IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

An Enterprise Must Have Cyber Resilience

Bill Basinas

Bill Basinas
Senior Director, Product Marketing
Infinidat

Biography

Bill Basinas is Senior Director, Product Marketing at Infinidat (https://www.infinidat.com) and has been focused in the storage industry since 1994 when he joined Legato Systems as the first field systems engineer.

He was also an early employee at Avamar and spent time at enterprise companies such as EMC and HPE Storage in Global Marketing and Engineering roles.

Bill blogs at https://www.infinidat.com/en/blog

Keywords Cybercrime, cyberattacks, Cyber resilience, Disaster Recovery (DR), InfiniBox, Network security
Paper type Research

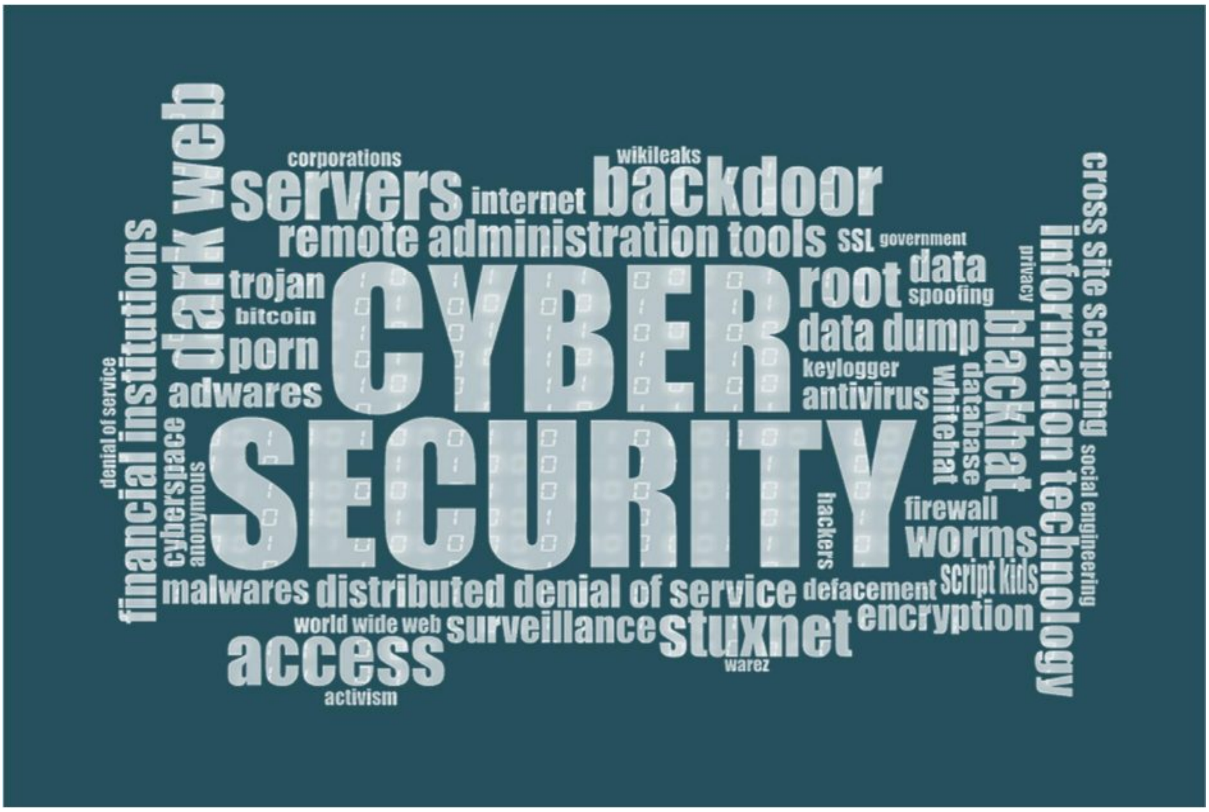
Abstract

How do you stop Cybercrime is the multi-billion dollar question. Every aspect of our IT infrastructures are part of it. The cyber “attack plane” is enormous, it is not just securing our network connections, but also extends to the people at their desks or at the edges of the company networks who can willingly or not, be the source of IT turmoil. In this paper, we will show you how Infinidat’s enterprise storage solutions with our InfiniSafe™ technology and reference architectures aligned to both our InfiniGuard and InfiniBox platforms help solve these challenges.

Introduction

We find ourselves in unprecedented times. The concern: Cybercrime. We all see it, either directly or indirectly, be it a company or individual. It encompasses comprehensive plans of theft and hostage taking of enterprise infrastructure, systems, and valuable corporate data. The cost to enterprises is in the ten’s to hundred’s of billions of dollars. With both the 2021 CEO surveys by KPMG and Fortune revealing that CEOs cite cyber security is now the Number 1 threat to their businesses, the question becomes will we ever be able to stop cybercrime attacks?

Cyberattacks are continual and done in shrouded secrecy. Industry data confirms the average dwell time for a cyberattack across your enterprise is up to 287 days! Cyber criminals believe patience and time is on their side. Taking systematic approaches, looking for the smallest cracks in system and network security and how to exploit them. They can and do build specific tools for that reason. Then at the right time, when they believe they have a comprehensive attack plan, BOOM … they attack!



What do cybercriminals want?

What do they want? Value! That is what they want, and it can come in many different forms, and you may not even know it. Many times they want a ransom paid, and many companies pay it, and now many are insured for it. Other types of value? What about account information, critical or maybe even classified documents, if they know there is a buyer for it, then that is the value and they get paid, just from a different source – and again, you may not even know they were there until it is too late. How many times have you been notified your information was part of a data breach? Yes, me too and free credit monitoring doesn't give me the warm and fuzzies!

On March 23, 2022, US President Biden signed a law, the Cyber Incident Reporting Act 2022 that requires all companies and government agencies to report cybercrime. Time will tell how effective this is based on when full enforcement goes into effect as the law becomes finalized. Is it too little too late, we'll see, but it is at a time where awareness of this is at an all-time high.

How should your company prepare?

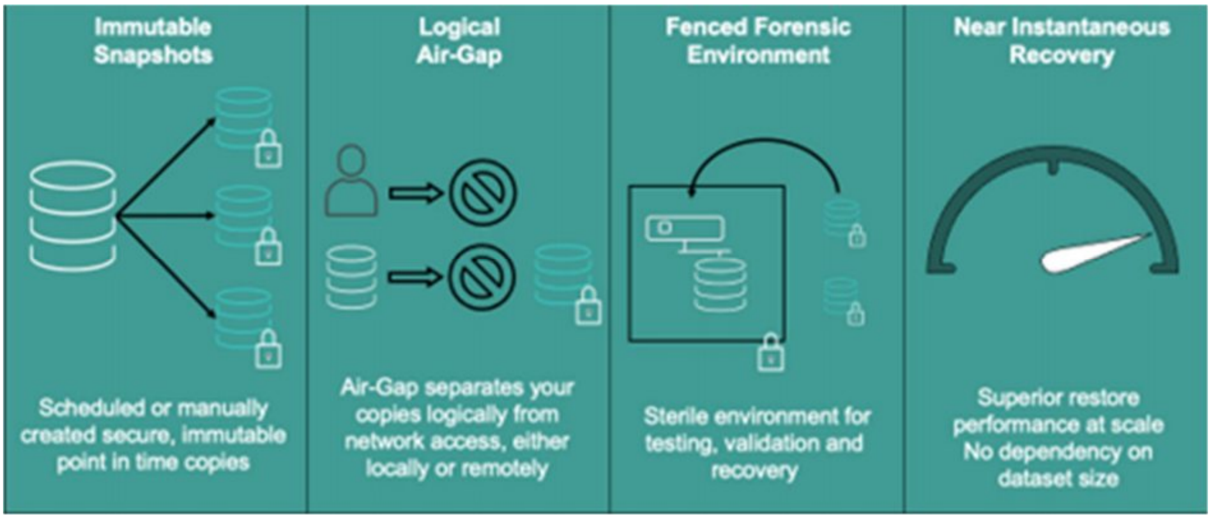
Not a simple answer, and many companies from small businesses to large global corporations are doing as much as they can to try and secure as much as possible.

A couple areas of late that have had a lot of attention is implementing a cyber strategy beyond just the compute and network level. Backups and primary storage are a huge focus area. If your company has known good copies of their data, and can easily recover that data, then the leverage cyber attackers have is eliminated. Remember, they are smart! They know that some of the first things to compromise are your backups, corrupt or disable them and they have leverage. Your backups hold all your data typically, critical and not so critical, thus protecting your backups is very important. That doesn't mean a backup of a backup, it's more than that. What about your primary enterprise storage – yes, the corporate jewels – your most critical apps and workloads, should you have a cyber strategy for that too? Yes, you should. A multi-tiered strategy gives you options.

InfiniSafe technology in our InfiniGuard solution helps give you that protection. Cyber protect your entire backup data set simply and easily. Make it easy to test and or validate it securely and allows you to recover your entire backup repository to your servers in minutes, regardless of how big they are – and I mean minutes, 30 minutes or less – in fact, 15 minutes or less in most cases . In our announcement of InfiniSafe for InfiniGuard in Feb 2022, we did a live demonstration of recovering 1.5PB's of Veeam backup repository data in 12 minutes and 27 seconds.

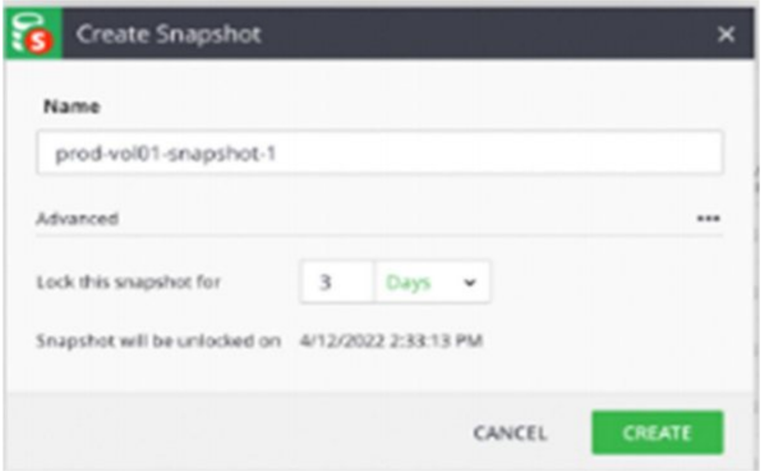
At Infinidat we have been heavily focused on the role of enterprise storage in cyber security strategy, and with our recent announcements we have technologies and capabilities within our InfiniGuard and InfiniBox enterprise primary storage systems.

Our InfiniSafe Reference Architecture for InfiniBox delivers the key four pillars of enterprise storage cyber resilience: immutable Snapshots, Logical Air-gapping, Fenced Forensic Environment, and Near Instantaneous Recovery.


Immutable Snapshots
Logical Air-Gap
Fenced Forensic Environment
Near Instantaneous Recovery
Scheduled or manually created secure, immutable point in time copies
Air-Gap separates your copies logically from network access, either locally or remotely
Sterile environment for testing, validation and recovery
Superior restore performance at scale No dependency on dataset size

Immutable Snapshots: Having this ability assures that the datasets are not capable of being tampered with, modified or deleted until the assigned expiration date. No administrator, rogue user ,or intruder can modify immutable snapshots.

Also, everything else has to support that too, may sound simple, but even making sure things like system clocks being modified will not accelerate these to expire. Immutable snapshots are core features on all our solutions and have the exact same functionality, because our core software is the same on InfiniGuard and InfiniBox, and InfiniGuard uses InfiniBox.



Name: prod-vol01-snapshot-1

Lock this snapshot for: 3 Days

Snapshot will be unlocked on 4/12/2022 2:33:13 PM

Logical Air Gap: An ability to separate the data from its source in a logical manner. Unlike physical air gapping, such as tape or optical media where you can take it out of a device and place it in an off-site location or a vault. Some will argue that the immutable snap on its own could be considered that because it is logically locked and not able to be tampered with. True to an extent, but take it to the next level, have the data someplace else too.

Our InfiniGuard system allows you to have a local logical air gap by providing a secure area within the same system and inaccessible by normal means, yes you can replicate as well.

With InfiniBox, we believe having data in a second location in immutable form is very important and done in conjunction with having your backup environment cyber secured as well. If you are already replicating with your InfiniBox, you are already on your way, a couple extra steps will help build your cyber resilience strategy.

Fenced Forensic Environment: In any of these cases or even others, a best practice is to “practice”, but do it in a secured environment. Be able to present your isolated immutable copies to a “sterile” network, with validated secure compute resources, tools and applications. You, then, look at, validate, and test or whatever you deem needed to verify that the copies are valid or not. Like with disaster recovery (DR), you need to plan for the worst and hope for the best. Testing and validating gives you options should you have any issues.

Near Instantaneous Recovery: If you suffer a malware or ransomware attack, it is essential to understand how fast you can recover a known good copy of your datasets. Again, by having tested and validated datasets, you have options, especially with Infinidat’s solutions. InfiniSafe with InfiniGuard gives you the ability to mount an entire backup set back to your production backup server in minutes, regardless of the repository size . This was demonstrated live with a 1.5PB Veeam backup dataset recovered in about 12 minutes and 30 seconds. It could have been much larger, same result, minutes.

With InfiniBox, it can be even faster, it is a snapshot and recovering a snapshot can be almost instantaneously, and if you are bringing it back from a remote link, a delta copy can often take place, again greatly reducing the time it takes to go recover. If you have a local immutable snapshot on as well (you can have both), that is about as instant as you can get.

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

In conclusion

Comprehensive cyber resilience is more than just a backup, it is securing your data at the next level. It is way more than DR as you are hundreds of times more likely to encounter a cyber event than a DR event. It is not, will you experience a cyberattack, but when and how often.

Be prepared with your primary storage with InfiniBox and its InfiniSafe reference architecture. Leverage our InfiniBox’s and InfiniGuard’s extensive cyber resilience to extend your overall cyber security strategy to include your primary and secondary enterprise storage estates. By incorporating Infinidat’s cyber resilience, to further secure your data and test, validate and practice we can help you save millions of dollars.