2024-25 DCIG TOP 5

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

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

Table of Contents

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

Hitachi Vantara
Virtual Storage Platform 5600

Dell Technologies PowerMax 8500

Huawei OceanStor Dorado 18000

Infinidat InfiniBox SSA II

NetApp AFF/ASA A900

**Products are listed with the licensee's product on top, followed by the other TOP 5 award recipients in alphabetical order.*

SOLUTIONS EVALUATED

Dell Technologies PowerMax 2500
Dell Technologies PowerMax 8500
Hitachi Vantara Virtual Storage Platform 5600
HPE Alletra 9000 (9080 4N)
HPE XP8 Gen2
Huawei OceanStor Dorado 18000
Huawei OceanStor Dorado 8000
IBM DS8900F (DS8980F)
Infinidat InfiniBox SSA II
NetApp AFF A900
NetApp AFF A800
NetApp ASA A900
NetApp ASA A800
Pure Storage FlashArray//XL

FEATURES EVALUATED

- *Data Immutability Features*
- *Encryption Options*
- *Replication & Snapshot Features*
- *Secure Administration Features*
- *Security Certifications/Technologies*
- *SIEM Integration*
- *Storage Analytics & Proactive Support*
- *Storage as a Service (STaaS) Options*

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.

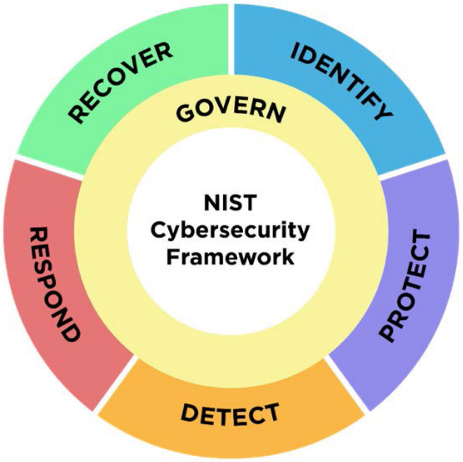
- **Protect** – the ability to secure assets through identity management, authentication, access control, awareness and training, data and platform security, and resilient technology infrastructure.

- **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.

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



Source: The National Institute of Standards and Technology Cybersecurity Framework 2.0

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.

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.

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

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.

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.

Only a subset ship with predefined security auditor, storage auditor, or security administrator roles. Only Huawei OceanStor Dorado 18000 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.

Differences Among the DCIG TOP 5 Cyber Secure High-End All Flash Arrays

One of the newer features for most high-end arrays is the requirement for multiple approvals for sensitive operations.

Near-instantaneous recovery/recovery guarantees. Advanced storage solutions enable near-instantaneous recovery of data in the event of a cyber attack, minimizing downtime and ensuring continuity. For example, Infinidat provides this feature with a one-minute cyber recovery guarantee. NetApp also guarantees ransomware recovery. Near-instantaneous recovery addresses the Recover function of the NIST Cybersecurity Framework.

File Protection. Of all the solutions we looked at, only three support file analytics and WORM file format, and two support file auditing. Huawei OceanStor Dorado 18000 and NetApp AFF/ASA A900 support all three. These features address the Protect and Detect functions of the NIST Cybersecurity Framework.

Fenced network forensic environment. This secure, isolated environment facilitates forensic analysis of compromised data without contaminating other systems, aiding in identifying the source of an attack. Infinidat supports this feature. This feature addresses the Respond function of the NIST Cybersecurity Framework.

Vendor management of arrays. Large storage vendors now commonly offer storage as a service (STaaS) options for customers. These programs transfer responsibility for storage array management to the vendors, including the installation of security patches. Customers manage the data, but the vendor manages the array. Many cybersecurity incidents result from known vulnerabilities for which patches were available but not installed. Most STaaS offerings enhance cyber security by ensuring that array software and firmware updates are installed in a timely manner. STaaS offerings may address multiple functions in the NIST Cybersecurity Framework, including Protect, Detect, Respond, and Recover.

SIEM integration. Security information and event management solutions perform real-time analysis when there is a security event. SIEM can be software applications or managed services. Hitachi Vantara and Infinidat document the integration of their high-end storage solutions with SIEM software. These integrations address the Detect and Respond functions of the NIST Cybersecurity Framework.

DCIG TOP 5 Cyber Secure High-End All Flash Array Profiles

The following pages contain solution profiles that identify some outstanding or distinctive features that helped each array earn a spot in this *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report.

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.

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

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 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.

Dell has applied the most stringent cybersecurity requirements as specified by the U.S. Department of Defense (DoD) and NIST guidelines for reducing the attack surface.

Dell PowerMax 8500

The Dell PowerMax 8500 is the highest end model of the PowerMax family. PowerMax is one of the most successful high-end storage array platforms in history. The Dell PowerMax supports block and file workloads and is one of two arrays in this report that provide FICON connectivity for mainframe storage.

Some of the features that helped the Dell PowerMax 8500 earn a spot in the *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report include:

Designed for zero trust security environments.

The PowerMax offers:

- Follows secure development lifecycle practices to ensure a shift left approach to security.
- Secure boot.
- Digitally signed software and firmware updates.
- Ransomware anomaly detection, including for both Open Systems and Mainframe hosts.
- Automated compliance monitoring/alerting.
- Granular cyber recovery at scale with up to 65 million policy-driven automated snaps per array, including immutable and secure snaps.
- Applies data encryption through self-encrypting drives (SEDs) to maintain protection when a drive is removed from the system.
- Allows external key managers for data at rest encryption. Supports ignition key with HashiCorp.
- Multi-factor authentication for Unisphere management
- Provides secure access controls and tamper-proof audit logs.
- Detects unauthorized access through secure logs of all events on PowerMax.
- Provides 2-factor authentication to management access using SecureID.
- Role-based access controls.
- Immutable hardware root of trust.
- Remote syslog integration.

DoDIN Approved Product List/STIG hardening. Dell has applied the most stringent cybersecurity requirements as specified by the U.S. government Department of Defense (DoD) and NIST guidelines for reducing the attack surface.

CloudIQ. Dell's arrays also include CloudIQ (for products with ProSupport or higher contracts) for tracking system health through pattern recognition and analytics. CloudIQ's cyber security features include anomaly detection for unusual access patterns and data reduction rates to detect ransomware or malware, this can also be accessed natively in PowerMax.

Cyber vault. PowerMax cyber vault isolates open systems data from the production network in a secure vault by implementing an SRDF airgap solution with secure snapshots.

Dell's cyber security features also include:

- Active-active data center replication and (through SRDF software) remote replication over distances or across sites.
- PowerMax supports periodic and continuous asynchronous replication, synchronous replication across Metro Clusters, and replication across three data centers.

Huawei OceanStor Dorado 18000

Huawei OceanStor Dorado 18000 is an end-to-end NVMe storage system that provides comprehensive data protection and disaster recovery capabilities to ensure data services run securely.

Some of the features that helped the Huawei OceanStor Dorado 18000 earn a spot in the *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report include:

Multilayer Ransomware Protection (MRP). MPP builds a six-layer in-depth defense system covering network intrusion prevention, network spread prevention, ransomware detection, secure snapshots, backup protection, and isolation zone protection. Huawei claims a ransomware detection rate of 99.99%. OceanStor Dorado can also recover in seconds with secure snapshots, mitigating the impact of ransomware attacks.

Air gap. OceanStor Dorado can build an isolated replication zone. During non-replication periods, the replication link is disconnected, so backups stay offline and invisible to ransomware.

Proactive honey file defense. The honey file algorithm intelligently generates honey files based on the types of files in the target file system and monitors these files for malicious behavior so that it can promptly alert users and minimize or prevent data loss.

Huawei HyperDetect. This anti-ransomware software deployed on Huawei storage systems helps detect ransomware attacks:

- Ransomware file interception intercepts the writes of files infected by known ransomware. When launching attacks, ransomware usually generates encrypted files with special file name extensions. HyperDetect intercepts the writes to files with specific file name extensions, protecting file systems on the array.
- Real-time ransomware detection analyzes file I/O logs and creates a secure snapshot when ransomware is detected. Many ransomware attacks have similar I/O behavior characteristics. By analyzing file I/O behavior characteristics, HyperDetect quickly filters out abnormal files and performs deep content analysis on the abnormal files to detect if they have been infected. It then creates secure snapshots of attacked files for file systems and sends alerts to the data protection administrator to limit the impact of ransomware.
- Intelligent ransomware detection leverages ML algorithms to compare a new snapshot with a known good secure snapshot, and marks the new snapshot as abnormal if an infection is detected. The system detects known ransomware attack features to identify any attacked file systems.

Security technologies/certifications. Huawei supports hardware root of trust, multi-factor authentication, and multiple approvals for some actions.

Other cyber security features for Huawei OceanStor Dorado all-flash arrays:

- HyperLock – WORM file format
- HyperReplication – synchronous replication across three or four data centers; asynchronous replication
- Encryption – array-based and self-encrypted drives; encrypts data at rest in the data center and in flight.
- Supports security auditor as well as storage admin role.
- Storage-as-a-service and methods for remote management.

OceanStor Dorado 18000 provides an in-depth, multilayer, intelligent defense system to mitigate the impact of ransomware attacks.

Infinidat InfiniBox SSA II

The InfiniBox SSA II is Infinidat's all flash array aimed at mission-critical workloads that demand greater performance than its hybrid InfiniBox arrays. It is highly focused on cyber storage resilience and recovery capabilities.

Features that helped Infinidat's InfiniBox SSA II earn a spot in the *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report include:

InfiniSafe is available with all InfiniBox arrays at no extra cost, bringing cyber resilience to the product family.

InfiniSafe cyber resilience. InfiniSafe is available with all InfiniBox arrays (including hybrid) at no extra cost, bringing cyber resilience to the product family.

InfiniSafe's features:

- Guaranteed recovery from the InfiniSafe repository in less than 1 minute, ensuring enterprises and service providers recover and restore data at near-instantaneous speed after a cyberattack.
- Immutable Snapshots.
- Logical Air Gap, which logically separates immutable data copies from network access either locally, remotely, or both.
- Fenced Forensic Network Environment allows customers to create a private network that is isolated for data validation, testing, and recovery.
- InfiniSafe Cyber Detection (purchasable option) adds deep content scanning.

Infinidat also protects and restores data through:

- Low-RPO Asynchronous replication – Infinidat claims it can deliver a four-second replication interval while using IP infrastructure to reduce complexity. Infinidat can asynchronously replicate to a third or fourth site at a distance with an RPO of less than 10 seconds.
- Synchronous replication for zero RPO and less than 400 microseconds of storage latency.
- Active-Active replication allowing simultaneous reads and writes to consistency groups over metro distances. Providing simultaneous access to data on each InfiniBox enables non-disruptive data migration.
- Encryption. Infinidat includes array-based encryption and self-encrypting drives. It encrypts data at rest in the data center and supports local or external key management systems such as Thales CipherTrust.
- Documented backdoor for debugging, emergency access, or to help investigate attacks.
- Storage administrator and storage auditor support.
- Security Information and Event Management (SIEM) software integration.

Other cyber security features

Infinidat's InfiniVerse leverages InfiniMetrics telemetry for cloud-based monitoring, AI-based predictive analytics, and AIOps support software. This allows Infinidat support engineers to take preventative actions before the customer is impacted.

Infinidat also provides and is well known for its white glove service for all consumers of their products, assigning a Technical Advisor, at no additional charge, to each customer for the duration of the support contract. The Technical Advisor is an experienced Storage Systems Engineer who provides a full spectrum of services, including non-disruptive in-family data migrations, and acts as a customer advisor. Infinidat's comprehensive service and support include its AIOps-based support software, and 24x7x365 technical support with rapid SLA response times.

NetApp AFF/ASA A900

NetApp's AFF A900 supports end-to-end NVMe via NVMe/FC to accelerate applications. It supports the full range of connectivity options, including 16/32 Gb FC and 10/25/40/100 Gb Ethernet. The AFF 900 supports block and file storage, while the NetApp ASA 900 is block-only.

Features that helped NetApp AFF A900 earn a spot in the *2024-25 DCIG TOP 5 Cyber Secure High-End All Flash Arrays* report include:

ONTAP and BlueXP's roles in cyber security. NetApp's ONTAP operating system that runs on its arrays includes data protection features such as snapshots, replication, mirroring, and cloud backup. Customers can manage ransomware protection, backup and recovery, and disaster recovery for all NetApp systems through its BlueXP unified hybrid multi-cloud management control plane. BlueXP backup and recovery protects ONTAP data, applications, databases, Kubernetes persistent volumes, and virtual machines on-premises and in the cloud.

NetApp customers can manage ransomware protection, backup and recovery, and disaster recovery through its BlueXP hybrid multi-cloud management control plane.

Ransomware guarantee. NetApp offers this guarantee on new purchases of all its AFF-A Series arrays, as well as other ONTAP-based storage systems. If NetApp can't help restore its snapshot data after a ransomware attack, it pledges to compensate the customer. NetApp also triggers rapid recovery by responding to threats in real-time by creating immutable recovery points or blocking user access to storage, applying forensics to identify the source of the threat, and determining which files to recover. NetApp promises to restore petabytes of data in minutes, either locally or remotely.

Other NetApp cyber security features:

- Storage-based anomaly and machine-learning file system monitoring. Sends customer alerts when suspicious activity is found, and automatically triggers the creation of a recovery point.
- Identifies user behavior anomalies to detect compromised user accounts or insider threats.
- Automatic data discovery and classification to identify vulnerable, sensitive, or critical data.
- Multi-admin verification, multi-factor authentication, and role-based access.
- Zero Trust architecture with logical air gap, WORM retention, and detailed logging.
- In-flight and at-rest encryption, both array-based and self-encrypted drives.
- Immutable snapshots.
- SnapLock feature prevents encryption and deletion of data with indestructible and efficient data copies.
- Intelligent forensics to help identify the source of the threat and which files to recover.
- ONTAP can block known malicious file extensions before they can be written to disk.

Inclusion and Evaluation Criteria

In this report, DCIG specifically focused on storage arrays possessing the following characteristics. DCIG identified fourteen arrays meeting these inclusion criteria.

- Be identified by the vendor as a high-end storage array.
- Must support multiple features that contribute to a cyber secure infrastructure.
- Must support high availability through multiple controllers in an Active-Active configuration.
- Must provide synchronous replication for non-disruptive operations across at least two data centers.
- Must provide block storage.
- Must be able to provide at least one (1) petabyte of raw storage capacity.
- Must offer proactive support based on fault data.
- Technician onsite with 4-hour GTD response.
- Commercially available on March 1, 2024.
- Sufficient publicly available information for DCIG to make an informed decision.

DCIG made a good faith effort to reach out and obtain product information from storage providers it believes met the inclusion criteria.

Ultimately, it was the professional judgment of DCIG whether a particular solution met the inclusion criteria.

DCIG Disclosures

Vendors of some solutions covered in this DCIG TOP 5 report are or have been DCIG clients. Please keep the following in mind when considering the information contained in this DCIG TOP 5 report and its merit.

- No vendor paid DCIG any fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any vendor that its solution would be included in this DCIG TOP 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a DCIG TOP 5 designation.
- DCIG bases all its research on publicly available information, the information provided by the vendor, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate whether the features worked as described.
- No negative inferences should be drawn against any vendor or solution not covered in this DCIG TOP 5 report.
- It is a misuse of this DCIG TOP 5 report to compare solutions included in this report against solutions not included in it.

No vendor was privy to how DCIG weighted individual features. In every case, the vendor only found out the rankings of its solution after the analysis was complete. To arrive at the DCIG TOP 5 cyber secure high-end all flash arrays included in this report, DCIG went through a seven-step process to reach the most objective conclusions possible.

1. DCIG established which features would be evaluated.
2. The features were grouped into six general categories.
3. DCIG identified arrays that met DCIG's definition of a high-end storage array.
4. DCIG created a survey that evaluates the features each array supports.
5. DCIG weighted each feature to establish a scoring rubric, focusing on the features that contribute to a resilient cyber secure infrastructure.
6. DCIG evaluated each array based on information gathered during its open survey period.
7. Arrays were ranked using standard scoring techniques. ■

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.**