RANSOMWARE DATA PROTECTION VENDOR SPOTLIGHT - NEUSHIELD

Ignorance is no longer an accepted excuse.

Security tools are failing to detect all ransomware/malware attacks. Don't find out too late that you are using the wrong products to protect your data from compromise and deliver instant recovery.

Prepared by:
Kevin Bailey
Chief Analyst
Synergy Six Degrees

SYNERGY
SIX DEGREES

INTRODUCTION

Report Purpose

Synergy Six developed the Ransomware Data Protection report to raise awareness of gaps that exist in information security technology, tactics and policies to protect data from being compromised when security tools have been evaded by ransomware. This report reviews the current solutions that organisations may choose to mitigate data compromise and accelerate the recovery of their business operations.

Method

Using primary and secondary research, Synergy Six analysed explicitly marketed anti-ransomware solutions and their effectiveness in mitigating an attack and minimising the impact on an organisations operations.

Leadership Perspective

During the research of this paper, Synergy Six found that the majority of senior management responsible for the protection against cyber attacks and any subsequent recovery of data (if compromised), believe that their existing security tools should stop all attacks and the conviction from traditional backup and recovery vendor products whose features should deliver their required recovery point (RPO) and time (RTO) objectives.

Appetite to Adopt

In an economic climate when budgets are tight, senior management are consciously looking to reduce rather than increase the number of tools they deploy to minimise resource management and gain possible budget advantages. Any ransomware protection solution needs to deliver demonstrative value without duplication of existing tools and minimal operational management.

CATEGORY UPDATE - 2024

RANSOMWARE DATA PROTECTION

In 2023, news coverage highlighted the widespread activity of Lockbit, BlackCat and C10p as prominent ransomware groups, while formerly notorious Conti and REvil fell apart. The start of 2024 has seen the emergence of threats from MalasLocker, 8BASE, and Akira. Hackers have not had it all their own way as law enforcement agencies from Britain's National Crime Agency (NCA) and the FBI disrupted, arrested and indicted members of the Lockbit ransomware gang.

The surge in ransomware attacks is partly fuelled by the proliferation of Ransomware as a Service (RaaS), where operators (Play, Black Basta, 8Base, Hunters, Medusa, etc.) sell or lease the software to cybercriminals who then independently target victims. However, the growing awareness and implementation of policies, processes and increased security aware infrastructure designs are making a positive impact to reduce cyber vulnerabilities, enabling some businesses to detect and address potential compromises earlier.

Evading Detection

Immaterial of security vendor and type of detection methodology (static analysis, dynamic analysis, and network traffic analysis) over 99% of detection products are solely dependent on the success of malware detection via AI-based malware engines. To increase data protection and detection success rates, detection products employ multiple malware engines or diversifies with non-core features such as VSS data copies.

Daily news coverage constantly declare business disruptions due to ransomware attacks, validating that hackers continue to evade security detection tools. Ranking only 2nd behind Denial of Service (DoS) attacks in the 2024 Verizon Data Breach Investigations Report, ransomware success critically disrupts business operations, breach data privacy governance seeking to extort ransom payments to release encrypted data.

In 2022 Hackers received ransom payments of $567 million[1], 43% less than 2021, whereas 2023 resumed prior predicted trends as organisations paid $1.1 billion in ransom payments.

Recovery Reality

Equally disturbing for IT operations is the unexpected extended recovery time periods being experienced to reestablish compromised systems and data following a ransomware attack.

Backup & recovery vendors sensationalise their product capabilities to differentiate themselves in a crowded market. Stretching reality has dramatic consequences for their clients that are expecting instant and rapid recovery. Realising that 'instant recovery' is unachievable if they cannot access onsite and offsite data during an incident causes weeks of delays and severe unbudgeted costs.

Every business operates with agreed operational services levels. Recovering data due to a hard disk failure is considered an 'operational event' with well understood recovery processes and service levels. However, recovering compromised data/devices following a ransomware attack is different and deemed as an 'exceptional event' as each successful attack will have different compromise variables to consider. Unless robustly tested, recovery service levels will be incalculable using traditional recovery tools.

1 - Several factors likely contributed to the decrease in ransomware activities in 2022, including geopolitical events like the Russian-Ukrainian conflict. This conflict not only disrupted the operations of some cyber actors but also shifted their focus from financial gain to politically motivated cyberattacks aimed at espionage and destruction.

Category Definition

What is Ransomware Data Protection?

Synergy Six Degrees defines ransomware data protection as vendor-developed solutions that prevent the compromising (encryption, deletion, modification, or exfiltration) of active data on devices. These solutions operate in real-time, delivering their value when enterprise security tools fail to detect and mitigate ransomware/malware attacks. Ransomware data protection can be offered as SaaS-based, on-premises, hybrid and can be a combination of software and hardware.

Synergy Six believe that organisations need an explicit ransomware data protection solution to protect and recover active data, recovery data, and installed device OS and services during exceptional operations. These solutions should not replace existing security and data backup and recovery tools.

Minimum solution capabilities must:

- Protect active/operational data from compromise.
- Include protection of all data types - files, operating systems, databases, virtual machines, applications.
- Protect data located in public cloud infrastructure, including multi-cloud and hybrid cloud architectures.
- Protect data located in cloud shares, Google, OneDrive, Sharepoint, Box, Dropbox, etc.
- Protect data located on mounted storage such as NAS.
- Create multiple point-in-time delta copies of the active data and OS for instant resiliency.
- Deliver enhanced cyber recovery point-and-time objectives for 'exceptional events'.
- Provide the capability for user and/or IT support to orchestrate recovery of data and OS.
- Immediately send and log alerts when attempted compromise of data is suspected.
- Provide a centralised management console.

Optional features may include:

- Protection of non-active, backup and recovery data.
- Protection of server based critical services.
- Optional use of malware engines.
- Additional device/data protection techniques: boot sector, anti-wiper, encryption key capture, root access protection, immutable data copies, etc.
- Limited control path dependency of networks to perform data recovery.
- Support for environments such as infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).
- Integration with security and information management (SIEM) and eXtended Detection and Response (XDR) tools.

Ransomware Data Protection solutions should not:

- Duplicate or restrict the malware detection features of any endpoint and network security tools.
- Store additional backup copies to recover data and systems during exceptional events.

RANSOMWARE IMPACT MAP

Figure 1 displays the 2024 Synergy Six Ransomware Impact Map, placing ransomware data protection vendors across four quadrants based on their scoring for each axis.

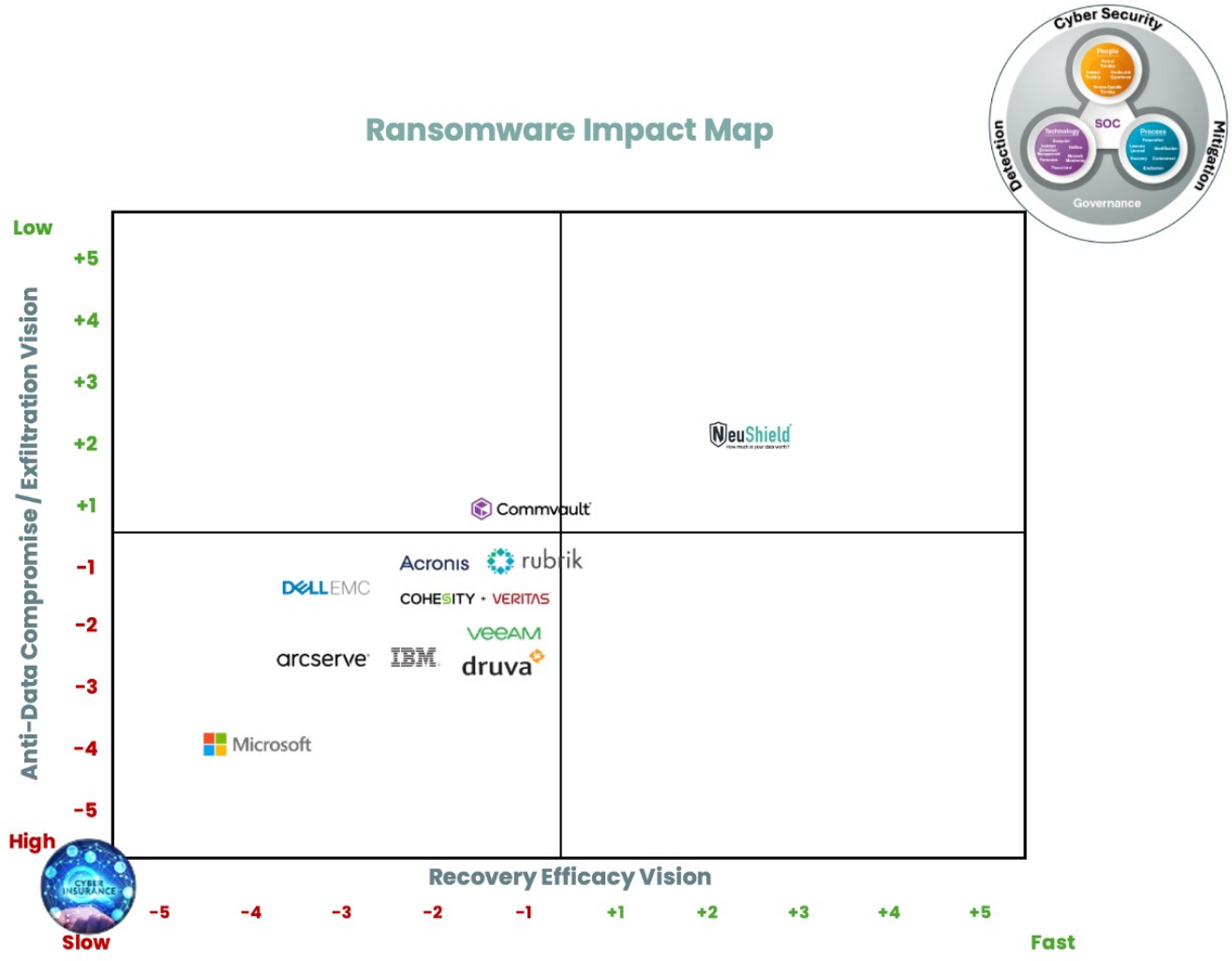
- **Anti-Data Compromise/ Exfiltration Vision**

On a scale of **-5** to **+5**, where -5 represents high data compromise and exfiltration and +5 represents low data compromise and exfiltration.

- **Recovery Efficacy Vision**

On a scale of **-5** to **+5**, where -5 represents slow (obstructed[2]) data recovery and +5 represents fast (instant[3]) data recovery.

Figure 1 - Ransomware Impact Map



[2] Obstructed – Speed of recovery can be compromised by the effects of a ransomware attack, such as loss/compromise of backup copies and internal and external network data transmission restrictions.
[3] Instant – Capability to commence instant recovery of compromised systems and data is not obstructed by technology to achieve the required recovery time objective that is aligned to the organisations Maximum Allowable Downtime (MAD).

RANSOMWARE IMPACT MAP OVERVIEW

The cyber security, detection and mitigation icon represents all pro-active boundary, network, communications and endpoint security products. **These solutions rely on malware engines and when successful will prohibit any data compromise and enable operations to continue operating effectively.**

Table 1 provides a list of leading ransomware data protection vendors that have been represented on the Ransomware Impact Map. These have been included based on their market visibility, product capabilities and consistent [ransomware] market positioning and messaging.

Table 1 – Ransomware Data Protection Vendors

Example Vendor	Rating		Active Data Protected	Other Data Protection	Tangible Value for Ransomware Protection
	Anti-Data Compromise	Active Recovery			
Acronis	-1.0	-2.0	CDP Deltas	Immutable Copy	Cyber Protect, immutable storage and instant restore of delta change backup copies.
Arcserve	-2.5	-3.1	CDP Files	Immutable Copy	OneXafe or AWS Object Lock safeguards from malicious exploits. UBA with CryptoGuard & WipeGuard.
Cohesity/Veritas	-1.5	-1.6	No	Immutable Copy	Zero Trust Security, immutable snapshots and DataHawk attack detection for backups.
Commvault	+1	-1.0	No	Immutable Copy	Air-Gap Protect, Clean room recovery and anomaly detection engine for backups. Platinum Resilience solution.
Dell EMC	-1.3	-3.0	No	Immutable Copy	Cyber Recovery Vault with immutable and air-gapped copies with Cybersense data compromise detection on backups.
Druva	-2.7	-1.3	No	Immutable Copy	Immutable and air-gapped copies and Curated Recovery for backups.
IBM	-2.0	-2.1	No	Immutable Copy	FlashSystem and ransomware cyber guarantee.
Microsoft Defender	-3.9	-4.0	VSS/VSCs	Immutable Copy	Immutable vaults, 365 advanced protection and volume shadow copy service (VSS).
NeuShield Business Edition	+2	+2.4	Mirror Shielding™	OS, Boot Drive, Anti-Wiper	Malware agnostic, patented active data protection, cloud drive protection, anti-encryption and deletion protection.
NeuShield Datacenter Edition	+2.5	+3	Database Guardian	Exfiltration Protection	NeuShield Business Edition features plus MS SQL anti-data exfiltration & modification, 64TB clusters, 2TB large files.
Rubrik	-1.0	-1.0	No	Immutable Copy	Rubrik Cloud Vault and Rubrik Radar for reactive anomaly detection.
Veeam	-2.0	-1.2	No	Immutable Copy	Immutable data copies and anomoly detection engine for backups.

An effective Cyber Insurance policy delivers value post breach: incident response specialisms, malware analysis and detection, legal costs & representation, breach response, client notification, credit monitoring, forensic investigations and PR to minimize reputational harm. **Cyber Insurance will not protect your organisation from a ransomware attack.**

Summary

The vendors included in the lower left quadrant of this report do not deliver any active primary data protection. The primary role of these solutions is to take periodic copies of data for future recovery. Their only value in a ransomware attack is achieved if they maintain a copy of data on an immutable/air-gapped technology. This choice of media ensures the backup data cannot be compromised and can be used for data recovery when the primary and secondary backup copies have been compromised.
The NeuShield solution (upper right quadrant) has been identified currently as the only solution purposely developed for ransomware protection, prohibiting direct data modification that may compromise (encrypt, delete, modify and/or exfiltrate) active data, delivering instant recovery.

Note: Morphisec and Agger Labs were suggested for inclusion as example vendors in Table 1. Both vendors have been omitted as their core functionality aligns to malware engine detection vendor behavioural analysis covered in the cyber security, detection and mitigation icon.

SPOTLIGHT VENDOR ASSESSMENT

Vendor - NeuShield, Inc. **Vendor Solution -** Data Sentinel Business Edition & Datacenter Edition

Who is NeuShield?

NeuShield, Inc. was founded in 2017, headquartered in Fremont, California. The company's founders have each spent 20-30 years developing endpoint, data loss prevention and network security products for Sygate, Websense, Symantec, Forcepoint, and Fireeye/Mandiant prior to establishing NeuShield.

CEO – Yuen Pin Yeap | **CTO** – Fei (Philip) Qi | **COO** – Elisha Riedlinger

Why NeuShield?

NeuShield was established specifically to address a growing number of recurring ransomware protection and recovery challenges. They observed that:

- Security teams are continually reactive against new forms of malware and can never guarantee successful mitigation 100% of the time, leaving their organisation exposed.
- Following a successful ransomware attack, organisations are confronted with compromised recovery data (backups & VSCs) dramatically impairing their ability to meet their recovery time objectives (RTO) and maximum allowable downtime (MAD).
- Upon notification of a ransomware attack, incident response processes that enable the commencement of data recovery transfers are severely delayed when organisations immediately disable their networks to contain the widespread threat of the malware reaching other parts of the organisation.

NeuShield's Data Sentinel multi-patented architecture prohibits any ransomware vector intent on compromising an organisation's protected data. Mirror Shielding™, Database Guardian, Exfiltration Protection and Data Engrams™ architecture protects data in real-time and accelerates instant recovery of data from the affected device, prohibiting database data modification and data exfiltration. All without any reliance on backup data or networks to transfer data.

What is NeuShield?

NeuShield is positioned as a growth player in ransomware protection. Analysis at the time of this report has not identified an architecturally similar competitive vendor. NeuShield's enterprise portfolio consists of Data Sentinel Business Edition and Data Sentinel Datacenter Edition[4]. At the time of this assessment, the products protect data for Windows OS workstations/PCs (7-11) and servers (2008-2022) from being encrypted or deleted. In addition to the functionality of the Business Edition, the enhanced Datacenter Edition protects large file servers (<64TB clusters) and has a specific feature set for Microsoft SQL Server (2008-2022) configurations; 1) Unauthorized data file modifications and 2) Anti-data exfiltration.

[4]NeuShield offers a Data Sentinel Home Edition for consumers.

What NeuShield is not?

At first glance, It can be easy to fall into the trap of assuming that the NeuShield solutions align to existing malware detection tools and/or backup and recovery products. NeuShield is neither of these. NeuShield has no requirement for a malware engine as its data protection capability comes from identifying on-device suspicious file activity that occurs when write actions (update, deletion, modification) on a file attempt to compromise the standard file format.

Ransomware Impact Map Analysis

NeuShield Data Sentinel - Business Edition

NeuShield Business Edition delivers real-time active data protection and instant recovery for PC/workstations and file servers.

Anti- Data Compromise/Exfiltration Vision +2

Strengths

- Data and OS/Apps are continually protected from compromise.
- No dependency upon malware detection engine.
- Patented architecture protects against known, unknown, fileless and zero days attacks where the purpose is to compromise the data.
- Supports all Microsoft supported operating systems.
- Microsoft/NeuShield digitally co-signed driver certificate.
- Immediate suspension of file modification Commit cycle from the Overlay when suspicious file activity is detected.
- Immediate alert to IT admin upon suspicious file activity.
- Centralised management portal with support for multi-tenancy and device grouping.

Limitations[5]

- Each device requires 10% available storage, calculated from total active data protected.
- Only supports Microsoft operating systems and devices[6].
- NeuShield protects the guest OS on a VM image, but not the VM image.
- Does not stop ransomware from exfiltrating data.

Recovery Efficacy Vision +2.4

Strengths

- All recover/revert functionality is only dependent on the targeted device.
- No dependency on backup data or networks [to move data] to recover/revert.
- No off-device data movement required to recover/revert.

[5]NeuShield have an unpublished roadmap that sets out their R&D activities. Organisations that wish to understand if any limitations are covered within their planned roadmap need to discuss this directly with NeuShield.
[6]NeuShield have stated that if a client is willing to purchase Data Sentinel to support operating systems other than Microsoft then they will adjust their roadmap. Synergy Six has be told that although the requirement for Linux/Mac support is discussed, it does not appear to be critical at this moment in time.

Strengths cont.

- Bulk (000's) file reverts achieved at the speed of [Overlay] data deletion (secs/mins).
- All device recover/reverts can be run simultaneously, accelerating the RTO.
- Allows data reverts and system recovery by user and/or IT admin.
- Multiple One-Click Restore images available to restore OS/Apps.
- Portal reverts and restores display alert message to user prior to execution.
- Allows IT team to reduce traditional copies of backup data that are only required for operational incidents (hardware, DR, purposes).

Limitations[5]

- Device file reverts and OS recovery need to be initiated individually.
- No recovery option for VM images. Need to use traditional backups to recover VM Image. IT admin can then use NeuShield One-Click Restore to recover the guest OS.

NeuShield Data Sentinel - Datacenter Edition

NeuShield Datacenter Edition includes the same strengths and limitations as Business Edition when used for file servers. The scoring below factor in the special features for large file and MS SQL servers available with Datacenter Edition.

Anti- Data Compromise/Exfiltration Vision +2.5

Strengths

- Increased single maximum file size of 2TB.
- 64 TB cluster server support.
- MS SQL data exfiltration protection.
- Prohibits unauthorised MS SQL process data modification.

Limitations[5]

- Only supports Microsoft SQL Database systems.

Recovery Efficacy Vision +3

Strengths

- Utilises the One-Click Restore feature to recover the entire database infrastructure in a single action (server, database, registries, data files, etc.).

Limitations[5]

- One-Click Restore recovery point may be 24 hours prior, requiring the business to roll forward data and log changes.

DATA SENTINEL CORE FUNCTIONALITY

NeuShield Agent

The agent must be deployed on each device, from the central management console or pushed out via software management tools. When the agent is executed, it deploys a NeuShield / Microsoft digitally signed driver certificate. The NeuShield agent can only be removed using the detailed uninstall process and authorisation credentials. The agent cannot be brute force removed by malware or by trying to compromise via higher administrator privileges.

NeuShield Protection

NeuShield have developed a multi-patent architecture. An interaction between the Windows OS and the NeuShield driver occurs when a user or program initiates the creation, access and modification of NeuShield protected data. Following completion of the NeuShield settings, all data on the device, common cloud shares OneDrive, Google, Dropbox, and Box, as well as custom folders on mounted storage are immediately protected with Mirror Shielding ™.

Multi-tenant and device grouping capability allows NeuShield customers and Managed Security Service (MSSP) partners to segment business units and clients individually.

When file creation, access and modification commands are requested, the Windows OS confirms that NeuShield is protecting the data and hands over control to NeuShield, redirecting write requests from occurring directly onto the protected file. All update/write requests (write/delete/modify) are stored on a virtual Overlay. Application controls are not affected, allowing automatic and manual file saves and commands to complete as if NeuShield is not present.

Following continuous validation and verification of the new data structure that has been redirected to the Overlay, NeuShield will Commit (move) data from the Overlay to NeuShield's protected Mirror Shielding™ area. Once the update data is Committed, the previous version(s) of the original file will be maintained by NeuShield on the device as Data Engrams™. The Overlay is cleaned of prior data ready for the next update to the file.

Ransomware Data Protection

When a ransomware payload is deployed, the write command (to encrypt or delete data) believes that it is compromising the active data. In reality, the malware is applying its payload to the virtual Overlay.

NeuShield has no purpose in detecting malware as its unique architecture is monitoring 'suspicious file activity'. NeuShield understands the agreed format of all files types. When ransomware encrypts the data, the automated Commit cycle is paused and the user and IT administrator is alerted. Immaterial of malware type, any ransomware payload deployment can only affect data residing on the Overlay. This makes the attack look successful [to the Hacker], but in reality, the malware has contaminated what may only be a 0 bytes tmp file on the Overlay, obscuring the protected data from normal access. No active data is compromised.

DATA SENTINEL CORE FUNCTIONALITY

Data Recovery (Revert)

Regaining access to the obscured protected data is performed either directly from the file manager on the device or via the NeuShield central management console. Selecting the folder(s) to be unobscured (reverted), NeuShield simply cleans the Overlay of anomalous encrypted data and presents the protected [untouched] data back for processing.

Synergy Six Test 1 - Revert / number of files

- The revert function reversed the effects of an encryption attack across 2,000 files in 28 seconds. No data was lost or needed to be rebuilt from backups in this exercise.

Synergy Six Test 2 - Revert / file size.

- 1TB of data was recovered from an on-device backup copy normally used to rebuild compromised data. This exercise completed in 52 mins.
- Executing the NeuShield Revert for the same compromised data took 6 mins 46 secs.

Note: The last test was performed to evaluate NeuShield and a backup recovery tool on-device capability. Normally this would be deemed as a non-comparable incident response test as the data used for the on-device backup copy would usually have been compromised by the ransomware and the user would be restricted by a lack of network connection to recover from an offsite backup copy.

Disable Services

Cyber Attacks attempt to disable an applications services to allow the malware to take control of the device and data. EDR products have 'Tamper Proofing' to stop users (malicious or by mistake) from disabling the security tool. Advancements in malware techniques may require EDR vendors to add additional protection in the future.

Synergy Six Test 3 - Continuous Write Disabled

- NeuShield services were disabled with administrator priviliges. Attempts to update, encrypt and copy the original read only data all failed.

OS Restore

If the device OS or applications have been compromised (embedded malware n templates), the user/IT administrator can activate the One-Click Restore feature that allows a NeuShield captured restore point to be selected. NeuShield creates a restore point once a day and maintains ~seven (7) at any one time.

Synergy Six Test 4 - Restore OS

- The re-imaging of the compromised OS followed Microsoft guidelines, took 75 mins to complete.
- NeuShield One-Click Restore function restored a Windows 11 OS in 20 mins.
- This test showed NeuShield RTO was ~74% faster.

As NeuShield has no external dependencies and runs independently on each device, an IT administrator could initiate the restore function across all of its Windows OSs from the NeuShield portal. This feature allows the IT administrator to simultaneously run the recovery of all devices.

If a PC/workstation device is unbootable, the NeuShield One-Click Restore Data Engrams™ will still be accessible, allowing NeuShield restore points to be found in the files available during a Windows Recovery (WinRE).

DATA SENTINEL CORE FUNCTIONALITY

MS SQL Database Protection

Following a request from a global corporation, NeuShield released their support for Microsoft SQL Databases. The Datacenter Edition provides all the functionality of Business Edition, albeit for larger files (up to 2TB files and 64TB server clusters). In addition, they added protection for MS SQL Servers.

Three functions were evaluated:

1. **One-Click Restore -** NeuShield eliminates the need to follow ~10 steps to restore a compromised MS SQL server system. Using NeuShield's One-Click Restore capability, the IT administrator can restore the entire architecture and data to a prior state. The test achieved completion of the restoration of a basic MS SQL Server setup in 28 minutes. Once the execution of One-Click Restore was started no other involvement was required until the login screen was presented.
2. **Database Guardian -** stops unauthorised modification of data files. Enabling this feature within the settings stopped the tester from modifying data when using a non-legitimate database process.
3. **Exfiltration Protection -** stops any non-legitimate database process from listing data files within the MS SQL server. The tester performed the first action of a ransomware attack, that would enable the attacker to target data files for exfiltration, deletion, encryption. When the tester attempted to list the data files the request returned no files, mitigating the testers ability to target the data files. This stopped all further attacker scenarios against the database.

Additional Features

All NeuShield Data Sentinel solutions deliver Boot Sector Protection and Anti-Wiper Protection.

Routes to Market

NeuShield's route to market is primarily via its channel partners, although the internal HQ team will engage directly with end users if requested. In addition to US/English the product can be sold globally with local language support for Spanish, French, Japanese and Korean.

Pricing & Support

NeuShield sells Data Sentinel solutions as a subscription model. Licenses are sold on a per device basis. Pricing variances are dependent on the type of device; workstation/pc, file server and MS SQL Server.

NeuShield Data Sentinel is a single SKU offering, related to the device type. Once a license is acquired, there are no additional feature uplift costs.

NeuShield provides 8 x 5 4-hour SLA pacific time zone support and maintenance as part of the license cost. Additional support and maintenance uplifts are available for 8 x 5 4-hour SLA local time, 12 x 7 4-hour SLA local time and 24 x 7 4-hour SLA.

Additional Content

During the evaluation period, NeuShield updated their central management console to display the number of files and combined storage under protection. In addition, NeuShield displays when it believes the last backup (performed by 3rd party tool) was taken of the data on the device.

SYNERGY
SIX DEGREES

Email: Kevin.Bailey@synergysixd.com
Web: www.synergysixd.com
Mobile: +44 (0)7541 888229

Synergy Six Degrees Limited
71-75 Shelton Street
Covent Garden
London
WC2H 9JQ

VENDOR SPOTLIGHT - NEUSHIELD

RANSOMWARE DATA PROTECTION