NeuShield Data Sentinel Data & Device Recovery

NeuShield
How much is your data worth?

Deployment and Recovery Quick Guide

Companies are spending millions of dollars on security but are still getting hit with ransomware causing them additional time and resources to recover. The average time it takes a corporation to recover after a data breach incident is 17 days[1]. Recovery typically involves reimaging the infected systems, restoring user files, and resetting up Outlook and other services.

This is where NeuShield comes in.

NeuShield Data Sentinel is designed to allow companies to instantly recover from ransomware attacks even when no security product can detect it. NeuShield does this using Mirror Shielding™ technology that makes an attacker believe they have access to a computer's original data files, but they are in fact only seeing a mirror image of them. If the device is attacked by ransomware the user or administrator can use One-Click Restore to remove the ransomware, by reverting the operating system back to a known good state before the ransomware attack. Then the user can easily recover the original files by simply clicking a single button.

To accomplish this revolutionary method of ransomware recovery, the administrator needs to ensure that they have configured their architecture to protect and recover the critical system and services needed to run operations.

Cyber criminals do not only target the data they are trying to compromise, but they will also attempt to compromise other services such as Active Directory (AD), Domain Name Servers (DNS), backup data servers, catalogues, backup copies, among other services. This level of targeting is aimed to disrupt the operational capability of an organization. It is essential [where possible] that your recovery plan is built around NeuShield speed of recovery, only utilizing other external solutions where NeuShield has advised against using NeuShield Data Sentinel to protect specific data types[2].

[1] IBM Data Breach report 2022

[2] Appendix A

NeuShield Enterprise Editions

NeuShield is deployed in a manner to actively protect your data and to enable the fastest possible recovery in the event of data and/or device compromise. Returning your data, devices, and services to an operational status.

Every organization should consider where relevant, deploying both NeuShield solutions.

NeuShield Data Sentinel – Business Edition

Supports unstructured data on Windows PC/Workstations and Servers
Windows 7,8.1, 10,11 & Windows Server 2008, 2012, 2016, 2019

NeuShield Data Sentinel – Datacenter Edition

Supports structured database and large unstructured data files on Windows Servers.
Windows Server 2008, 2012, 2016, 2019

NeuShield Data Sentinel Deployment

NeuShield Business Edition - can be deployed on physical and virtual servers/ workstations/ PCs.
Features
In addition to the core features provided by NeuShield Data Sentinel (Boot Protection, Data Engrams, Disk protection, Cloud Drive Protection, File Lockdown and Zero Performance Impact), The Business Edition also provides:

- **Mirror Shielding™** will protect the data on your server or workstations.
- **One-Click Restore** will protect & recover a good known state of the device operating system.

NeuShield Datacenter Edition - can be deployed on physical and virtual servers.
Features
In addition to the core features provided by NeuShield Data Sentinel (One-Click Restore, Boot Protection, Disk protection, File Lockdown and Zero Performance Impact), The Datacenter Edition also provides:

- **Database Guardian** will protect & recover large data files and database configurations on your server.

Data Protection Guidance

NeuShield does not recommend protecting data that is continually opened for exclusive access by an application, such as active database data files and active virtual machine (VM) images and other files that act like a database file (such as the Windows user profile .dat file, etc.). You can, however, install NeuShield on the guest VM to protect its data.[3]

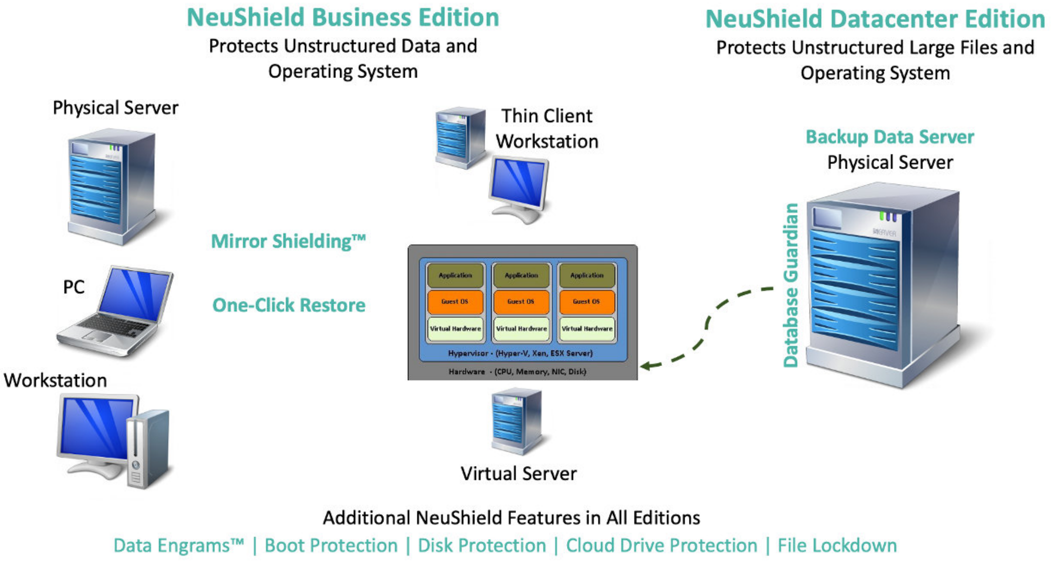
We recommend installing NeuShield to protect all your backup & recovery data and backup databases. NeuShield outlines below how using its Datacenter Edition, you can protect the Backup Data Server from compromise, ensuring recovery of this data to efficiently recover the non-NeuShield protected data.

[3] See Appendix A

Deployment and Protection

The following NeuShield configuration guide will outline how to protect those data across your physical and virtual environments, currently being protected by your backup & recovery product.

Phase One - NeuShield Business Edition can be deployed on physical and virtual servers. Following implementation of NeuShield Business Edition on each server, core NeuShield functionality ensures that all unstructured data and the Microsoft Server operating system are fully protected. As outlined previously NeuShield does not recommend protecting the virtual data images and files with Data Sentinel. Phase Two outlines how you can configure your servers to ensure protection and NeuShield recovery of these data.


NeuShield Business Edition
Protects Unstructured Data and Operating System
NeuShield Datacenter Edition
Protects Unstructured Large Files and Operating System
Physical Server
Thin Client Workstation
Backup Data Server
Physical Server
Mirror Shielding™
One-Click Restore
PC
Application
Guest OS
Virtual Hardware
Hypervisor - (Hyper-V, Xen, ESX Server)
Hardware - (CPU, Memory, NIC, Disk)
Database Guardian
Workstation
Virtual Server
Additional NeuShield Features in All Editions
Data Engrams™ | Boot Protection | Disk Protection | Cloud Drive Protection | File Lockdown

Active Data Protection

In addition to the unstructured and operating system data referenced previously, you will need to ensure that the backups for virtual machine active data is protected with NeuShield. We recommend that the Backup Data Server [a physical server], that will contain the primary backup copies and possibly the backup database[4] are protected with NeuShield Datacenter Edition.

Phase Two – If the operating system needs to be reverted, the User or IT administrator should select One-Click Restore and select the desired Recovery Point Objective (RPO) from the Data Engrams™ displayed. NeuShield will perform all recovery tasks and return the device back to operational status.

On completion of the One-Click Restore operation (if required), the User or IT Administrator can then revert all folders/files by selecting the desired Recovery Point Objective (RPO) from the Data Engrams™ displayed. Once completed NeuShield will send an email to the User / IT Administrator that the task and number of files reverted has been completed successfully.

See Datacenter Edition phase two below for the steps required to recover all data compromised on the Backup Data Server.

[4] If the backup database is not on the same server, we recommend protecting the backup database with the same configuration.

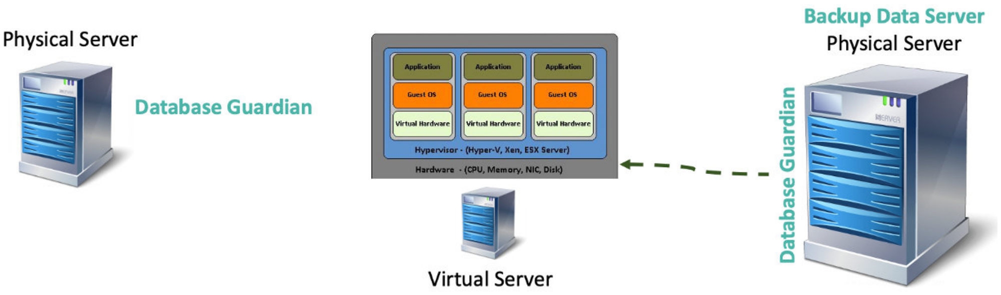
NeuShield Datacenter Edition

NeuShield Datacenter Edition - can be deployed on physical and virtual servers.

The primary role of NeuShield Datacenter Edition and its Database Guardian feature is to protect and revert your Active SQL Databases plus all the supplementary binaries and files for the database instance as a set and unstructured large data files.

NeuShield Datacenter Edition

Protects Unstructured Large Files and Operating Systems



Additional NeuShield Features in All Editions

One-Click Restore | Boot Protection | Disk Protection | Cloud Drive Protection | File Lockdown

Phase One - Following the implementation of **NeuShield Datacenter Edition** on each server, core NeuShield functionality ensures that all large unstructured data, database, and the Microsoft Server operating system are fully protected. As outlined previously NeuShield does not recommend protecting the virtual machine data images and files with Data Sentinel.

Phase Two outlines how you can configure your database/large file servers to ensure protection and NeuShield recovery of these data.

Phase Two - We recommend that the Backup Data Server [a physical server], that will contain the primary backup copies and possibly the backup database[5] are protected with NeuShield Datacenter Edition.

In the event of a ransomware attack that has attempted to encrypt the complete virtual machine active data files on your primary database/large file servers and attempted to encrypt all the data on the Backup Data Server(s), NeuShield will utilize its Database Guardian feature to immediately restore all necessary data plus all the supplementary binaries and files for the database instance are restored together as a set (Microsoft Server operating system and the large unstructured files) to the last good known state prior to the attack.

Once the Backup Data Server is operational, your organization should recover (using the recovery feature of your backup solution) only the relevant virtual machine active data onto your primary virtual servers (VM images in this case). On completion, NeuShield can be engaged to immediately and simultaneously revert all primary server [OS, database, and large unstructured data] to their last good known state prior to the attack[6].

[5] If the backup database is not on the same server, we recommend protecting the backup database with the same configuration.

[6] Reverting Servers with NeuShield can be undertaken simultaneously with any reverts for other NeuShield protected devices and data

Phase Two cont.

No requirement exists to utilize your backup solution once the relevant virtual machine active data has been restored. Using traditional backup recovery procedures for databases and large unstructured files will incur lengthy sequential rebuilding of compromised operating systems and data from backups. NeuShield protection of the Backup Data Server ensures instant recovery and availability of the data, but will not accelerate the time required to move and rebuild data on the compromised servers.

Additional Critical Device Support

NeuShield Data Sentinel provides you the confidence to protect and revert any data, application and services that are installed on Microsoft operating system devices. NeuShield recommends that **NeuShield Business Edition** is installed on these physical servers.

This include, but not limited to:

Active Directory (AD)

Active Directory Domain Services (AD DS) provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. Active Directory (AD) operates as a database and set of services that connect users with the network resources, they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who’s allowed to do what.

Mirror Shielding™ and **One-Click Restore** will protect all AD files and services.

Network Policy Access Services (NPAS)

NPAS enables admins to connect users to the internal network, as well as the external internet. It features several specific roles: Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP). With these, admins secure network connections similarly to the RADIUS protocol.

Mirror Shielding™ and **One-Click Restore** will protect all files and services related to the NPAS roles.

File Services Server

File Services Server provides shared data storage, authorizing access to files based on domain permissions. It also encrypts data as needed and enables remote network storage access through VPN.

Mirror Shielding™ and **One-Click Restore** will protect all files, services, and settings.

Additional Microsoft Critical Services

Other Microsoft critical services may be applicable to NeuShield on a case-by-case basis.

Windows Server Update Services (WSUS) Server

WSUS Server allows IT admins to control how and when their Windows systems update. The server downloads patches, hotfixes, and other updates from Microsoft Update, distributing them across a system fleet as IT organizations deem necessary.

Mirror Shielding™ and **One-Click Restore** will protect all files, services, and settings.

The following Microsoft services can be protected with Mirror Shielding™ and One-Click Restore but may require the user to manually add the folders where the files are stored.

Domain Name System

The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP addresses for those sites. Browsers then use those addresses to communicate with origin servers or CDN edge servers to access website information. This all happens thanks to DNS servers: machines dedicated to answering DNS queries.

Web & Application Servers

Web & Application servers allow organizations to create and host websites and other web-based applications using on-prem server infrastructure. Specifically, the web server handles the HTTP/HTTPS requests/responses of a standard web page. The application server provides a development environment and hosting infrastructure for applications usable through the internet.

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Server assigns IP addresses and other network configurations to systems and servers so that they may communicate with other IP networks. This functionality shoulders the burden of managing system IP addresses, creating new ones as needed.

Appendix A

There are two main types of files that it is not recommended to protect:

NeuShield does not recommend protecting data that is continually opened for exclusive access by an application. Examples of this are:

- Active database (Oracle, QuickBooks, etc.) data files. The exception is Microsoft SQL that is supported in the Datacenter Edition.
- Active VM images (VMware, VirtualBox, Hyper-V, etc.). You can, however, install NeuShield on the guest VM to protect its data.
- Other files that act like a database file (such as the Windows user profile .dat file, etc.)
- NeuShield does not recommend protecting active application files, such as .exe, .dll, and other application files.

Note: Keep in mind that NeuShield also has operating system rollback (with One-Click Restore), so there is usually no need to protect the application files as they will be rolled back with One-Click Restore.