NeuShield® Data Sentinel

Protect Your Data from Ransomware

Overview

One of the security challenges that companies face is how to protect their important data from ransomware and other cybersecurity threats. Ransomware can hold company files or devices hostage using encryption or other means until the victim pays a ransom in exchange for access to the files or device.

NeuShield Data Sentinel solves this challenge with patent pending technology called **Mirror Shielding™** which uses **Data Engrams™** to protect your data and computing resources. Mirror Shielding™ creates a protective shield between your files and your applications. When malicious applications make changes to a file, the original copy of that file stays intact allowing you to revert any undesired change. In addition, multiple revisions of the file are stored using Data Engrams™ allowing you to go back to previous versions.

Unlike other ransomware prevention technologies, NeuShield Data Sentinel offers:

Full protection even against undetected ransomware

With NeuShield Data Sentinel the effects of ransomware can always be undone because changes are never made directly to the protected files. Even changes from zero-day or unknown ransomware can be reverted.

Any unwanted file modification can be undone

Sometimes modifications to files are made unintentionally or without you knowing. However, Data Sentinel protects your files over time using Data Engrams™ which allow you to revert any unwanted change.

Virtually no impact on performance

While other products will create backup copies of your files which can dramatically increase disk usage and cause a significant performance overhead. NeuShield's revolutionary technology can preserve the original file without requiring a backup allowing Data Sentinel to protect files with virtually no additional disk activity (I/O).

Cloud Drive Protection

Many ransomware programs will encrypt files on your cloud drive which can spread to other devices. Data Sentinel automatically protects your cloud drive, allowing you to revert changes and recover these files.

NeuShield Data Sentinel

Security products are continuously adding new types of technologies to detect and block malware. These could include technologies like machine learning, exploit detection, or behavior analysis. But as soon as these technologies are introduced attackers find ways around them. NeuShield stops this cycle by protecting your critical files and allowing any unwanted changes to be reversed.

Features:

- Mirror Shielding™
- File revisions using Data Engrams™
- Boot sector protection
- Disk wiper protection
- Cloud drive protection:
  - Microsoft OneDrive
  - Google Drive
  - DropBox
  - Box Sync
- Cloud management
- Realtime alerting
- Email notifications
- Strengthens your antivirus

Three layers of defense for your computer

NeuShield Data Sentinel offers comprehensive protection by adding three layers of defense to protect your critical files from all types of cybersecurity threats.

Boot Protection

The first layer of defense that Data Sentinel offers is boot protection. This protection will monitor the boot portion of your drive to prevent aggressive types of ransomware, such as Bad Rabbit, Satana, or MBR-ONI "Night of the Devil", from overwriting the boot record (MBR) and leaving the device unable to boot. NeuShield Data Sentinel blocks applications from writing to the boot record without affecting normal Windows functions.

Disk Wiper Protection

Some types of destructive ransomware, such as Shamoon, NotPetya, and Ordinypt, will attempt to wipe the disk to hide a hacking campaign or to cause damage. With NeuShield all raw disk access, which is required for disk wipers, can be prevented, stopping malicious ransomware from destroying the data on your hard drive or SSD.

File and Folder Protection

In addition to boot and disk wiper protection, Data Sentinel uses patent pending Mirror Shielding™ technology to protect your important files. Ransomware programs, such as Locky, WannaCry, or Cerber, will attempt to encrypt files to prevent you from accessing them until you pay a ransom. However, Mirror Shielding™ will block these ransomware programs from making changes directly to your files, allowing you to revert any undesired change.

Data Sentinel uses Data Engrams™ to store up to 7 revisions of your protected files giving you the ability to go back to any of these revisions. Integration with Windows Explorer is also supported allowing you to easily revert or restore files to a previous state by right-clicking on a protected file or folder.

Information about protected files is stored so that Data Sentinel can also revert metadata about your files, such as the modified date, file name and file size.

File Lockdown

After a ransomware attack it can take time before your antivirus is able to cleanup your computer. During this period, it may be important to access your files and documents. NeuShield Data Sentinel can lockdown files allowing you to safely access them even before the system has been fully cleaned.

System Requirements

OS:	Windows 7 SP1 (with IE 11 and KB4054518) Windows 8.1 (with KB2999226) Windows 10
Processor:	1 gigahertz (GHz) or faster processor
Memory:	1 gigabyte (GB) for 32-bit or 2 GB for 64-bit
Disk Space:	500 MB free disk space
Display:	1366 x 768 or higher resolution monitor

NeuShield™
How much is your data worth?

200 Brown Road, Suite 306, Fremont, CA 94539 | (510) 270-8408 | www.neushield.com