NeuShield Data Sentinel Differentiation

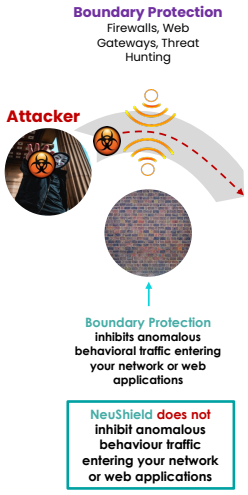
NeuShield Data Sentinel allows you to shield and protect your data from malware or human error. The only anti-ransomware technology that can recover your damaged data from malicious software attacks without a backup. As an all-in-one solution our features include boot protection, disk protection, file and folder protection, data inspection, One- Click Restore and cloud protection. Data Sentinel uses its patented Mirror Shielding™ to protect files ensuring that you can instantly recover your important data from **any ransomware** attack.

How does NeuShield Data Sentinel differ from existing cyber protection & recovery tools?

What happens today to stop cyber-attacks?

Let's take you through the intent of a cyber-criminal and the purpose of existing tools that attempt to stop their attack and mitigate data from being compromised, stolen or deleted.

NeuShield plays **no part in identifying, stopping or notifying analysts** when malware breaches the following parts of your infrastructure.



In most instances, an external cyber-attack will need to breach your network boundary to gain entry to your infrastructure and data.

Hardware and software solutions will inhibit traffic from entering your network or web applications.

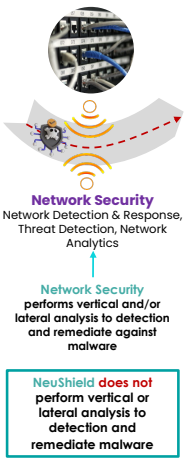
Various anomaly detection methods are used to stop known and unknown attack vectors achieving a presence on networks.

Another entry point for malware is via your organization's communication and business applications.

Email, social media and websites are great communication tools, but they are also some of the most targeted applications.

Security tools looking for phishing and business email compromise as well as embedded malware are commodity tools in an organizations stack.

But this is one of the most successful routes for cyber attackers

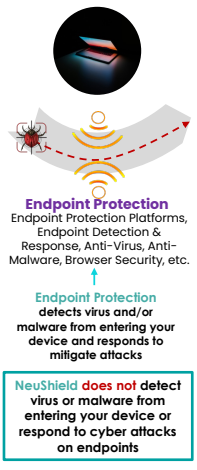


If Boundary Protection fails, then the cyber malware will gain entry to an organizations network.

The malware will be looking to traverse (vertically and vertically and laterally) across the internal and connected networks.

Cyber security tools will be analyzing networks 24/7 looking for anomalous traffic behaviour to detection and respond, nullifying its attack objective(s).

Network Security is good, but attacks do get through.



Endpoint security is the last line of defense against the cyber criminals.

EPP, EDR and other endpoint solutions provide some of the most advanced threat detection and response capabilities.

Cyber criminals are illusive in their attacks, specifically attacking the architecture of EDR and EPP providers.

These new vectors will continue to create exceptional events against endpoint protection.

cybrilliance
Empower Your Business with Cyber Resilience.

What is NeuShield Data Sentinel

How does NeuShield Data Sentinel differ from existing cyber protection & recovery tools?

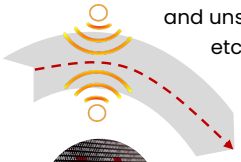
What happens today to recover data?

Let's take you through the purpose of existing tools that attempt to recover data after it has been compromised, stolen or deleted.

NeuShield has architected a new patented technology that stops cyber-attacks [that have evaded cyber tools] intent to delete, steal and/or compromise the data in real-time on endpoints, servers and storage shares.

Data Protection

Data Protection
Unstructured, Semi-structured, Structured, Files, Databases, Images, Audio, Video



Backup & Recovery
involves full, differential, images, shadow copies of the primary data

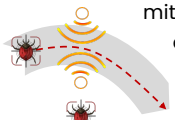
One of the most valuable assets an individual or organization retains, Data can take many forms, structured (databases) and unstructured (files, images, audio, etc.), shareable to individuals and organizations.

Organizations will deploy data backup tools to ensure that they have the capability to capture various extracts or complete copies of data at any given time. This allows them to use the same tool to recover those data copies within an agreed time period and also to a specific point in time .

Mitigate Active Data Compromise

Data used for operational purposes can be compromised by intentional (cyber-attacks) and unintentional (mistakes) activities.

Active Data Protection
Real-time protection for all data, applications, system files & OS



NeuShield encases files, applications and operating system with a protective barrier, preventing harmful code from compromising operations or stealing your data

NeuShield ensures that data is continually protected in real-time to mitigate any attempt to steal, delete or compromise data on any device that NeuShield Data Sentinel is installed.

The introduction of NeuShield's patented Mirror-Shielding™ technology never provides access to the complete data.

Any updates or amendments to the data are stored on the device that the data resides (in an overlay facility) and applied to the original data periodically, following checks for data validity.

The data validation step ensures that irregular data such as encryption, malware, hidden executables, etc. are not imbedded in the overlay and may compromise the original data when applied.

Backups

Backups

Backups
create physical or immutable copies of data aligned to the NIST 3-2-1 framework

NeuShield **does not** rely on any backups from traditional backup & recovery solutions

As mentioned previously, organizations take multiple extracts and full copies of data.

In addition to this, trusted institutions advise Backup Administrators to keep a minimum of three duplicated sets of these copies. One onsite (original data location), one offsite and another on a different storage medium (immutable, tape, etc.).

These duplicated copies provide a further level of protection of the backup copies.

All of these data copies are managed and recorded by the backup software database.

Unfortunately, unless the duplicated copies are on immutable, read only or a physical device such as tape, which tends to be only one set of duplicated data, the remaining two sets of copies are exposed and can be compromised by intentional (cyber-attacks) and unintentional (mistakes) activities.

Mitigate Lengthy Data Recovery

It may take twice as long to recover compromised data, than the time it took to make the original backup copy. If the data backup copies were not successful, or the backup database had been compromised during an incident your capability to restore data and your operations may take days or weeks.

Time-Sensitive Reverts

NeuShield saves Data Engrams & OS images to provide access to your last know good state

NeuShield does not rely on using traditional backups to restore your data to its 'last-good-known state'. Residing on the device that the original data is present, NeuShield keeps Data Engrams (changes), and copies of your OS that allow you to restore your device and data in a matter of minutes or hours in the case of hundreds of thousands of files.

As every device that NeuShield is installed operates independent of other devices, networks or backups, you can achieve operational status across hundreds or thousands of devices in the same time.