Cyber Resilience Strengthens Cyber Security

The importance of time-sensitive cyber resilience
when cyber security tools fail to stop the damage

The element of surprise "mystify, mislead, and surprise[1]" by cyber criminals means that combinations of the most advanced cyber security tools will always be reactive, exposing organizations to the continual risk of being breached.

Cyber resilience describes the ability to continue delivering intended business and operational outcomes despite experiencing challenging cyber events, such as mitigating successful cyberattacks and responding to cyber incidents.

Why should cyber resilience be as profound as cyber security?

Cyber security is how individuals and organizations reduce the risk of a successful cyber-attack.
Cyber resilience is vital for business continuity, providing benefits beyond increasing an enterprise's security posture and reducing the risk of exposure to its critical infrastructure. Cyber resilience also helps reduce financial loss and reputational damage. A cyber-resilient company can optimize the value it creates for its customers, increasing its competitive advantage through effective, efficient and responsive operations.

What is effective cyber resilience?

A measured level of information security proficiency and resilience affects how well an organization can continue business operations with little to no downtime, in other words.

Effective cyber resilience must be an enterprise-wide risk-based strategy, a collaborative approach driven from executives to everyone in the organization, partners, supply chain participants and customers. It must proactively manage risks, threats, vulnerabilities and the effects on critical information and supporting assets.

---

[1] — Sun Tzu, The Art of War

Effective cyber resilience also involves governance, risk management, an understanding of data ownership and incident management. Assessing these characteristics demands experience and judgment.

Further, an organization must also balance cyber risks against attainable business opportunities and competitive advantages. It must consider whether cost-effective prevention is viable and whether, instead, it can achieve rapid detection and correction with a good short-term effect of cyber resilience. To do this, an enterprise must find the right balance between three types of controls: preventative, detective and corrective. These controls prevent, detect and correct incidents that threaten an organization's operational resilience.

Cyber resilience will continually provide an organization a competitive advantage over companies without it. Enterprises that develop management systems based on best practices, such as Information Technology Infrastructure Library (ITIL), create an effective operation. So, too, do they when developing a management system for cyber resilience. And as a result, these systems create value for their customers.

CyBrilliance - Advancing Cyber Resilience

While you're reading this, attackers are persistently working to breach your networks and they are using increasingly successful sophisticated methods to find a way in.

Should you rely on Cyber Security?

Why waste budgets on Cyber Resilience?
If the efforts of cyber security vendors stopped all cyberattacks, resist attempts to breach your defences and find those already on the inside, why are you continually confronted with successful attacks?
These organisations have cyber security tools deployed but were still critically damaged;

NHS
LockBit
Data Breach &
System Disruption

Conti
Ransomware

CHRISTUS
Health.
AvosLocker
Ransomware

SAMSUNG
Data Breach

Cyber Resilience Strengthens Cyber Security

Digital businesses will always be at the mercy of the latest cyber vectors, so they need to adopt a more effective cyber security and cyber resilience strategy that has the capability to deliver real-time active data protection and when required time sensitive instant recovery of data and devices.

Cyber Resilience Strategy - Based on your organization's objectives, any strategy work needs to identify critical assets, such as information, systems and services that matter most to it and its stakeholders. This work also includes identifying vulnerabilities and the exceptional risks they may encounter.

Cyber Resilience Design - selects the management system's appropriate and proportionate controls, procedures and training to prevent harm to critical assets, where practical to do so. The work also identifies who has what authority to decide and act.

Cyber Resilience Transition - from design to operational use tests controls and refines incident detection to identify when critical assets are under stress from internal, external, exceptional or accidental action.

Cyber Resilience Operational - controls and detects and manages the resilience of all assets during and after cyber events and incidents, including continual control testing to ensure effectiveness, efficiency and consistency.

Cyber Resilience Evolution - continually protects an ever-changing environment. As organizations recover from incidents, they must learn from the experiences, modifying their procedures, training, design and even strategy.

Cyber Resilience Strengthens Cyber Security

CyBrilliance Selects Neushield to Advance Cyber Resilience

Smart Cyber Resilience to Stop the Weaponization of Availability

- Continuously protect data during compromise attacks.
- Recover from an incident in hours, rather than days.

CyBrilliance is a business cyber continuity hub. We focus on finding the most advanced cyber resilience and recovery offerings on the market. We test the best and help CIOs, CTOs and CISOs add them to their existing security and operations stacks.

NeuShield Data Sentinel has been named the winner in the Best Emerging Technology category of the 2022 SC Awards.

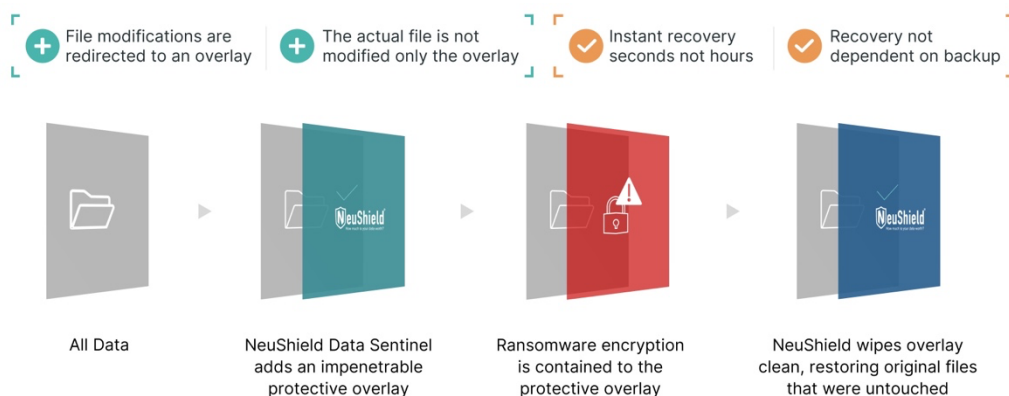## How fast could you recover from a cyber incident?

NeuShield is the only solution that can recover all your encrypted data and operating systems **instantly**. NeuShield's patented anti-ransomware technology can recover your original data from malicious software attacks **without a backup**.

---

5   Cyber Resilience Strengthens Cyber Security

Traditional protection and recovery methods are not delivering the cyber resilience that digital operations require today. If they did then we wouldn't be seeing the increasing levels of frustration when a cyber-attack results in a cyber incident, marginalizing business operations often for extended periods.

Could your company survive that?

Active data protection and instant data and device recovery.

- NeuShield is an overlay polarization tool. Any changes to documents, software and operational processes are safely protected behind NeuShield's Mirror Shielding™.
- Any cyber-attack (ransomware, malware, data breach) that evades your security tools and attempts to compromise your data will never be successful.
- You no longer have to worry about executing lengthy (or failing) backup restores when responding to cyber incidents or payments to criminals.
- Instant recovery if you ever need it with **NeuShield Data Sentinel**. It is no longer necessary to rely on lengthy backup and restore processes, rollback or cloud copies of your data.
- The average time to recover from a ransomware attack is 17 days. NeuShield Data Sentinel can do it in minutes or hours, at the click of a button.
- Adding NeuShield advances your cyber resilience stack. It works alongside existing data protection and recovery strategies.

| File modifications are redirected to an overlay | The actual file is not modified only the overlay | Instant recovery seconds not hours | Recovery not dependent on backup |

All Data → NeuShield Data Sentinel adds an impenetrable protective overlay → Ransomware encryption is contained to the protective overlay → NeuShield wipes overlay clean, restoring original files that were untouched

NeuShield Cyber Resilience Value

Mirror Shielding™

Patented technology that adds a barrier to protected files preventing them from being modified. Mirror Shielding™ 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.

One-Click Restore

Restores operating system files and settings back to a known good state allowing you to quickly regain access to your computer after a ransomware attack. One-Click Restore also removes both known and unknown malware.

Boot Protection

Protects the boot portion of a drive to prevent aggressive types of ransomware from taking over the boot process and preventing applications from writing to the boot record.

Data Engrams™

Leverages Mirror Shielding™ to create copies of modified data at different points in time. Data Engrams™ work like file revision history, allowing files to be restored to previous versions.

Disk Protection

Monitors all direct disk access preventing malicious programs from destroying data on the hard drive or SSD. Protects against destructive ransomware or wipers that attempt to wipe the disk.

Cloud Drive Protection

Protects local cloud drive folders allowing destroyed or corrupted data to be recovered quickly without an Internet connection. Supports popular solutions, such as: OneDrive, Google Drive, DropBox, and Box.com.

File Lockdown

Temporarily blocks write access to protected files preventing them from being modified during an active attack from Fully UnDetectable (FUD) ransomware.

Zero Performance Impact

Extremely small client engine using less than 10MBs of memory, making decisions about critical files with virtually no CPU or disk (IOPS) overhead.

Cyber Resilience Strengthens Cyber Security

It's not all criminal!

A number of unintentional internal actions can cause a computer or application to stop working. It could be as simple as a bad Microsoft patch, a system setting change or even a newly installed application. NeuShield makes it easy to efficiently regain access to your computer, applications and data.

Rollback technologies rely on various backups of your data. These can be limited in terms of location, network access and storage architectures. If there is too much encryption going on, or disk space becomes limited, it can be difficult to recover all your data and your recovery time objective will be compromised.

Go to the CyBrilliance website and read how some of NeuShield customers are using NeuShield Data Sentinel to deliver active data protection and instant recovery.

HST Pathways
HST Pathways Deploys NeuShield Sentinel for Data Protection

Randolph
Community College Counts on NeuShield to Protect Data

Central Computer & Networks
Central Computer & Networks Trusts NeuShield to Protect its Client's Systems and Data

CyBrilliance Cyber Resilience| Cyber Resilience Strengthens Cyber Security | Industry Report

About CyBrilliance

CyBrilliance is an internationally minded global master distributor headquartered in Ontario, Canada.

With CyBrilliance you have a diverse group of experts in marketing, sales, cyber, operational technologies, advertising, and other disciplines, representing EMEA, India, Canada, and the US.

We are all devoted to telling the Cyber Resilience story and serving customers in ways that account for local needs and cultures, as well as addressing the needs and wants of specific audiences and stakeholders.

We are a channel partnership focused organization that extends across EMEA, Asia Pacific, North and Southern America.

CyBrilliance LLP
The organization is registered as a limited liability partnership registered in Canada.
CyBrilliance LLP, Burlington, Ontario, L7L 4C4, Canada.