

Stop Ransomware in Its Tracks with InfiniGuard® CyberRecovery

THE CHALLENGE

Ransomware is a malicious software that takes data hostage by encrypting it.

Traditionally, companies with a working backup process could restore good data to affected production systems. But ransomware code gets steadily more sophisticated, and today commonly attacks backup as well. With companies averaging a ransomware attack every 11 seconds¹, the old "If they attack us, we'll just restore the backup!" approach isn't good enough anymore.

Victims have no good options. Some choose to pay and are lucky enough to get the encryption key. Many choose to pay and get nothing. Others go with expensive encryption remediation services, and still others use a truck, literally, to retrieve off-line tape cartridges — and prepare for an arduous recovery process.

The cost? IDC estimates that ransomware costs enterprises alone \$20 billion USD per year. That number grows when you add in mid-sized and small businesses as ransomware targets.

Ransomware Today

In the first months of 2021, cybersecurity provider BlackFog² reported some of the largest incidents of cyberattacks: An attack on Victor Central School District in New York encrypted data and systems and locked out users. All district schools were forced to close. And in March, computing manufacturer Acer was hit with a \$50 million ransom to keep the hackers from publishing exfiltrated sensitive data.

An even more recent hack is the infamous ransomware attack on Colonial Pipeline, who supplies as much as 45% of the fuel on the U.S. east coast. The attack was carried out by a Russian hacking group, and the pipeline operator quickly shut down its systems to contain the attack from spreading. Even so, gas stations throughout much of the country struggled to get fuel supplies.

Smaller companies get hit too. Security firm Infracore estimated that 46% of small businesses have experienced ransomware attacks, and 73% reported that they paid the ransoms. These ransom demands may not be \$50 million, but they are costly with no guarantee that the hackers will keep their doubtful word.

Backup to the Rescue – Maybe

You are certainly better off if your backup survives the attack. But even if it does, restoring large backup sets to compromised primary systems is labor-intensive and time-consuming.

Traditionally, IT teams augment backup speeds by adopting synthetic full backups and deduplicated backup storage. But large-scale recovery in the case of a cyberattack means assembling data from multiple generations of backups, resulting in a highly random read IO pattern on the backend storage, which means prolonged recovery and potentially serious business impact.

Key Features and Benefits of InfiniGuard CyberRecovery include:

- ▶ Enterprise-level rapid restores at petabyte scale
- ▶ Protect backup against cyberattacks with immutable snapshots that cannot be deleted, encrypted, or changed
- ▶ Prove regulatory compliance with consolidated backup and immutable snapshots
- ▶ Support multiple simultaneous backup and recovery operations without impacting performance
- ▶ Validate recovery environment
- ▶ Redundant deduplication engines in an active/active/passive configuration protect data and fails over backup and recovery operations
- ▶ Lower energy costs and management overhead by consolidating backup up to 50PB
- ▶ Extreme scalability and multi-protocol support for VTL, NFS, CIFS, OST, RMAN and DB/2
- ▶ Minimize lost revenue and reputation by restoring data near-instantaneously and safely
- ▶ Recover data without compromising integrity, no matter what the cause: cyberattacks, technical malfunctions, natural disasters or human error

¹ Cybersecurity Ventures <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021>

² BlackFog <https://www.blackfog.com/the-state-of-ransomware-in-2021>

THE SOLUTION: InfiniGuard with CyberRecovery

CyberRecovery is included in Infinidat's data protection and recovery solution, InfiniGuard. CyberRecovery is built on InfiniGuard's data protection architecture, which enables rapid recovery at a fraction of the cost of competing PBBA's. InfiniGuard uses multi-PB InfiniBox as its backend and adds an innovative software layer to optimize data layout for rapid recovery, without sacrificing backup speeds.

InfiniGuard's innovative technology leverages a thick dynamic random-access memory (DRAM) layer as the primary cache, coupled with an even thicker solid-state drives (SSDs) layer as the secondary cache. A proprietary TRIE algorithm (a node tree instead of a binary tree or hashing algorithm) predicts IO patterns and pre-caches data to accelerate backup and recovery time.

Instead of trying to recover data from multiple backup appliances, media types and storage sites, InfiniGuard consolidates multiple backups into a single, easily manageable appliance that scales to 2PB of usable capacity and up to 50PB of effective capacity. Parallel restores from all spindles in the array contribute to recovery speeds.

A Closer Look at CyberRecovery

InfiniGuard's native CyberRecovery capabilities take protection and recovery even further. CyberRecovery protects against ransomware attacks by taking immutable snapshots of your backup that cannot be deleted, encrypted, or changed. You can validate your recovery environment and start the recovery process almost instantaneously. Recovery is rapid and ensures data integrity.

The immutable snapshot mechanism is encompassed into a policy-based scheduling and expiration engine, enabling the creation and management of multiple, secure, and comprehensive point-in-time copies of the backup environment.

CyberRecovery's immutable snapshots and InfiniGuard's rapid recovery architecture enables an enterprise-class backup solution with five nines (99,999%) of availability, even in the face of a cyberattack.

Even better, CyberRecovery is a native feature in the InfiniGuard appliance and is therefore part of its all-inclusive pricing.

Immutable Snapshots

CyberRecovery creates write once, read many (WORM) snapshots of an entire environment along with policy-based, point-in-time recovery. The immutable snapshots cannot be corrupted by a ransomware attack. Even if ransomware lurks undetected in a network, a backed-up file cannot affect existing snapshots. With point-in-time recovery IT can recover the latest good snapshot within minutes.

³ Infracore 2020 survey <https://www.infracore.com/press-release/infracore-survey-reveals-close-to-half-of-smb-s-have-been-ransomware-attack-targets/>

InfiniGuard with CyberRecovery enables protection of your entire backup storage via Infinidat's immutable snapshots. Each deduplication engine (DDE), can be restored to a point in time separately. CyberRecovery or discovery tests can also be enabled in a standby environment.

DDE_INSTANCE_1



Current

InfiniBox-pool1

PIT-1	PIT-9	PIT-17
PIT-2	PIT-10	PIT-18
PIT-3	PIT-11	PIT-19
PIT-4	PIT-12	PIT-20
PIT-5	PIT-13	PIT-21
PIT-6	PIT-14	PIT-22
PIT-7	PIT-15	PIT-23
PIT-8	PIT-16	...

DDE_INSTANCE_2



Current

InfiniBox-pool2

PIT-1	PIT-6	PIT-12
PIT-2	PIT-7	...
PIT-3	PIT-8	PIT-100
PIT-4	PIT-9	PIT-101
PIT-5	PIT-10	...
	PIT-11	PIT-300
		PIT-301
		...

STANDBY_INSTANCE



Copy of SnapShot:

DDE_INSTANCE_1



PIT-xxx

OR

Copy of SnapShot:

DDE_INSTANCE_2



PIT-yyy

Isolated Environment

INFINIDAT

IT has great flexibility in creating snapshots:

1. System snapshot. System snapshots are immutable and cannot be deleted or changed. Infinidat's expert support works with you to configure your system snapshots to optimize for your cybersecurity needs, including retention settings and scheduled snapshots. It is not possible for a malicious actor, or an inexperienced IT staff member, to change your immutable snapshot settings or delete an existing immutable snapshot.
2. User snapshot. User snapshots support home-based and remote workers by protecting their data. Single user snapshots are not immutable, and IT can configure their settings. These snapshots can be used the same way as System Snapshots for any recovery operation.
3. Manual snapshot. IT can take additional snapshots of the backup environment at any time.
4. Pre-recovery snapshot. System policies automatically take snapshots of the backup environment before performing any recovery operation. You can use this snapshot to go back and recover to the point of time just before a previous recovery.

Recovery becomes systematic, fast, and verifiable; with near-instantaneous recovery from any point in the history of the data. A simple to use, isolated test environment enables businesses to verify data before restoring to the business operational environment as well as support routine validations of secure backup without interrupting day to day backup operations.

SUMMARY

One should not fear an attack that might not happen. But neither should one underestimate the possibility and the painful consequences of a cyberattack.

And don't put yourself in the doubtful position of depending on hacker incompetence. Assume that the hacker is smart enough to try for your backup as well as your primary systems.

Be smarter. Implement InfiniGuard with CyberRecovery to guard against a plethora of threats from cyberattacks, technical breakdowns, and disasters, to sheer human error. InfiniGuard with CyberRecovery gives you the confidence you need to rapidly recover your data and get your organization back up and running.

