NeuShield®

How much is your data worth?

NeuShield's Unfair Advantage

NEUSHIELD STANDS ALONE IN THE ANTI-RANSOMWARE PROTECTION LANDSCAPE

NeuShield Data Sentinel Challenges Anti-ransomware Competitors

The growth in ransomware as an attack scenario has meant that ransomware protection market positioning and differentiation is being abused by almost every cyber security and data protection vendor.

NEUSHIELD GUARANTEES

- No exfiltration of data or unauthorized data modification
- 99% faster business continuity after a ransomware attack
- Minimized recovery costs
- Never pay a ransom demand

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**

Eradicate the Smoke and Mirrors from Reality of Vendor Claims

Ransomware payments in 2023 surpassed the $1 billion mark , the highest number ever observed. Although 2022 saw a decline in ransomware payment volume, the overall trend line from 2019 to 2023 indicates that ransomware is an escalating problem. This does not capture the economic impact of productivity loss and repair costs associated with attacks.

Malware designed to encrypt files on a device, ransomware renders them and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data. The application of both tactics is known as "double extortion."

Organizations of all levels of maturity and size should be prepared for ransomware and data extortion incidents.
The growth in ransomware as an attack scenario has meant that ransomware protection is being abused as market positioning and a differentiator by almost every cyber security and data protection vendor.

In order to eradicate the smoke and mirrors from reality, this paper outlines the explicit moment of ransomware protection effectiveness for existing security and data protection tools.

By understanding the reality of effectiveness from existing security and data protection tools, we show how NeuShield Data Sentinel has a precise role in mitigating the effects of ransomware.

Anti-Ransomware Effectiveness Stages

Table 1 outlines the two phases of product effectiveness for ransomware detection, mitigation, and recovery. Each is very explicit in their roles and very rarely is a security or data protection tool core functionality effective across both

TABLE 1 – PHASES OF RANSOMWARE DETECTION, MITIGATION, AND RECOVERY

PRIMARY	First line of defense to detect and block active ransomware entering and/or attempting to executing across an organization's infrastructure before it has the opportunity to encrypt, delete and/or copy sensitive data for the purpose of financial extortion.
SECONDARY	Minimizes and nullifies the spread and effect of the ransomware attack. Recovers compromised sensitive data using prior data backups, volume shadow copies or other techniques such as capturing encryption keys to decrypt the data. These actions minimize the need to pay the ransom demand.

Anti-Ransomware Mitigation Effectiveness Categories

The cyber security ransomware protection landscape has a multitude of different categories, the primary security and data protection tools used to detect and mitigate ransomware attacks are:

EMAIL SECURITY

According to the most recent StationX statistics, an estimated 35% of ransomware attacks are delivered via email. Email security tools fit into three categories Gateways, Cloud and Data Protection from software vendors such as Abnormal, Barracuda, Cloudfare, Cisco, Echoworx, Fortra, IronScales, Microsoft, Proofpoint, and Tessian amongst many others that are used to detect and mitigate ransomware attacks in messaging before it can compromise endpoint devices.

NETWORK AND PERIMETER BOUNDARY

Security tools fit into categories such as NextGen Firewalls, Network Detection & Response (NDR) and Intrusion Protection & Detection from vendors; Barracuda, Check Point, Cisco, DarkTrace, ExtraHop, Palo Alto, SonicWall, Trellix, Vectra AI amongst many others are used to detect and mitigate ransomware attacks from entering and traversing across an organization's networks.

ENDPOINT

Security tools fit into categories such as Endpoint Detection & Response (EDR), Endpoint Protection Platforms (EPP), NextGen Antivirus (NGAV) and Extended Detection & Response (XDR) from vendors; Crowdstrike, Cybereason, Datto, ESET, Kaspersky, Malwarebytes, Microsoft, Sentinel One, Sophos, Trend Micro, VMware (Carbon Black), WithSecure, amongst many others are used to detect and mitigate ransomware attacks from compromising endpoint devices and servers.

BACKUP & RECOVERY

Data protection tools from vendors such as Acronis, Arcserve, Cohesity, Commvault, Dell EMC, Druva, IBM, Microsoft, Rubrik, Unitrends, Veeam, Veritas amongst many others are used to replicate active data for future recovery purposes. In addition, these tools may offer features that detect and remove malware in data copies, alongside using immutable storage to mitigate unauthorized changes to the data.

OTHER

Malware detection and data recovery tools and cyber insurance can be implemented alongside tools in the previous categories. These tools and policies offer additional ransomware mitigation, recovery of encrypted data or lessen the impact for organizations that can reclaim elements of the costs required to recover operations.

Ransomware Protection Effectiveness

Table 2 places example vendors for each of the ransomware protection categories aligned to their effectiveness across phases of ransomware detection, mitigation, and recovery.

The 'Flow of Response' arrows indicate the order that security tools will engage and respond to attempted and successful ransomware attacks. Dependent upon the primary attack vector being used by the Hacker, email security and network & perimeter security tools can be interchanged as the first and second lines of defense.

TABLE 2 – PHASES OF RANSOMWARE DETECTION, MITIGATION, AND RECOVERY

	FLOW OF RESPONSE	EMAIL SECURITY	NETWORK & PERIMETER SECURITY	ENDPOINT SECURITY	OTHERS	BACKUP & RECOVERY
		1	2	3	4	5
PRIMARY	1	Abnormal, Barracuda, Cloudfire, Cisco, Echoworx, Fortra, IronScales, Microsoft, Proofpoint, and Tessian	SonicWall, Cisco, Barracuda, Check Point, Palo ALto, Trellix, ExtraHop, DarkTrace, Vectra AI	Crowdstrike, Microsoft, Sentinel One, Kaspersky, Sophos, VMWare (Carbon Black), Cybereason, ESET, Datta, Malwarebytes, Trend Micro, WithSecure	Morhpisec	
Vendors & channel sales partners offering the above categories as MDR, XDR, MSSP, MSP services have no additional features.						
SECONDARY	2			Microsoft - VSS Sentinel One - VSS	Halcyon Cyber Insurance	Veeam, Commvault, Rubrik, Veritas, Cohesity, Dell EMc, Arcserve, Druva, Acronis, IBM, Microsoft, Unitrends

PRIMARY PHASE RANSOMWARE EFFECTIVENESS

Immaterial of vendor, malware detection and blocking for the security tools 1 to 3 are reliant on their anti-malware engine architecture. Security tools in phase 4 work independently of the security tools in phases 1-3, attempting to detect what has been missed in previous phases. Phase 5 does not stop the ransomware from compromising the active operational data. Once the malware engines in security tools 1-4 have been evaded, these tools play no further part in ransomware mitigation.

SECONDARY PHASE RANSOMWARE EFFECTIVENESS

All security tools in the Primary phase of ransomware detection have no core functionality to assist with secondary ransomware effectiveness.

- Vendors identified in Secondary phase 3, offer external features (for additional cost) such as Microsoft Virtual Shadow Services (VSS) to capture Volume Shadow Copies (VSC) upon data modification. The VSCs are used to reverse the effects of encryption on protected data. In order to use a VSC to recover the encrypted data. Vendors offering VSS must detect and block the ransomware in their endpoint security tool; no detection and block, renders their VSCs unusable.

- Phase 4 security tool category does not stop the ransomware from executing as these tools are reactive and require the ransomware variant to be listed in their intelligence engine. When the variant is known, the tool captures the encryption key and uses this to decrypt the data. If the variant is listed in malware engines, the ransomware would be blocked in the Primary phase by the leaders in malware detection, without need for these secondary tools.

- Phase 5 invokes traditional recovery procedures from prior versions of data backups and restore points. Product vendor claims of effectiveness for ransomware protection occurs solely to inhibit the malware from compromising a copy of the backup data that is stored on immutable, tape or air-gapped storage.

NeuShield is Truly the Only Anti-ransomware Solution

NeuShield was specifically built to stop ransomware attacks at the data level. It should never be considered as a replication of the traditional malware detection or backup recovery purposes of categories 1-5.

Table 3 identifies the value of NeuShield's patented architecture across Primary and secondary phases of ransomware mitigation and recovery when tools in categories 1-5 have failed. NeuShield delivers the only capability to immediately revert your data directly from the targeted device.

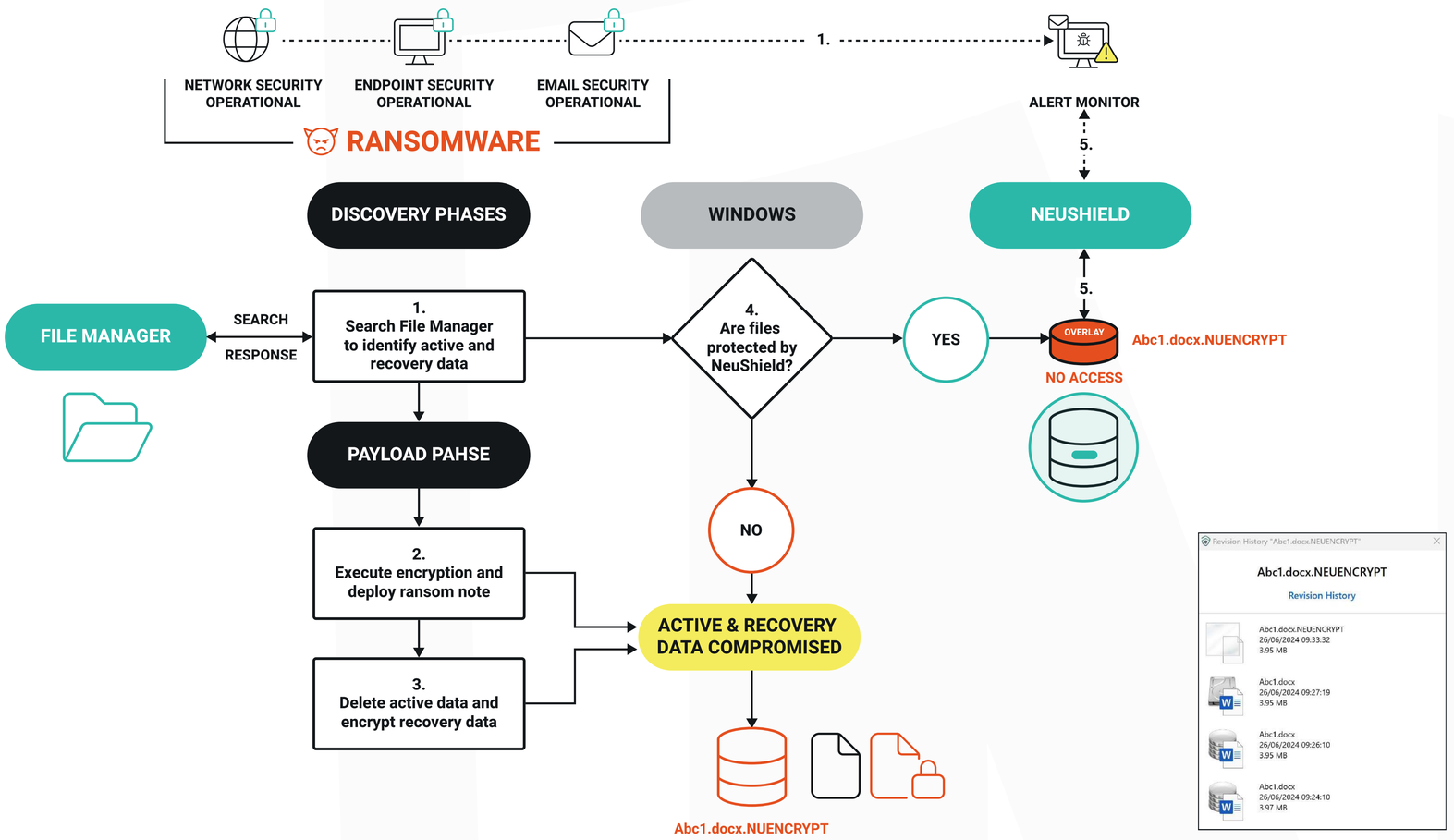
TABLE 3 - NEUSHIELD ANTI-RANSOMWARE EFFECTIVENESS

	EXISTING CATEGORIES EFFECTIVENESS	NEUSHIELD EFFECTIVENESS
PRIMARY	First line of defense to detect and block active ransomware entering and/or attempting to executing across an organization's infrastructure before it can encrypt, delete and/or copy sensitive data for the purpose of financial extortion.	If security tools have been evaded, NeuShield is the first line of defense immediately alerting IT administrators and users that malware is attempting to compromise their data. NeuShield architecture is not dependent on knowing the attack vector/type. NeuShield stops any suspicious updates on protected active data, boot sector and data from being exfiltrated (MS SQL). NeuShield cannot be removed /compromised by ransomware or using stolen credentials (admin privilege).
SECONDARY	Minimizes and nullifies the spread and effect of the ransomware attack. Recovers compromised sensitive data using prior data backups, volume shadow copies or other techniques such as capturing encryption keys to decrypt the data. These actions attempt to minimize the need to pay the ransom demand	All NeuShield protected devices can be restored without network connectivity by the user or IT support. Recovery starts instantly, requiring only two clicks by the user or IT administrator to return the device (OS & data) back to operational status within minutes/hours. Recovery can be undertaken simultaneously without data transfer delays as NeuShield only reverts data and restore points already resident on the protected device.

Unstructured Data Ransomware in Action

Diagram 1 explains how NeuShield protects your unstructured data from a ransomware attack, compared to your continued reliance of existing security solutions.

DIAGRAM 1 – NEUSHIELD MITIGATES UNSTRUCTURED DATA RANSOMWARE ATTACK



UNSTRUCTURED DATA RANSOMWARE ATTACK – EXISTING PROTECTION CATEGORIES

Ransomware has evaded your security detection tools. The tools are fully operational with their malware engine signatures and AI algorithms up to date.

- Failure to detect the ransomware means no alerts have been passed to the IT/SOC alert monitor and the malware can start to list all data in your file systems.
- The Hacker can initiate its attack, unnoticed, compromising your active data, dumping a ransomware note in your encrypted files.
- The Hacker will now encrypt and/or exfiltrate all identified recovery data, backups and VSCs.

UNSTRUCTURED DATA RANSOMWARE ATTACK – NEUSHIELD PROTECTED

NeuShield proves its true value by continually protecting the data and device OS, immaterial of attack type.

- Failure to detect the ransomware means no alerts have been passed to the IT/SOC alert monitor and the malware can start to list all data in your file systems.
- Windows OS checks if the data being requested by the malware is managed by NeuShield. Once Windows OS passes the ransomware commands to NeuShield, the malware is unaware it is now working with zero-byte virtualized images of the data.
- NeuShield Instantly alerts the user & IT support team that suspicious file activity is occurring. All data modifications are happening on the NeuShield overlay with no access to the protected active data. If the Hacker is monitoring the files, they will believe the attack is successful as NeuShield's overlay provides the impression that files have been compromised.

As the Hacker/malware is unaware that its attack is being undermined, the ransomware will continue its attack with no effect on the protected live data.

MS SQL Structured Database Data File Ransomware in Action

NeuShield Datacenter Edition delivers increased protection for organizations with MS SQL servers in addition to file servers with large (<2TB) individual data files and 64TB server clusters. Additional features for MS SQL servers prohibits updates to data files and stop data files from being exfiltrated when commands are executed from non-SQL processes. The feature rich capability of a NeuShield Datacenter license is provided for one price. NeuShield has no hidden pricing in any of its products.

DATABASE GUARDIAN

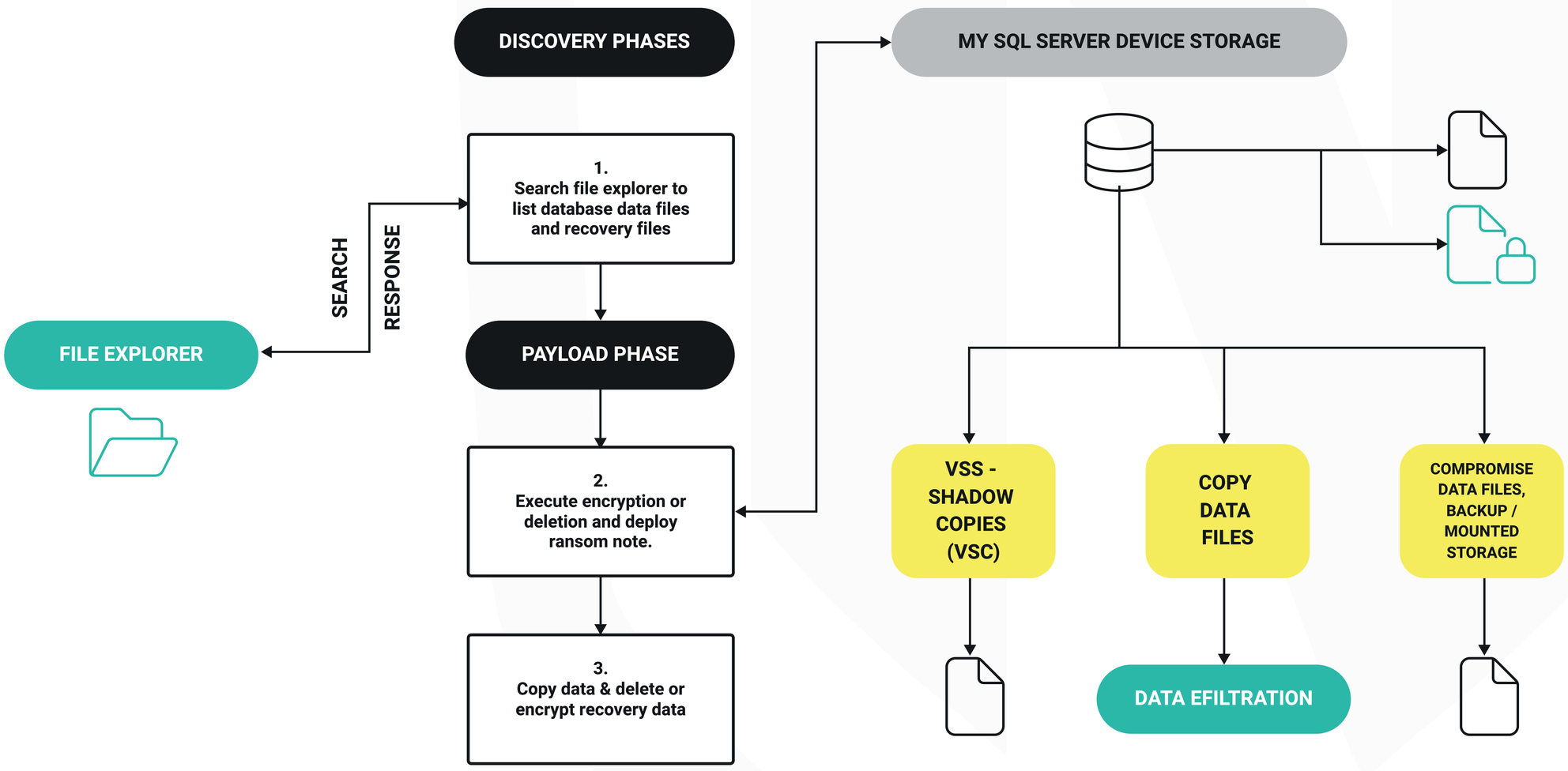
Database Guardian offers the ability to protect the database data files from being modified. When Database Guardian is enabled, it will prevent modifications to all files in the 'Data' folder. If there are multiple data folders or multiple instances of SQL, then all the data folders will be protected. This helps prevent the SQL data files from being ransomed. Database Guardian is different from Mirror Shielding. Mirror Shielding redirects changes to an overlay, Database Guardian prevents modifying the data altogether.

EXFILTRATION PROTECTION

Exfiltration protection is designed to prevent local or remote attackers from stealing data files from the database server. This is done by hiding the data files. Similar to Database Guardian, which prevents the data files from being modified, with exfiltration protection, the files are completely hidden from any application or program. Attackers or malicious insiders will not be able to see the SQL files and will not be able to steal them or copy them off the disk.

DIAGRAM 2 – MS SQL DATA RANSOMWARE ATTACK

Diagram 2 illustrates how a ransomware attack can execute successfully against your MS SQL database and data files when you continue to rely on existing security solutions.

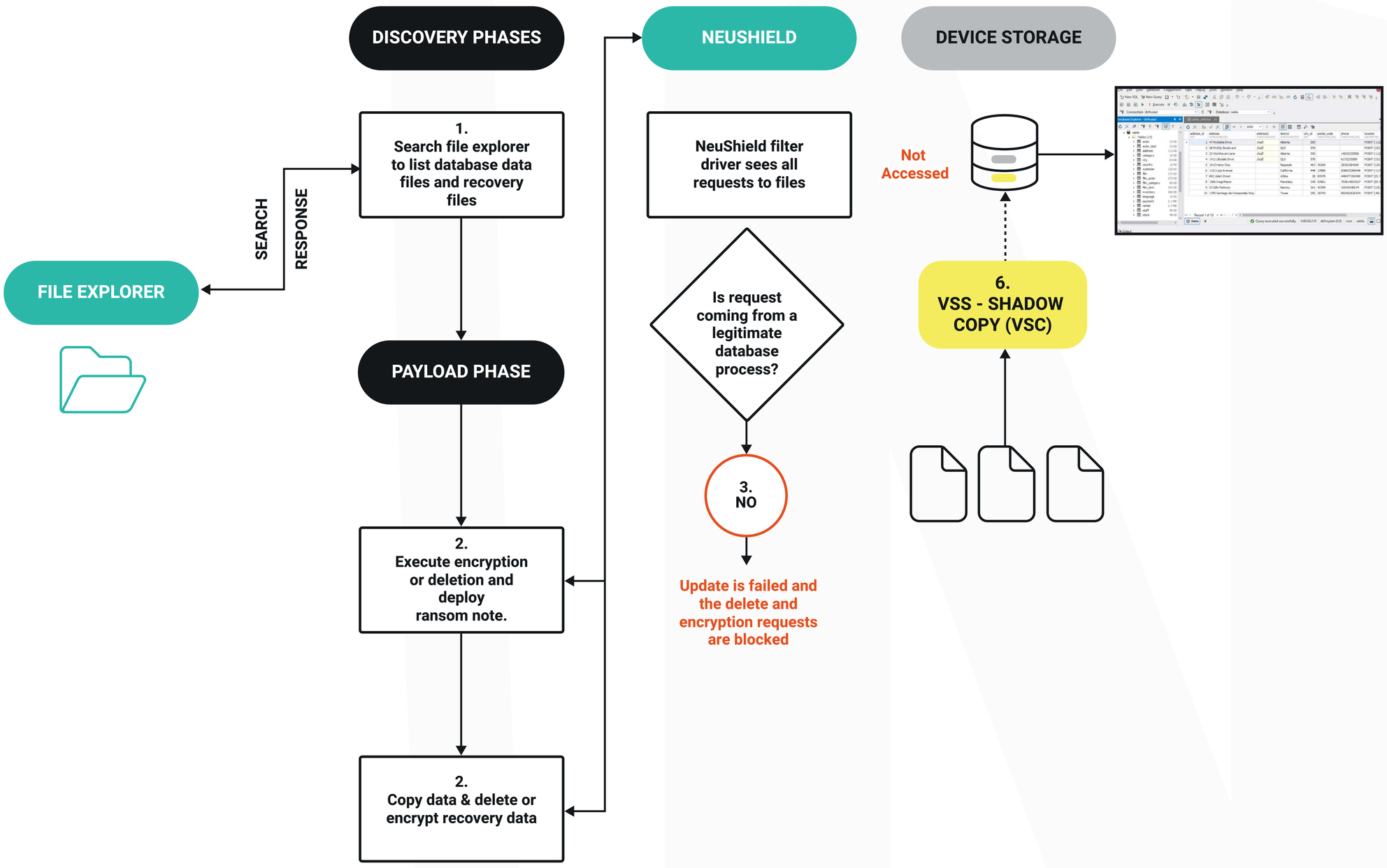


1. Failure to detect the ransomware means no alerts have been passed to the IT/SOC alert monitor and the malware can start to list all data in your file systems.
2. The Hacker can initiate its attack, unnoticed, compromising your database data files, dumping a ransomware note in your encrypted files.
3. The Hacker will now encrypt, delete or exfiltrate all identified recovery data, backups and VSCs.

Ransomware Attack Scenario – NeuShield Database Guardian

DIAGRAM 3 – NEUSHIELD DATABASE GUARDIAN - MS SQL DATA RANSOMWARE ATTACK

Diagram 3 illustrates how to mitigate a ransomware attack that is attempting to modify/encrypt the data files in your MS SQL database when you have the NeuShield Database Guardian feature activated.



Ransomware has evaded your security detection tools. The tools are fully operational with their malware engine signatures and AI algorithms up to date.

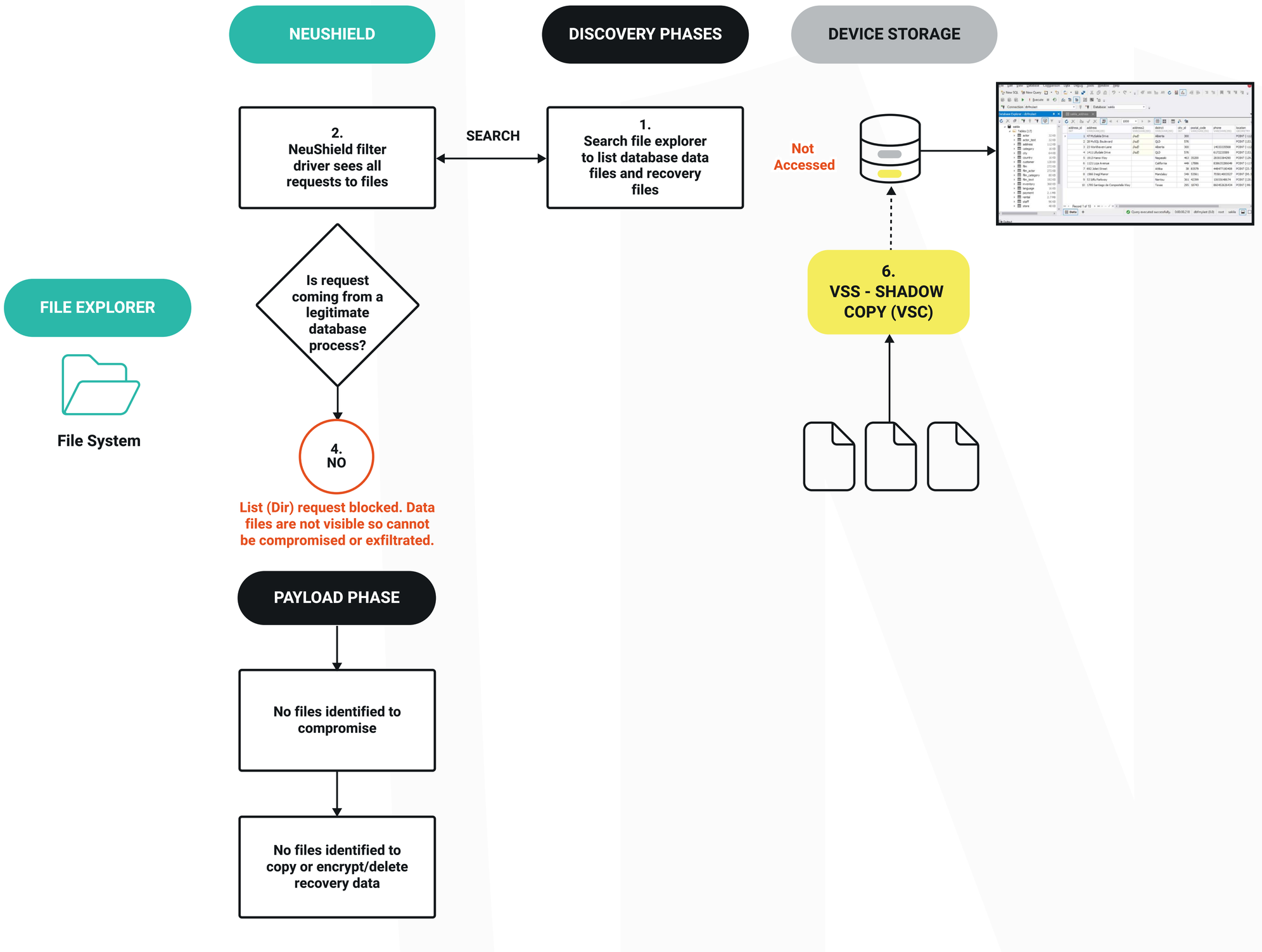
1. Failure to detect the ransomware means no alerts have been passed to the IT/SOC alert monitor and the malware can start to list all data in your file systems.
2. Equipped with a list of data files, the Hacker sends the ransomware to encrypt or delete the data files.
3. The NeuShield Driver filters every request to the MS SQL database.
4. NeuShield will block the request as it knows the request is coming from a non-legitimate database process.
5. The Hacker will either attempt to resend the same malware request or believe that the first payload phase has been successful and attempt to compromise the recovery data. The recovery VSCs and backup data are held on another device and would be protected with a version of NeuShield Data Sentinel Business Edition.

No MS SQL database data files have been encrypted or deleted.

Ransomware Attack Scenario – NeuShield Exfiltration Protection

DIAGRAM 4 – NEUSHIELD EXFILTRATION PROTECTION - MS SQL DATA RANSOMWARE ATTACK

Diagram 4 illustrates how to mitigate a ransomware attack that is attempting to exfiltrate data files in your MS SQL database when you have the NeuShield Exfiltration Protection feature activated.



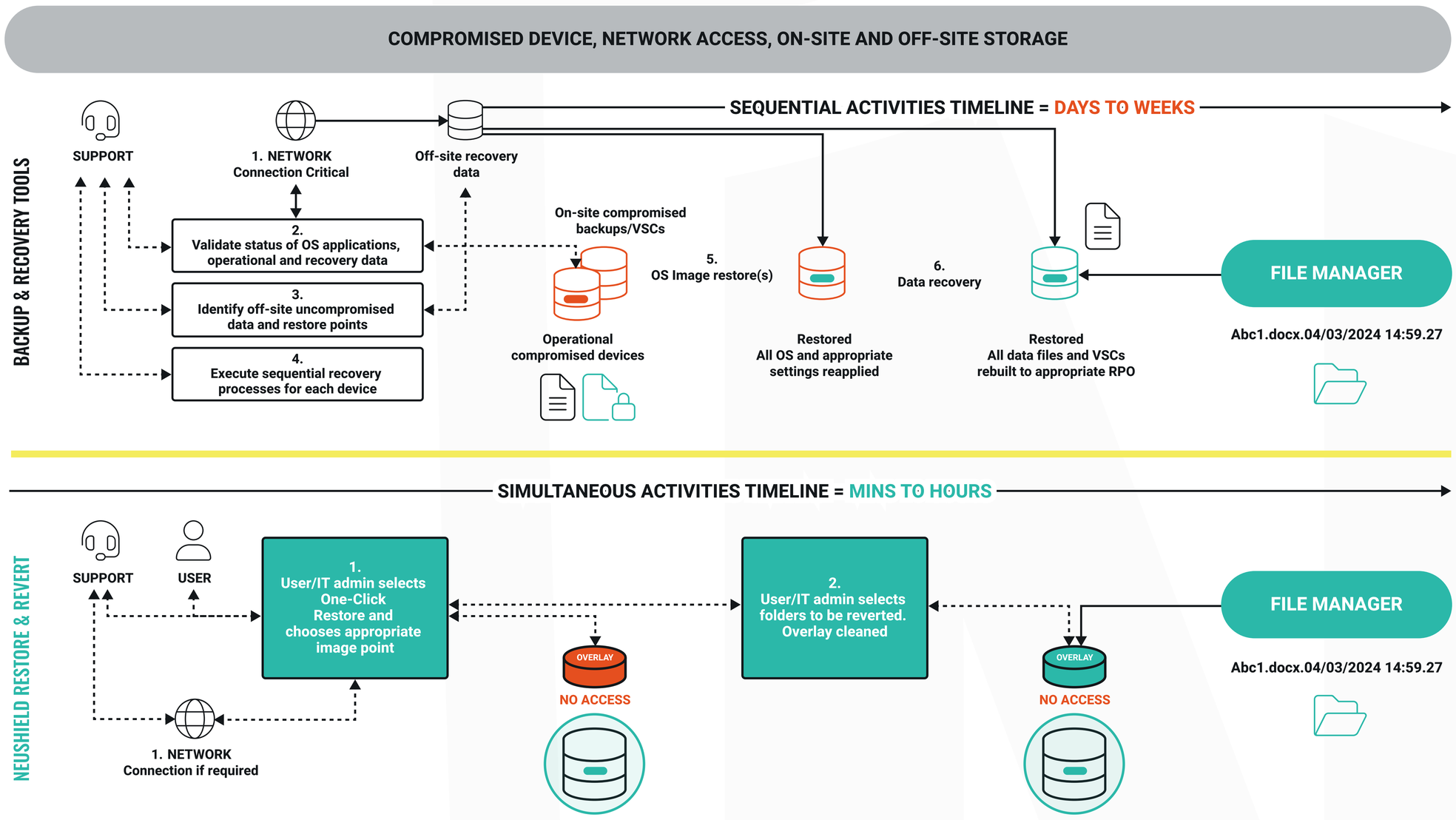
Ransomware has evaded your security detection tools. The tools are fully operational with their malware engine signatures and AI algorithms up to date. When NeuShield's Exfiltration Protection is enabled, the NeuShield Driver will filter every request across the MS SQL environment and moves earlier in the chain of permissions.

1. The ransomware will attempt to list all database data files in the file system.
2. NeuShield identifies that the command is coming from a non-legitimate database process.
3. The command is blocked. The Hacker will be presented with empty data folders.
4. The Hacker has not been provided with locations of data files; they are unable to send their payload phases of the attack.
5. This mitigates data exfiltration, modification, deletion, and encryption.

No MS SQL database data can be viewed for exfiltration, modification, deletion, and encryption.
Whatever their claims, no other anti-ransomware product in categories 1-5 can deliver NeuShield's data and device unique protection capability.

Speed of Recovery from a Ransomware Attack is Critical

DIAGRAM 5 – EXISTING AND NEUSHIELD RECOVERY FROM AN UNSTRUCTURED DATA RANSOMWARE ATTACK



Equally critical when dealing with a ransomware attack is the recovery of operations. Speed is now your friend as every minute, hour, day, or week that systems are unavailable, a business suffers, revenues decline, reputation is damage, customers are lost, and ongoing costs are needed to re-establish internal and external operations.

Diagram 5 maps the effectiveness of claims for phase 2 anti-ransomware mitigation for unstructured data. In the majority of organizations, they will deploy the recovery features of their backup & recovery tool to re-establish your data and devices.

The same diagram shows how the user/IT administrator can use NeuShield, which has already protected your active data, to revert data and restore the devices simultaneously to regain visibility to your data and devices.

If you follow the flow of diagram 5 above the centre line, data management and IT administrators will be familiar with the process required to recover devices and data during a cyber incident using data copies taken previously by the backup & recovery tool shown in Table 2 category 5. There are dependencies in this flow and many activities have to be performed sequentially due to data transfers, network availability and sustained data rates, including the prioritization of device restores based on their criticality to operations.

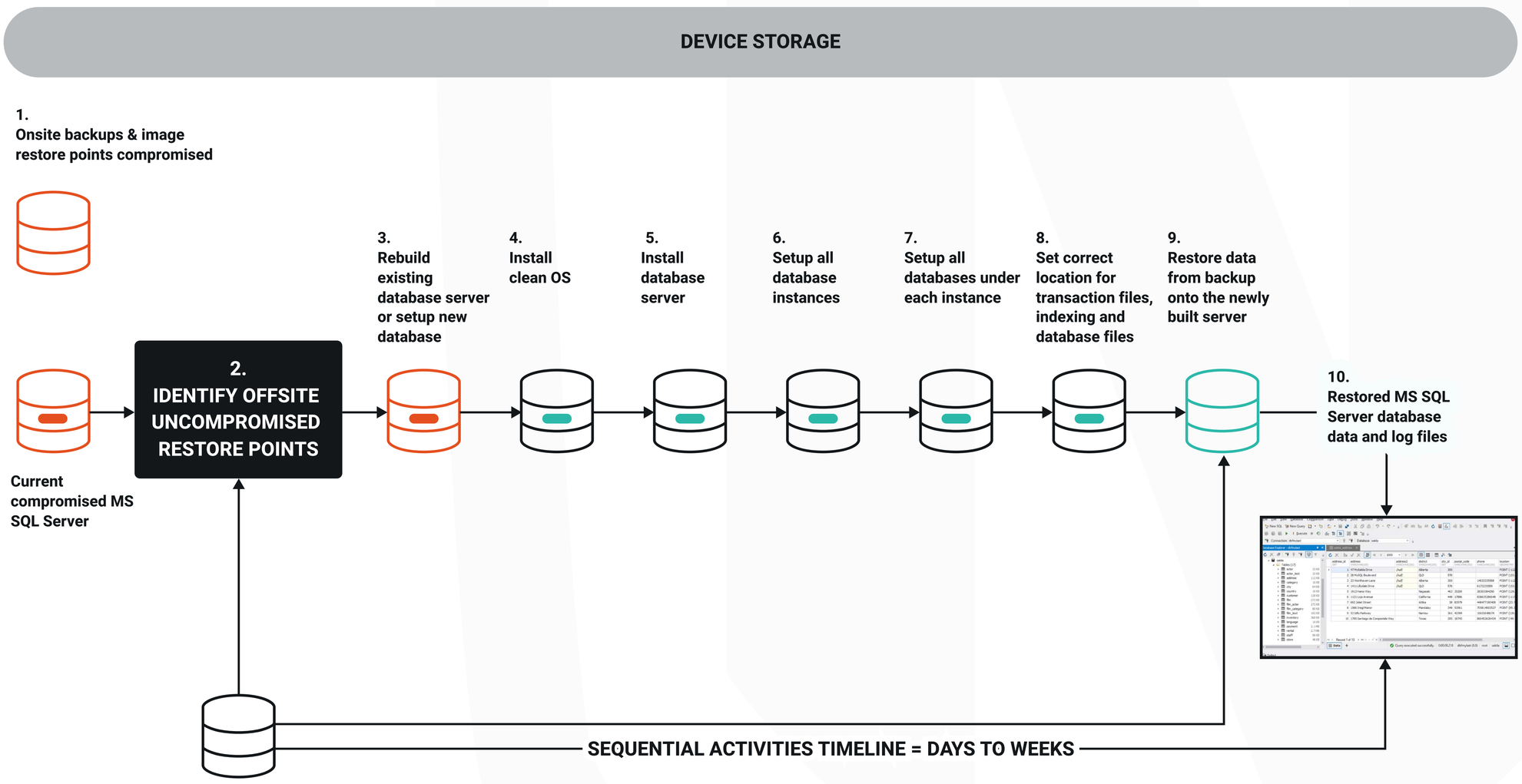
NeuShield Device and Data Recovery

The flow of diagram 5 below the centre line, illustrates how NeuShield device restore points and data reverts can be executed simultaneously across every affected device, by either the user or the IT administrator.

1. User or IT administrator determines if the device requires the OS/applications to be restored. If yes, the user or IT administrator selects One-Click Restore from NeuShield portal or within the NeuShield File Manager, chooses the appropriate restore point and confirms. When finished NeuShield will present the device login screen. If remote access to the devices is required, a network connection is used to send a command from the NeuShield portal to the device. No recovery data needs a network connection.
2. Once the restore of the OS/applications has completed or if you didn't need to restore the OS, the user or IT administrator will select 'Revert' from NeuShield portal or within the folder in the File Manager. Once the user or IT administrator has confirmed their revert selection, NeuShield cleans the Overlay and provides instant access to protected folders and files

Standard MS SQL Device, Settings, and Data File Recovery

DIAGRAM 6 – 10 STEPS TO RECOVER FROM AN MS SQL RANSOMWARE ATTACK

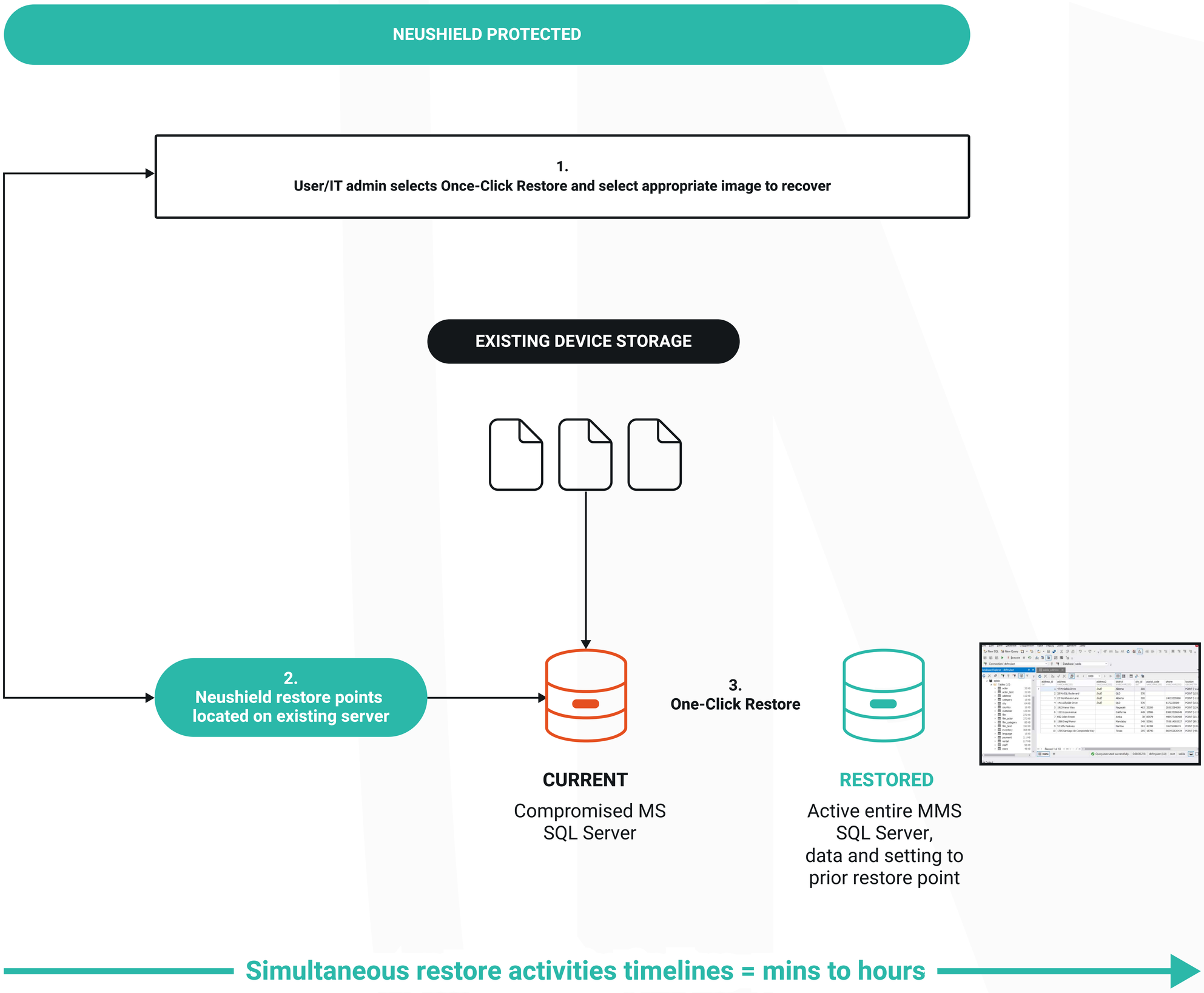


The flow of Diagram 6 will be familiar to IT administrators and Database Administrators (DBA). It is critical that this flow is always followed. The only area that an alternative choice can be made is at task 3, when the IT administrator or DBA identifies if the existing server can be used to rebuild their MS SQL environment, or they need to allocate a new server.

Diagram 6 illustrates the process using data copies taken previously by the backup & recovery tool shown in Table 2 category 5. Similar to the unstructured data recovery dependencies, the IT administrator will perform these tasks sequentially due to MS SQL rebuild processes, data transfers, network availability and sustained data rates.

DIAGRAM 7 – NEUSHIELD 3 CLICKS TO RECOVER FROM AN MS SQL RANSOMWARE ATTACK

Diagram 7 illustrates the simplicity to recover the entire MS SQL server OS, database applications, database instances, registries, data files and settings in 3 clicks.



3 Clicks

1. The DBA or IT administrator accesses the NeuShield portal and selects One-Click Restore from the device list.
2. The appropriate restore point is selected.
3. Confirmation of the restore point executes One-Click Restore that will run unattended and restore the entire MS SQL Server.

All data and restore points use NeuShield protected data on the device. Once the DBA /IT administrator has started the restore of a server, they can start another restore immediately.

*Network connectivity is only required for access to the NeuShield portal and sending a single command when centralized recovery is undertaken. Users and IT administrators can perform all NeuShield folder/file reverts directly from the File Manager on the targeted device.

NeuShield delivers unrivalled speed of recovery and confidence that once completed the MS SQL server will be operational and all data and settings are aligned to the chosen restore point.

Summary

Anti-ransomware products will deliver value to organizations based on their core capability. Once email, endpoint and network security tools have been evaded, they no longer play an active role in protecting and recovering data that has been compromised.

This report has shown how NeuShield works alongside existing security tools and adds operational awareness and value to protect sensitive data against ransomware incidents, exfiltration and can instantly recover your targeted data and devices simultaneously.

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