NeuShield®

How much is your data worth?

VSS Concerns

FACT: VSS SNAPSHOTS ARE FALLIBLE

Compare NeuShield Recovery vs Shadow Copy, Rollback and Restore Points

It’s time to address the real limitations of VSS data recovery that contribute heavily to recurring failures during incident response.

1. How can you reclaim your important data from any ransomware attack or operational oversight?
2. How do you prevent unauthorized data manipulation, encryption, exfiltration and deletion?
3. How can you achieve near real-time business continuance in the event of an incident?

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**

VSS is not a “get out of jail free” tool

Most ransomware detection, remediation and recovery tools focus heavily on methods of active data encryption and compromise. These normally follow a narrow set of techniques such as behavior- based indicators of attack (IOAs) and signatures of known malware.

Equally critical - but often overlooked - is understanding the operational limitations of Microsoft’s Volume Shadow Copy Service (VSS) data recovery tool. Often perceived as a “get out of jail free” tool, today’s cyber hackers understand the mechanics of VSS meticulously. They regularly target VSS by hijacking system tools such as vssadmin.exe, LOLbins, Powershell and COM objects to compromise recovery and rollback data to thwart system recovery.

NeuShield has identified seven critical limitations of VSS effectiveness that may impact the restoration of operations when cyber hackers render your recovery efforts obsolete.

These limitations increase your incident response risk. They will also fail your attempts to establish a dependable and robust data protection and recovery policy.

VSS, Rollback and Restore Point - Limitations

1. ENDPOINT FAILSAFE

VSS and rollback technologies are used by EDR/ XDR/NGAV tools to detect a malware file incident. During the detection time that file can encrypt a quantity of your good files. A quantity of the volume shadow copies (VSCs) can be targeted and compromised along with other good active data and backup files during this period of attack.

2. STORAGE & RESTORE

All VSS and rollback capabilities have a finite amount of data they can store [“diff area”] and in some cases even a limit on the size of file they backup. This means they are limited on what they can restore. If you only have 50GB of free space for VSC deltas and 100GB of data is encrypted, VSS cannot restore the 100GB as it will never have retained all the data.

3. REGISTRY

VSS and rollback operations managed via the EDR/XDR/ NGAV tools are only concerned with data file changes. Windows Registry Service supports a VSS writer so IT Administrators can backup and secure the system registry. Many endpoint solutions only use VSS for data recovery with no integrity of alignment to the RPOs of the Windows Registry Service VSCs.

4. DETECTION

Many of the solutions that rely on VSS and rollback technologies must detect the attack to restore the data. Even if they could backup all your data you may not have any way of getting your data back. No Detection = No Rollback.

5. DATA EXPOSURE

Maintaining up to 64 shadow copies and updates will retain a lot of expired data. If a user or program deletes files, you still need to remove existing shadow copies. Attackers may be able to retrieve deleted files from exfiltrated shadow copies.

6. OPERATIONAL COMPLEXITY

VSS is a mature service, but IT administrators are continually confronted with regular errors (VSS freeze, lost files, incomplete copies, writers in failed state, etc.) that will compromise VSC recovery expectations. Troubleshooting VSS errors during an attack may expose the recovery of compromised data, requiring you to rely on recovering from offsite incremental backups.

7. OS DELETION EFFECTS ON VSS CACHE LIMITATIONS

The device OS will delete the VSS cache data if any number of circumstances are met. Such as:

- The VSS cache data exceeds the specified disk percentage, which is usually only a single decimal percentages (4% or 5%, etc.).
- The hard drive gets low on disk space. Ransomware attacks will fill the disk space.

If all your data on the device has become encrypted, there is good chance that all the data is not available or the OS has deleted it (unless you store only a very small amount of data on the PC or server storage drive). The OS deletion feature was added by endpoint security vendors as a stop-gap in case a few files were encrypted. It will not help if all data on the hard drive are encrypted.

Take Control Now to Avoid the Devastating Effects of Business Repercussions of a Ransomware Attack

NeuShield Guarantees Full Control of Your Data and Systems

NeuShield is the only anti-ransomware technology that instantly and accurately recovers your damaged data and operating systems. It doesn't matter if the malicious software is known or yet to be detected. NeuShield recovers without requiring any VSS VSCs, rollback, restore points (RRP) or backups.

SIGNED AND CERTIFIED BY MICROSOFT

The NeuShield Data Sentinel driver is co-signed with Microsoft. We protect all your OS, system and data files from compromise both during and after an attack. The close relationship with Microsoft ensures that NeuShield conforms and seamlessly supports of all Windows OS and recovery programs.

NeuShield complements (it does not compete) with existing security tools (EDR, NDR, SIEMs etc.) and can support your data recovery software to meet your recovery point objective (RPO) and reduce costs – all while increasing your recovery time objective (RTO) by 99%.

NeuShield Addresses VSS Limitations

NO LEARNING

Solutions that use VSS for recovery need to continually learn what is bad (malware signatures, IOCs, or abuse of vssadmin.exe, etc.) so they know what VSCs they need to use to undo/rollback. NeuShield never needs to understand the type of attack method, only that it is attempting to compromise the data. Addressing the VSS Endpoint Failsafe and Detection limitations, NeuShield stops all attempts to compromise any data immediately.

COMPLETE RECOVERY

VSS requires separate data and system file VSC schedules and recovery procedures. NeuShield's settings constantly protect all your OS, system files and data. Our single portal instantly reverts all protected data aligned to your RPOs. Addressing the VSS Storage & Restore limitation, NeuShield guarantees seamless RPO and RTO activity across OS, system and data files.

FILE INTEGRITY

VSS creates a delta (VSC) copy prior to the application directly updating the active file. NeuShield always stores OS and data updates separately, preserving the 'last known good state' of each file. Addressing the VSS Registry limitation, NeuShield continually maintains the integrity of the original files.

NO EXFILTRATION

VSS protection has no capability to stop the exfiltration of data. NeuShield can restrict direct or indirect file access to copy and exfiltrate data, even if the attacker has stolen privileged access credentials. Addressing the VSS Data Exposure limitation, NeuShield stops any exfiltration of your MS SQL data.

DATA VISIBILITY

VSS cannot stop malware encrypting and compromising the integrity of the original data. NeuShield never exposes the protected data to any write operation. Any malware write command, such as encryption, is only ever performed on our virtual Overlay. Addressing the VSS Operational Complexity limitation, NeuShield immediately alerts users of suspicious file activity, then the virtual Overlay can be instantly cleaned, with no impact on the protected data.

NEVER DELETED

Windows OS has multiple scenarios that will delete the VSS cache. NeuShield never deletes the files and alerts the IT administrator when a device may be low on available storage. Addressing the VSS OS Deletion limitation, NeuShield maintains the integrity of OS and data files even if your storage space is critical.

NEUSHIELD DATA SENTINEL DELIVERS IMMEDIATELY

Test our ransomware protection promises without obligation.

For questions about the content of this paper and to understand more about how NeuShield works contact us:

Sales@NeuShield.com or call **+1 510-239-7962**

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