SOLUTION BRIEF

InfiniBox® for U.S. Government Agencies Data Defense: Whatever the threat—ransomware, natural disaster, systems failure, human error—InfiniBox has your back.

THE CHALLENGE

Today data lives in a more dangerous world than ever. Natural disasters are on the rise and simple human error may make entire volumes of your valuable data completely useless. Today add to that cybercrime, such as ransomware and malware, which is at the top of the list of concerns for Chief Executive and Chief Information and Security Officers.

If this all sounds dramatic and dangerous, that's because it is—or it can be if you are unprepared. Most businesses practice typical data protection (backups) to shield their data in the face of these threats. Many also practice business continuity planning, which keeps their data reliable and available despite interruptions and attacks. Such planning is complicated further by the rise in ransomware and malware.

Even sophisticated organizations are not always sure if they have sufficiently protected their data. In order to ensure the latest in modern data protection, including data and cyber resilience, InfiniBox and InfiniBox SSA deliver the InfiniSafe® Reference Architecture that enables you to establish the right processes with the right tools and technologies to help keep your data safe, available, and verified to be reliable.

In this Solution Brief, we'll examine one of the most common and serious threats to data: cybercrime and ransomware.

> *"...cybercrime has become so serious that recent surveys of CEOs by Fortune in May 2021 and KPMG in March 2021 cited cybersecurity risks as the #1 threat to their businesses."*

Cybercrime is Growing Exponentially

- It is not IF, it is WHEN will you be attacked and how often might it happen. Today it is inevitable and all businesses must be prepared.
- Cybercrime isn't limited to a single attack type. Some of the most popular include phishing scams, online IP theft, and Internet fraud (the ubiquitous UN Secretary General offering tens of millions of dollars to the lucky recipient).
- Sophisticated malware attacks such as Advanced Persistent Threat (APT) take more resources to pull off, but the payoffs are large. APT hackers target data-rich networks with valuable data, deep pockets, and the potential for maximum public embarrassment should an attack succeed.[1]
- In fact, cybercrime has become so serious that recent surveys of CEOs by Fortune in May 2021[2] and KPMG in March 2021[3] cited cybersecurity risks as the #1 threat to their businesses.
- It is well documented that cyberattacks are executed with months of planning. Average dwell times are beyond 9 months that intruders have infiltrated a company's environment.

Ransomware

Ransomware is a form of malware. But unlike high-risk, high-reward APT attacks, hackers can buy ransomware off the dark web shelf. A lot of it is cheap, and some enterprising sellers even rent ransomware, which has created Cybercrime-as-a-Service (CaaS).[4]

[1] "What is an Advanced Persistent Threat?" Kaspersky
[2] "Fortune 500 CEO survey"
[3] "KPMG 2021 CEO Outlook Pulse Survey"
[4] "Revealed: The Supermarkets that Will Sell You Malware for $50" Forbes

INFINIDAT
FEDERAL

Ransomware attacks introduce software that automatically encrypts all the files and volumes it can access. If the ransomware attacks a networked computer, the encryption process will spread onto the network impacting all primary and secondary storage, including backups and archives. In many cases, secondary storage is actually targeted first, limiting your ability to recover and strengthening the position of the intruder. The hackers then demand payment from the victims to release the decryption key.

Why Not Pay the Money?

Many victims would rather pay the ransom and hope they get the key than outright lose their data.

That's a losing proposition. Sophos' **"State of Ransomware 2021"** report reveals the results of their investigation into ransomware incidents: 92% of organizations who paid a ransom in the past 12 months did not recover all their data. 65% was the average amount of recovered data for all respondents, meaning that some of them recovered partially, some fully, and some not at all. The Sophos report also revealed that the average cost of recovery in the first part of 2021 has already doubled from 2020. In the end, the cost of recovery can be millions of dollars.

Additionally, governments around the world are establishing rules, regulations, and laws around the payment of ransoms and the reporting of incidents. It is important that companies stay informed of the requirements in their particular regions.

> *"I have been very impressed by the performance, cost effectiveness, and management of the system that OFFSITE has in place...Their [Infinidat's] immutable snapshot functionality has been a great value add to protect data against ransomware."*
>
> — **Chief Technology Officer**, OFFSITE

THE SOLUTION

Infinidat Federal's powerful storage system, InfiniBox, delivers an AI-driven, set-it-and-forget-it solution with unprecedented 100% availability, unmatched performance, and a substantially lower total cost of ownership. Distinct management and data planes build powerful data protection into the system architecture.

InfiniBox's defensive capabilities allow you to protect data better with snapshots/immutable snapshots, replication, encryption, and access management controls; detect threats faster with storage pool capacity threshold alerts and rapidly recover with local and replicated snapshots.

InfiniSafe: Reference Architecture for the InfiniBox Family

Understanding how to build a cyber-resilient environment for your primary storage is more important than ever. Companies need a multi-tiered strategy for further protecting their most critical data assets. InfiniSafe's reference architecture defines methodologies that can be easily implemented to help enhance cyber resilience. This is based on a four-pillar approach:

- **Immutable snapshots**
- **Logical remote air gap**
- **Fenced forensic environment**
- **Near-instantaneous recovery**

Creating locked and unchangeable copies of your data is of the utmost importance. These can be considered logically air-gapped on their own, but extending that via a replication best practice to a second immutable copy is important, just like with DR. You then need to test and/or validate your data in that copy. Having a fenced environment (sometimes referred to as zero trust) separates you from production and is only active during the time needed to validate what you specifically want to make sure is clean. You are able to use the tools and applications that are best for you to validate and or test the data. Lastly, once you have validated those points in time, you have the ability to recover that data in seconds to minutes. Leveraging our capabilities within our InfiniBox family gives you all of this with no proprietary need or lock-in to a particular vendor or toolset.

Snapshots: The Backbone of Data Protection and Business Continuity

InfiniSnap® extends critical data protection capabilities without impacting scalability or performance. InfiniSnap uses a non-locking, redirect-on-write mechanism that creates snapshots and immutable snapshots, and enables rapid restore on demand.

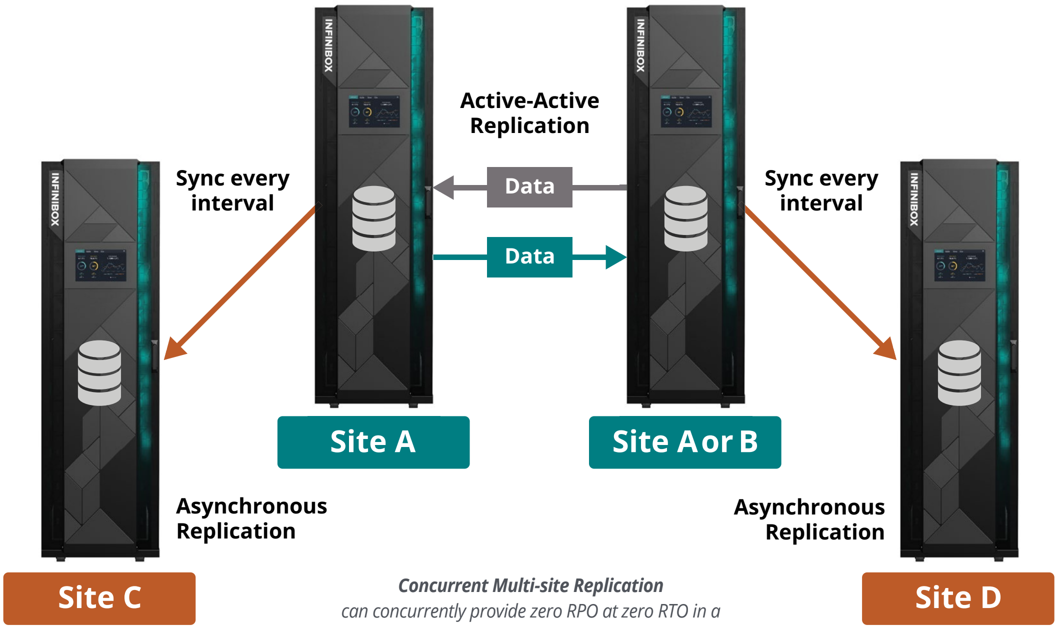
Snapshots may be read-only or writable, and each dataset can store up to 1000 snapshots. InfiniSnap snapshots enable immutable snapshots for volumes, filesystems, and consistency groups. Snapshot Directory allows end-users to easily browse, select, and recover files that have been inadvertently deleted or modified.

- **Immutable Snapshots:** Immutable snapshots cannot be modified or deleted within a set retention period. Although administrators can extend the lock expiration date, they cannot shorten it. The immutable snapshot feature also enables hidden snapshots as backup images, which further protects snapshots from attack.
- **Threat Detection:** Ransomware encryption increases data sizes, which increases the size of the data's snapshots. Admins can set capacity consumption thresholds to alert them if the snapshot volume suddenly grows outside of average parameters. If they detect an attack, admins can quickly access and test the data, and rapidly recover from the latest good snap.

Replication: Empower Business Continuity

Replication extends the power of snapshots to protect and recover threatened data. InfiniBox enables multiple replication types for changing environmental needs.

- **Asynchronous Replication:** Enables 4-second Recovery Point Objective (RPO). Using an IP infrastructure, reduces cost and complexity.
- **Synchronous Replication:** Enables zero-second RPO with latency below 400 microseconds for mission-critical applications. Should the WAN lag or fail, InfiniBox synchronous replication fails back to asynchronous mode. When the WAN is restored, the engine will automatically replicate all missing data and resume sync replication without disrupting I/O.
- **Active-Active Replication:** InfiniBox systems enable simultaneous read and write to consistency groups over metropolitan areas. The volumes are external images that appear as multi-paths to the same volume. Synchronous replication always keeps volumes consistent. There is no master-slave relationship, and no extra round trips to perform write updates to any volume. If needed, an external, lightweight witness can exist on a stand-alone node or cloud-based VM.
- **Concurrent Multi-site Replication:** InfiniBox can simultaneously replicate consistency groups from main replication sites to another site in a metro area. From there, users can asynchronously replicate to a third remote location.



Concurrent Multi-site Replication
can concurrently provide zero RPO at zero RTO in a metropolitan area while asynchronously replicating data to a third or fourth site located at distance with near-zero RPO.

Encryption: Protecting Encrypted Data

Ransomware can re-encrypt encrypted files, which is why snapshots and replication are the first line of defense. But the stronger your encryption, the harder it will be for hackers to re-encrypt them.

- **Federal Information Processing Standards (FIPS) 140-2 Validated:** The National Institute of Standards and Technology (NIST) awarded FIPS 140-2 validation to InfiniBox's cryptographic module. The standard certifies InfiniBox for use in a defined set of U.S. government and regulated industries' IT projects.
- **Standard Self Encrypting Drives (SEDs) with AES-256 Encryption:** InfiniBox uses standard Self Encrypting Drives (SEDs) with FIPS 140-2 compliant AES-256 encryption, the strongest authentication keys supported by the drives.
- **Key Derivation Functions (KDF):** InfiniBox uses U.S. federal government-approved KDF technology, which generates globally unique keys per drive. Our pluggable key manager facilitates external key management via the Key Management Interoperability Protocol (KMIP).
- **Integrates with Third Parties:** Maintains deep integration with any encryption product like Thales, VMware, Oracle TDE, or Microsoft TDE without specialized programming or high cost.

Access Management: No Trespassing

There are several routes that cybercriminals can take into a network. The most prized are administrator credentials. InfiniBox is already set to keep cyber attackers from getting that far: all access comes through the API, and the API prevents any modification to snapshots even with admin credentials.

And with InfiniBox access management, attackers won't get far to start with.

- **Role-based Access Control (RBAC):** RBAC runs in the system control plane to protect local accounts and domain/LDAP groups. Assigned group roles allow users to have full control, control over a limited capacity pool, or read-only permissions. Users can disable or lock local accounts, so they are only usable when Infinidat Federal's technicians perform maintenance activities. Session authentication further protects management access.
- **Host Authentication:** iSCSI employs CHAP to authenticate hosts on the data plane. CHAP requires multi-factor host authentication to prevent one host from accessing another host's data.
- **Third-party Access Management Integration:** InfiniBox integrates with external, enterprise-grade, privileged access management solutions, such as CyberArk.
- **Management Station Access and Audits:** Access management also includes management station access over a secure link, while audit trails log all operations that change a machine's configuration/state or components. Auditing also logs the admin making the configuration changes.

CONCLUSION

Protecting your data is critical to the success of your business. InfiniBox's rich, enterprise feature set enables you to develop comprehensive data and cyber resilience, making storage a part of your overall corporate cyber security strategy.

When you invest in InfiniBox, you not only gain superior performance, 100% availability, set-it-and-forget-it ease of use, and a dramatically lower total cost of ownership at scale, you also frustrate would-be ransomware attackers. Cybercriminals make their money on the backs of unprepared victims. They don't expect to find powerful data protection defenses.

Repel those attacks with InfiniBox immutable snapshots, powerful replication, sophisticated encryption, and strong access management; and do it with an all-inclusive model tailored to your storage budget, staff, and business objectives.

sales@InfinidatFederal.com

|

INFINIDAT
FEDERAL