Solution Profile

2024-25 DCIG TOP 5

CYBER SECURE HIGH-END ALL FLASH ARRAYS // GLOBAL EDITION

Hitachi Vantara Virtual Storage Platform 5600 Solution Profile

Author: Dave Raffo, Consulting Analyst
Lead Researcher: Ken Clipperton, Principal Storage Analyst & Partner

Cyber Secure High-end All Flash Arrays // Global Edition

Hitachi Vantara Virtual Storage Platform 5600 Solution Profile

Cyber Secure High-End All Flash Arrays
2024-25
DCIG
TOP 5
Global Edition

SOLUTION

Hitachi Vantara Virtual Storage Platform 5600

COMPANY

Hitachi Vantara
2535 Augustine Drive
Santa Clara, CA 95054
hitachivantara.com

DISTINGUISHING FEATURES OF HITACHI VANTARA VIRTUAL STORAGE PLATFORM 5600

- Hitachi Ops Center Suite for AIOps
  - Near-instant ransomware recovery
  - Cloud-based system observability
  - Real-time monitoring and performance tuning
- Mainframe-specific cybersecurity

DISTINGUISHING FEATURES OF TOP 5 SOLUTIONS

- Ransomware anomaly detection and recovery
- Advanced encryption
- Automated compliance monitoring and alerting
- Security technologies/certifications
- Multiple array management roles

Critical Need for Cyber Secure High-End Arrays

Cyber crimes and data breaches have become an everyday threat for IT professionals. More than 330 publicly disclosed data breaches and cyber attacks occurred in just the first two months of 2024. These included:

- A ransomware attack at a United Healthcare subsidiary that caused havoc among medical professionals and pharmacies.
- An attack known as the “Mother of All Breaches” exposed 26 billion user records from Adobe, Dropbox, LinkedIn, and other popular online platforms.
- Microsoft and HPE disclosed they were victims of Russian hackers.

These developments highlight the need for organizations, especially those that provide critical infrastructure services, to detect and thwart cyber attacks and ensure cyber resiliency—the ability to continue operations after falling victim to an attack. Many companies with crucial business and customer data depend on high-end storage arrays to provide uninterrupted access to their data. These high-end storage arrays require built-in cyber resilience to keep that data safe and enable quick recovery if data is compromised.

Recent Advances in Cyber Secure Storage

The cyber threat landscape calls for a multi-layered approach to securing data infrastructure. The National Institute of Standards and Technology, an agency of the U.S. Government, promulgated a cybersecurity framework that provides actionable guidance to help organizations manage, reduce, and communicate cybersecurity risks for systems, networks, and other assets that process data.

This report looks at how various features and capabilities of high-end all flash arrays help customers address the six functions of the NIST Cybersecurity Framework 2.0. Those functions are:

- **Govern** – how an organization establishes its cybersecurity strategy and cybersecurity supply chain risk management, along with its policies and oversight of that strategy.
- **Identify** – how an organization understands assets related to its data, hardware, software, and systems so it can identify, prioritize, and improve risk management strategies and practices.
- **Protect** – the ability to secure assets through identity management, authentication, access control, awareness and training, data and platform security, and resilient technology infrastructure.
- **Detect** – an organization’s ability to make timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate a cybersecurity attack is underway.
- **Respond** – the ability to contain the impact of a cybersecurity event through incident management, analysis, mitigation, reporting, and communication.
- **Recover** – the ability to restore assets and operations affected by a cybersecurity attack, return to normal operations, and enable effective communication during a recovery.

Critical Features of the Cyber Secure High-End All Flash Arrays

DCIG believes it is only a matter of time before a cyberattack successfully breaches any organization's security defenses. Storage arrays and their providers have a role to play in preventing, mitigating, and recovering from cybersecurity incidents.

It is only a matter of time before a cyberattack successfully breaches any organization's security defenses.

Every enterprise storage vendor is addressing customer concerns around data security and cyber resilience, especially the threat of ransomware. Most high-end storage arrays have improved their security posture by implementing multiple technologies, including FIPS 140-2, T10 PI, and multi-factor authentication.

For this report, we examined 14 high-end storage arrays. The primary cyber security traits we looked at were:

- Data immutability
- Encryption
- Replication/snapshots
- Security technologies (FIPS 140, hardware root of trust, multi-factor authentication, multiple roles, multiple approvals)
- Security information and event management (SIEM) Integration
- Storage analytics and proactive support
- Vendor management of arrays (STaaS)

Common Features Across High-End All Flash Arrays

Immutable snapshots. All the DCIG TOP 5 Cyber Secure High-end All Flash Arrays support immutable snapshots, which are read-only copies of data that cannot be changed or altered. Because snapshots are a fundamental part of the backup and recovery process, they have become a prime target of cybercriminals. Immutable snapshots have become common in storage systems, as 13 of the 14 arrays we looked at support them. Immutable snapshots address the Protect and Recover functions of the NIST Cybersecurity Framework.

Encryption. All 14 arrays we looked at support encryption, either array-based or through self-encrypted drives. Encryption addresses the Protect function of the NIST Cybersecurity Framework.

Non-disruptive upgrade features. The DCIG TOP 5 Cyber Secure High-end All Flash Arrays all support non-disruptive upgrades for adding and replacing controllers, upgrading controller code, migrating data, adding storage nodes or shelves, and upgrading firmware for storage media and network ports. Non-disruptive upgrade features address the Protect function of the NIST Cybersecurity Framework, by enabling organizations to keep array software and firmware up-to-date without having to schedule a downtime maintenance window.

Distinguishing Features of the DCIG TOP 5 Cyber Secure High-End All Flash Arrays

The top 5 arrays in our report stood out in these areas:

Ransomware anomaly detection and recovery. These features identify suspicious changes in data access patterns that could be indicative of ransomware encryption, allowing for early intervention. The DCIG TOP 5 solutions include features such as anomaly detection, ransomware file interception, and machine learning for detection. The most comprehensive implementations of these features address the Detect, Respond, and Recover functions of the NIST Cybersecurity Framework.

Cyber Secure High-end All Flash Arrays // Global Edition

Hitachi Vantara Virtual Storage Platform 5600 Solution Profile

Advanced encryption. All 14 arrays we looked at support encryption, either on the arrays or via self-encrypted drives. Three of the DCIG TOP 5 solutions support both approaches. While all 14 arrays we looked at supported encryption at rest in the data center, not all documented support for encryption at rest in the cloud or in-flight encryption. Three of the DCIG TOP 5 support encryption at rest in the cloud, and four support in-flight encryption. These advanced encryption features address the Protect function of the NIST Cybersecurity Framework

Automated compliance monitoring and alerting. Some high-end storage systems can automatically monitor compliance with relevant data security regulations and generate alerts for any discrepancies, streamlining the process for security teams. Almost all high-end arrays do remote monitoring, but the DCIG TOP 5 Cyber Secure High-end All Flash Arrays are more likely to generate alerts than the others. These features address the Identify function of the NIST Cybersecurity Framework.

Security technologies/certifications. All the arrays support FIPS-140 encryption. However, the DCIG TOP 5 Cyber Secure High-End All Flash Arrays are more likely to support Hardware Root of Trust, T10 PI, and multi-factor authentication. These features address the Protect function of the NIST Cybersecurity Framework.

Multiple array management roles. Storage array providers are responding to the evolving security landscape by supporting multiple storage system administration roles. These roles include storage and security administrators, storage and security auditors, data protection admins, and a requirement for multiple approvals for sensitive storage operations. Multiple array management roles and multiple approvals address the Protect function of the NIST Cybersecurity Framework.

Non-disruptive upgrade features enable organizations to keep array software and firmware up to date without having to schedule downtime.

Only a subset ship with predefined security auditor, storage auditor, or security administrator roles. Only Huawei OceanStor Dorado 18000/8000 indicated support for a security auditor and a data protection administrator. Two of the DCIG TOP 5 support a storage auditor, and three support a security administrator.

One of the newer features for most high-end arrays is the requirement for multiple approvals for sensitive operations. This requirement protects against attacks based on compromised administrative accounts or the actions of a disgruntled administrator. A second pair of eyes helps spot things that appear suspicious and helps protect against catastrophic unintended errors.

Hitachi Vantara Virtual Storage Platform 5600

The Hitachi Vantara VSP 5600 is the high-end of the Hitachi VSP storage product line. The VSP 5600 is an all-flash model with NVMe drives and SAS SSDs. Hitachi Vantara guarantees 100% data availability and a 4:1 “sight unseen” data reduction guarantee with deduplication and compression. It is one of two TOP 5 Cyber Secure High-End All Flash Arrays with FICON connectivity for mainframe storage.

Features that earned Hitachi Vantara VSP 5600 a spot in the *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report include:

Hitachi Vantara VSP supports role-based access control, including security auditor and storage administrator roles, security information and event management (SIEM) software, and requires multiple approvals for some actions. Hitachi also sells VSP as a full storage-as-a-service on the customer’s premises or in a Hitachi-managed data center.

Hitachi Ops Center Suite. This integrated AIOps management software suite provides many VSP security and data protection features, including:

- Near-instant ransomware recovery.
- Cloud-based system observability.
- Real-time monitoring and performance tuning.

Hitachi Vantara VSP supports multiple roles, requires multiple approvals for some actions, integrates with SIEM solutions, and offers mainframe-specific security features.

Hitachi Ops Center Protector creates policy-based copy data management workflows for both primary and secondary storage. It supports:

- Data protection for two- and three-data center topologies to ensure business continuity.
- Immutable snapshots and creates new versions of data rather than overwriting when changes occur.
- Anomaly detection.
- Air gap that isolates primary storage and backup systems.
- Array-based encryption for data-at-rest and data-in-flight encryption, including integration with key management systems on VSP arrays.
- Other Hitachi data replication software that runs on VSP arrays provide:
  - Synchronous replication (TrueCopy).
  - Asynchronous replication (Universal Replicator).

Mainframe cybersecurity. Hitachi also has mainframe-specific security features:

- Ability to make multiple copies of the whole set of production data without impacting production.
- Isolation from the mainframe storage to avoid unwanted access to data and any modification to production images.
- Possibility to recover data to a different storage than the main one used to create fortress images.
- Immutable production images with no possibility to access, modify or delete the fortress data within the specified retention period.
- Management of the solution outside of the mainframe.
- Capability to protect mainframe storage locally or remotely.
- Critical management actions protected with dual acknowledgment. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of DCIG TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**