$170,000 off your Anti-Ransomware costs every year

Cybrilliance research[1] has found that current data protection and recovery policies are no longer fit for purpose.

Businesses are increasingly dependent on “Always-Available” devices and data for operations, customers, partners and employees. Safeguarding this means keeping backups. Often, the cost and time involved in reinstating data from backups is not realised until data recovery is needed / disaster has struck. This can come as a nasty shock. It can also be readdressed before a successful event.

The value of your business data and its monetization by cyber criminals, combined with the growth in government, industry and privacy regulatory data compliance has changed the way that you manage and protect data today.

Cybrilliance proposes a new data protection and recovery policy, one where all active data recovery is performed immediately ‘on-device’ and is immune from compromise - without restrictive dependencies (such as network availability for accessing backups). It means that in addition to the on-device data only one copy of data is retained on immutable technology (off-site) to prevent malicious or inadvertent data tampering.

Back up and recovery services are often focused only on the backup function. The recovery service is an additional cost. Our research uncovered that attempting to recover 5TB of data within a 5-hour recovery window only 4% (230GB) of the data was available to the business.

- Data is being retained “just-in-case” it may be needed.
- Research found current backups typically accumulate 54 times the 5TB original data in one year (e.g.: 207TB).
- Up to two-thirds of this data is at risk (stolen, encrypted, deleted) from cyber criminals.
- It is critical to recover the data in a realistic time frame to restore operations following an incident.
- Further analysis found that the initial costs of ~$10-26k is only for the backup and storage service. It does not represent the real costs for tamper-proof data protection, or delivering the recovery of data in a realistic time.
- The hidden costs (just to recover the data) often only becomes visible during incident recovery activities.
- These costs can climb to 17 times ~$150-190k of the initial costs.

The research found that NeuShield Data Sentinel only needed to retain 7.02TB of protected data to keep your operations running. This is far more cost effective than needing to keep 207TB accumulated from multiple backup copies. With NeuSheild from Cybrilliance, the time to recover the original 5TB of data was less than one hour, costing $22,387, saving you <$170,000 per year.

$170,000 off your Anti-Ransomware costs every year

Cybrilliance research[1] has found that current data protection and recovery policies are no longer fit for purpose.

Existing Policy

COST
$152,192 -----> $191,848

RECOVERY EFFICIENCY
2% - 4%

RANSOMABLE DATA
<138TB

TIME-SENSITIVE SCALABILITY
Dependent on backup accessibility and networks.

NeuShield Policy

COST
$16,500 -----> $22,387

RECOVERY EFFICIENCY
100%

RANSOMABLE DATA
Zero

TIME-SENSITIVE SCALABILITY
No backup or network dependencies.

Diagram relates to a mix of 100 devices (workstations & servers), 5TB of initial data accumulating 69TB of primary data over one year, 207TB of backed up data using either on-premise or cloud-native providers, accessing 51-100Mbps network bandwidth for recovery.

[1] Synergy Six Degrees: **3-2-1 no longer fit for purpose with high hidden costs for today’s “always available” needs.**