NeuShield®

How much is your data worth?

NeuShield for Unstructured Data

HOW TO ACHIEVE SEAMLESS UNSTRUCTURED DATA PROTECTION AND ACCELERATED RECOVERY

NeuShield Data Sentinel Architecture Challenges the Norm

This paper outlines how the NeuShield architecture mitigates existing file processing vulnerabilities. It also shows how to ensure that MS SQL database data remains secure and operationally accessible to your organizations database processes only during a cyber-attack, specifically ransomware.

NEUSHIELD GUARANTEES

- No ransom payments
- Instant OS and data recovery
- Minimized recovery costs

TEST OUR RANSOMWARE PROTECTION PROMISES WITHOUT OBLIGATION.

For questions about this paper and to find out more about how NeuShield works:
Sales@neushield.com or call **+1 510-239-7962**

The Value of a Data File

The contents of a data file can be of immense value to a hacker if stolen or compromised. The effects of ransomware are devastating and expensive to organizations and their customers. Hits have recently been recorded at: Bank of America, Norton Health Care, Indian Council of Medical Research, Air Europa, NHS UK, and the British Museum to name just a few.

Ransomware (or some type of extortion) appears in 92% of industries as one of the top threats[1].

The purpose of this paper is to delve into the vulnerabilities of unstructured data protection and recovery in cyber warfare. Structured data vulnerabilities can be found in our paper addressing MS SQL databases: NeuShield for Structured Data.

We have outlined the standard creation, updates, and deletion processes for files that are controlled by the operating system (OS) and independent software vendor applications (Microsoft, Adobe, Salesforce, Intuit, Dropbox, Autodesk, etc.).

Lifecycle and Definitions of an Unstructured File

Files relate to data at a specific point in time. File types are indicated by filename extension that determines how the bytes (of data) must be organized and interpreted. Every file has a specific
size indicating how much storage is occupied by the file.

Once a file has been created, the most basic operations that programs and users can perform are:

- Change the access permissions and attributes of a file.
- Open a file, which makes the file contents available to the program.
- Read data from a file.
- Write (update) data to a file.

The user of programs can control files with a File Manager program such as Windows Explorer, Discovery Opus, FreeCommander, etc. (on Microsoft OS devices) or by command line interface (CLI).

FILE PROTECTION

File permissions control who may or may not modify, delete, or create files and folders. Users may be given permission to read and modify files or folders, alongside permissions that protect against unauthorized tampering or destruction of information in files. Read-only file attributes or immutable storage technologies can also help to protect against malware and ransomware.

FILE CORRUPTION

When a file is said to be corrupted, its contents have been saved to the computer in such a way that they cannot be properly read by either a human or by a software program. Files can also become corrupt following the execution of malicious software, such as ransomware that encrypts the data.

[1] 2024 Data Breach Investigations Report

FILE SYSTEMS AND MANAGERS

The way a computer organizes, names, stores, and manipulates files is globally referred to as its file system. The NTFS file system is the normal file system for the most recent versions of Windows. File Manager allows you to move, create, delete, and rename files and folders. They do not allow you to read the contents of a file or store information in it, this is performed by the relevant application.

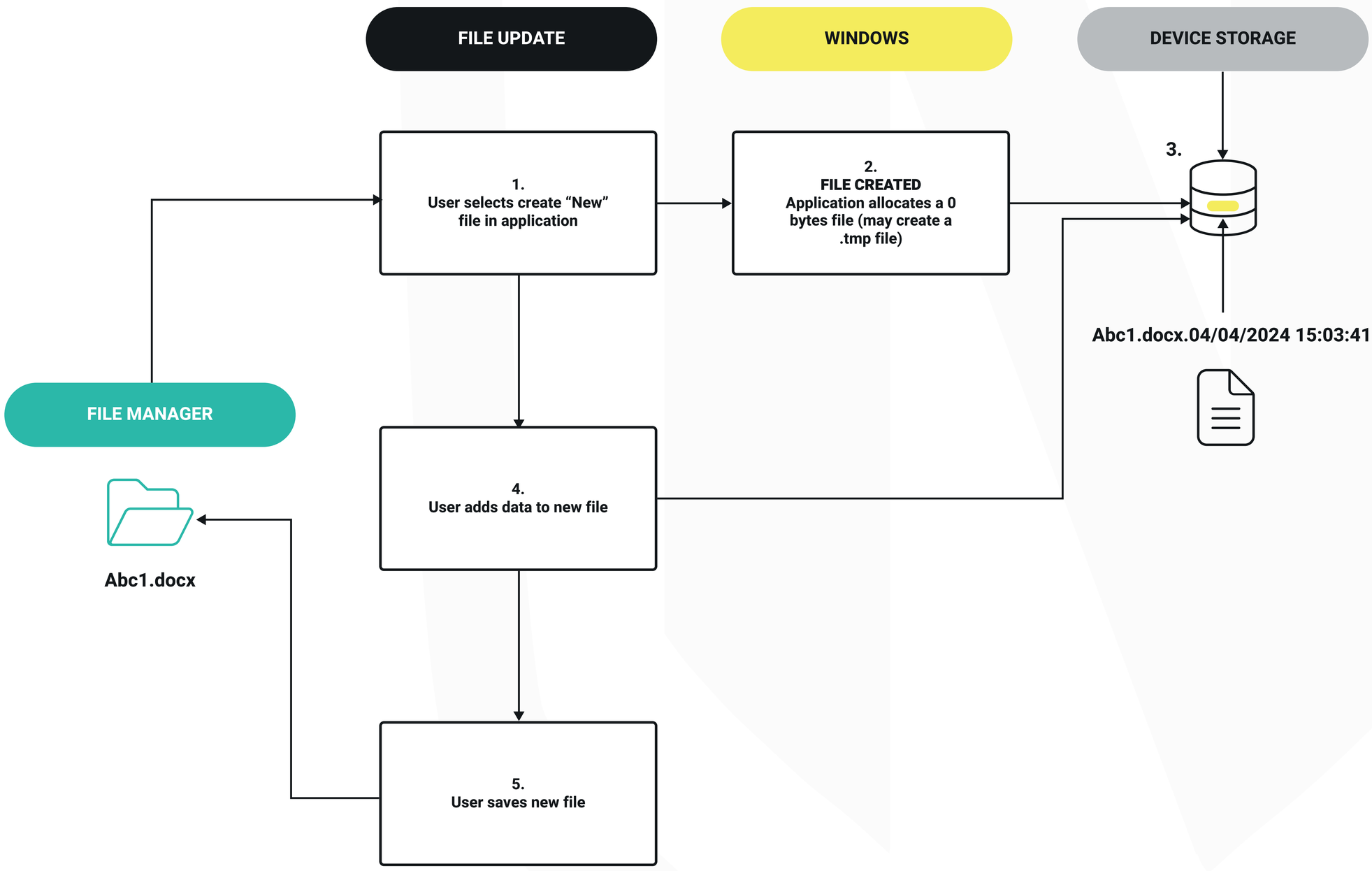
Standard File Processing

The following section provides an overview of the interaction of operating systems, applications, device storage and the File Manager when executing file instructions by a user or program.

File Creation and Update Architecture

DIAGRAM 1 - FILE CREATION AND SAVE

The diagram below provides an overview of the creation and save of an unstructured file.

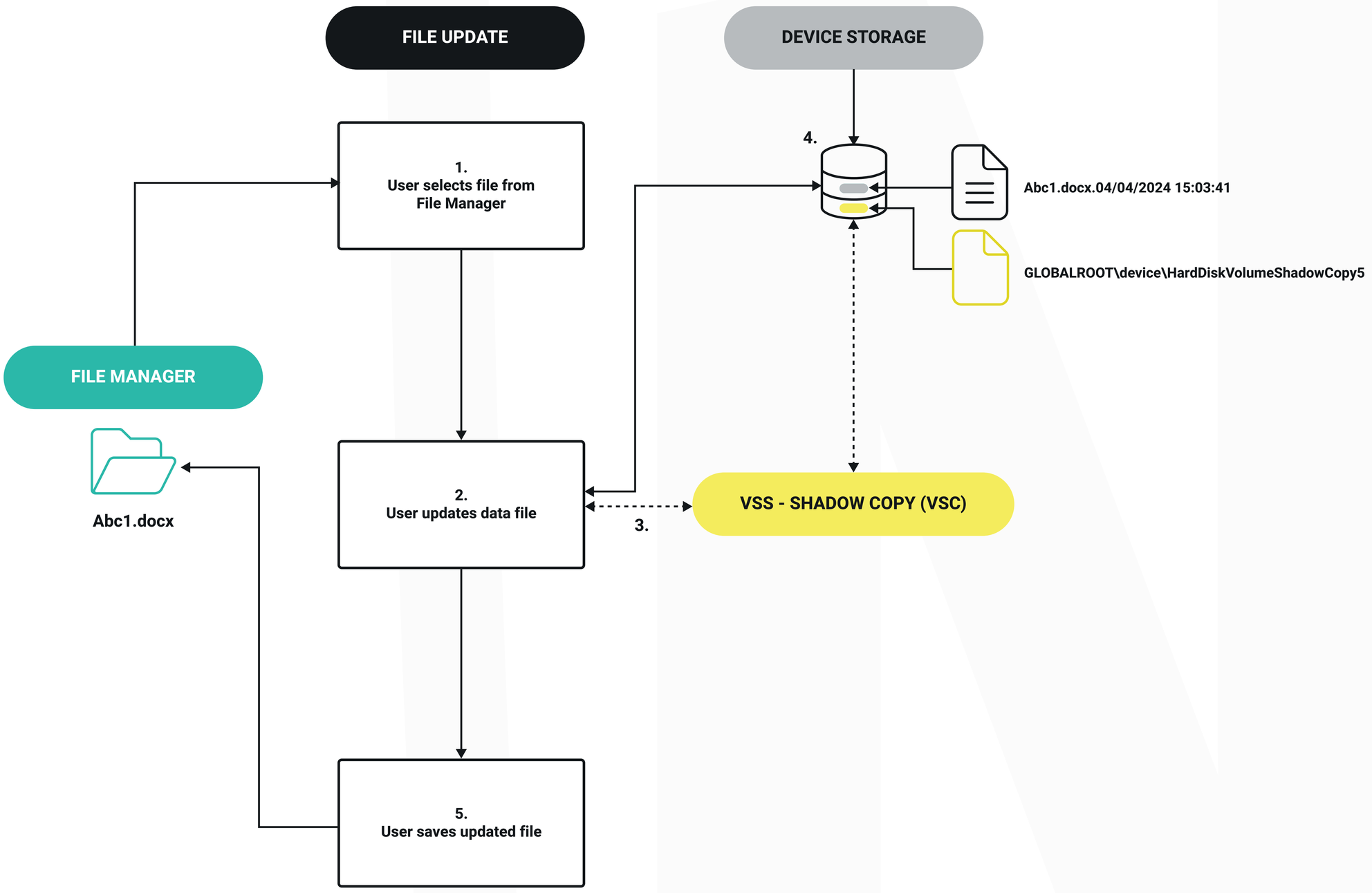


Phases:

1. Open application and select ‘new’ file.
2. Application creates a 0 bytes or .tmp file.
3. The 0 bytes (or .tmp) file is stored directly on the storage device.
4. User adds data to the file, that is written directly to the storage device.
5. User saves file, NTFS saves the file to the File Manager and the OS saves the file with a timestamp.

DIAGRAM 2 - FILE MODIFICATION & VSS VSC FILE CREATION

The diagram below provides an overview of a file modification, including the effect on the file modification when Microsoft Volume Shadow Services are enabled.



Phases:

1. User selects a file from the File Manager or recent file list in the application.
2. User modifies data in the file.
3. Prior to the application updating the file, VSS mirrors the sector in the file in a reserved storage location. Depending on the size of the update, VSS may need to create more than one VSC*. Each VSC will only contain the changed deltas of a file.
4. Once VSS has completed creating its VSC, the file is then directly modified on the storage. The updated file contains all data for the file.
5. User saves file, NTFS saves the file to the File Manager and the OS saves the file with an updated timestamp.

*__Note:__
You can have a maximum of 64 VSCs at any one time. If you reach the maximum number of VSCs or exceed the allocated storage space, VSS will start deleting older VSCs.

NeuShield Patented Architecture

To fully grasp the unique processing architecture enabled by NeuShield, it is critical that you understand how NeuShield Data Sentinel has been developed and its individual components.

NeuShield is Zero-Trust

NeuShield provides Zero Trust data protection using an endpoint agent that operates virtually unnoticeably. It consumes negligible CPU cycles and less memory than opening your web browser.

NeuShield architecture components align to Microsoft development and operating standards. Microsoft's OS works seamlessly with the Microsoft signed NeuShield Driver certificate and
passes file handles to NeuShield when it is protecting the data being accessed.

NeuShield Architecture Components and Functions

NEUSHIELD DRIVER

Permanently present following implementation of the NeuShield agent and accessible following an attack attempting to compromise the device. The only secure method to remove the NeuShield Driver is to perform an uninstall of NeuShield Agent using the uninstall password. Users with or acquiring (account takeover) privilege access cannot uninstall the NeuShield agent without the password.

RESTORE POINTS

Images of the OS and settings taken once day and used to restore full operations to a prior point in time.

OVERLAY

A virtualized section of the disk used to provide access to mirror images (for reading) and store updates to files.

COMMIT CYCLE

The scheduled transfer and integrity checking of file updates and commands from the Overlay to Mirror Shielding™ protected data.

ONE CLICK RESTORE

Restore the OS/applications and settings to a prior point in time. Removing any known and unknown malware.

MIRROR SHIELDING™

Patented technology that 1) shields protected files from being updated directly, and 2) presents a mirror image of files onto the Overlay.

DATA ENGRAMS™

Revisions ('Last Known Good States') of individual file updates that can be reverted as the primary file.

CLOUD DRIVE PROTECTION

Protects local cloud drive folders allowing destroyed or corrupted data to be recovered quickly without an Internet connection

DISK PROTECTION

Monitors all direct disk access preventing malicious programs from destroying data on the hard drive or SSD. Protects against destructive ransomware or wipers that attempt to wipe the disk.

BOOT PROTECTION

Protects the boot portion of a drive to prevent aggressive types of ransomware taking over the boot process and preventing applications from writing to the boot record.

Terminology

RESTORE

The ability to replace the current OS and settings with a prior Restore Point version.

REVERT

The ability to replace the current file to a prior Data Engramn" "Last Known Good State."

LAST KNOWN GOOD STATE

A version of a file or OS that has been committed as a Data Engram• and has not previously encountered any suspicious file activity.

NeuShield File Processing Flow

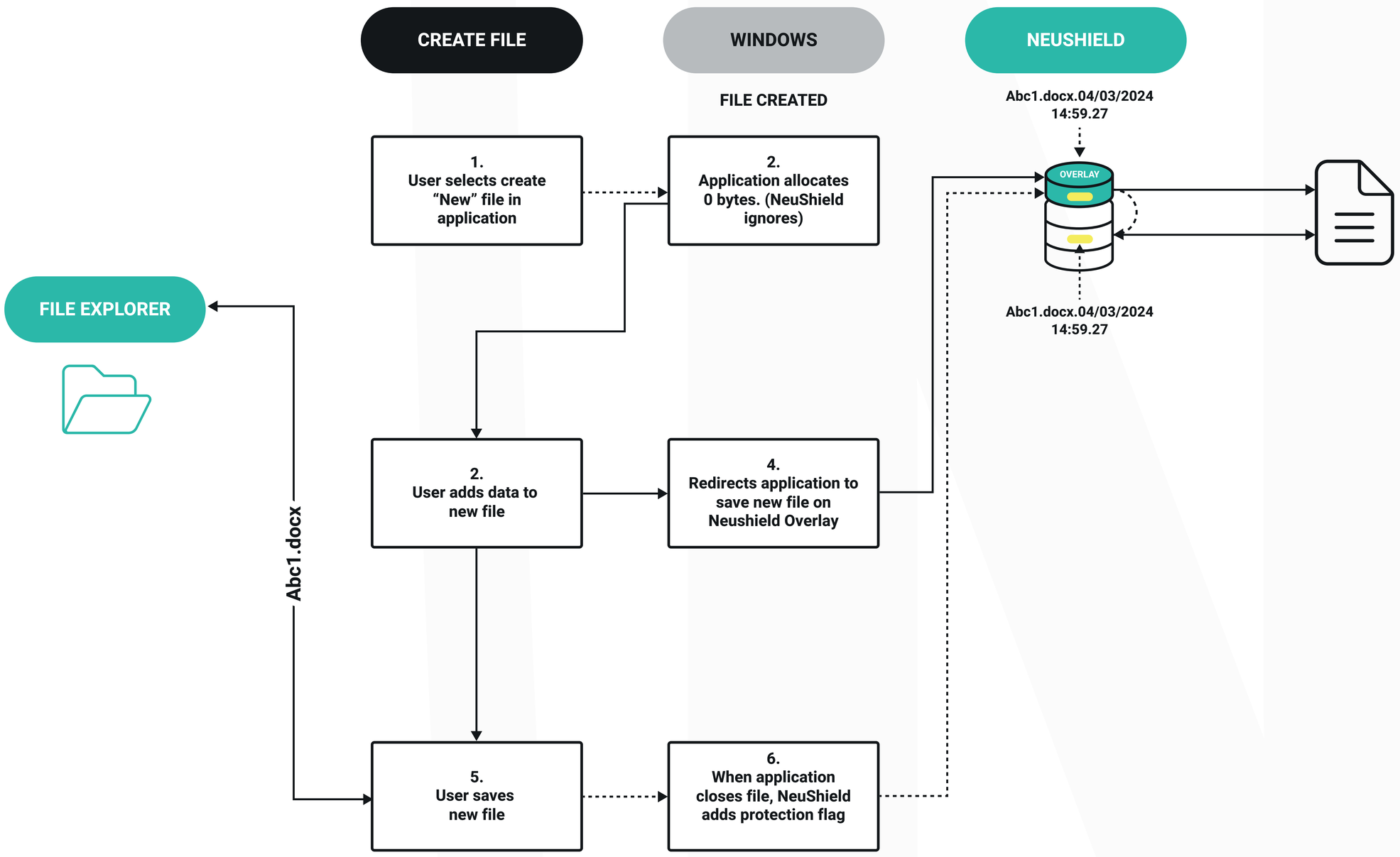
When a user updates an existing file under NeuShield protection, all updates to the file remain in the NeuShield Overlay. When the user saves the updated file, the applicable application will save the updates to the file and reflect these changes in the File Manager. At the time of application save, the NeuShield Driver will assign a protection flag to the file updates that are in the Overlay.

When the next NeuShield Commit Cycle occurs, the NeuShield Driver will undertake its file integrity checks, looking for suspicious file activity within the updates. When the Commit Cycle is complete the updated file (previous version and updates) is now fully protected by NeuShield's Mirror Shielding™, reflecting the same timestamp as that shown in the File Manager. NeuShield will create a new Data Engram™ ('Last Known Good State') of the previous version of the file for future recovery or operational uses.

NeuShield Interacting with Standard File Processing

DIAGRAM 3 - NEUSHIELD CONTROLLED FILE CREATE AND SAVE

The diagram below provides an overview of the creation and saving of an unstructured file using NeuShield.

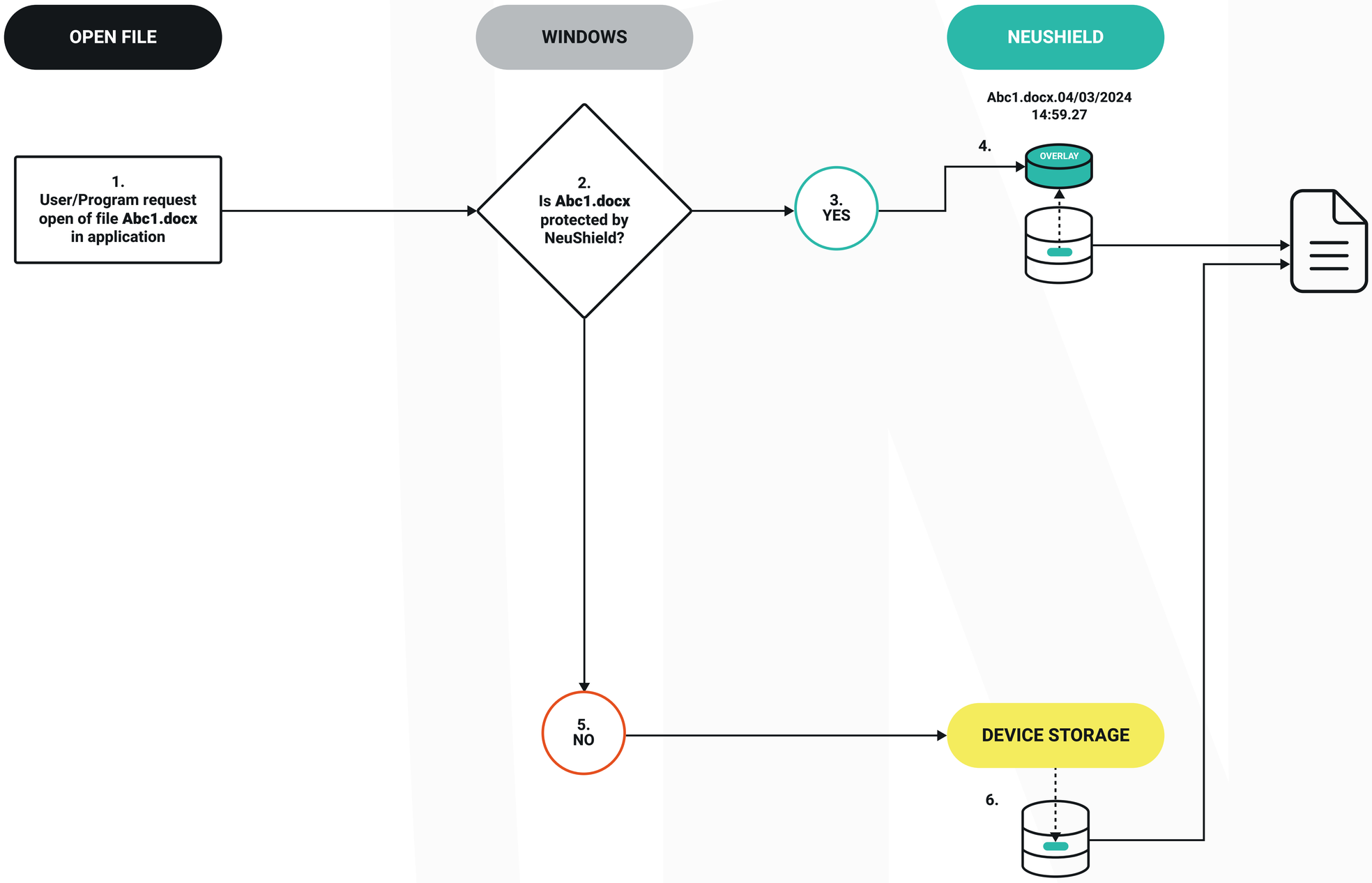


Phases:

1. Open Application and select a new file.
2. Application creates a 0 bytes or .tmp file. NeuShield ignores the creation of this file.
3. User adds data to the file.
4. The OS redirects applications to store data on the NeuShield Overlay.
5. User saves file. NTFS saves the file to the File Manager and the OS saves the file with a timestamp.
6. When the file is saved NeuShield adds a protection flag.
7. The application saved file can be viewed and will show the file with its timestamp in the Overlay.
8. NeuShield Commit cycle schedule will move data from the Overlay to the protected storage, following file integrity checks. This creates a new protected file’ “Last Good Known State” Abc1.docx.04/03/2024 14:59.27. The Overlay will be cleaned, ready for new data collection.

DIAGRAM 4 - NEUSHIELD & STANDARD FILE READ

Diagram 4 below provides an overview of a file read when NeuShield is protecting data in the organization, compared to data that is not protected by NeuShield.

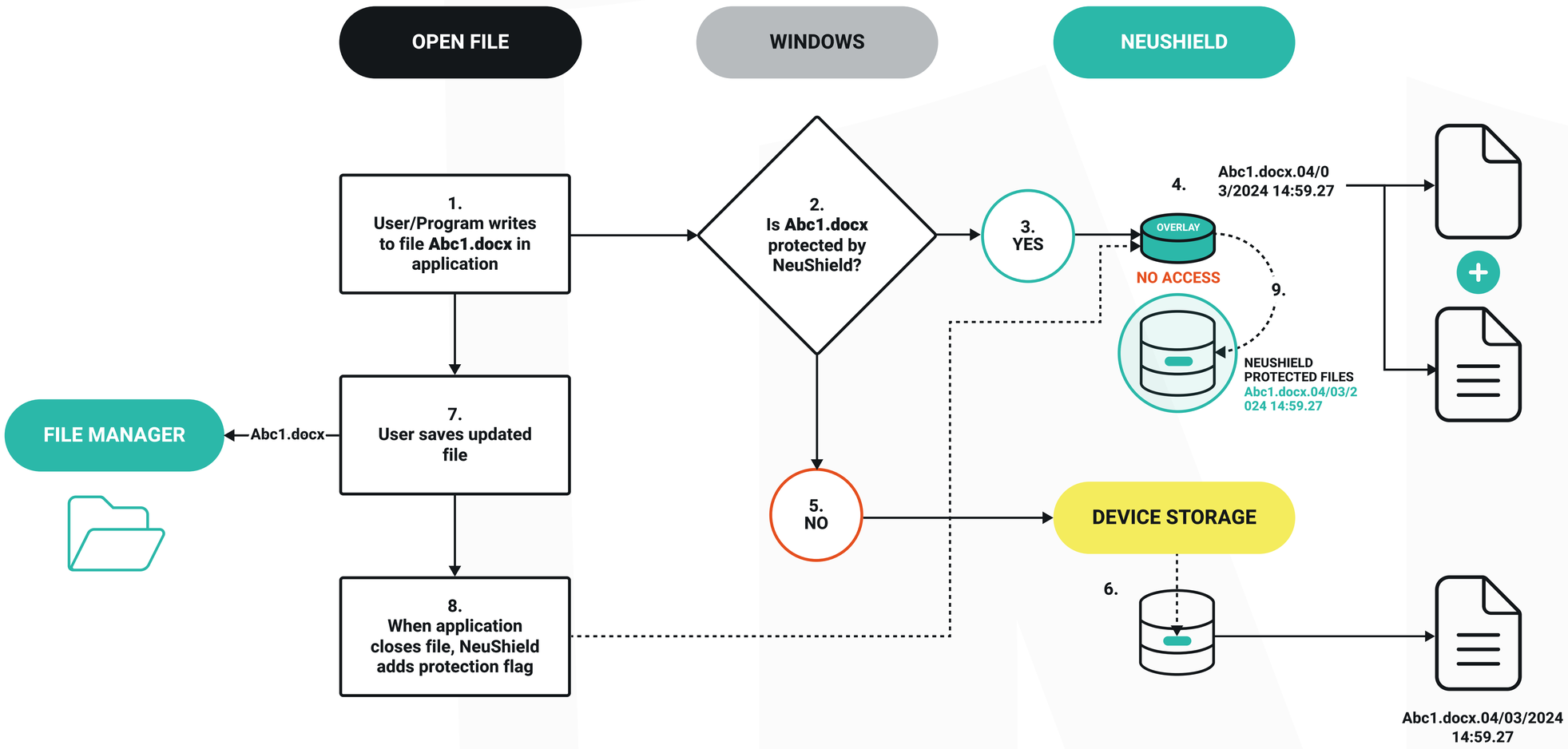


Phases:

1. User opens an existing file.
2. The OS determines if the file is managed by NeuShield.
3. If the file is managed by NeuShield.
4. The OS passes the handle to NeuShield. NeuShield then opens the handle to the file and creates a new handle to a mirror image (zero byte) file on the Overlay and gives the handle back to the application. NeuShield will read the data from the file and pass it to the application via the mirror handle.
5. If the file is not managed by NeuShield.
6. The OS will use the handle to read the data directly from the device storage and pass it to
7. the application.

DIAGRAM 5 - NEUSHIELD & STANDARD FILE UPDATE

The diagram below provides an overview of a file modification when NeuShield is protecting some of the data in organization, compared with data that is not protected by NeuShield.



Phases:

1. User selects a file from the File Manager or recent file list and updates the data.
2. The OS determines if the file is managed by NeuShield.

If the file is managed by NeuShield:

• (3) The OS passes the handle to NeuShield.
• (4) NeuShield opens the handle to the file and creates a new handle to a mirror image (zero byte) of the file on the Overlay. It then gives the handle to the application in use. All data updates will then be written to the Overlay.

The file is not managed by NeuShield:

• (5) The OS will use the handle.
• (6) Application updates the data directly to the device storage.

File Manager:

1. When the file is saved, NTFS saves it to the File Manager and the OS sets an updated timestamp. NeuShield adds a protection flag to the data in the Overlay. The (application) saved file can be viewed in the File Manager or viewed via NeuShield showing the file with its latest timestamp in the Overlay.

NeuShield Commit Cycle:

8. The Commit Cycle schedule will move data from the Overlay to the protected storage, following file integrity checks. This creates a new protected file ‘Last Good Known State’ Abc1.docx.04/03/2024 15:02:23. The Overlay will be cleaned, ready for new data collection.

How to Stop Ransomware Compromising Unstructured Data

The following section shows how NeuShield Data Sentinel patented architecture stops ransomware from compromising your data during its discovery and payload phases.

When compared to the continued processes of standard file controls. NeuShield's depth of protection and recovery value has the following additional benefits:

- Prohibits direct writes to the boot portion of your disk drives preventing malware from writing to the boot record.
- Protects against destructive ransomware or wipers that attempt to wipe the disk.
- Protects local cloud drive folders.
- Protects the OS and settings.

Ransomware Stages

A cyber hacker will send hundreds or thousands of attacks attempting to penetrate organizations. An attack will comprise of two phases:

DISCOVERY PHASE

Once an organization has been breached the malware will move vertically and laterally around the network. It will be looking for sensitive and recovery data stored within file systems and File Managers. Once it has a full topology of data locations it will compromise all accessible recovery data, normally by encrypting or deleting it.

PAYLOAD PHASE

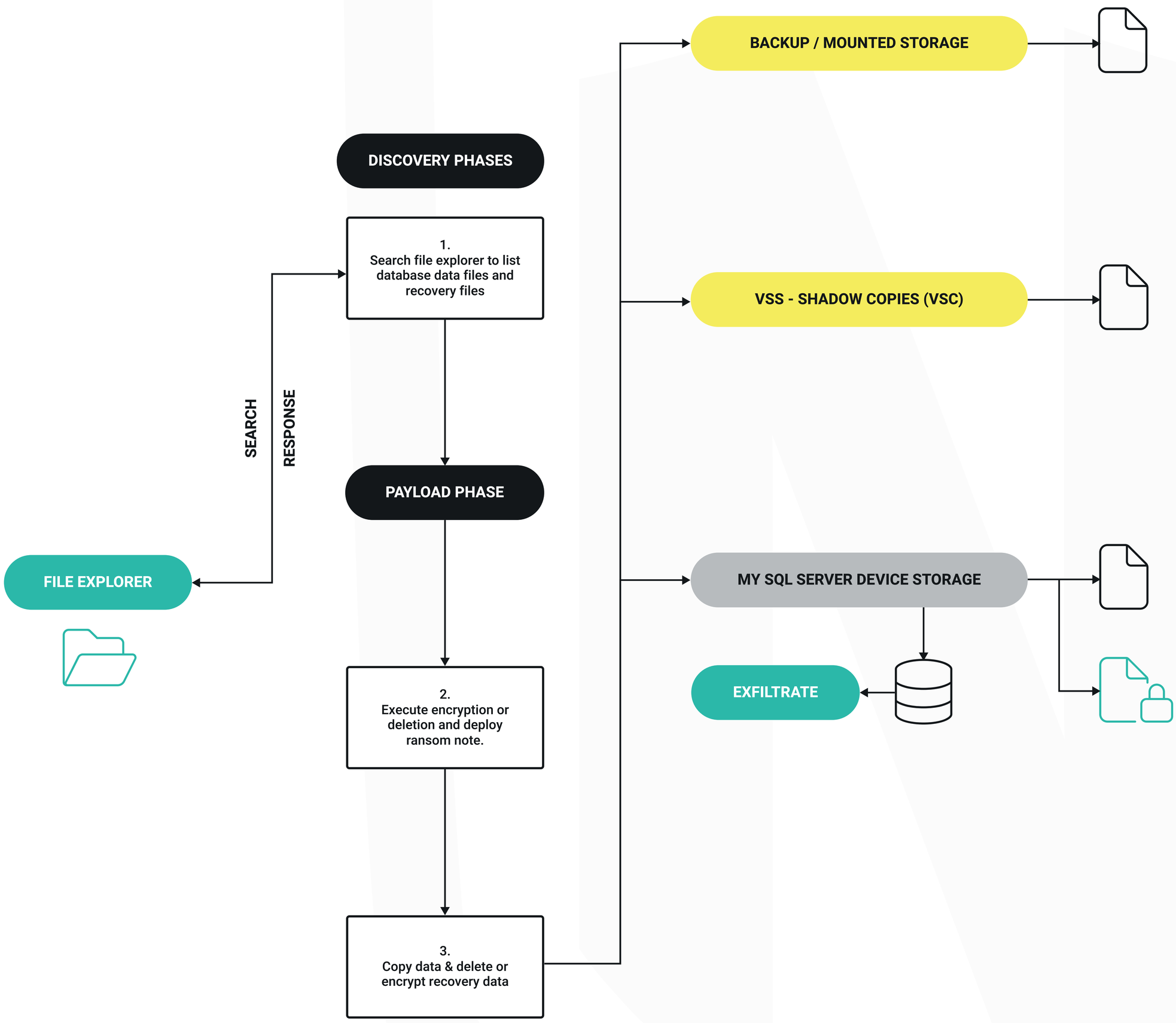
This uses information from the discovery phase, breaching the organization's network to deploy the intended payload to encrypt and copy (exfiltrate) data. A ransomware note will be embedded in the files to alert the organization to the hacker's demands.

With standard file processing the organization will be left with two options:

1. Pay the ransom and hope the hacker provides the decryption key.
2. Do not pay the ransom and rebuild the data from uncompromised backup data.

DIAGRAM 6 - RANSOMWARE ATTACK - WITHOUT NEUSHIELD

The diagram below provides an overview of a ransomware attack when data is not protected by NeuShield.

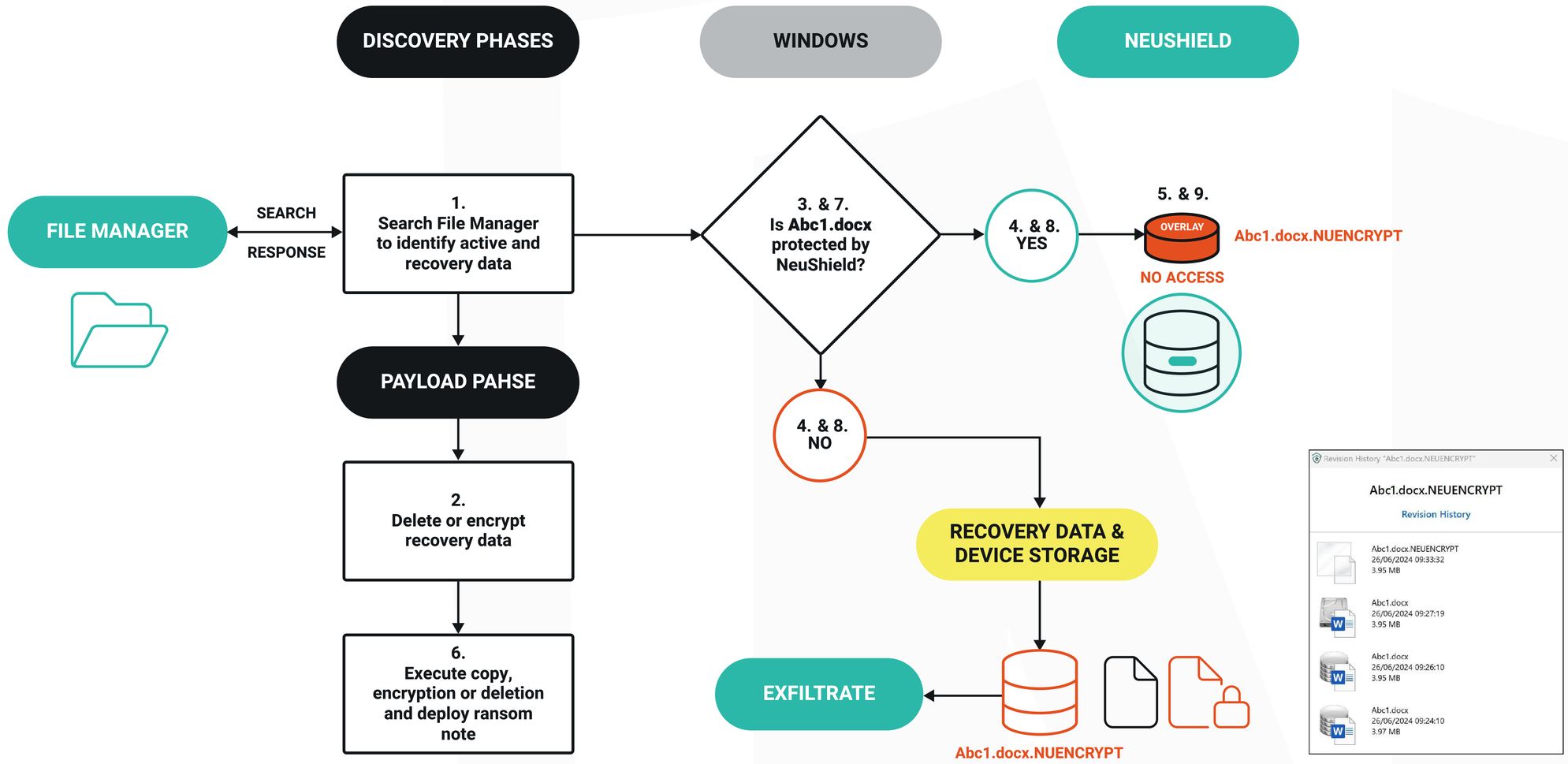


Phases:

1. Hacker malware gains entry to the network and searches for sensitive and recovery data.
2. Hacker sends ransomware to encrypt and exfiltrate data. The malware will deposit a ransomware note in the files outlining their demands.
3. Hacker sends malware to copy and exfiltrate data, encrypt or delete all accessible recovery data.

DIAGRAM 7 - RANSOMWARE ATTACK - WITH NEUSHIELD

The diagram below provides an overview of a ransomware attack when data is protected by NeuShield.



Phases:

Ransomware Discovery:

1. Hacker gains entry to network and searches for sensitive and recovery data

.

Ransomware Payload:

2. Hacker sends malware to compromise data.
3. The OS determines if the file is managed by NeuShield.

The file is managed by NeuShield:

• (4) The OS passes the handle to NeuShield.

• (5) NeuShield opens the handle to the requested file(s) and creates new handles to a mirror image (zero byte) of the files on the Overlay. This handle is given to the ransomware. All encrypted data or delete commands will be written to the Overlay. Any ransomware note is stored on the Overlay within the file update. No write or delete operations can penetrate beyond the Overlay.

The file is not managed by NeuShield:

6) The OS will use the handle to update data with the malware operation (encryption /delete) directly to the files on the device storage.

7. Following the compromise of active data, further ransomware is executed to compromise the recovery data. The interaction between Windows OS and NeuShield will follow the same processes as outlined in steps 3-6.

NeuShield Data Sentinel Business Edition is unable to stop the malware from copying and exfiltrating data from the device storage. See our paper on structured data protection that provides anti-exfiltration support.

Recovering from a Ransomware Attack

Standard Incident Response in the Event of a Successful Attack

- The organization will be unable to read any of its compromised data.
- All compromised systems will become inoperable and associated business operations will come to a halt.
- Organizations will invoke their incident response strategy, disable networks to minimize the spread of the malware and mitigate secondary attacks.
- Senior management will need to decide if they will pay the ransom or rebuild their devices and data from any offsite or uncompromised backup data.
- Assuming that no ransom will be paid, and depending on the scale of the attack, the recovery of data will be determined by accessibility to any uncompromised data and networks to move the data from its current location back on to operational devices.
- In many use cases, it can take 14 days to eradicate and start rebuilding data. Full operations will be established incrementally over ~34 weeks[2] .
- Immaterial if you decide to pay the ransom or not, you will be expected to find extreme budgets you never planned. The average cost of a data breach (without the ransom payment) increased by 12% to $4.5million in 2023[3].

A successful ransomware attack indicates that your endpoint security tools have been evaded and your data has been compromised without IT support being aware that such an attack is active.

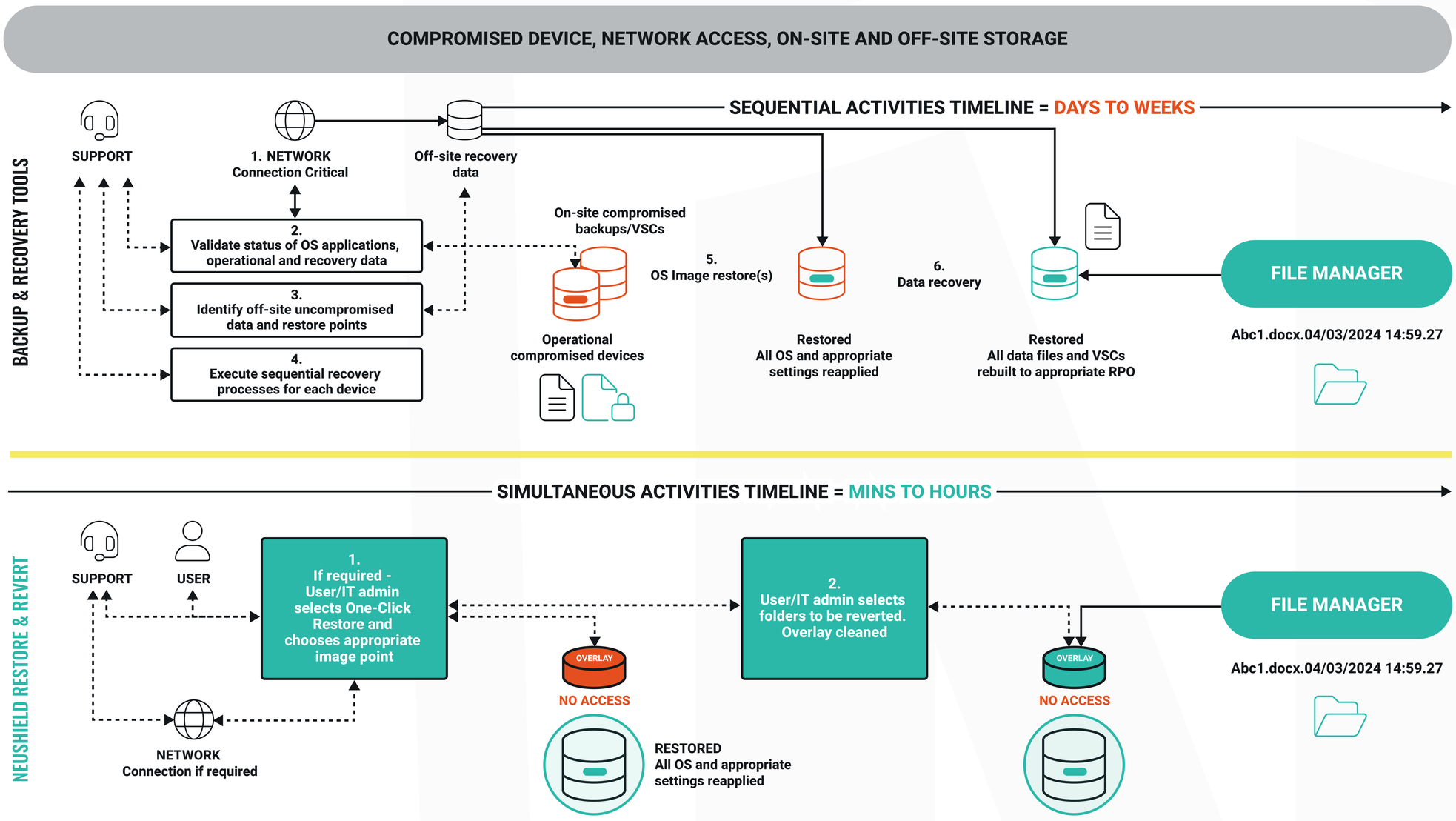
Without the security tools detecting and blocking the attack, no alerts can be sent to an appropriate security information and event management (SIEM) system or on the security tool user portal.

IT support will only be alerted to the ransomware attack following failure of an operational system or a user informing them that they are unable to access their device data.

[2] Ransomware survival guide: Recover from an attack, https://dxc.com/us/en/insights/perspectives/paper/ransomware-survival-guide-recover-from-an-attack
[3] Ponemon Institute: 2024 Cost of a Data Breach Report

DIAGRAM 8 – TRADITIONAL INCIDENT RESPONSE FOLLOWING A RANSOMWARE ATTACK

The diagram provides an overview of recovering data and OS as part of standard incident response activities following a ransomware attack.



Standard Recovery Process

The following process aligns to the illustration in diagram 8 above the centre line.

Incident Response Phases:

1. IT Support teams disable all network connections to minimize the spread of malware. Following initial high level attack appraisal, IT Support teams re-establish a network connection.
2. Validate status of OS, applications and data on all devices.
3. Validate all offsite uncompromised recovery data and restore points.
4. If OS and applications need to be recovered, execute recovery processes to rebuild from appropriate system OS image(s).
5. OS system images are complete.

(4) Execute the sequential recovery of device data.

6. All data files and VSCs (if required) have been restored. File Manager reflects recovered data.

Each of the OS and data recovery phases have to be performed sequentially.

Network connectivity will be at a premium and the sustained rate of the bandwidth will determine the speed that restore points and data can be transferred between external and internal devices. Priority will be given to operational systems and devices. All employee devices will be recovered based on the users role in re-establishing business operations. All other employees will need to wait until operations are re-established before they can safely reconnect and operate across the IT infrastructure.

Incident Response with NeuShield in the Event of a Successful Attack

The illustration below the center line in diagram 8, shows the flow of incident response when NeuShield is protecting the device and data.

Each NeuShield device recovery can be performed simultaneously.

NeuShield Incident Response Phases:
NeuShield will alert the user/IT administrator immediately when it detects suspicious file activity. The NeuShield alert will be your first notification of an attack.

1. The IT administrator can access the NeuShield portal to restore the OS if it has been compromised. Alternatively, the user can select One-Click Restore from the File Manager.

2. The user/IT administrator will access either the File ManagerΔ or NeuShield portal and select the folder(s) to revert. NeuShield will clean the Overlay of compromised data and revert all files in the folder(s).

Δ - If the user cannot access the NeuShield portal or contact IT Support, reverting files can also be executed directly within the File Manager. Users right-click the compromised folder(s) to select the NeuShield logo. This will allow you to choose Commit/ Revert. Selecting Revert will clean the compromised data. Although slightly slower as you revert one folder at a time, this enables users to recover their devices immaterial of location or network connectivity.

Windows Recovery

If the device is unbootable or access to NeuShield portal is not available, the user/IT administrator should run the Windows Recovery process. Select one of the NeuShield restore points that will be available as this will be faster than recovering using a Windows image.

Summary

This paper has outlined how NeuShield Data Sentinel device data and OS protection can be delivered with no impact to your existing operations and work seamlessly with all Microsoft architecture and applications.

NeuShield increases your capability with minimal controls to instantly recover system, operational and user device data. User capability to recover their devices and data reduces the impact on IT Support during incident recovery.

When time is a critical dependency during a ransomware attack, the simplicity of reverting and restoring data simultaneously reduces your incident response down to minutes and hours, not days and weeks.

NeuShield®
How much is your data worth?

Contact us today to actively protect your data and deliver instant recovery. Re-establish operations faster without additional costs.

NeuShield Data Sentinel does more than just detecting and blocking ransomware. We're the only anti-ransomware solution that can recover encrypted data from any known, unknown or zero-day threat. No matter how much data is encrypted NeuShield can get it back instantly from any laptop, desktop or server. NeuShield is an endpoint agent that works locally to recover data without using a backup or internet connection.

sales@neushield.com

NeuShield, Inc
200 Brown Road, Suite 306
Fremont, CA 94539
Main: +1 510-239-7962
Toll Free: +1 888-999-0965 (U.S.)

WWW.NEUSHIELD.COM