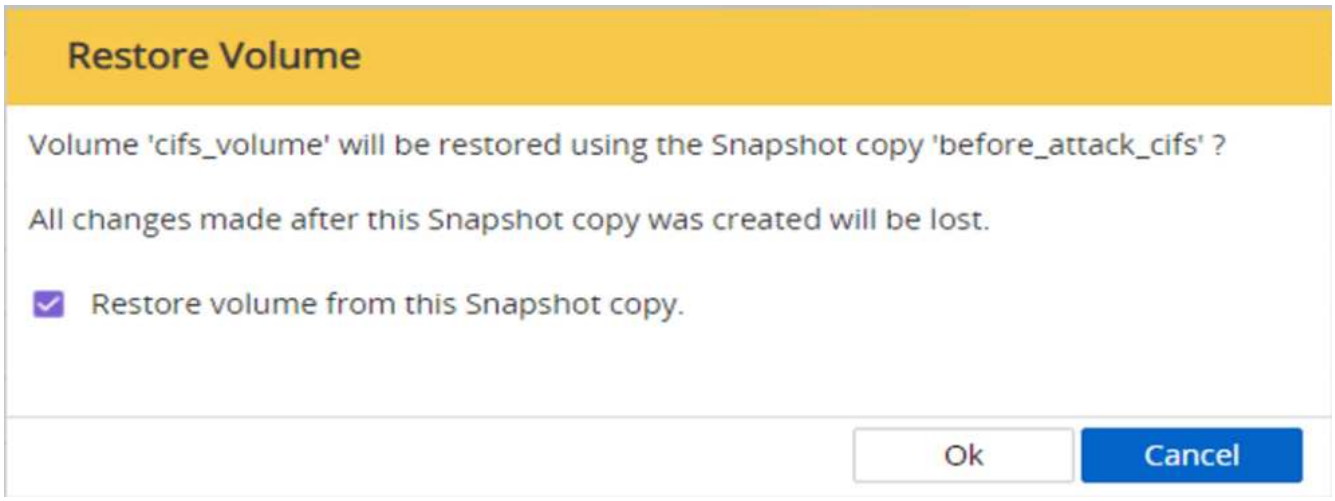
Restore CIFS Share

To restore the CIFS share, complete the following steps:

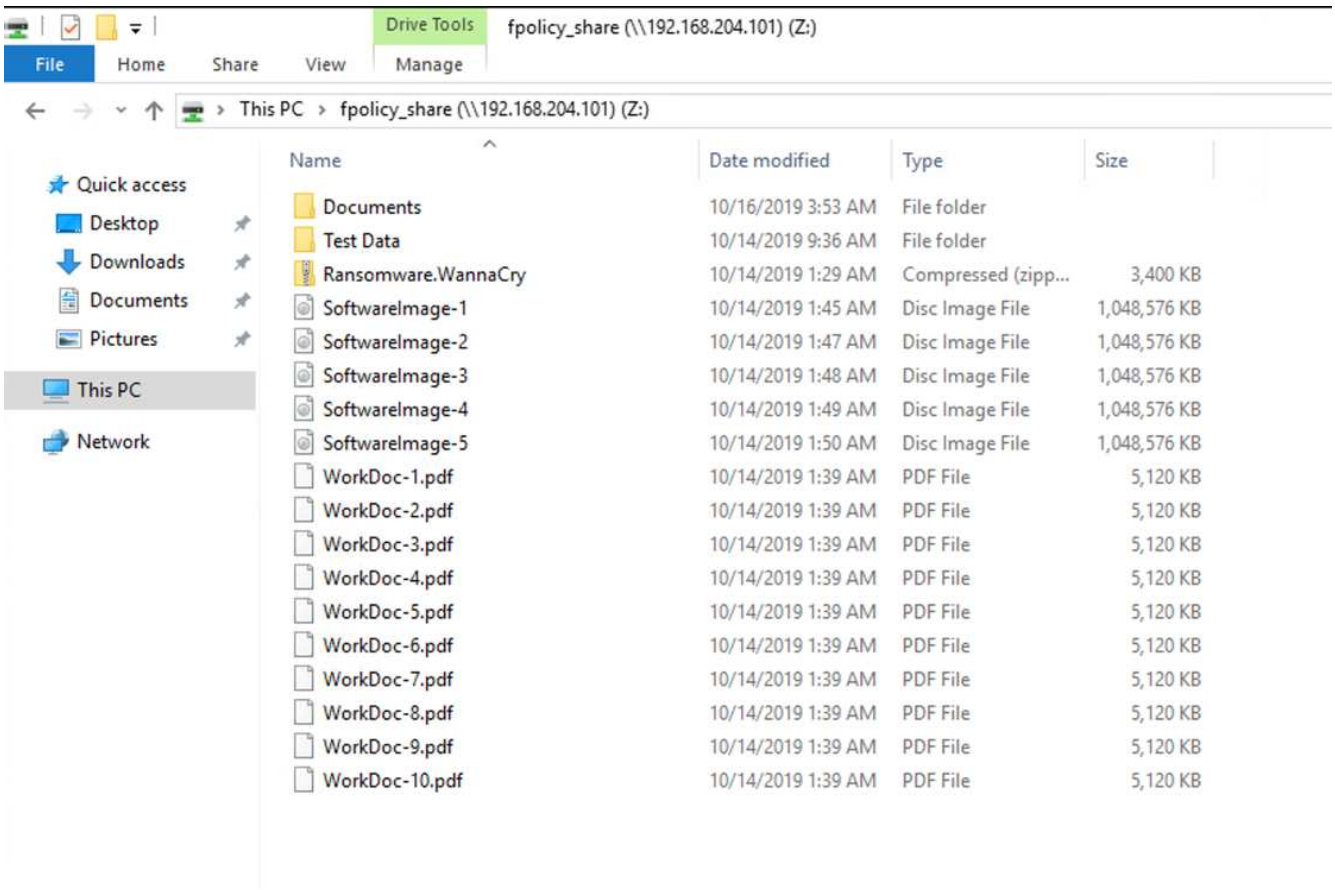
1. Use the Snapshot copy of the volume taken prior to the attack to restore the share.



2. Click OK to initiate the restore operation.



3. View the CIFS share after the restore.



Case 2: WannaCry encrypts file system within the VM and tries to encrypt the mapped CIFS share that is protected through FPolicy

Prevention

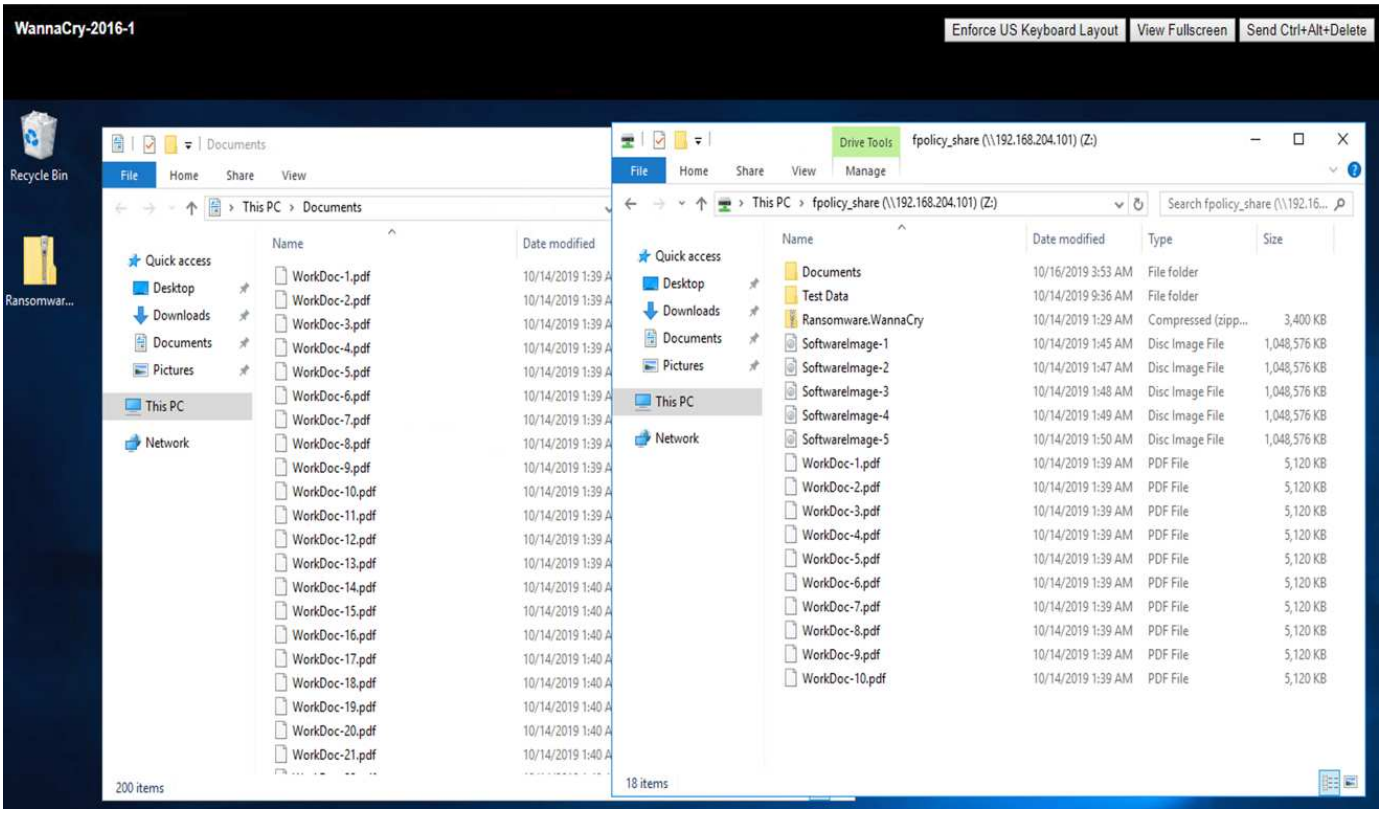
Configure FPolicy

To configure FPolicy on the CIFS share, run the following commands on the ONTAP cluster:

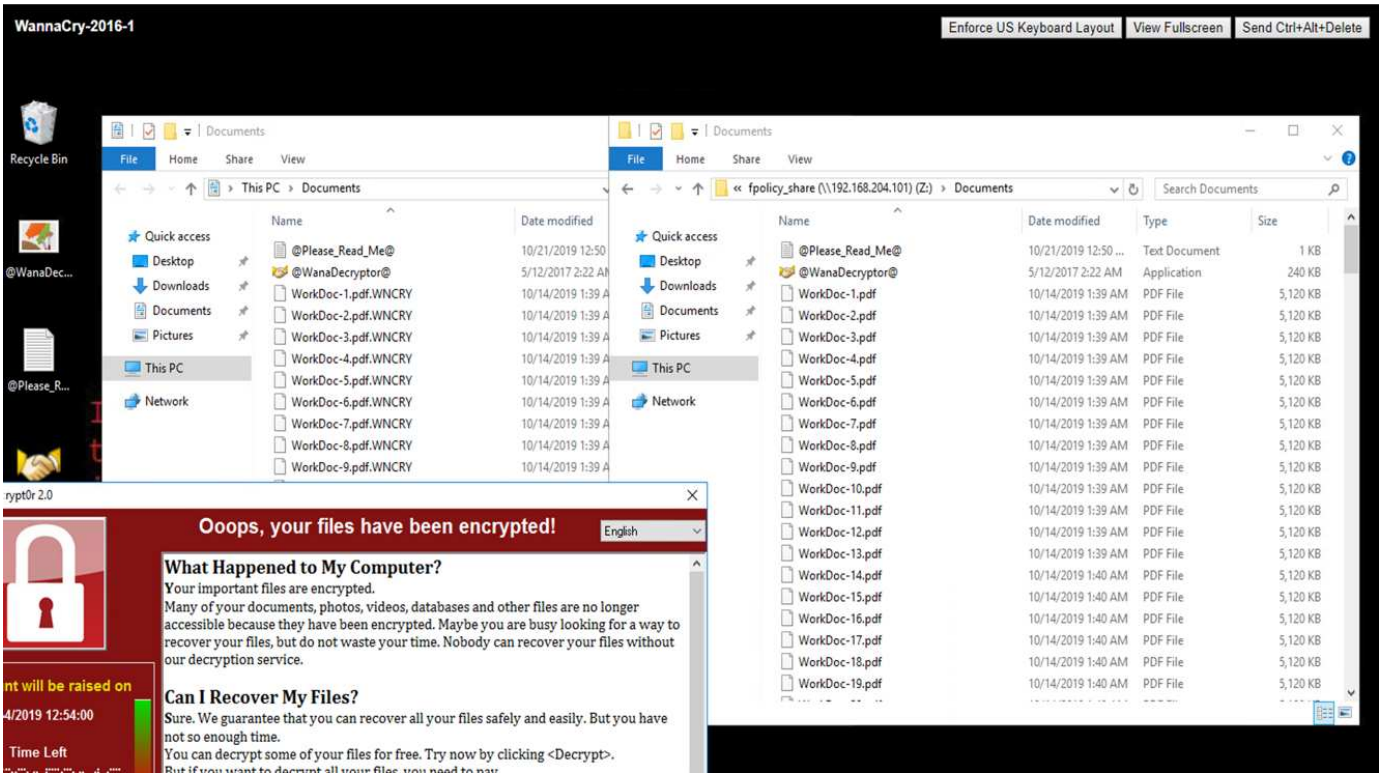
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

With this policy, files with extensions WNCRY, Locky, and ad4c are not allowed to perform the file operations create, rename, write, or open.

View the status of files prior to attack—they are unencrypted and in a clean system.



The files on the VM are encrypted. The WannaCry malware tries to encrypt the files in the CIFS share, but FPolicy prevents it from affecting the files.



Continue business operations without paying ransom

The NetApp capabilities described in this document help you restore data within minutes after an attack and prevent attacks in the first place so that you can continue business operations unhindered.

A Snapshot copy schedule can be set to meet the desired recovery point objective (RPO). Snapshot copy-based restore operations are very quick; therefore, a very low recovery time objective (RTO) can be achieved.

Above all, you do not have to pay any ransom as a result of an attack, and you can quickly get back to regular operations.

Conclusion

Ransomware is a product of organized crime, and the attackers do not operate with ethics. They can refrain from providing the key for decryption even after receiving the ransom. The victim not only loses their data but also a substantial amount of money and will face consequences associated with the loss of production data.

According to a Forbes article, only 19% of ransomware victims get their data back after paying the ransom. Therefore, the authors recommend not paying a ransom in the event of an attack because doing so reinforces the attacker's faith in their business model.

Data backup and restore operations play an important part of ransomware recovery. Therefore, they must be included as an integral part of business planning. The implementation of these operations should be budgeted for so that there is no compromise on recovery capabilities in the event of an attack.

The key is to select the correct technology partner in this journey, and FlexPod provides most of the needed capabilities natively with no additional cost in an all-flash FAS system.

Acknowledgements

The author would like to thank the following people for their support in the creation of this document:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp Snapshot software

  https://www.netapp.com/us/products/platform-os/snapshot.aspx

- SnapCenter Backup Management

  https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx

- SnapLock Data Compliance

  https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx

- NetApp Product Documentation

  https://www.netapp.com/us/documentation/index.aspx

- Cisco Advanced Malware Protection (AMP)

  https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

- Cisco Stealthwatch

  https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html

FIPS 140-2 security-compliant FlexPod solution for healthcare

TR-4892: FIPS 140-2 security-compliant FlexPod solution for healthcare

JayaKishore Esanakula, NetApp
John McAbel, Cisco

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires Federal Information Processing Standard (FIPS) 140-2-validated encryption of electronic Protected Health Information (ePHI). Health information technology (HIT) applications and software are required to be compliant with FIPS 140-2 for obtaining the Promoting Interoperability Program (formerly, Meaningful Use Incentive Program) certification. Eligible providers and hospitals are required to use a FIPS 140-2 (level 1)

compliant HIT for receiving Medicare and Medicaid incentives and for avoiding reimbursement penalties from the Center for Medicare and Medicaid (CMS). FIPS 140-2 certified encryption algorithms qualify as technical safeguards that are required as per the Security Rule of the Health Information Portability and Accountability Act (HIPAA).

FIPS 140-2 is a U.S. government standard that sets security requirements for cryptographic modules in hardware, software, and firmware that protect sensitive information. Compliance with the standard is mandated for use by U.S. government agencies, and it is also often used in such regulated industries as financial services and healthcare. This technical report helps the reader to understand the FIPS 140-2 security standard at a high level. It also helps the audience understand various threats faced by healthcare organizations. Finally, the technical report helps one to understand how a FIPS 140-2 compliant FlexPod system can help secure healthcare assets when deployed on a FlexPod converged infrastructure.

Scope

This document is a technical overview of a Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS and NetApp ONTAP-based FlexPod infrastructure for hosting one or more healthcare IT applications or solutions that require FIPS 140-2 security compliance.

Audience

This document is intended for technical leaders in the healthcare industry and for Cisco and NetApp partner solutions engineers and professional services personnel. NetApp assumes that the reader has a good understanding of compute and storage sizing concepts as well as a technical familiarity with healthcare threats, healthcare security, healthcare IT systems, Cisco UCS, and NetApp storage systems.

Next: Cybersecurity threats in healthcare.

Cybersecurity threats in healthcare

Previous: Introduction.

Every problem presents a new opportunity—an example of one such opportunity is presented by the COVID pandemic. According to a report by the Department of Health and Human Services (HHS) Cybersecurity Program, the COVID response has resulted in an increased number of ransomware attacks. There were 6,000 new internet domains registered just in the third week of March 2020. More than 50% of the domains hosted malware. Ransomware attacks were responsible for almost 50% of all healthcare data breaches in 2020 affecting more than 630 healthcare organizations and approximately 29 million healthcare records. Nineteen leakers/sites doubled the extortion. At 24.5%, the healthcare industry saw the highest number of data breaches in 2020.

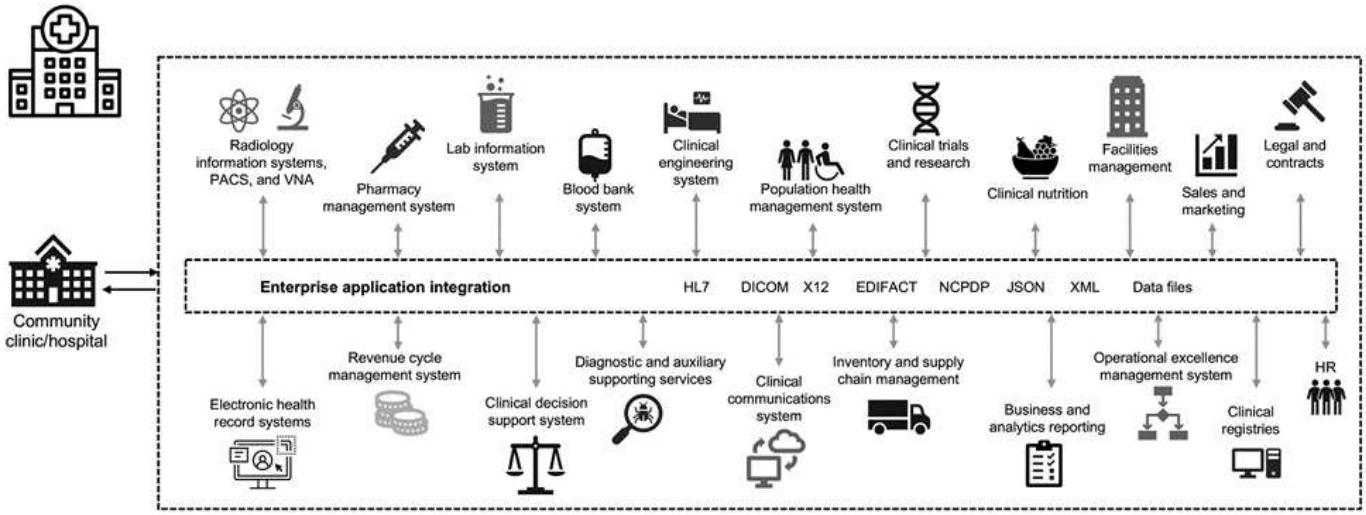
Malicious agents attempted to breach security and privacy of Protected Health Information (PHI) by selling the information or by threatening to destroy or expose it. Targeted and mass-broadcast attempts are frequently made to gain unauthorized access to ePHI. Approximately 75% of the exposed patient records in the second half of 2020 were due to compromised business associates.

The following list of healthcare organizations were targeted by the malicious agents:

- Hospital systems
- Life science labs

- Research labs
- Rehabilitation facilities
- Community hospitals and clinics

The diversity of applications that constitute a healthcare organization is undeniable and increasingly growing in complexity. Information security offices are challenged to provide governance for the vast array of IT systems and assets. The following figure depicts the clinical capabilities of a typical hospital system.



Patient data is at the heart of this image. The loss of patient data and the stigma associated with sensitive medical conditions is very real. Other sensitive issues include the risk of social exclusion, blackmail, profiling, vulnerability to targeted marketing, exploitation, and potential financial liability toward payers about medical information beyond the payer's privileges.

Threats to healthcare are multidimensional in nature and in impact. Governments worldwide have enacted various provisions to secure ePHI. The detrimental effects and the evolving nature of the threats to healthcare make it difficult for healthcare organizations to defend all threats.

Here is a list of common threats identified in healthcare:

- Ransomware attacks
- Loss or theft of equipment or data with sensitive information
- Phishing attacks
- Attacks against connected medical devices that can affect patient safety
- E-mail phishing attacks
- Loss or theft of equipment or data
- Remote desktop protocol compromise
- Software vulnerability

Healthcare organizations operate in a legal and regulatory environment that is as complicated as their digital ecosystems. This environment includes, but is not limited to, the following:

- Office of the National Coordinator (for Healthcare Technology) ONC Certified Electronic Health Information Technology interoperability standards
- Medicare access and the children's Health Insurance Program Reauthorization Act (MACRA)/Meaningful

Use

- Multiple obligations under the Food and Drug Administration (FDA)
- The Joint Commission accreditation processes
- HIPAA requirements
- HITECH requirements
- Minimum Acceptable Risk Standards for payers
- State privacy and security rules
- Federal Information Security Modernization Act requirements as incorporated into federal contracts and research grants through agencies such as the National Institutes of Health
- Payment Card Industry Data Security Standard (PCI-DSS)
- Substance Abuse and Mental Health Services Administration (SAMHSA) requirements
- The Gramm-Leach-Bliley Act for financial processing
- The Stark Law as it relates to providing services to affiliated organizations
- Family Educational Rights and Privacy Act (FERPA) for institutions that participate in higher education
- Genetic Information Nondiscrimination Act (GINA)
- The new General Data Protection Regulation (GDPR) in the European Union

Security architecture standards are fast evolving to stop the malicious actors from impacting healthcare information systems. One such standard is FIPS 140-2, defined by the National Institute of Standards and Technology (NIST). FIPS publication 140-2 details the U.S. government requirements for a cryptographic module. The security requirements cover areas related to a secure design and implementation of a cryptographic module and can be applied to HIT. Well-defined cryptographic boundaries allow for easier security management while staying current with the cryptographic modules. These boundaries help prevent weak crypto modules that can be easily exploited by malicious actors. They can also help prevent human errors when managing standard cryptographic modules.

NIST along with the Communications Security Establishment (CSE) have established the Cryptographic Module Validation Program (CMVP) to certify cryptographic modules for FIPS 140-2 validation levels. Using a FIPS 140-2 certified module, federal organizations are required to protect sensitive or valuable data while at-rest as well as while in motion. Due to its success in protecting sensitive or valuable information, many healthcare systems have chosen to encrypt ePHI by using FIPS 140-2 cryptographic modules beyond the legally required minimum level of security.

Leveraging and implementing the FlexPod FIPS 140-2 capabilities only takes hours (not days). Becoming FIPS compliant is within reach for most healthcare organizations, regardless of size. With clearly defined cryptographic boundaries and well-documented and simple implementation steps, a FIPS 140-2 compliant FlexPod architecture can set a solid security foundation for infrastructure and allow for simple enhancements to further increase protection for security threats.

Next: Overview of FIPS 140-2.

Overview of FIPS 140-2

Previous: Cybersecurity threats in healthcare.

FIPS 140-2 specifies the security requirements for a cryptographic module used within a security system that protects sensitive information in computer and telecommunication

systems. A cryptographic module should be a set of hardware, software, firmware, or a combination. FIPS applies to the cryptographic algorithms, key generation and key managers contained within a cryptographic boundary. It is important to understand that FIPS 140-2 applies specifically to the cryptographic module, not the product, architecture, data, or ecosystem. The cryptographic module, which is defined in the key terms later in this document, is the specific component (whether it's hardware, software, and/or firmware) that implements approved security functions. In addition, FIPS 140-2 specifies four levels. Approved cryptographic algorithms are common to all levels. Key elements and requirements of each security level include:

- **Security level 1**
  - Specifies basic security requirements for a cryptographic module (at least one approved algorithm or security function is required).
  - No specified physical security mechanisms are required for level 1 beyond the basic requirements for production-grade components.
- **Security level 2**
  - Enhances the physical security mechanisms by adding the requirement for tamper-evidence by using tamper-evident solutions such as coatings or seals, locks on removable covers or doors of the cryptographic modules.
  - Requires, at minimum, role-based access control (RBAC) in which the cryptographic module authenticates the authorization of an operator or administrator to assume a specific role and perform a corresponding set of functions.
- **Security level 3**
  - Builds on the tamper-evident requirements of level 2 and attempts to prevent further access to critical security parameters (CSPs) within the cryptographic module.
  - Physical security mechanisms required at level 3 are intended to have a high probability to detect and respond to attempts at physical access, or any use or modification of the cryptographic module. Examples might include strong enclosures, tamper detection, and response circuitry that zeros all plaintext CSPs when a removable cover on the cryptographic module is opened.
  - Requires identity-based authentication mechanisms to enhance the security of the RBAC mechanisms specified in level 2. A cryptographic module authenticates the identity of an operator and verifies that the operator is authorized to use a role and perform the functions of the role.
- **Security level 4**
  - The highest level of security in FIPS 140-2.
  - The most useful level for operations in physically unprotected environments.
  - At this level, the physical security mechanisms are intended to provide complete protection around the cryptographic module with the responsibility of detecting and responding to any unauthorized attempts at physical access.
  - Penetration or exposure of the cryptographic module should have a high probability of detection and result in the immediate zeroization of all unsecure or plaintext CSPs.

Next: Control plane versus data plane.

Control plane versus data plane

Previous: Overview of FIPS 140-2.

When implementing a FIPS 140-2 strategy, it is important to understand what is being protected. This can easily be broken down into two areas: control plane and data plane. A control plane refers to the aspects that affect the control and operation of the components within the FlexPod system: for example, administrative access to the NetApp storage controllers, Cisco Nexus switches, and Cisco UCS servers. Protection at this layer is provided by limiting the protocols and cryptographic cyphers that administrators can use to connect to devices and make changes. A data plane refers to the actual information, such as the PHI, within the FlexPod system. This is protected by encrypting data at rest and again for FIPS, ensuring that the cryptographic modules in use meet the standards.

Next: FlexPod Cisco UCS compute and FIPS 140-2.

FlexPod Cisco UCS compute and FIPS 140-2

Previous: Control plane versus data plane.

A FlexPod architecture can be designed with a Cisco UCS server that is FIPS 140-2 compliant. In accordance with the U. S. NIST, Cisco UCS server can operate in FIPS 140-2 level 1 compliance mode. For a complete list of FIPS-compliant Cisco components, see Cisco's FIPS 140 page. Cisco UCS Manager is FIPS 140-2 validated.

Cisco UCS and Fabric Interconnect

Cisco UCS Manager is deployed and runs from the Cisco Fabric Interconnects (FIs).

For more information about Cisco UCS and how to enable FIPS, see the Cisco UCS Manager documentation.

To enable FIPS mode on the Cisco fabric interconnect on each fabric A and B, run the following commands:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> To replace an FI in a cluster on Cisco UCS Manager Release 3.2(3) with an FI on a release earlier than Cisco UCS Manager Release 3.2(3), disable FIPS mode (disable `fips-mode`) on the existing FI before adding the replacement FI to the cluster. After the cluster is formed, as part of the Cisco UCS Manager boot up, FIPS mode is automatically enabled.

Cisco offers the following key products that can be implemented in the compute or application layer:

- **Cisco Advanced Malware Protection (AMP) for endpoints.** Supported on Microsoft Windows and Linux operating systems, this solution integrates prevention, detection, and response capabilities. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses. The Malicious Activity Protection (MAP) component of AMP continually monitors all endpoint activity and

provides run-time detection and blocking of abnormal behavior of a running program on the endpoint. For example, when endpoint behavior indicates ransomware, the offending processes are terminated, preventing endpoint encryption and stopping the attack.

- **AMP for email security.** Emails have become the prime vehicle to spread malware and to carry out cyberattacks. On average, approximately 100 billion emails are exchanged in a single day, which provides attackers with an excellent penetration vector into user's systems. Therefore, it is absolutely essential to defend against this line of attack. AMP analyzes emails for threats such as zero-day exploits and stealthy malware hidden in malicious attachments. It also uses industry-leading URL intelligence to combat malicious links. It gives users advanced protection against spear phishing, ransomware, and other sophisticated attacks.
- **Next- Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS can be deployed as a physical appliance in the data center or as a virtual appliance on VMware (NGIPSv for VMware). This highly effective intrusion prevention system provides reliable performance and a low total cost of ownership. Threat protection can be expanded with optional subscription licenses to provide AMP, application visibility and control, and URL filtering capabilities. Virtualized NGIPS inspects traffic between virtual machines (VMs) and makes it easier to deploy and manage NGIPS solutions at sites with limited resources, increasing protection for both physical and virtual assets.

Next: FlexPod Cisco networking and FIPS 140-2.

FlexPod Cisco networking and FIPS 140-2

Previous: FlexPod Cisco UCS compute and FIPS 140-2.

Cisco MDS

Cisco MDS 9000 series platform with software 8.4.x is FIPS 140-2 compliant. Cisco MDS implements cryptographic modules and the following services for SNMPv3 and SSH.

- Session establishment supporting each service
- All underlying cryptographic algorithms supporting each services key derivation functions
- Hashing for each service
- Symmetric encryption for each service

Before you enable FIPS mode, complete the following tasks on the MDS switch:

1. Make your passwords a minimum of eight characters in length.
2. Disable Telnet. Users should log in using SSH only.
3. Disable remote authentication through RADIUS/TACACS+. Only users local to the switch can be authenticated.
4. Disable SNMP v1 and v2. Any existing user accounts on the switch that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
5. Disable VRRP.
6. Delete all IKE policies that either have MD5 for authentication or DES for encryption. Modify the policies so they use SHA for authentication and 3DES/AES for encryption.
7. Delete all SSH Server RSA1 keypairs.

To enable FIPS mode and to display FIPS status on the MDS switch, complete the following steps:

1. Show the FIPS status.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Set up the 2048 bits SSH key.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Enable FIPS mode.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Show the FIPS status.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Save the configuration to the running configuration.

```
MDSSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Restart MDS switch

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Show the FIPS status.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

For more information, see Enabling FIPS Mode.

Cisco Nexus

Cisco Nexus 9000 series switches (version 9.3) are FIPS 140-2 compliant. Cisco Nexus implements cryptographic modules and the following services for SNMPv3 and SSH.

- Session establishment supporting each service
- All underlying cryptographic algorithms supporting each services key derivation functions
- Hashing for each service
- Symmetric encryption for each service

Before you enable FIPS mode, complete the following tasks on the Cisco Nexus switch:

1. Disable Telnet. Users should log in using Secure Shell (SSH) only.
2. Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
3. Delete all SSH server RSA1 key-pairs.
4. Enable HMAC-SHA1 message integrity checking (MIC) to use during the Cisco TrustSec Security

Association Protocol (SAP) negotiation. To do so, enter the sap hash-algorithm `HMAC-SHA-1` command from the `cts-manual` or `cts-dot1x` mode.

To enable FIPS mode on the Nexus switch, complete the following steps:

1. Set up 2048 bits SSH key.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Set up the 2048 bits SSH key.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Enable FIPS mode.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Restart the Nexus switch.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Show the FIPS status.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Additionally, Cisco NX OS software supports the NetFlow feature that enables enhanced detection of network anomalies and security. NetFlow captures the metadata of every conversation on the network, the parties involved in the communication, the protocol being used, and the duration of the transaction. After the information is aggregated and analyzed, it can provide insight into normal behavior. The collected data also allows identification of questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed. NetFlow uses flows to provide statistics for network monitoring. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow. You can export the data that NetFlow gathers for your flows by using a flow exporter to a remote NetFlow collector, such as Cisco Stealthwatch. Stealthwatch uses this information for continuous monitoring of the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Next: FlexPod NetApp ONTAP storage and FIPS 140-2.

FlexPod NetApp ONTAP storage and FIPS 140-2

Previous: FlexPod Cisco networking and FIPS 140-2.

NetApp offers a variety of hardware, software, and services, which can include various components of the cryptographic modules validated under the standard. Therefore, NetApp uses a variety of approaches for FIPS 140-2 compliance for the control plane and data plane:

- NetApp includes cryptographic modules that have achieved level 1 validation for data-in-transit and data-at-rest encryption.
- NetApp acquires both hardware and software modules that have been FIPS 140-2 validated by the suppliers of those components. For example, the NetApp Storage Encryption solution leverages FIPS level 2 validated drives.
- NetApp products can use a validated module in a way that complies with the standard even though the product or feature is not within the boundary of the validation. For example, NetApp Volume Encryption (NVE) is FIPS 140-2 compliant. Although not separately validated, it leverages the NetApp cryptographic module, which is level 1 validated. To understand the specifics of compliance for your version of ONTAP, contact your FlexPod SME.

NetApp Cryptographic modules are FIPS 140-2 level 1 validated

- The NetApp Cryptographic Security Module (NCSM) is FIPS 140-2 level 1 validated.

NetApp self-encrypting drives are FIPS 140-2 level 2 validated

NetApp purchases self-encrypting drives (SEDs) that have been FIPS 140-2 validated by the original equipment manufacturer (OEM); customers seeking these drives must specify them when ordering. Drives are validated at level 2. The following NetApp products can leverage validated SEDs:

- AFF A-Series and FAS storage systems
- E-Series and EF-Series storage systems

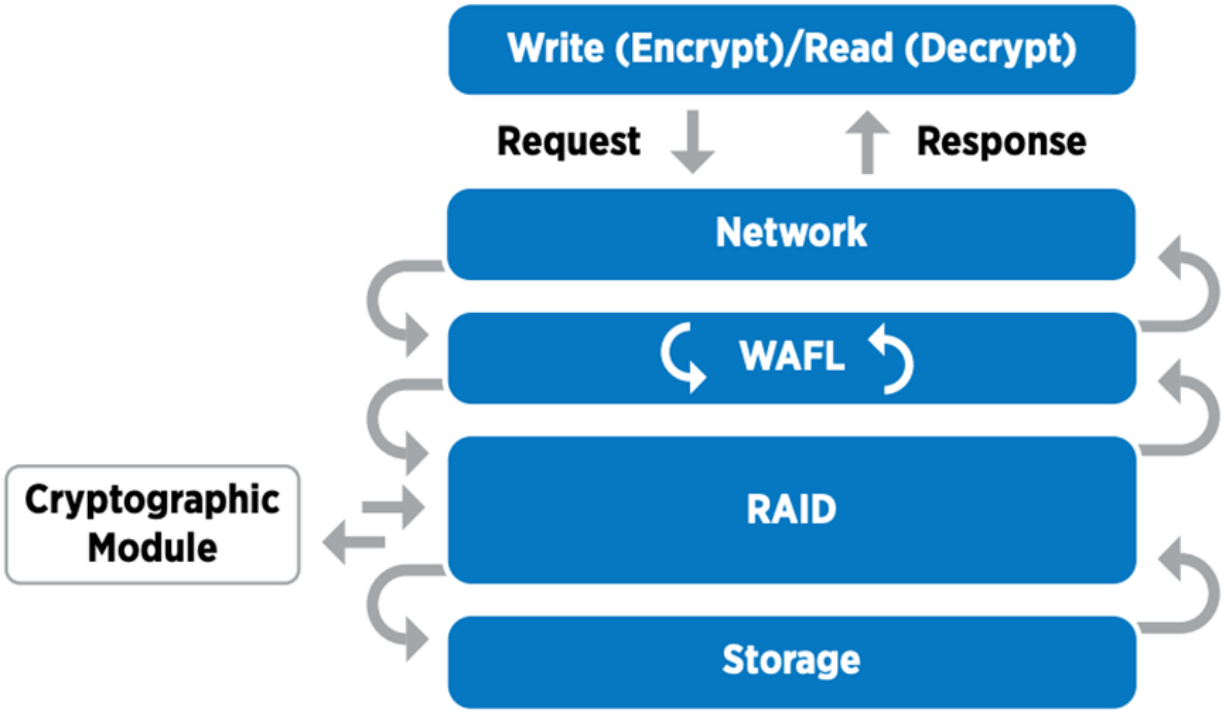
NetApp Aggregate Encryption and NetApp Volume Encryption

NVE and NetApp Aggregate Encryption (NAE) technologies enable encryption of data at the volume and aggregate level respectively, making the solution agnostic to the physical drive.

NVE is a software-based, data-at-rest encryption solution available starting with ONTAP 9.1, and it has been FIPS 140-2 compliant since ONTAP 9.2. NVE allows ONTAP to encrypt data for each volume for granularity. NAE, available with ONTAP 9.6, is an outgrowth of NVE; it allows ONTAP to encrypt data for each volume, and the volumes can share keys across the aggregate. Both NVE and NAE use AES 256-bit encryption. Data can also be stored on disk without SEDs. NVE and NAE enable you to use storage efficiency features even when encryption is enabled. An application- layer- only encryption defeats all benefits of storage efficiency. With NVE and NAE, storage efficiencies are maintained because the data comes in from the network through NetApp WAFL to the RAID layer, which determines whether the data should be encrypted. For greater storage efficiency, you can use aggregate deduplication with NAE. NVE volumes and NAE volumes can coexist on the same NAE aggregate. NAE aggregates do not support unencrypted volumes.

Here’s how the process works: When data is encrypted, it is sent to the cryptographic module which is FIPS 140-2 level 1 validated. The cryptographic module encrypts the data and sends it back to the RAID layer. The encrypted data is then sent to the disk. Therefore, with the combination of NVE and NAE, the data is already encrypted on the way to the disk. Reads follow the reverse path. In other words, the data leaves the disk

encrypted, is sent to RAID, is decrypted by the cryptographic module, and is then sent up the rest of the stack, as shown in the following figure.



NVE uses a software cryptographic module which is FIPS 140-2 level 1 validated.

For more information about NVE, see the NVE Datasheet.

NVE protects data in the cloud. Cloud Volumes ONTAP and Azure NetApp Files are capable of providing FIPS 140-2 compliant data encryption at rest.

Starting with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the NVE license and onboard or external key management. Starting with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default. You can override the default when you encrypt the volume.

ONTAP NAE CLI commands

Before you run the following CLI commands, make sure the cluster has the required NVE license.

To create an aggregate and encrypt it, run the following command (when run on an ONTAP 9.6 and later cluster CLI):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

To convert a non-NAE aggregate to an NAE an aggregate, run the following command (when run on an ONTAP 9.6 and later cluster CLI):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

To convert an NAE aggregate to an non-NAE an aggregate, run the following command (when run on an ONTAP 9.6 and later cluster CLI):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE CLI commands

Starting with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default.

To create a volume on an aggregate that is NAE enabled, run the following command (when run on an ONTAP 9.6 and later cluster CLI):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

To enable encryption of an existing volume “inplace” without a volume move, run the following command (when run on an ONTAP 9.6 and later cluster CLI):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

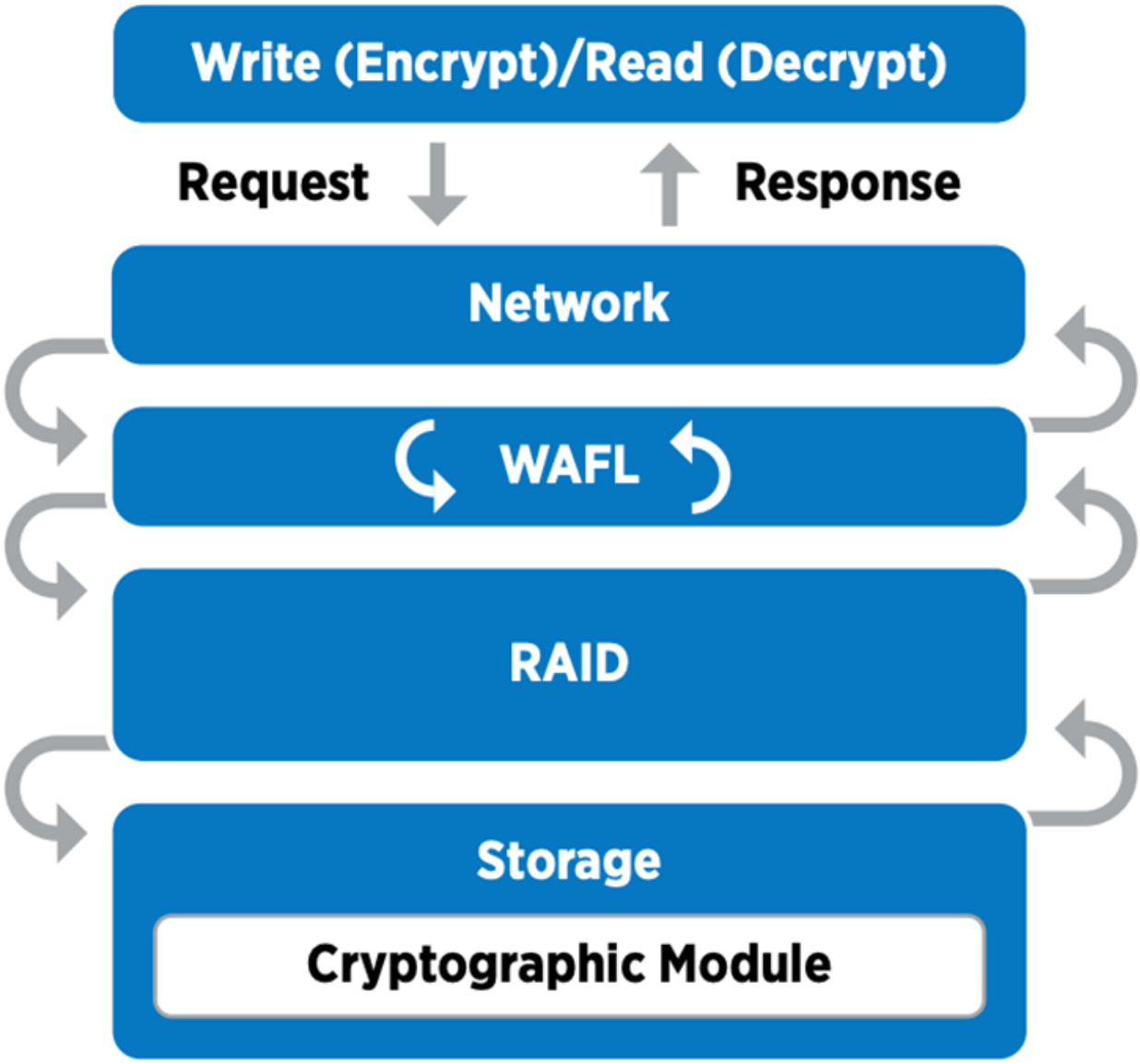
To verify that volumes are enabled for encryption, run the following CLI command:

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE uses SEDs to perform the data encryption through a hardware-accelerated mechanism.

NSE is configured to use FIPS 140-2 level 2 self-encrypting drives to facilitate compliance and spares return by enabling the protection of data at rest through AES 256-bit transparent disk encryption. The drives perform all of the data encryption operations internally, as depicted in the following figure, including encryption key generation. To prevent unauthorized access to the data, the storage system must authenticate itself with the drive using an authentication key that is established the first time the drive is used.



NSE uses hardware encryption on each drive, which is FIPS 140-2 level 2 validated.

For more information about NSE, see the NSE datasheet.

Key management

The FIPS 140-2 standard applies to the cryptographic module as defined by the boundary, as shown in the following figure.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

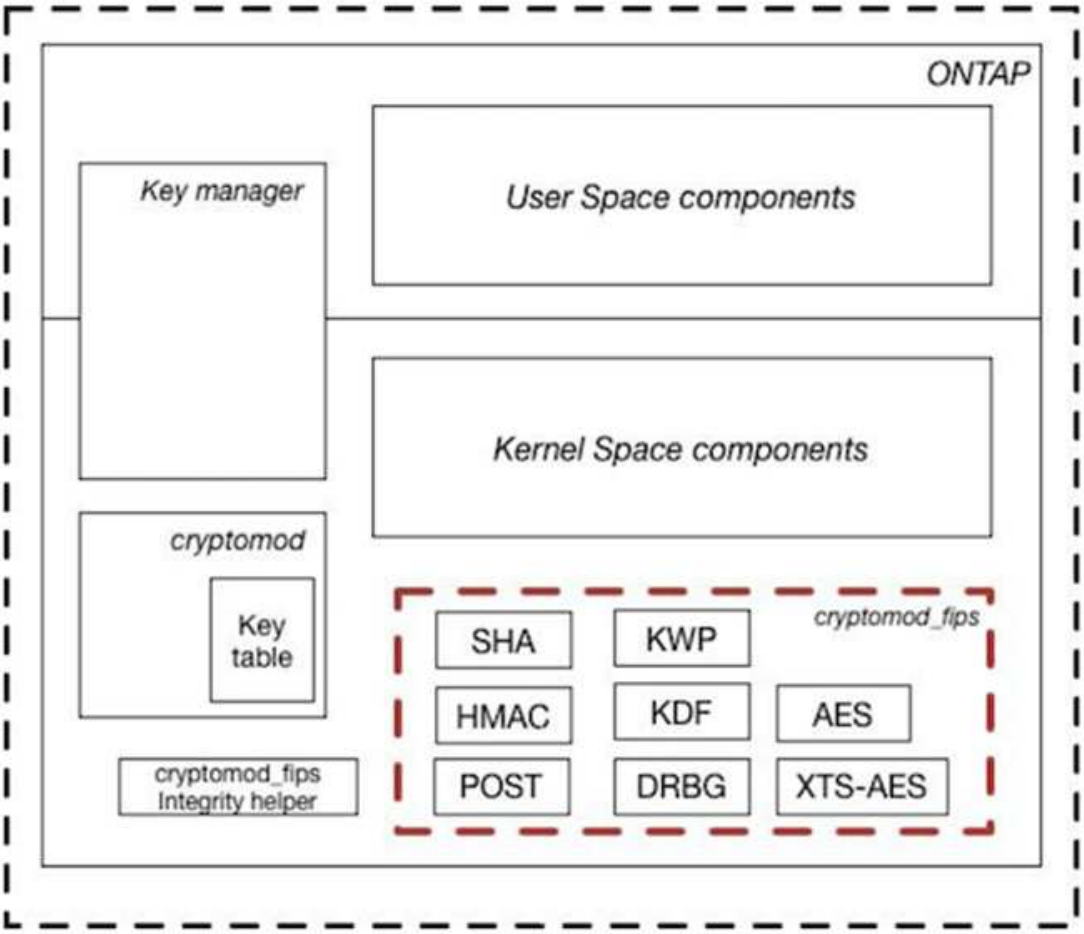


Figure 1 - Block Diagram

Key manager keeps track of all the encryption keys used by ONTAP. NSE SEDs use the key manager to set the authentication keys for NSE SEDs. When using the key manager, the combined NVE and NAE solution is composed of a software cryptographic module, encryption keys, and a key manager. For each volume, NVE uses a unique XTS-AES 256 data encryption key, which the key manager stores. The key used for a data volume is unique to the data volume in that cluster and is generated when the encrypted volume is created. Similarly, an NAE volume uses unique XTS-AES 256 data encryption keys per aggregate, which the key manager also stores. NAE keys are generated when the encrypted aggregate is created. ONTAP does not pregenerate keys, reuse them, or display them in plain text—they are stored and protected by the key manager.

Support for external key manager

Beginning with ONTAP 9.3, external key managers are supported in both NVE and NSE solutions. The FIPS 140-2 standard applies to the cryptographic module used in the specific vendor's implementation. Most often, FlexPod and ONTAP customers use one of the following validated (per the NetApp Interoperability Matrix) key managers:

- Gemalto or SafeNet AT

- Vormetric (Thales)
- IBM SKLM
- Utimaco (formerly Microfocus, HPE)

NSE and NVMe SED authentication key is backed up to an external key manager by using the industry-standard OASIS Key Management Interoperability Protocol (KMIP). Only the storage system, drive, and key manager have access to the key, and the drive cannot be unlocked if it is moved outside the security domain, thus preventing data leakage. The external key manager also stores NVE volume encryption keys and NAE aggregate encryption keys. If the controller and disks are moved and no longer have access to the external key manager, the NVE and NAE volumes won't be accessible and cannot be decrypted.

The following example command adds two key management servers to the list of servers used by the external key manager for store virtual machine (SVM) `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

When a FlexPod Datacenter is being used in a multitenancy scenario, ONTAP enables users by providing tenancy separation for security reasons at the SVM level.

To verify list of external key managers, run the following CLI command:

```
fp-health::> security key-manager external show
```

Combine encryption for double encryption (layered defense)

If you need to segregate access to data and make sure that data is protected all the time, NSE SEDs can be combined with network- or fabric-level encryption. NSE SEDs act like a backstop if an administrator forgets to configure or misconfigures higher-level encryption. For two distinct layers of encryption, you can combine NSE SEDs with NVE and NAE.

NetApp ONTAP cluster-wide control plane FIPS mode

NetApp ONTAP data management software has a FIPS mode configuration that instantiates an added level of security for the customer. This FIPS mode only applies to the control plane. When FIPS mode is enabled, in accordance with key elements of FIPS 140-2, Transport Layer Security v1 (TLSv1) and SSLv3 are disabled, and only TLS v1.1 and TLS v1.2 remain enabled.

> ONTAP cluster-wide control pane in FIPS mode is FIPS 140-2 level 1 compliant. Cluster-wide FIPS mode uses a software-based cryptographic module provided by NCSM.

FIPS 140-2 compliance mode for cluster-wide control plane secures all control Interfaces of ONTAP. By default, the FIPS 140-2 only mode is disabled; however you can enable this mode by setting the `is- fips-enabled` parameter to `true` for the `security config modify` command.

To enable FIPS mode on the ONTAP cluster, run the following command:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

When SSL FIPS mode is enabled, SSL communication from ONTAP to the external client or server components outside of ONTAP will use FIPS complaint cryptographic for SSL.

To show the FIPS status for the entire cluster, run the following commands:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

Next: Solution benefits of FlexPod converged infrastructure.

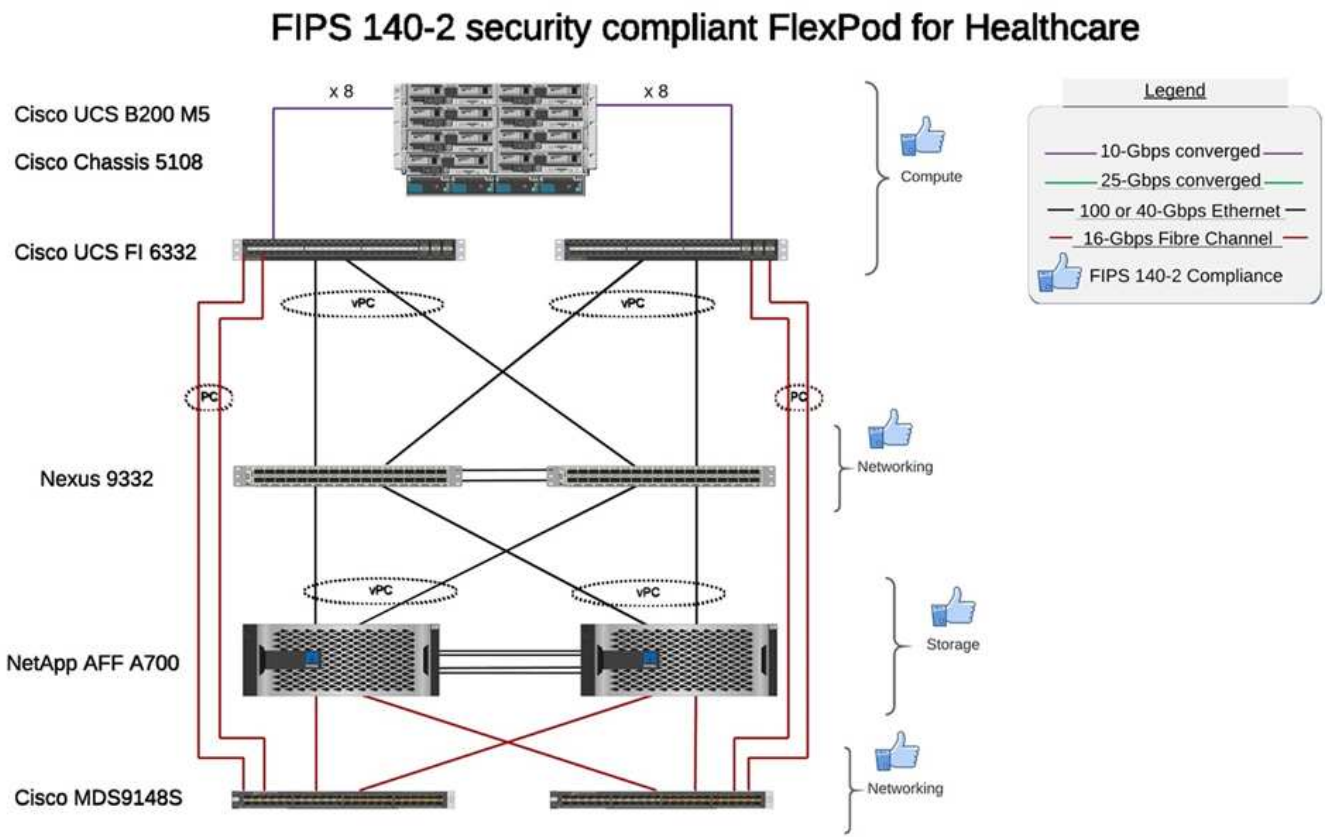
Solution benefits of FlexPod converged infrastructure

Previous: FlexPod NetApp ONTAP storage and FIPS 140-2.

Healthcare organizations have several mission-critical systems. Two of the most critical systems are the electronic health record (EHR) systems and medical imaging systems. To demonstrate the FIPS setup on a FlexPod system, we used an open-source EHR and an open-source picture archiving and communication system (PACS) system for the lab setup and workload validation on the FlexPod system. For a complete list of EHR capabilities, EHR logical application components, and how EHR systems benefit when implemented on a FlexPod system see TR-4881: FlexPod for Electronic Health Record Systems. For a complete list of a medical imaging system capabilities, logical application components, and how medical imaging systems benefit when implemented on FlexPod, see TR-4865: FlexPod for Medical Imaging.

During the FIPS setup and workload validation, we exercised workload characteristics that were representative of a typical healthcare organization. For example, we exercised an open-source EHR system to include realistic patient data access and change scenarios. Additionally, we exercised medical imaging workloads that included digital imaging and communications in medicine (DICOM) objects in a `*. dcm` file format. DICOM objects with metadata were stored on both the file and block storage. Additionally, we implemented multipathing capabilities from within a virtualized RedHat Enterprise Linux (RHEL) server. We stored DICOM objects on an NFS, mounted LUNs using iSCSI, and mounted LUNs using FC. During the FIPS setup and validation, we observed that the FlexPod converged infrastructure exceeded our expectations and performed seamlessly.

The following figure depicts the FlexPod system used for FIPS setup and validation. We leveraged the FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7 Cisco Validated Design (CVD) during the setup process.



Solution infrastructure hardware and software components

The following two figures list the hardware and software components respectively used during the FIPS testing enabling on a FlexPod. The recommendations in these tables are examples; you should work with your NetApp SME to make sure that the components are suitable for your organization. Also, make sure that the components and versions are supported in the NetApp Interoperability Matrix Tool (IMT) and Cisco Hardware Compatibility List (HCL).

Layer	Product family	Quantity and model	Details
Compute	Cisco UCS 5108 chassis	1 or 2	
	Cisco UCS blade servers	3 B200 M5	Each with 2x 20 or more cores, 2.7GHz, and 128-384GB RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	See the
	2x Cisco UCS Fabric Interconnects	6332	-
Network	Cisco Nexus switches	2x Cisco Nexus 9332	-
Storage network	IP network for storage access over SMB/CIFS, NFS, or iSCSI protocols	Same network switches as above	-
	Storage access over FC	2x Cisco MDS 9148S	-

Layer	Product family	Quantity and model	Details
Storage	NetApp AFF A700 all-flash storage system	1 Cluster	Cluster with two nodes
	Disk shelf	One DS224C or NS224 disk shelf	Fully populated with 24 drives
	SSD	>24, 1.2TB or larger capacity	-

Software	Product family	Version or release	Details
Various	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bit)	-
	NetApp ONTAP	ONTAP 9.7 or later	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 or later	-
	Cisco Ethernet 3000 or 9000 series switches	For 9000 series, 7.0(3)I7(7) or later For 3000 series, 9.2(4) or later	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) or later	-
	Hypervisor	VMware vSphere ESXi 6.7 U2 or later	-
Storage	Hypervisor management system	VMware vCenter Server 6.7 U3 (vCSA) or later	-
Network	NetApp Virtual Storage Console (VSC)	VSC 9.7 or later	-
	NetApp SnapCenter	SnapCenter 4.3 or later	-
	Cisco UCS Manager	4.1(1c) or later	
Hypervisor	ESXi		
Management	Hypervisor management systemVMware vCenter Server 6.7 U3 (vCSA) or later		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 or later	
	NetApp SnapCenter	SnapCenter 4.3 or later	
	Cisco UCS Manager	4.1(1c) or later	

Next: Additional FlexPod security considerations.

Additional FlexPod security considerations

Previous: Solution benefits of FlexPod converged infrastructure.

The FlexPod infrastructure is a modular, converged, optionally virtualized, scalable (scale out and scale up), and cost-effective platform. With the FlexPod platform, you can independently scale out compute, network, and storage to accelerate your application deployment. And the modular architecture enables nondisruptive operations even during your system scale-out and upgrade activities.

Different components of an HIT system require data to be stored in SMB/CIFS, NFS, Ext4, and NTFS file systems. This requirement means that the infrastructure must provide data access over the NFS, CIFS, and SAN protocols. A single NetApp storage system can support all these protocols, eliminating the need for the legacy practice of protocol-specific storage systems. Additionally, a single NetApp storage system can support multiple HIT workloads such as EHRs, PACS or VNA, genomics, VDI, and more, with guaranteed and configurable performance levels.

When deployed in a FlexPod system, HIT delivers several benefits that are specific to the healthcare industry. The following list is a high-level description of these benefits:

- **FlexPod security**. Security is at the very foundation of a FlexPod system. In the past few years, ransomware has become a threat. Ransomware is a type of malware that is based on cryptovirology, the use of cryptography to build malicious software. This malware can use both symmetric and asymmetric key encryption to lock a victim's data and demand a ransom to provide the key to decrypt the data. To learn how the FlexPod solution helps mitigate threats like ransomware, see TR-4802: The Solution to Ransomware. FlexPod infrastructure components are also FIPS 140-2-compliant.
- **Cisco Intersight.** Cisco Intersight is an innovative, cloud-based, management-as-a-service platform that provides a single pane of glass for full-stack FlexPod management and orchestration. The Intersight platform uses FIPS 140-2 security-compliant cryptographic modules. The platform's out-of-band management architecture makes it out of scope for some standards or audits such as HIPAA. No individual identifiable health information on the network is ever sent to the Intersight portal.
- **NetApp FPolicy technology.** NetApp FPolicy (an evolution of the name file policy) is a file-access notification framework for monitoring and to managing file access over the NFS or SMB/CIFS protocols. This technology has been part of the ONTAP data management software for more than a decade—it is useful in helping detect ransomware. This Zero Trust engine provides extra security measures beyond permissions in access control lists (ACLs). FPolicy has two modes of operation: native and external:
  - Native mode provides both blacklisting and whitelisting of file extensions.
  - External mode has the same capabilities as native mode, but it also integrates with an FPolicy server that runs externally to the ONTAP system as well as a security information and event management (SIEM) system. For more information about how to fight ransomware, see the Fighting Ransomware: Part Three – ONTAP FPolicy, Another Powerful Native (aka Free) Tool blog.
- **Data at rest**. ONTAP 9 and later has three FIPS 140-2-compliant, data-at-rest encryption solutions:
  - NSE is a hardware solution that uses self-encrypting drives.
  - NVE is a software solution that enables encryption of any data volume on any drive type where it is enabled with a unique key for each volume.
  - NAE is a software solution that enables encryption of any data volume on any drive type where it is enabled with unique keys for each aggregate.

> Starting with ONTAP 9.7, NAE and NVE are enabled by default if the NetApp NVE license package with name VE is in place.

- **Data in flight**. Starting with ONTAP 9.8, Internet Protocol security (IPsec) provides end-to-end encryption support for all IP traffic between a client and an ONTAP SVM. IPsec data encryption for all IP traffic includes NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.
- **End-to-end data encryption across a hybrid, multicloud data fabric**. Customers who use data-at-rest encryption technologies such as NSE or NVE and Cluster Peering Encryption (CPE) for data replication traffic can now use end-to-end encryption between client and storage across their hybrid multicloud data fabric by upgrading to ONTAP 9.8 or later and using IPsec. Beginning with ONTAP 9, you can enable the FIPS 140-2 compliance mode for cluster-wide control plane interfaces. By default, the FIPS 140-2-only mode is disabled. Starting with ONTAP 9.6, CPE provides TLS 1.2 AES-256 GCM encryption support for ONTAP data replication features such as NetApp SnapMirror, NetApp SnapVault, and NetApp FlexCache technologies. Encryption is setup by way of a pre-shared key (PSK) between two cluster peers.
- **Secure multitenancy**. Supports the increased needs of virtualized server and storage shared infrastructure, enabling secure multitenancy of facility-specific information, particularly when hosting multiple instances of databases and software.

Next: Conclusion.

Conclusion

Previous: Additional FlexPod security considerations.

By running your healthcare application on a FlexPod platform, your healthcare organization is better protected by a FIPS 140-2-enabled platform. FlexPod offers multilayered protection at every single component: compute, network and storage. FlexPod data protection capabilities protect data at rest or in flight, and keep backups safe and ready when needed.

Avoid human errors by leveraging the FlexPod prevalidated designs that are rigorously tested converged infrastructures from the strategic partnership of Cisco and NetApp. A FlexPod system engineered and designed to deliver predictable, low-latency system performance and high availability with little impact, even when FIPS 140-2 is enabled in the compute, networking, and storage layers. This approach results in a superior user experience and optimal response time for users of your HIT system.

Next: Acknowledgements, version history, and where to find additional information.

Acknowledgements, version history, and where to find additional information

Previous: Conclusion.

To learn more about the information that is described in this document, review the following documents and websites:

- Cisco MDS 9000 Family NX-OS Security Configuration Guide

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp and Federal Information Processing Standard (FIPS) Publication 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- NetApp ONTAP 9 Hardening Guide

  https://www.netapp.com/us/media/tr-4569.pdf

- NetApp Encryption Power Guide

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE and NAE Datasheet

  https://www.netapp.com/us/media/ds-3899.pdf

- NSE Datasheet

  https://www.netapp.com/us/media/ds-3213-en.pdf

- ONTAP 9 Documentation Center

  http://docs.netapp.com

- NetApp and Federal Information Processing Standard (FIPS) Publication 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco and FIPS 140-2 Compliance

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Cybersecurity practices for medium and large healthcare organizations

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco and Cryptographic Module Validation Program (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption, and NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption and NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod for Electronic Health Record Systems

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Data Now: Improving Performance in Epic EHR Environments with Cloud-Connected Flash Technology

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- FlexPod Datacenter for Epic EHR Infrastructure

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- FlexPod Datacenter for Epic EHR Deployment Guide

  https://www.netapp.com/media/10658-tr-4693.pdf

- FlexPod Datacenter Infrastructure for MEDITECH Software

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- The FlexPod Standard Extends to MEDITECH Software

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod for MEDITECH Directional Sizing Guide

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod for medical imaging

  https://www.netapp.com/media/19793-tr-4865.pdf

- AI in Healthcare

  https://www.netapp.com/us/media/na-369.pdf

- FlexPod for healthcare Ease Your Transformation

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod from Cisco and NetApp

  https://flexpod.com/

Acknowledgements

- Abhinav Singh, Technical Marketing Engineer, NetApp
- Brian O'Mahony, Solution Architect Healthcare (Epic), NetApp
- Brian Pruitt, Pursuit Business Development Manager, NetApp
- Arvind Ramakrishnan, Senior Solutions Architect, NetApp
- Michael Hommer, FlexPod Global Field CTO, NetApp

Version History

Version	Date	Document version history
Version 1.0	April 2021	Initial release