NeuShield®

How much is your data worth?

Making Ransomware Obsolete

HOW NEUSHIELD CAN SUPERCHARGE EXISTING BACKUP STRATEGIES

Fast-track Recovery and Storage at Lower than Zero Cost, Without Waiting for Expenditure Approvals

NeuShield exists to supercharge your existing backup software strategies.

NEUSHIELD GUARANTEES

- No exfiltration of data or unauthorized data modification
- 99% faster business continuity after a ransomware attack
- Minimized recovery costs
- Never pay a ransom demand

TEST OUR RANSOMWARE PROTECTION PROMISES WITHOUT OBLIGATION.

For questions about this paper and to find out more about how NeuShield works:
Sales@neushield.com or call **+1 510-239-7962**

Next Generation of Backup & Recovery is Here

Fast-track recovery and storage at lower than zero cost, without waiting for expenditure approvals.

NeuShield’s instant operational and cyber incident data recovery method uses device based active data. It eliminates superfluous copies of data backups.

NeuShield's approach maintains Recovery Point Objective (RPO) targets and delivers Recovery Time Objectives (RTO) that align to your business continuity plan’s maximum allowable threshold or “tolerance”.

Deploy NeuShield in minutes without the requirement for expenditure approvals. Upfront costs will be returned from planned spend based on storage savings.

> **NEUSHIELD EXISTS TO SUPERCHARGE YOUR EXISTING BACKUP SOFTWARE STRATEGIES.**
>
> • Reduce storage requirements by ~64%
> • Accelerate data recovery time by 99%
> • Save ~$25,000 (or 133TB storage costs)

Backup and Recovery Software Purpose

Organizations safeguard their critical business data, categorized as sensitive or essential, across devices in varied formats.

NeuShield’s instant operational and cyber incident data recovery method uses device based active data. It eliminates superfluous copies of data backups.

NeuShield's approach maintains Recovery Point Objective (RPO) targets and delivers Recovery Time Objectives (RTO) that align to your business continuity plan’s maximum allowable threshold or “tolerance”.

Deploy NeuShield in minutes without the requirement for expenditure approvals. Upfront costs will be returned from planned spend based on storage savings.

GENERIC DATA PROTECTION OVERVIEW

Specialized software facilitates regular backups on-premises, in the cloud, or both. Aligned with a specific RPO via periodic schedules — incremental, daily, weekly, monthly, and quarterly. RTO uses an explicit RPO to recover data operations in line with the business continuity plan's maximum allowable threshold or “tolerance”.

3-2-1 BACKUP STRATEGY

Currently the standard for mitigating single points of failure.

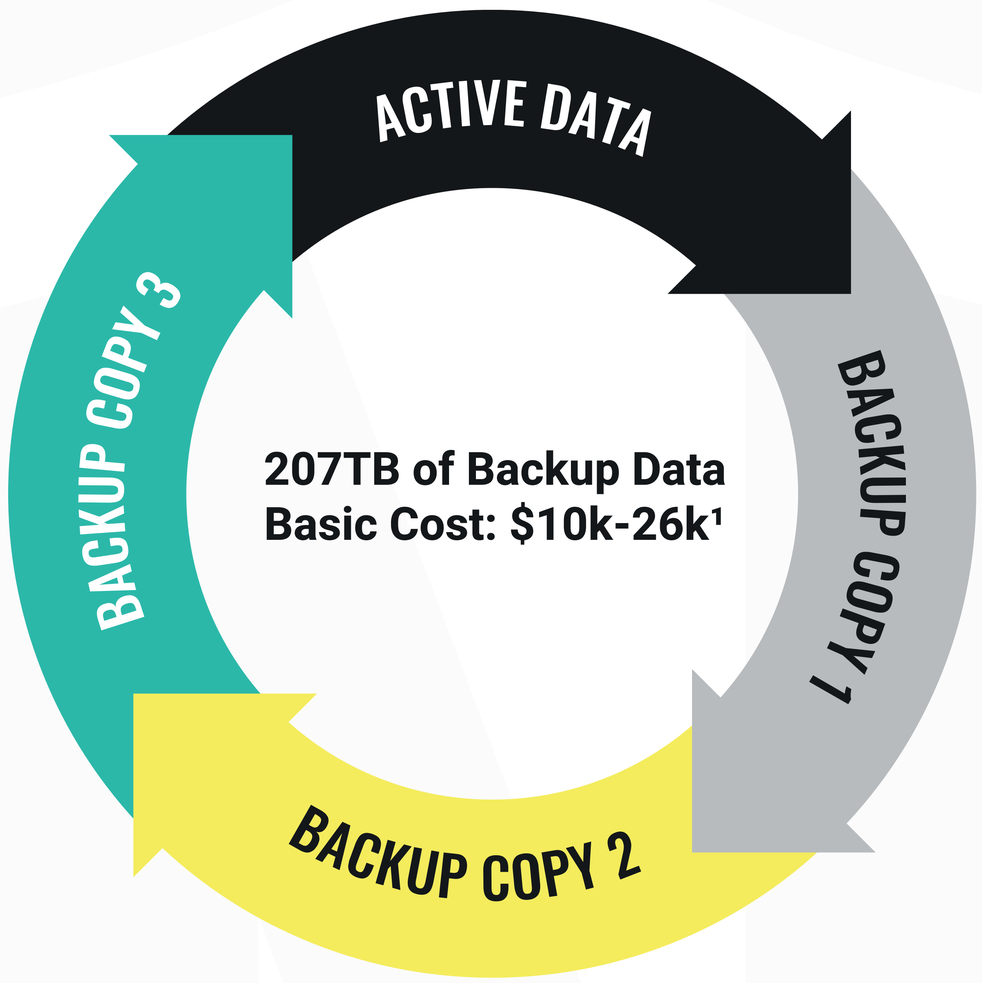
1. In case of on-site data loss.
2. Off-site cloud-based backup serves as the crucial second copy.
3. This is commonly stored off-site on immutable or tape media to prevent tampering.

BACKUP DATA ACCUMULATION

- 3-2-1 ensures accessibility of any RPO from each backup copy within the last 12 months.
- Using the 3-2-1 strategy, an organization with 100 devices and 5TB of operational data (on day one) can accumulate up to 207TB of backup data (Table 1) over a 12-month period.

3-2-1 Backup Strategy

5TB BASE DATA - RESIDENT ON 100 DEVICES
DATA ACTIVE OVER 12 MONTHS
RPO - DAILY, WEEKLY, MONTHLY, QUARTERLY



Active Data - Operational Data. 12 months = 69.2TB.
Backup Copy #1 - On-site for immediate access. 12 months = 69.2TB.
Backup Copy #2 - Off-siteand used if backup copy 1 is unavailable or for BC/DR purposes. 12 months = 69.2TB.
Backup Copy #3 - Off-siteon different media (immutable/tape). Used when backups 1 & 2 are unavailable or for BC/DR purposes. 12 months = 69.2TB.

Critical Data To Backup	5.0TB	Backups Retained			
Growth/New Data Per Day	10%				
Number Of Devices To Protect	100				
BACKUP FREQUENCY		**DAILY**	**WEEKLY**	**MONTHLY**	**QUARTERLY**
Initial Critical Data Retained		5.0TB	7.0TB	39.0TB	52.0TB
Accumulated Backup Data (7 days, 4 weeks, 12 months, 4 quarters)		7.0TB	39.0TB	52.0TB	69.2TB
3-2-1 BACKUP POLICY		**DAILY**	**WEEKLY**	**MONTHLY**	**QUARTERLY**
Primary Backup - On-Site		7.0TB	39.0TB	52.0TB	69.2TB
Secondary Backup - Off-Site/Cloud		7.0TB	39.0TB	52.0TB	69.2TB
Third Backup - Different Media Type[2]		7.0TB	39.0TB	52.0TB	69.2TB
TOTAL BACKUP DATA HELD		**21.1TB**	**117.1TB**	**155.9TB**	**207.5TB**

Source: https://www.synergysixd.corn/Results - Is 3-2-1 still fit for purpose in today's "always available" world?
Microsoft devices protected: 50 x PC/Workstations; 40 x Servers;10 x MS SQL Servers.

[1] Excludes premium features, plus immutable media, mounted devices (NAS), applications (MS365, Salesforce), etc.
[2] Stored off-site to protect from acts of god, fire, flood, earthquake etc.

Cost Analysis[3]

Backup and storage of the initial 5TB of data from 100 devices incurs an annual licensing cost ranging from $10,000 to $26,000, dependent on the vendor and location (on-premises or cloud) of the backup data.

BACKUP AND RECOVERY OPERATIONAL PROCESS

Backup activities require full data and infrastructure availability.

BACKUP AND RECOVERY PROCEDURES

Backup Data

Maintain daily, weekly, monthly and quarterly schedule to capture backups and snapshots of structured and unstructured data

Recovery of data (RPO & RTO) is undertaken by the IT Admin when one of two events occur.

1. Operational Incident: Data is deleted, corrupted in error by a user, a system program or software update is invalid. During normal operations the IT Admin would follow the standard operational data recovery processes for stages 1-4 (see diagram below).

2. Cyber Incident: An attacker or malware attack has thwarted security tools, encrypted, or deleted data (including backups and critical services) and incapacitated devices (via operating system corruption). During a cyber incident event the IT Admin will need to adjust their cyber incident data recovery processes for stages 1-4 (see diagram below).

OPERATIONAL DATA RECOVERY

Data Selection

Choose on-site 3-2-1 copy that holds RPO data

Operational Devices

Target devices are operational or have been replaced

Networks

Active and sustainable networks to transmit data

Recover Data

Restore full and incremental data to achieve RPO

CYBER INCIDENT DATA RECOVERY

Data Selection

If the on-site copy is compromised, select RPO data from the off-site (if available) or 3rd copy

Operational Devices

If OS is compromised, restore or replace ir prior to data recovery. Network availability could delay recovery

Networks

Wait until malware is removed and networks are re-established to transmit data

Recover Data

Restore full and incremental data to achieve RPO

[3] All data points within this report come from the Synergy Six Degrees report "Is 3-2-1 still fit for purpose in today's 'always available' world? ". www.synergysixd.com/results.

CYBER INCIDENT DELAYS AND COSTS

All on-site data copies may be compromised, requiring IT to recover from off-site locations. As networks will be intentionally disabled by operations or via the attack vector, any recovery of data and device operating system will be delayed. Once full or partial network connectivity is re- established, additional bandwidth (2Gbps) needs to be purchased for ~$100k-$153k to meet the RTO or accept that the RPO will take over four (4) days. The IT Administrator will then need to recover all on-site backups or initiate immediate backups to provide new RPO recovery capabilities.

CYBER INCIDENT DELAYS

CYBER ATTACK

Malware reconnaissance will identify and compromise (encrypt/ delete) backups, snapshots, image copies.

DEVICE COMPROMISE

Malware will compromise OS, applications and virtual images, rendering devices inoperable until restored.

DISABLE NETWORKS

IT / IR teams disable all networks upon notification of an incident. When restored, bandwidth is shared across IT.

RECOVER DATA

Restore full and incremental data to production system from 2nd / 3rd copy to achieve RPO. Then Recover on-site backups.

Operational Storage / RPO Strategy

The NextGen Backup and Recovery strategy can immediately reduce your backup storage requirements by ~64% (133TB). This is achieved by transitioning from your current 3-2-1 policy to the NextGen 1-1 policy4.

NEXT GEN BACKUP POLICY	DATA LOCATION	DAILY	WEEKLY	MONTHLY	QUARTERLY
ORIGINAL BACKUP DATA REQUIRED	**On-site & Off-site**	**21.1TB**	**117.1TB**	**155.9TB**	**207.5TB**
Additional Costs to Meet RTO (3-2-1 Strategy)	Additional on-device storage[5]	0.5TB	0.7TB	3.9TB	5.2TB
Costs to Deliver RTO (3-2-1 Strategy)	Off-site backup	7.0TB	39.0TB	52.0TB	96.2TB
Next Gen RTO Capability (using NeuShield)	On-device & Off-site	7.5TB	39.7TB	55.9TB	74.4TB
Costs to Deliver RTO (3-2-1 Strategy)		13.5TB	77.4TB	100.0TB	133.1TB

NeuShield will be implemented as the best-practice policy for: data protection (Mirror Shielding™), instant recovery of active and prior data (Data Engrams™), and device operating systems.
Every file protected by NeuShield can retain up to thirty (30) prior versions and seven (7) days of operating system images. In addition, protection of Microsoft SQL Databases with Datacenter Edition will mitigate exfiltration attempts and unauthorized data compromise.

NeuShield recovers the entire SQL database and server infrastructure to a specific RPO.

The second element of the NextGen 1-1 policy requires the copying of data at periodic stages (incremental, daily, weekly, monthly, quarterly). Only a single copy will be required to be stored off- site on a tamper-proof media such as immutable storage. The purpose of this data is to assist with data recovery in the event of device hardware failures, non-NeuShield protected data, and BC/DR.

[4] All data points in this report come from the Synergy Six Degrees report "Is 3-2-1 still fit for purpose in today's 'always available' world? ".

NextGen Storage Lower than Zero Cost

Our model[5] calculated that retaining 207TB of backup data may cost ~$64,727 per year compared to ~$23,198 for the immutable backup copy for your NextGen Backup Policy.

That's an immediate ~$41,529 (64%) saving in storage license costs. When you add ~$16,500 for the NeuShield Data Sentinel licenses (for the 100 devices in our model), the NextGen Backup Policy can still save ~$25,029 of planned spend from your IT budget. NeuShield costs come from existing planned spend. If you pay for storage as metered (pay-per-use), your monthly savings can be used for NeuShield licenses. If you buy your storage as a yearly subscription, the storage savings from NextGen Backup Strategy can be consumed by planned (non-backup) storage expansion needs. There is no requirement to wait for expenditure approvals.

CHALLENGE	BASE COSTS
Current Backup Storage (inc Server) per Year	$64,727
Next Gen Backup Storage (Inc Server) per Year	$23,198
Data Storage Cost Saved per Year	$41,529
Device Licenses: NeuShield Data Sentinel Business & Datacenter Editions: 50 x PCs / 40 x MS Servers / 10 x MS SQL Servers. No additional cost for amount of storage	$16,500
NextGen Backup Storage Budget Claw-Back	**$25,029**

CYBER INCIDENT RTO STRATEGY

The NextGen Recovery strategy can immediately reduce your RTO by 99% with no additional costs for cyber incident recovery.

COSTS FOR RTO OF RPO: 3-2-1 & NEXT GEN STRATEGIES	BASE COSTS	5TB RPO@100MBPS	ADDITIONAL BANDWITH & COSTS FOR 5-HOURS GTO	5-HOURS RTO
Current RPO & RTO Capability (3-2-1 Strategy)	$26,062	104 Hours	2 Gbps	5.5 Hours
Additional Costs to Meet RTO (3-2-1 Strategy)			>$100,000	
Costs to Deliver RTO (3-2-1 Strategy)				**>$126,062**
Next Gen RTO Capability (using NeuShield)	**$16,500**	**<1 Hour**	**None[6]**	**$16,500**

NextGen (Hours)

$$\text{Percentage Reduction} = 1 - \left(\frac{1}{104}\right) \times 100 \approx 99.04\%$$

3-2-1 Strategy (Hours)

RECOVER IN MINUTES

All from the affected device with no backups or network connectivity. Every device is independent allowing the IT Admin to revert all device data simultaneously, without external data or infrastructure dependencies.

[5] Additional storage is aggregated across the 100 devices dependent on frequency of file updates.
[6] - If NeuShieldneeds to wait for networksto be available to allow the IT Admin to recover data centrally, the existing bandwidthis suitable to send commands from the NeuShield portal. NeuShield does not require bandwidth to move data.

NextGen cyber incident RTO has no additional costs

An existing recovery policy following a cyberattack using 100 Mbps sustained network takes 104 hours (4 days 8 hours) to recover the RPO data. Operations will miss the 5-hour RTO window by 4 days and 3 hours.

To achieve the 5-hours RTO with the existing RPO would require a 2Gbps sustained network. Implementing this increase of network bandwidth will incur costs of ~$100,000 - $154,345.

NeuShield achieves the desired RPO with the existing sustained network within a 1-hour RTO. NeuShield requires no additional costs to meet the RTO.

NextGen Backup and Recovery Summary

Adopting a NextGen Backup and Recovery Strategy will save you in excess of 64% in additional yearly storage costs of $25,029 or greater.

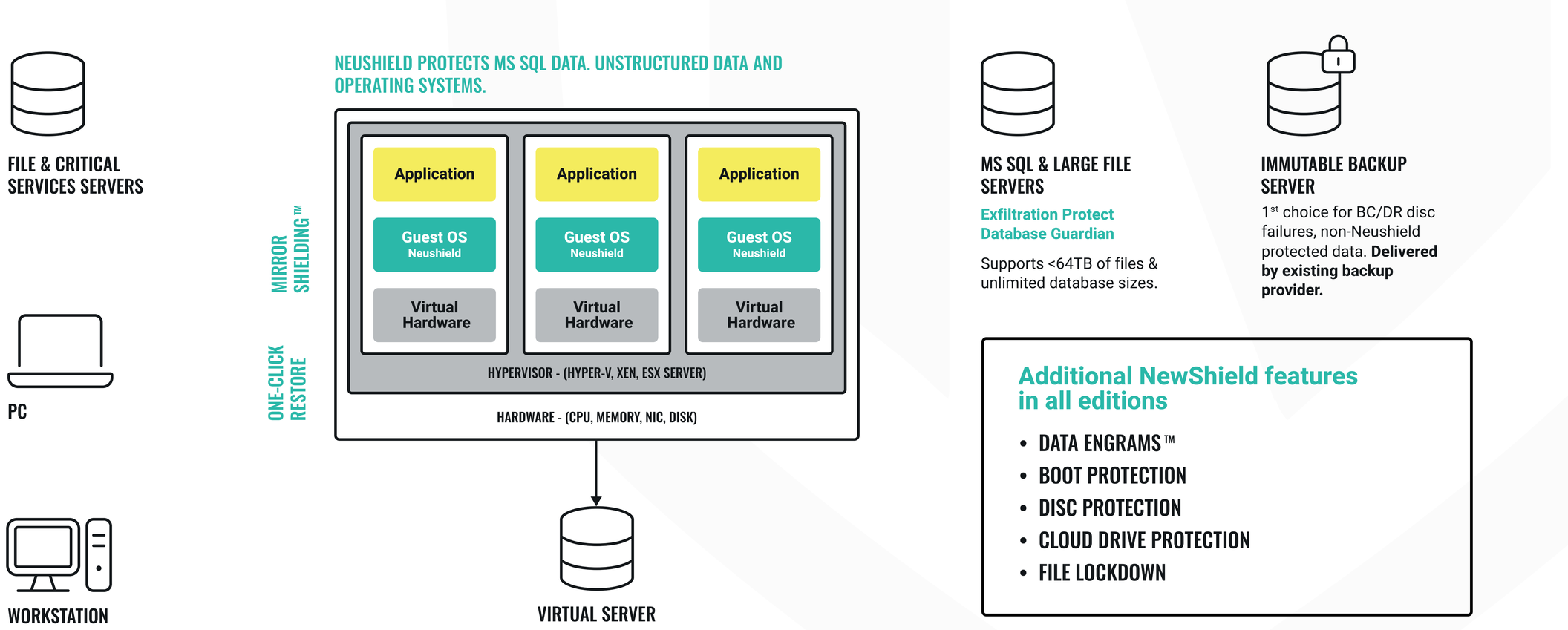
Utilizing NeuShield Data Sentinel Editions and retaining an off-site copy of your data on immutable media (from your existing backup provider) will transition you from the historical 3-2-1 backup policy to a more secure and instant 1-1 NextGen Backup and Recovery Strategy.

Your RTO objectives will be met by using NeuShield Revert (for data) and One-Click Restore (for operating systems). Together they can accelerate your data operations by 99%, saving
$100,000-$154,345 in unbudgeted / excessive expenditure currently required to meet your desired RTO.

NEXT GEN BACKUP AND RECOVERY STRATEGY

NeuShield Business and Datacenter Editions Plus and Immutable Backup

1st choice for instant data recovery and anti-ransomware protection



Additional NewShield features in all editions

- DATA ENGRAMS™
- BOOT PROTECTION
- DISC PROTECTION
- CLOUD DRIVE PROTECTION
- FILE LOCKDOWN

NeuShield®
How much is your data worth?

Contact us today to actively protect your data and deliver instant recovery. Re-establish operations faster without additional costs.

NeuShield Data Sentinel does more than just detecting and blocking ransomware. We're the only anti-ransomware solution that can recover encrypted data from any known, unknown or zero-day threat. No matter how much data is encrypted NeuShield can get it back instantly from any laptop, desktop or server. NeuShield is an endpoint agent that works locally to recover data without using a backup or internet connection.

sales@neushield.com

NeuShield, Inc
200 Brown Road, Suite 306
Fremont, CA 94539
Main: +1 510-239-7962
Toll Free: +1 888-999-0965 (U.S.)

WWW.NEUSHIELD.COM