# New tactics for active protection and recovery

## Advance your cyber resilience with an active data protection & instantaneous recovery strategy

## Why NeuShield, and why now?

- A single full featured tool that delivers **active** data protection and instant recovery.
- Multi-layered endpoint (PCs, workstations & servers) protection with local and cloud management.
- Instant recovery of data (device and cloud shares), applications, and operating systems.
- Removal of hidden or polymorphic malware by returning the computer to a known good state.
- Recovery from attacks yet to be detected, and alerts raised during data divergence analysis.
- Higher data assurance protects against ransomware, fileless malware and data breach incidents.

Data protection, backup & recovery has been the foundation for securing data and applications for organizations and individuals for more than 40 years.

However, the world that required data backup & recovery at the beginning is a far cry from the highly digital one we work and play in today. Dominating the explosion of the data age are two major security factors:

1. Adhering to data protection and privacy regulations to stay legal, compliant, and reputable, such as: CCPA, GDPR, One Identity, Data Protection Regulation, etc.
2. Combating the arsenal of cyber vectors from a variety of cyber criminals constantly trying to breach your security.

For the last 20 years, technology vendors (established enterprise experts as well as some truly innovative expert startup shakers) have been tirelessly working to progress and protect in this era of exponential data growth. This growth includes the management of data and applications, alongside global operational requirements.

Another massive market that has risen out of the digital revolution is the need for smarter data storage that can efficiently handle terabytes in various formats. Modern storage products or services now, typically, enforce proprietary protection technologies. While this is absolutely a positive, increasing the variety of architectures can hinder efficiency, become resource heavy and complicate file (data) organization and administration.

So, what is the next move for improving the way you improve your cyber resilience to protect, restore, and refine your data recovery management?

**In this document, you will discover what NeuShield is, what it isn't, what it does, and how you can benefit with it.**

**We look at how:**

- **NeuShield has reacted to CIOs acceptance that cyber-attacks will breach their defenses, exposing data, devices, employees and customers.**
- **You will learn how NeuShield strengthens operational protection and recovery policies, part of existing cyber resilience plans by adding a protective layer to business data activity, and the instant recovery of data in one click.**
- **NeuShield's value is not just technology, it goes further and stimulates savings on storage space, software licenses, resource management and costs.**

# Data security through the decades

## Cyber plundering

In the 1990s, the world went online. And so did the first polymorphic viruses. Cyber criminals had more devices and software vulnerabilities to exploit than ever before. And as data was increasingly being kept in digital format online, there was even more to plunder.

Consequently, the **malware** numbers rapidly went from tens of thousands at the beginning of the decade to five million every year by 2007.

And the cyber criminals weren't done yet. The next wave of security issues came in the form of zero-day attacks. This development meant that antivirus software was becoming less effective. The problem is that you can't check code against existing attack signatures *unless* the virus already exists in the database.

A positive development during this decade was OS security. Cybersecurity was being built into **operating systems** to provide an additional layer of protection.

Still, the 2010s saw many high-profile breaches and attacks that impacted the national security of countries and cost businesses millions. As cybersecurity vendors continued to try and keep up with the expanding range of attack types, criminals kept on responding with their own innovations, multi-vector attacks and social engineering. Security vendors were then forced to move on from purely signature-based methods of detection, and usher in new security techniques.

## 21st century data risks

The tireless development of the attack vectors used by hackers means that even the best security tools continue to miss their tricks. This is evident in the number of cyber incidents being reported which are causing obfuscation, destruction, and exfiltration of personal, sensitive and intellectual property data.

When the attacker targets the primary data (not confused with the primary backup), a breach becomes an immediate risk. Hackers also target (to compromise) online backups, the directories that control the management of backups and recovery, as well as the active directory database that controls access and privilege credentials for users.

# Deficient recovery

Prior to the 2010s, backup and recovery excellence was still focused on the validity of testing disaster recovery and business continuity (BC/DR) exercises. That means, the capability to restore all or part of a system during a designated testing period. Non-time sensitive or operational restores (caused by hardware failures or lost personal devices, for example) were also performed as non-priority activities.

And largely this is still the situation today, even with the benefits of cloud services.

The inability to speedily restore operations following data loss incidents — whether it's a ransomware attack, hardware compromise, accidental or intentional data destruction — is having catastrophic effects on organizations and their customers.

One reason for this is that current recovery policies and traditional backup & recovery tools cannot meet the recovery time objectives (RTO) that businesses need today.

This is due to a) the dependencies that restores have on network availability, and b) the availability of the compromised devices' operating systems. To put it another way, devices need to be accessible and operational before data can be recovered.

Other considerations that hamper traditional backups being used for recovery these days include: the attacker has saturated all networks (DDoS), primary backup is compromised, active directory (AD) and/or backup databases are compromised, all of which harm the organization in terms of expensive time, reputational and resource distractions.

## Why it's time to advance to active data protection & instantaneous recovery

*There has been no progress for data recovery that can match the real-time RTO that a modern business requires.*

Security tools have evolved amazingly. Great. Now active data protection in real-time, and instant recovery options need to do the same to start achieving more business continuity and efficient RTOs.

Yes, there have been incremental adjustments to the types of backups, frequency, relevance to physical and virtual, various tiers of storage protection technologies, RAID, encryption, immutable (write once), etc. But there has been no progress for data recovery that can match the real-time RTO that a modern business requires.

To help minimize the current impacts seen during in-process and/or past cyber incidents, backup & recovery needs to be elevated from a passive reaction function. It needs to evolve to be a critical element of cyber resilience and become the **active data protection & instant recovery tool**. It is this that will help drive real operational continuity.

# NeuShield delivers real-time protection and continuity

## Primary purpose

- NeuShield takes **active** data protection and anti-ransomware tactics to another level.
- It encases files with a protective barrier – which is periodically set to **commit** updates - to prevent harmful code from getting in to corrupt your data, applications and operating system.
- Any malicious code attempts on the encased data will be futile.
- Only the very latest, miniscule file updates (e.g.: a change of a few words in a file or numbers in a spreadsheet), not the entire file or it's backup copies are ever at risk in the event of a successful attack. Should this happen, one simple click restores the encased 'good state' updates from the data engram to the original file.

## Added benefits

NeuShield dramatically reduces storage requirements for file versions of data engrams. The administration of **recovering the required engram to be associated with the original file is simple with NeuShield Data Sentinel**. This approach negates the need to retain current primary [onsite] backups (part of your 3-2-1 policy) taken by your backup and recovery. This removes the need for your backup and recovery tool to store the multiple copies of your primary [onsite] daily, weekly, monthly and quarterly recoveries of full, incremental and/or differential backups.

- So, where your backup & recovery tool is costed via front end terabytes (FETB), **NeuShield can support you to reduce software licenses and hardware costs**, freeing up sizeable amounts of disk storage for future data assets.
- NeuShield protected organizations will realize a **dramatic reduction of heavy resource requirements** (associated with recovering data), freeing up time for more priority work.

- When centralized IT management is not required, NeuShield provides users with **local restore capability**.

## How NeuShield fits in with your current backup and recovery strategy.

Adopting NeuShield does not mean removing your existing backup & recovery tool. **NeuShield is collaborative**, in the same way that endpoint and network security works in harmony with SIEM and XDR.

- NeuShield is for active data protection and instant recovery (data, applications, OS).
- Your existing backup & recovery tool should focus on BC/DR and other non-time sensitive recovery operations.
- The National Institute of Standards and Technology (NIST) best practices of a 3-2-1 strategy for backups still stands:
  1. Keep three copies of any important file: one primary (e.g., behind NeuShield) and two backups.
  2. Keep the files on two different media types to protect against different types of hazards.
  3. Store one copy offsite (outside the business facility and if possible, air-gapped/immutable).

*Diagram 1 (below) provides an example of how NeuShield Data Sentinel integrates with existing backup & recovery strategies.*

## Diagram 1 - NeuShield advances your active backup & recovery strategy