NeuShield® Data Sentinel

Protect Your Data from Ransomware

Overview

Over the past few years, ransomware has grown to become one of the largest problems in cybersecurity. A challenge that companies face is how to protect their important data from ransomware. Traditional ransomware protection is often ineffective in stopping new or unknown attacks.

NeuShield Data Sentinel takes a different approach using patent pending technology called **Mirror Shielding™** to protect 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 undesired changes. In addition, multiple revisions of the file are stored using **Data Engrams™** allowing you to go back to previous versions of a file.

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.

Does not rely on backup copies

Other products will backup files so changes can be rolled back. However, this process can be error prone 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

Ransomware will commonly 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
- One-Click Restore
- File Lockdown
- Cloud management
- Realtime alerting
- Email notifications
- Strengthens your antivirus

Three layers of defense for your computer

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

1. 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.

2. Disk Protection

Some types of destructive ransomware, such as NotPetya, Shamoon, and Ordinypt, will attempt to wipe the disk to hide a hacking campaign or to cause damage. With NeuShield all direct (raw) disk access is monitored, preventing malicious ransomware from destroying data on your hard drive or SSD.

3. File and Folder Protection

In addition to boot and disk protection, Data Sentinel uses patent pending Mirror Shielding™ technology to protect your important files. Ransomware programs, such as WannaCry, Locky, or Cerber, will attempt to encrypt files to prevent you from accessing them until you pay a ransom. However, Mirror Shielding™ technology 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, you can recover the original files by simply clicking a single button.

System Requirements

OS:	Windows 7, 8.1, 10 Windows Server 2008 R2, 2012 (including R2), 2016
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

Data Sentinel also 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.

Restore computer to a known good state

NeuShield Data Sentinel's One-Click Restore capabilities can also undo damage to the operating system caused by ransomware or other cybersecurity attacks. NeuShield can reset the whole computer back to a known good state, allowing you to quickly regain access to your device, files, and data where traditional security and storage methods fail.

NeuShield™
How much is your data worth?

200 Brown Road, Suite 306, Fremont, CA 94539 | (802) 870-6387 | www.neushield.com