Hitachi Vantara | veeam

Zero Trust Data Resilience with Hitachi Vantara and Veeam

Table of Contents

Introduction

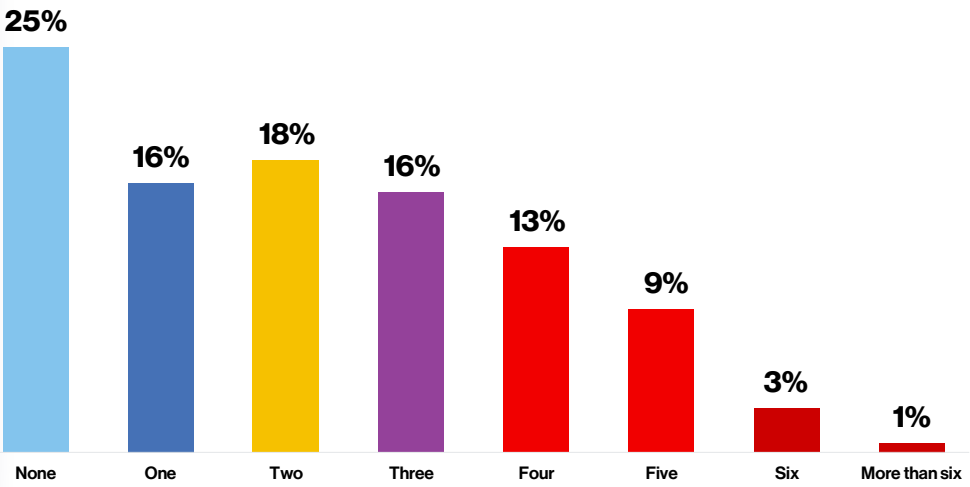
The stories are everywhere, not just in technology news, but also in business news and — even worse — in mainstream news. Organization after organization find they have fallen victim to malicious malware attacks like ransomware. According to the 2024 Veeam Data Protection Trends report, 75% of organizations had at least one ransomware attack in the last 12 months, with many having reported multiple attacks (and the 25% that reported they didn't get attacked, may not be aware of an attack in progress).

75% Suffered Ransomware Attacks in 2024

More organizations were hit quarterly (26%)than believe were not hit at all (25%)

Source: Data Protection Trends Report 2024
https://vee.am/DPR24

How many ransomware attacks has your organization suffered in the last 12 months?
(n=710)



For years organizations have invested heavily in cyber defenses, like Intrusion Detection Systems (IDS), firewall software, and end-point protection software, but this has not stopped cyberthreats, nor has it slowed the pace of actual intrusions.

And malware is not the only threat, outages and data loss caused by accident are still significant risks. Cyber defense investments can't help with outages caused by accidental, or even malicious, insider threats.

What Is an IT Organization to Do?

According to Gartner Maverick leading edge research from 2022, organizations should increase their investment in cyber resilience (i.e. SIEM, SOAR, XDR/MDR, modern data protection, and immutable and performant storage) so they can respond and recover from attacks and outages with minimal disruption.

When organizations balance their investments in cyber defenses with those in cyber resiliency, they can not only prevent the vast majority of attacks, but they also develop an IT architecture and strategy for being able to recover quickly and cleanly when attacked, or when experiencing an outage.

Fast and clean recovery are core capabilities of a successfully resilient IT architecture and strategy. Hitachi Vantara and Veeam provide IT organizations with critical hardware and software infrastructure to build a robust cyber resilient IT architecture and strategy.

Zero Trust Principles

Zero trust is a cybersecurity model that aims to reduce uncertainty around unauthorized access to systems and services. It's based on the principle that companies should not trust anyone by default and should verify every request for access. Zero trust security uses several principles to achieve this, including:

- **Least-privilege access:** Access is restricted to what is essential at the right time and with just enough access. This prevents lateral movement and unauthorized access to other parts of the network.
- **Verify explicitly:** Departing from traditional "trust but verify" methods, this principle focuses on always authenticating and authorizing based on all available data points.
- **Assume breach:** Operating under the assumption that breaches will happen, zero trust prioritizes detection, response, and rapid recovery to minimize the impact of security breaches and the subsequent blast radius.

Zero Trust Data Resilience

To achieve cyber resilience, where you can reliably and quickly recover clean data from any outage whether man-made or natural, the data protection environment is arguably the most important environment. When zero trust is applied to the data protection environment, it is referred to as **zero trust data resilience.**

The core principles of zero trust data resilience extend the zero trust principles, and are key elements in protecting your organizations data:

- **Immutable and encrypted backup storage:** Protect backup data from modification or deletion
- **Separation of backup software and backup storage:** Minimize attack surface and blast radius
- **Multiple resilience zones:** 3-2-1 backup rule

Zero Trust Principles

Assume breach.	Verify explicitly.	Use least-privilege access.
Minimize attack surface and blast radius	Verify every access attempt using IAM context and MFA	For every user, device and application

Extending Zero Trust Principles to Data Resilience

Immutable backup storage	Separation of Backup Software and Backup Storage	Multiple resilience zones
Protect backup data from modification or deletion	Minimize attack surface and blast radius	3-2-1 Backup Rule

Immutable and Encrypted Backup Storage

Immutable backup storage is the cornerstone of a sound cyber resilient IT architecture. Immutable backup storage refers to any form of data storage that prevents the alteration, deletion, or unauthorized access of backup data. It is achieved by enforcing a strict read-only policy, making the stored data immutable.

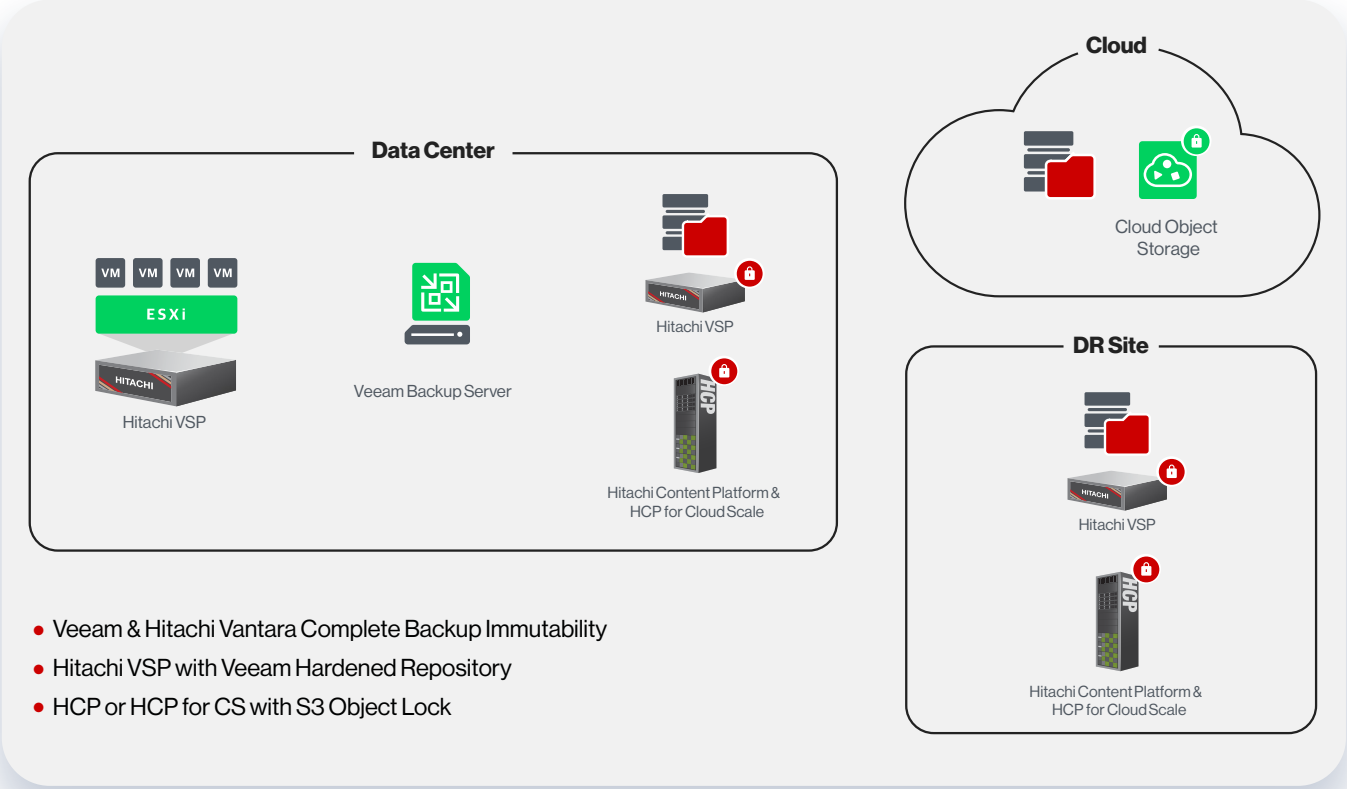
The importance and value of immutable and encrypted backup storage can be highlighted in the following ways:

1. **Data protection:** Immutable backup storage ensures protection against accidental or intentional data deletion or change. By preventing any changes to the stored data, it mitigates the risk of data loss due to human error, malware attacks, or system failures.
2. **Data integrity:** Immutable storage guarantees the integrity of the backup data by making it tamper-proof. It helps in complying with data regulations and maintaining an unaltered record of data for regulatory audits, compliance audits, or legal proceedings.
3. **Compliance and audit requirements:** Many organizations have regulatory requirements to maintain immutable records of certain types of data. Immutable backup storage assists in meeting these requirements, ensuring that the data remains unchangeable and auditable for compliance purposes.
4. **Encryption of backup data:** Prevent exfiltrated data from being used by criminals to demand an alternative ransom by encrypting all backup data.

Hitachi Vantara storage solutions, whether block or object storage, can provide both immutable and encrypted backup storage in a Veeam Data Platform deployment.

Immutable Backup Storage

Protect backup data from modification or deletion



- Veeam & Hitachi Vantara Complete Backup Immutability
- Hitachi VSP with Veeam Hardened Repository
- HCP or HCP for CS with S3 Object Lock

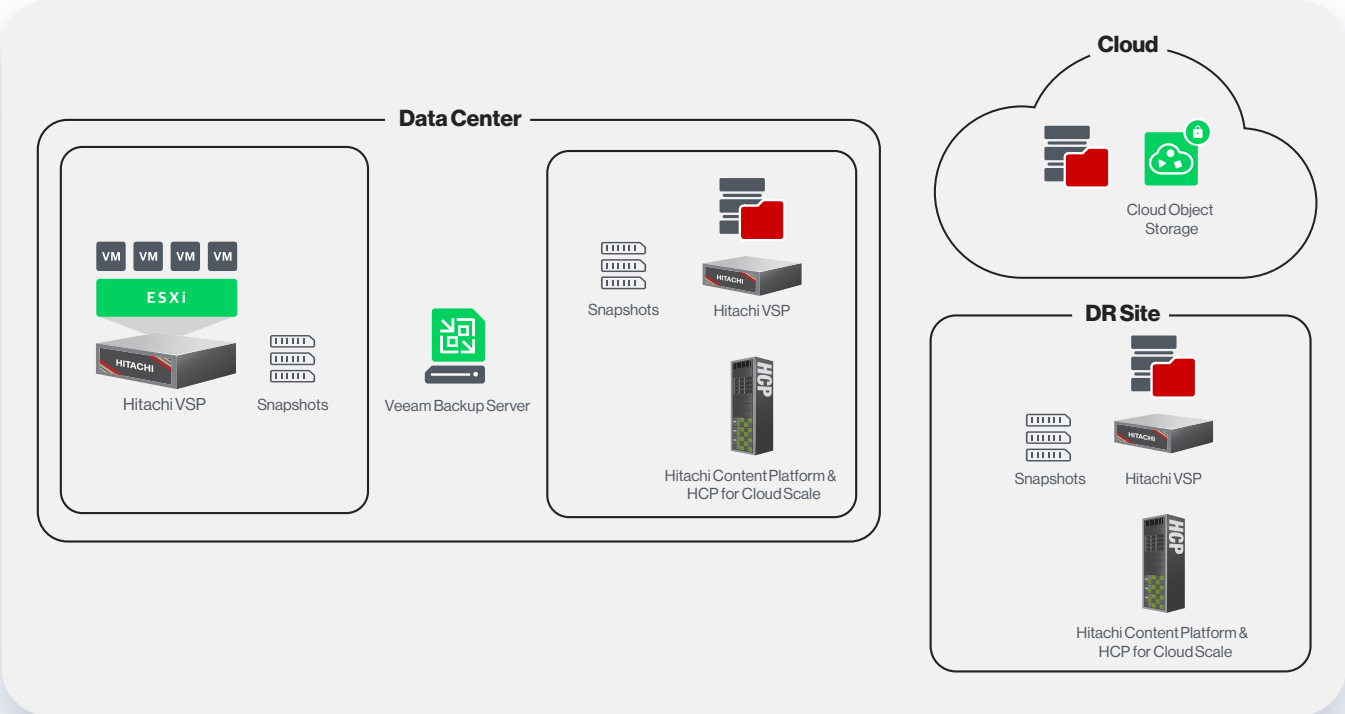
Separation of Backup Software and Backup Storage

A key principle of zero trust data resilience is ensuring that backup software and backup storage are separated between different systems with different and separate authentication. This separation ensures that there will be no loss of data for your organization in the case your backup software is damaged or compromised. By separating backup management systems and backup repositories onto different systems, threat actors will have minimal access or connection to both, making the compromise of multiple systems much harder. Additionally, strong controls should be placed around accessing these segregated systems to ensure that only authorized users can access only what they need when they need to. This helps reduce attack surfaces for all networks and their components.

Hitachi Vantara storage solutions for backup, whether block or object storage, are never configured on the same server as the Veeam Data Platform software, so should any component be compromised in a ransomware attack, it will not impact any other component in the backup infrastructure. Minimize attack surface and blast radius.

Separation of Backup Software and Backup Storage

Minimize attack surface and blast radius



Multiple Resilience Zones

The 3-2-1 backup rule remains the gold standard data protection strategy. This rule focuses on maintaining multiple copies of your organization's data to ensure that you can recover quickly and securely, no matter what caused the outage. Here's the breakdown:

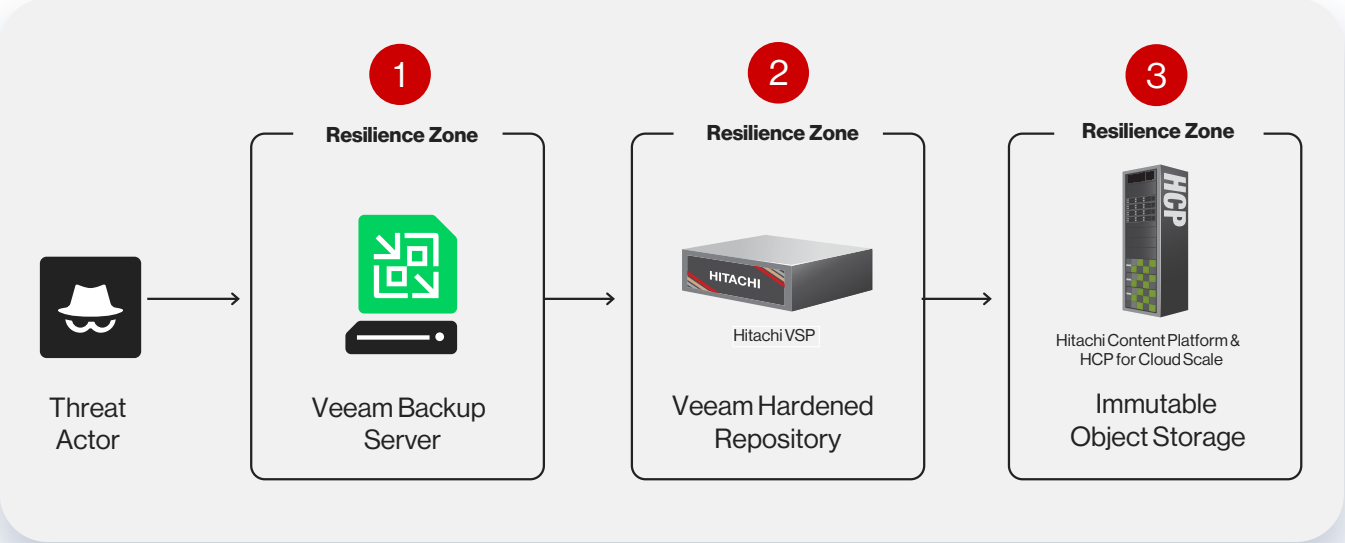
- Three copies of your data: Including the production data and two backup copies
- Two different media: Store your data on two different storage media to enhance data security and redundancy
- One copy off-site: To ensure data safety, have one backup copy stored in a remote location, more than a few miles away from the other two copies

By architecting your data into multiple resilience zones, you can prevent the loss of all your organization's data. The loss, or compromise, of one resilience zone will have no negative impact to the data stored in the other zones.

Hitachi Vantara storage solutions for backup have strong authentication and authorization controls so no matter what backup storage is chosen it can be an independent hardened and immutable resilience zone.

Multiple Resilience Zones

3-2-1-1 Backup Rule



Can You Have Data Security and Flexibility?

There are some data protection providers that say that the only way to secure your backups is to choose their prescriptive, typically appliance-based, solutions. Veeam and Hitachi Vantara beg to differ. With Veeam cyber resilience products, like Veeam Backup & Replication, you can choose your backup repository storage from several Hitachi Vantara products, including Hitachi Virtual Storage Platform, Hitachi Content Platform and Hitachi Content Platform for Cloud Scale. These choices enhance the security and cyber resiliency of the overall system as they all offer immutability, encryption, and strong authentication.

Components of Secure Data Infrastructure

Hitachi Vantara offers three storage products that are ideal for Veeam backup repository storage:

1. Hitachi Virtual Storage Platform (VSP)
2. Hitachi Content Platform (HCP)
3. Hitachi Content Platform for Cloud Scale (HCP for CS)

Hitachi Virtual Storage Platform (VSP)

Hitachi VSP is a line of block storage systems that offer scalability, performance, and high availability in a range of configurations from all-flash to hybrid storage. When paired with Veeam Hardened Repository, they offer backup targets that provides both highly performant and immutable backup storage.

Hitachi Content Platform (HCP)

HCP is an object storage solution designed for enterprises to store, manage, and access massive amounts of unstructured data. HCP can handle exponentially growing data volumes by scaling storage capacity and performance on-demand. HCP offers features like encryption, access control lists, and audit logging to ensure data security and compliance. HCP supports S3 Object Lock immutability, providing immutable backup storage.

Hitachi Content Platform for Cloud Scale (HCP for CS)

HCP for CS is a software-defined object storage solution that leverages a microservices architecture that provides unrivaled scalability, flexibility, and ease-of-use. HCP for CS supports S3 Object Lock immutability, providing immutable backup storage.

Veeam Data Platform

The Veeam Data Platform is designed to help organizations protect, manage, and utilize their data efficiently. Here are the main products that make up the Veeam Data Platform:

- **Veeam Backup & Replication** provides comprehensive backup, recovery, and replication capabilities for virtual, physical, unstructured data, and cloud environments. It ensures the availability of critical data, minimizes downtime, and accelerates recoverability.
- **Veeam ONE** offers real-time monitoring, reporting, and resource optimization for Veeam backup infrastructure. It provides detailed insights into the environment's health, performance, and configuration, enabling administrators to proactively resolve issues.
- **Veeam Recovery Orchestrator** allows organizations to automate and streamline the disaster recovery (DR) and cyber recovery (CR) orchestration process. It enables IT teams to create, document, and test disaster recovery plans for their virtualized and physical environments. With automated plan testing and failover, it ensures business continuity in case of a disaster.

Hitachi Vantara & Veeam Bringing Zero Trust Data Resilience Together

Veeam's zero trust data resilience, along with Hitachi Vantara storage offerings, offer organizations a comprehensive and advanced approach to secure and protect their critical data assets. By adhering to the principles of zero trust, Veeam and Hitachi Vantara ensure that there are no inherent trust assumptions within the infrastructure, minimizing the risk of unauthorized access or data breaches.

Hitachi Vantara and Veeam provide organizations with a set of comprehensive, robust, and adaptable solutions to safeguard their critical data assets. By implementing this approach, organizations can minimize the risk of data breaches, ensure continuous data availability, and maintain regulatory compliance. With Veeam and Hitachi Vantara, organizations can confidently embrace zero trust principles while maintaining the resilience and integrity of their data infrastructure.

Resources:

For more information visit: hitachivantara.com/en-us/partners/technology-alliance-partner/veeam

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Hitachi Vantara
A Hitachi Group Company

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

© Hitachi Vantara LLC 2024. All Rights Reserved. HITACHI and Pentaho are trademarks or registered trademarks of Hitachi, Ltd.
All other trademarks, service marks and company names are properties of their respective owners.

HV-NS-SO-Zero-Trust-Data-Resilience-with-Hitachi-Vantara-and-Veeam-5Aug24-A