Solution Profile

2024-25 DCIG TOP 5

2PB+ CYBER SECURE BACKUP TARGETS // GLOBAL EDITION

Infinidat InfiniBox/InfiniGuard Solution Profile

By DCIG Principal Data Protection Analyst, Jerome M Wendt

2PB+ Cyber Secure Backup Targets // Global Edition

Infinidat InfiniBox/InfiniGuard Solution Profile

SOLUTION

Infinidat InfiniBox/InfiniGuard

COMPANY

Infinidat
500 Totten Pond Road
Waltham, MA 02451
info@infinidat.com
Infinidat.com

DISTINGUISHING FEATURES OF INFINIBOX AND INFINIGUARD

- 100 percent system availability guarantee.
- Built-in InfiniSafe cyber storage technology.
- Fenced forensic environment to analyze backups before restoring data.
- InfiniSafe Cyber Detection option for intelligent deep data scanning.
- InfiniSafe data immutability and recovery time guarantee.
- High availability with redundant storage hardware.

CYBER SECURE BACKUP TARGET FEATURES EVALUATED:

- API/network protocols supported.
- Data protection.
- Hardware configuration.
- Management.
- Technical support.

Cyber Security Becomes Core Backup Target Feature

Enterprises have historically measured backup targets based on how well they minimally deliver on the following three features:

- Backup throughput speeds.
- Data reduction.
- Economical storage.

Ransomware threats and attacks have forced enterprises to add at least one more core feature to this list: cyber security.

Enterprises and managed service and technology providers now report that many ransomware strains routinely target their backup infrastructures. Some ransomware strains even start their attacks by seeking to compromise or disable backup targets. They do so in one or more of the following ways:

- Compromise or obtain administrative logins to these systems.
- Delete backups residing on them.
- Encrypt backups residing on them.
- Exfiltrate, or copy, backups from the system to the hacker's site.

The Incentive for Hackers to First Attack Backup Targets

Ransomware first attacking backup targets hinders an enterprise's ability to recover from an attack. Having compromised the backup target in any of these ways, the ransomware then turns to attacking production IT data and systems. If it then succeeds in these attacks in production, enterprises may find themselves without any restoration or recovery options.

Further adding to the danger of ransomware attacks, 90 percent of these attacks exfiltrate data.[1] Hackers may use exfiltrated data as another means to extract a ransom. Alternatively, hackers may sell the data to third parties, release it publicly, or take all these actions. Further complicating matters, enterprises may lack clarity into how hackers accessed their IT infrastructure and the data they stole.[2]

Hackers may also attempt to obtain a backup target's administrative logins and passwords. If they log into the backup target with administrative permissions, a hacker may perform any number of nefarious activities. These can range from deleting backups to copying backups offsite to changing file permissions and backup retention periods.

Finally, even if the backup target repels a ransomware attack, the ransomware may still compromise production systems and data. In this common scenario, enterprises may need the backup target to assume additional roles. These can include performing instant restores and hosting recoveries even as the solution continues functioning as a backup target.

Repelling these different attack types and needing broader recovery capabilities demand that enterprises choose cyber secure backup targets. These backup targets still deliver on the core three features that enterprises expect backup targets to possess. However, cyber security features have become prerequisites for enterprises seeking to protect their backups and facilitate fast restores and recoveries.

1. https://www.blackfog.com/the-state-of-ransomware-in-2023/. Referenced 1/8/2024.
2. Ibid.

Infinidat InfiniBox/InfiniGuard Solution Profile

This report focuses on cyber secure backup targets that offer file protocol support.

The State of Cyber Secure Backup Targets

Only recently have storage providers, as a group, begun positioning their network attached storage (NAS) solutions as backup targets. Prior to that, few storage providers formally marketed their NAS systems as backup targets. While NAS systems could serve in this role, providers downplayed this functionality.

Today, few providers exhibit any concerns about their NAS solutions being used as backup targets. More than 20 different storage providers promote more than 100 production storage systems on their respective websites as backup targets.

While many of these storage systems support multiple storage protocols, this report focuses on solutions that offer file protocol support. These support either the Network File System (NFS), the Common Internet File System (CIFS), or both. These NAS solutions provide the following benefits for backup that enterprises frequently want:

- Backup software can easily discover and utilize these solutions as backup targets.
- Client-side software available to accelerate backup throughput.
- Facilitate fast application, and data, restores.
- Fast, easy deployment, setup, and management in enterprise backup infrastructures.
- Readily recognized as a storage target by all commonly used operating systems.
- Utilize standard, cost-effective Ethernet for network connectivity.

Available Backup Target Cyber Security Features

All the backup targets evaluated offer cyber secure capabilities, though the availability, breadth, and implementation of these features vary.

Data Immutability

Data immutability, or storing data in an unchangeable format, represents one feature nearly every backup target supports. When enabled, this feature prevents ransomware attacks from either deleting or encrypting backups stored on the backup target.

Encryption

Encryption represents another backup target feature that has seen an uptick in adoption. Many backup targets have offered at-rest encryption for years. However, few enterprises used it due to the overhead it incurs while encrypting or decrypting backups.

This corporate mindset toward using at-rest encryption has since changed. Many ransomware strains attempt to exfiltrate data as part of their attack. Admittedly, encrypting backups does not prevent ransomware from exfiltrating them outside of the enterprise. However, hackers will find it almost impossible to decrypt and read any encrypted backups they obtain.

Multi-factor Authentication

Using multi-factor authentication (MFA) to log into a cyber secure backup target represents perhaps the most significant enhancement in recent years. Implementing MFA helps ensure only the appropriate administrators access and manage the backup target.

Some backup targets even require a second administrator to authenticate before it allows certain configuration changes. These may include tasks such as changing folder permissions or deleting data, among others.

High Availability

High availability (HA) also appears as a cyber security enhancement with more backup targets offering highly available controller configurations. Enterprises may not normally view HA in the context of cyber security. However, HA has become relevant due to the role that backup targets play in helping enterprises recover from a ransomware attack.

HA has become relevant due to the role that backup targets play in helping enterprises recover from a ransomware attack.

During restores and recoveries, backup targets may have to perform the following tasks, which include:

- Scanning backups to be used for restores and recoveries for the presence of ransomware.
- Providing fast response times for instant restores.
- Hosting recovered applications and/or data.
- Continuing to serve as a backup target for those parts of the enterprise unaffected by ransomware and still operating normally.
- Retrieving backups from the cloud or offsite locations.

Using backup targets that offer HA better equips them to simultaneously perform some or all these tasks. They give enterprises the extra raw resources (computing, memory, networking, and storage) that they need at these times.

Artificial Intelligence/Machine Learning

Artificial intelligence (AI) has yet to make significant inroads as a cyber secure feature on most backup targets. This slow adoption of AI in backup targets somewhat stems from other trends already in play.

For instance, enterprise backup software has often implemented AI to detect ransomware in backups. This development has somewhat negated the need for backup targets to include AI that detects ransomware.

Rather, enterprises will primarily find AI in backup targets in its first iteration, machine learning (ML). Currently backup targets may use ML for improved technical support and performing proactive maintenance on their systems. DCIG anticipates through their use of ML to perform these tasks that backup targets will soon offer more sophisticated AI functionality.

Common Features across All 2PB+ Cyber Secure Backup Targets

DCIG evaluated over 100 different backup targets of which 27 met DCIG's criteria for a 2PB+ cyber secure backup target. DCIG evaluated over 170 specific features on each one of these 27 solutions. This evaluation revealed that the software and hardware feature differences between them far outnumber their similarities.

Yet similarities between them do exist. DCIG identified the following attributes that all 27 solutions shared as supported features.

1. ***Offers Ethernet network connectivity.*** All 27 solutions include Ethernet ports that enterprises may use to connect these backup targets to their network infrastructure. Each one includes at least two Ethernet ports for network connectivity. The maximum number of Ethernet ports each one supports may, however, vary greatly by product offering.
2. ***Achieve a minimum of 100 raw storage terabytes per rack unit (TB/RU) in storage density.*** Effectively using available data center floor space remains important among many enterprises. Each one of these 27 backup targets can minimally achieve 100 TB/RU of storage density as measured by raw storage capacity.

Enterprises may only assume that every backup target provider offers email and phone technical support.

3. ***Compression.*** Compressing backups can typically increase effective storage utilization by a factor of two. Each of these 27 backup targets offers compression as a standard feature.
4. ***All support the NFSv3 and SMBv2 file sharing protocols.*** NFS and SMB represent the two standards of file sharing protocols. Further, each protocol has at least four versions available that NAS backup targets may potentially support. Among these multiple protocol versions, each backup target supports the ones that enterprises commonly use, NFSv3 and SMBv2. These two versions also possess the features needed to ensure the fast and secure transmission of data over networks.
5. ***Web-based management console.*** There exist at least fourteen different options that backup targets offer for enterprises to manage them. Yet among them, a web-based graphical user interface (GUI) for web-based management represents the only one they all support.
6. ***Integrate with both AD and LDAP.*** Integration with Active Directory (AD) and/or the lightweight directory access protocol (LDAP) was once unusual for backup targets. No more. To prevent ransomware from accessing them, all backup targets now integrate with both directory services to better secure user logins.
7. ***Email and phone support.*** The level and availability of technical support often represents a primary feature that enterprises evaluate when considering these solutions. This technical support can include everything from community forums to knowledge-bases to remote monitoring. Among all these possibilities, enterprises may only assume that every backup target provider offers email and phone technical support.

Infinidat InfiniBox/InfiniGuard Solution Profile

Upon DCIG's completion of reviewing 27 2PB+ cyber secure backup targets, DCIG ranked the Infinidat InfiniBox F6320 and InfiniGuard B4320 as TOP 5 solutions. These two complementary cyber secure backup targets meet competing enterprise backup requirements.

Both backup targets utilize the same underlying operating system (InfuzeOS) that facilitates fast backups. However, each model includes specific features to address the competing backup and recovery requirements that enterprises may have.

Each enterprise's requirements for how they manage backups and for facilitating fast recoveries will influence their choice between these two Infinidat systems. Enterprises that need a backup target that maximizes available storage capacity should choose the InfiniGuard B4320. This model scales to over 50PBs of storage capacity, offers data deduplication, and uses an InfiniBox as its back-end storage. Those enterprises that need the backup target to host application and data recoveries should give preference to the InfiniBox F6320.

Other features that the InfiniBox F6320 and the InfiniGuard B4320 offer that further help differentiate them from other 2PB+ cyber secure backup targets include:

- ***Built-in InfiniSafe cyber storage technology.*** The InfiniSafe feature represents, perhaps, Infinidat's most distinguishing feature set when compared to other cyber secure backup targets. Included as a core feature on both the InfiniBox and InfiniGuard, InfiniSafe offers key cyber security features that enterprises need today.

  These include immutable snapshots, logical air-gapped data protection, a fenced forensic network, and near-instantaneous recoveries. Infinidat guarantees recoveries in 20 minutes or less for the InfiniGuard B4320 and under one minute for the InfiniBox F6320, regardless of the dataset size.

The InfiniSafe feature represents Infinidat's most distinguishing feature set when compared to other cyber secure backup targets.

Its fenced forensic network specifically stands out among available backup targets. Enterprises may validate backups during recoveries in a private network environment. This helps to ensure recovered backups are ransomware-free so enterprises may safely use the data in production.

- ***Both systems offer high availability with redundant storage hardware.*** The two Infinidat solutions illustrate why highly available backup targets have become a necessity for enterprises. In addition to continually servicing backups, backup targets may also need to facilitate fast restores and perform forensic analysis.

  The Infinidat InfiniBox and InfiniGuard facilitate both of those activities with the InfiniBox optimized for hosting recoveries. Infinidat delivers these high levels of availability and performance. Its storage architecture inherently provides a triple-active redundant architecture. The triple-active architecture ensures that the critical hardware and software components of each system have at least two redundancies. Further, its InfiniRAID technology maintains data integrity beyond normal RAID limitations.

- ***100 percent system availability guarantee.*** Many providers of high-end storage systems jockey for position as to how many "nines" of availability their solution provides. Infinidat minimizes the need for enterprises to have to make any calculations for how much downtime they might expect annually. Rather, it provides a 100 percent system availability guarantee specifically for its InfiniBox systems. ■