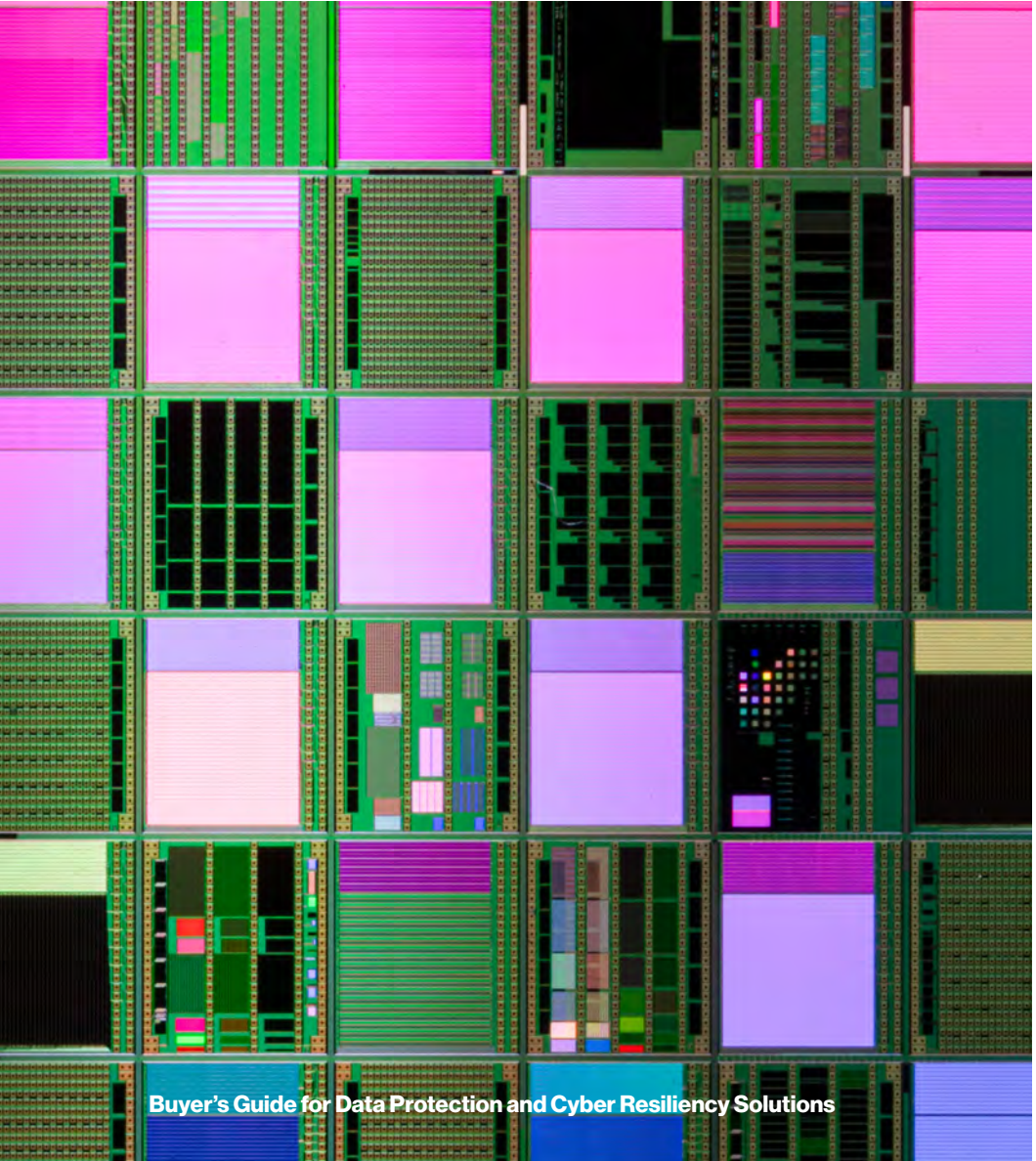
EBOOK

Hitachi Vantara

Buyer's Guide for Data Protection and Cyber Resiliency Solutions

Strategies to improve RPO/RTO and cyber resiliency.

hitachivantara.com



Executive Summary

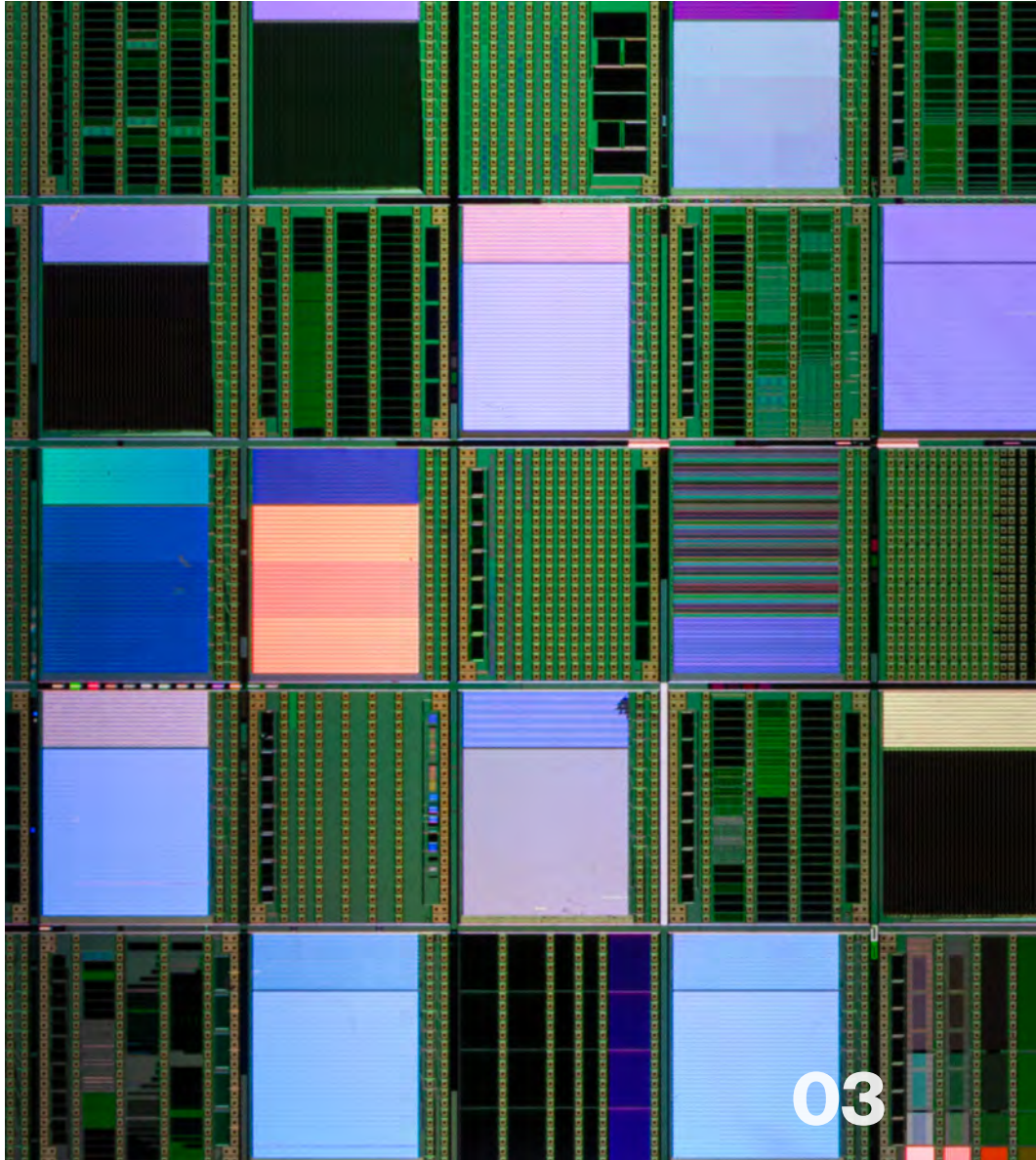
Enterprise data is more valuable than ever before and growing at an astounding rate, placing increasing pressure on IT teams to protect this critical resource. But they're up against a lot: system failures, user errors and malicious attacks are unpredictable and unavoidable.

The costs, downtime, reputation impact, data loss and other implications can be devastating if you're not prepared.

Growing and evolving security risks, combined with increasingly complex IT landscapes, have made the job of protecting enterprise data challenging. But with the right combination of tools to achieve more reliable backups, faster recovery and enhanced cyber protection, you can minimize downtime and cost to the organization if something goes wrong.

This guide will help you keep your data safe with the latest replication, backup and security strategies.

Table of Contents



Today's Data Protection Challenges

Your current backup and recovery solutions were not designed to protect against the sophisticated threats your business is facing today. Because of this, you've probably had to adapt how you work, incurring unnecessary hardware and staffing costs, and creating a more complex environment.

The result is a greater dependency on staffing resources, an inability to quickly adopt new technologies and data silos that prevent you from seeing all your data and acting on it.

Manual efforts introduce risk and are **inefficient**

Lack of support for hybrid infrastructure **limits flexibility**

Management complexity, inconsistent policies, and **lack of data visibility**

Lack of automation **slows response times**

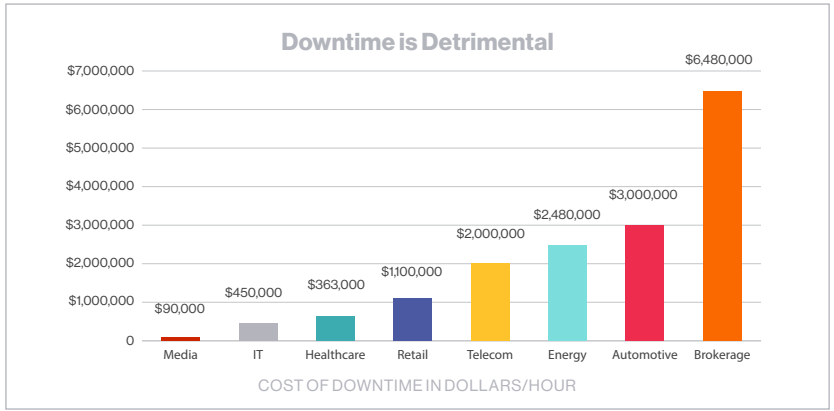
Weak cyber resiliency **exposes risk of ransomware and malware**

The Cost of Going Down

The bigger your industry, the more expensive it is to not have access to your data, adding RTO/RPO pressures to IT teams. Because if something goes wrong (and it eventually will), you need to be able to get your data back online before it affects your business.

If you're a brokerage, every hour could cost upwards of $6 million. If you're a healthcare provider, you could be sacrificing patient care and potentially lives by delaying access to patient data.

How quickly can you get your data back online?



Evolving Cyber Threats

One of the greatest threats to businesses today is ransomware. In 2021, a business, consumer or device was attacked every 11 seconds and ransomware did $20 billion of damage, a figure that is projected to more than double by 2024.

Attacks are becoming so sophisticated they even target the backup environment, meaning you need to protect your protection too.

Buying Criteria for Data Protection

Your key defenses revolve around rapid recovery from large-scale data loss and protection of backups from ransomware.

When evaluating ways to augment data protection, ask yourself how each solution stacks up against the following criteria:

Availability

Back up

Protection

Always Available

With businesses running 24/7/365, data needs to be always available. Replication helps you maintain multiple, synchronized instances of IT resources in geographically dispersed locations, ensuring continuous operations for mission critical applications. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. Nonstop, uninterrupted data access helps achieve strict objectives.

A replication policy is used to copy data to/from geographically dispersed locations. This framework is designed to efficiently spread data across multiple sites. The following replication features should be integrated into your disaster recovery plan:

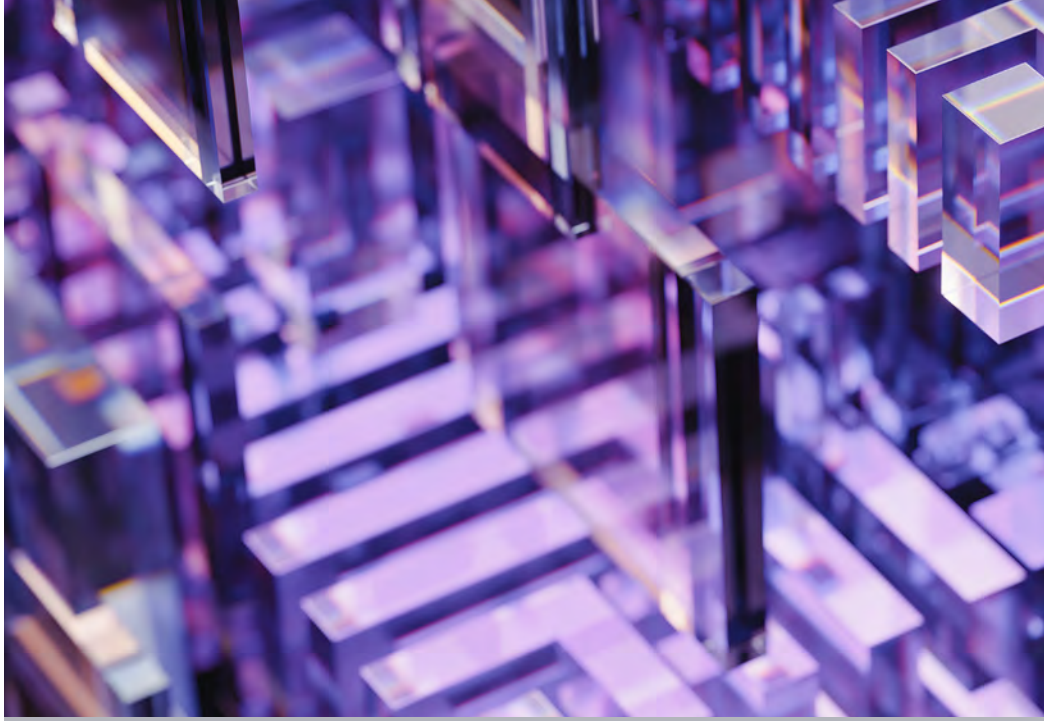
One-to-Many Sync-To:
Replicate objects across multiple destination targets.

Many-to-One Sync-From:
Bring data from external sources back to the storage platform.

Did you know?

The Hitachi Virtual Storage Platform offers a 100% availability guarantee.

Hitachi Content Platform delivers six 9s of availability and fifteen 9s of durability.



Checklist:

- ☑ Enterprise-class replication policy for block, file, and object to prevent business disruption.
- ☑ Highly reliable, highly resilient data infrastructure.

Always Backed Up

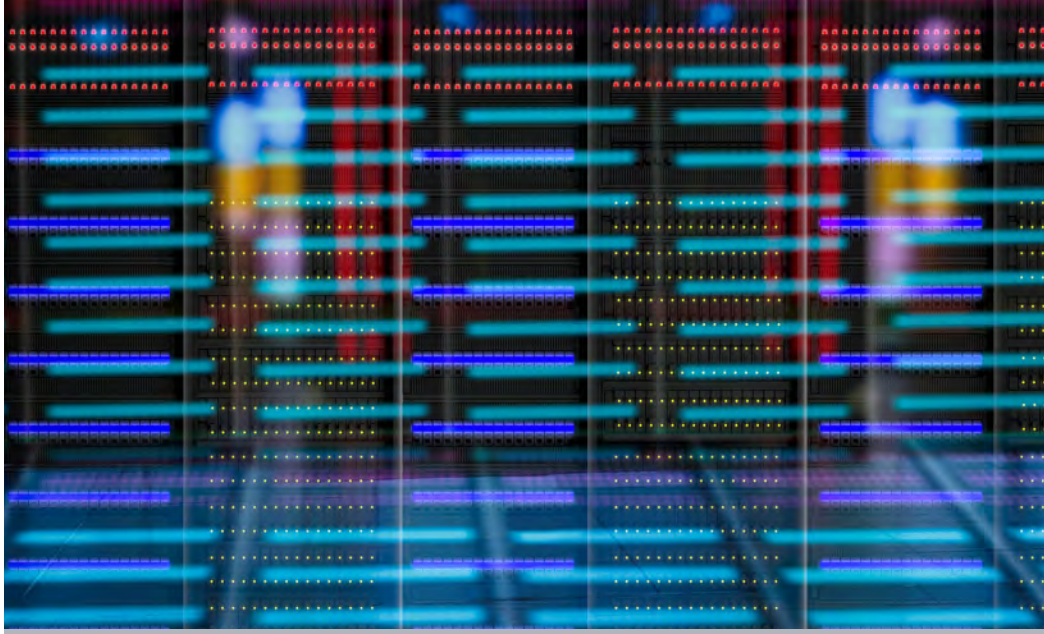
To restore data quickly, first you need to back it up. But, in today's complex storage environments, backup can be complicated, with multiple backup apps for different data types and sources, which may include multiple cloud providers. As complexity and data volumes increase, backup takes longer and costs more, which affects your RPO/RTO objectives.

To streamline backup, start with a simple rule of thumb:

3 Copies of data **2** Different media **1** Copy being offsite **1** Copy being offline, air-gapped or immutable **0** Errors

Then, modernize your technology to reduce the cost and operational burden of managing backup storage. Select backup applications that include features such as automated tiering, direct-to-object connectivity and support for object lock to enable immutability of backup data.

Prioritize broad support for diverse data protection needs by favoring backup applications that support workloads deployed on-premises, in the cloud, or in SaaS applications.



Checklist:

- ☑ Automated tiering.
- ☑ Low-cost archival storage.
- ☑ Support for multiple cloud providers.
- ☑ Support workloads deployed onpremises, in the cloud or in SaaS applications.

Always Protected

Being able to explicitly guard data against unauthorized access is mission critical. Compromises in security can quickly lead to the accidental or unlawful destruction, loss, alteration, access, or unauthorized disclosure of protected data. Ransomware attacks are a key factor compelling organizations to make changes, as these attacks are now focusing on targeting the backup safety net that enterprises rely on for recovering from these incidents.

Organizations are seeking a cohesiveness of security measures to avoid data breaches and data leaks. A layered approach to cyber resiliency helps secure data against attacks.

Checklist:

- ☑ Encryption
- ☑ WORM
- ☑ Versioning
- ☑ Access control
- ☑ Role-based authentication
- ☑ Event logging
- ☑ AI powered anomaly detection

How to Take a Layered Approach to Cybersecurity

Protect your data:
If the data is well protected, then you know you can recover. Immutability ensures that snapshots, files and other data cannot be corrupted or deleted. Role based access controls, event logging, and data integrity checks ensure authenticity, enhance privacy and security, and provide full audit and search capabilities.

Detect intruders:
Bring in technologies and services to help you detect and intercept malware at the point of attack. The sooner you know an attack is happening, the sooner you can isolate affected system to prevent the spread and the less data loss you are likely to experience.

Automate recovery:
Next, empower your organization to automate recovery at scale. The less time you spend recovering the better.

Did you know?

Hitachi Vantara offers the world's fastest automated ransomware recovery.

Measured in Minutes for Thousands of VMs (1500 VMs in 70 min)

Strategy Recommendations

Protect your data with the right infrastructure and tools.

Replicate
Maintain multiple, synchronized instances of IT resources in geographically dispersed locations.

Backup
3 copies of data on 2 different media with 1 copy being offsite
1 copy being offline, air-gapped or immutable, and 0 errors.

Secure
Encryption, WORM, versioning, access control, role-based authentication.

Build Secure and Resilient Data Storage with Hitachi Vantara

Unlock End-To-End Data Protection and Cyber Resiliency.

Hitachi Vantara provides agile and adaptable solutions to empower you with the choice and control to augment hybrid-environment data storage protection in ways that work best for you. Enterprises as well as smaller organizations can assure business continuity and gain compliance and cyber resilience quickly and cost-effectively—with fully transparent SLAs backed by a trusted partner.

Availability

Storage Systems

Ensure continuous operations for mission critical applications with nonstop, uninterrupted data access to achieve strict zero RTO and RPO objectives

Learn More 

Global Active Topology (HCP), Global Active Device (VSP)

Enterprise-class replication for block, file, and object to prevent business disruption.

Learn More 

Backup

VSP, HCP

Deliver robust protection of data where it lives to reduce the cost of traditional data protection and reduce the risk of data loss.

Learn More 

Ops Center Protector, DPaaS, Hitachi Data Protection Suite, CyberVR

Sustainable protection against and fast recovery from system failures, user errors, and malicious attacks.

Learn More 

Protection

HCP, VSP

Safeguard data for security and privacy to prevent data loss, theft, and tampering.

Learn More 

Hitachi Security Systems

Hitachi Security Systems provides cybersecurity, compliance, and personal information and privacy solutions to all businesses battling current and future cyberthreats.

Learn More 

HITACHI VANTARA AT A GLANCE

Hitachi Vantara, a wholly-owned subsidiary of Hitachi Ltd., delivers the intelligent data platforms, infrastructure systems and digital expertise that supports more than 80% of the Fortune 100. To learn how Hitachi Vantara turns businesses from data-rich to data-driven through agile digital processes, products, and experiences, visit www.hitachivantara.com.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

Partner Connect Portal
partnerportal.hitachivantara.com

Buyer's Guide for Data Protection and Cyber Resiliency Solutions