Thwarting Cybercrime with Infinidat

Tim Dales

Tim Dales
Product Marketing Manager
Infinidat

Biography

Tim Dales is a Product Marketing Manager at Infinidat (https://www.infinidat.com). Tim has over 30 years' experience in the development, marketing and sales of IT infrastructures.

A former Senior Analyst at a storage analyst firm working with the Dell/EMC product team on APEX and creating launch collateral for Pure Storage.

He has also held positions as an executive for networking vendor Solarflare, product marketing and sales for a CDP startup, MTI, and Emulex.

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

Keywords Cyber resilience, Automation, InfiniSafe Cyber Stack, Cybersecurity and Infrastructure Security Agency (CISA)
Paper type Research

Abstract

According to Cybersecurity Ventures[1], Cybercrime is predicted to cost the world $8 trillion USD in 2023 alone. With October's cyber security awareness month upon us, the Cybersecurity and Infrastructure Security Agency (CISA) has launched a new cybersecurity program to educate enterprises on how to stay cyber secure. As one of the Cybersecurity Awareness Month Champions[2] Infinidat is dedicated to promoting a safer, more secure environment for all. In this article, the author explains how they are helping their enterprise customers to be cyber resilient.

Introduction

October's Cybersecurity Awareness Month is a collaboration between government and private industry to raise awareness about digital security and empower everyone to protect their personal data from digital forms of crime. The reality of not helping ourselves is the growing cost to all of us. The fact that cyber security experts estimate the cost of cybercrime globally is over $8 trillion USD this year shows the magnitude of the threat. It's no wonder that in the 2023 Fortune 500 CEO survey the #2 threat cited by CEOs was cybersecurity.

We've all seen the ongoing stats, the most recent "headline" being the breaches in the gaming industry that cost millions of dollars per day. Guests were not able to check in or out, casino floors dark and other internal businesses like restaurants, shops, etc., all affected. Now there is even follow-on lawsuits against the companies for what happened.

How is it that enterprises continue to get hacked?

One of the reasons we see with large enterprises is that cybersecurity and cyber storage resilience are usually treated separately. This separation exposes a huge disconnect when creating a comprehensive enterprise cybersecurity strategy. But, when they are considered together, they plug this critical gap that cybercriminals have been exploiting. The exponential growth and intensity of cyber threats have escalated the need for cyber storage resilience to be part of every enterprise's cybersecurity strategy. The debate about it is over. Now is the time for action.

Enterprises need to make sure they are securing their storage systems and especially their data, both at rest and in-motion. With datastores moving between on-premises enterprise data centres and the public cloud, in hybrid environments, security experts agree that it's vital to invest in creating secure datastores for both primary and secondary (backup) datasets that use immutable snapshots and air-gapping. Another major focus area is to modernize data centres and eliminate wherever possible, legacy systems and applications that may not be able to be updated to current security standards.

Cyberattacks have become a matter of enterprise CEO focus because of the mission-critical nature of data in the enterprise – attacking operational technology (OT) environments to successfully cause tremendous damage: ambulances get rerouted, gas supplies are disrupted leading to days of long lines and high prices, disruption to food suppliers causing shortages are just a few examples of the impact of cyberattacks.

The 2021 attack on one of the largest energy companies in the United States, which provides bout 45% of the U.S. East Coast's fuel, disrupted gas supplies for days. The damage could have been worse if the operational technology (OT) systems weren't shut down to pre-empt attackers from gaining access to the industrial space.

The impact may not always be so drastic, although it can be in mission-critical situations, which large enterprises have, whether a health system, a governmental body, a financial institution, a retailer, a utility, a large university, a pharmaceutical company, or countless other enterprise organizations. CEOs and Boards of Directors are taking cyber risk as one of the most serious risks facing their companies. The damage cyber threats cost is the massive financial risk and the aftermath of damaged reputation, huge recovery costs, and loss of trust, all of which can be devastating to any large organization.

The top three areas of focus to thwart cyberattacks

1. **Embedded Cyber Storage Resilience** – Enterprises and service providers are more proactively deploying enterprise storage platforms that have embedded, core cyber storage resilience capabilities, such as rapid cyber recovery, immutable snaps, air-gapping, and fenced forensic environments,

that complement and enhance the broader enterprise security strategies designed to protect data.

To facilitate rapid cyber recovery, copies of data, especially critical data, must be unalterable. Data integrity cannot be compromised while combatting a cyberattack.

2. **Develop a "must protect" mindset** – Just reading the statistics and headlines you can quickly get a sense that more organizations that are not properly cyber secure will see more cyberattacks in the months and years ahead, not fewer attacks. Companies won't just get hit with one cyberattack and then have years to recover. Hackers have become highly skilful at hiding malicious code and exposing vulnerabilities. The attacks have become an ongoing threat that requires a different mindset about how both cybersecurity and enterprise storage must be tightly integrated and better aligned.

   The acceleration of digital transformation at many companies, institutions, and government agencies during the COVID pandemic from 2020 to 2022, coupled with the spike in remote working, generated volumes of new targets for ransomware and malware. As a result, the size of demands, as well as the sheer volume of attacks, increased exponentially and will continue to accelerate. Be vigilant!

3. **Automation** – With the vast amounts of big data in data lakes increasing, the only way that is humanly possible to manage all this data is with machine learning-based automation to hone enterprise security infrastructures. CIOs and CISOs are increasingly looking to enterprise storage solutions that are not only AI/ML-friendly (artificial intelligence (AI) and machine learning (ML), but also have autonomous automation that makes the infrastructure smarter to avoid and/or recover from cyberattacks.

   Autonomous automation enables an enterprise to deal with its massive amounts of data that are simply too much for human beings to handle alone. This has huge ramifications for security. The adoption of these more sophisticated tools will only increase over time and help safeguard data.

   While ML-based automation is definitely an area that enterprises need to fully utilize, cybercriminals are simultaneously also using AI/ML to automate their cyberattacks. They are using various model stealing and data-poisoning techniques. Metaphorically and literally, there is a battle underway of corporate automation vs. criminal automation on the security front.

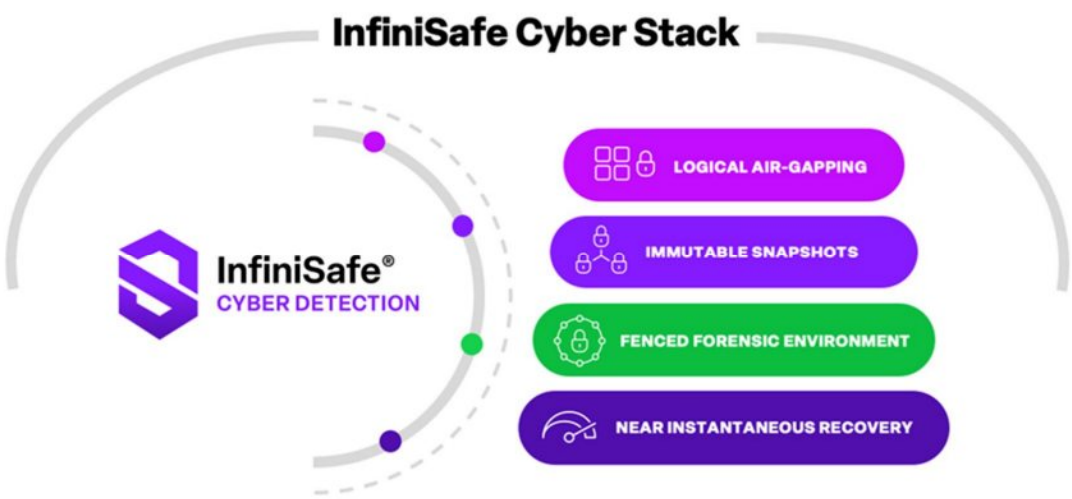
In conclusion

The combination of cybersecurity and cyber resilient storage is so vast that it's not a matter for one company alone. It may start with an IT solutions provider working with the IT team within an enterprise to bridge the two worlds of security and enterprise storage. Then the capabilities can be identified, as well as the solutions that deliver these required capabilities.

For cyber resilience to be integrated as part of a larger cybersecurity solution, a cyber resilient storage architecture is needed to map to the broader data infrastructure. This is where Infinidat comes in with its industry acclaimed InfiniSafe® cyber storage resilience software coupled with Infinidat's powerful position in the enterprise and service provider markets.

We focus on those areas and we are great at it. They include immutable snapshots, logical air-gapping, fenced forensic environments in which you can perform data forensic analysis before you begin your recovery, and guaranteed – all weaved together into a cyber stack that is empowered by autonomous automation.

Figure 1: InfiniSafe Cyber Stack



Source: Infinidat

Additionally, with InfiniSafe Cyber Detection you can scan files to detect ransomware and malware attacks with up to 99.5% accuracy, enabling near instantaneous recovery of data from clean "known good" copies on the InfiniBox® and the InfiniBox™ SSA platforms. You gain leverage back from the attackers by knowing you have good and easily recoverable copies of your data or identifying where data may have been compromised before a full-fledged attack is launched. Attackers are looking for leverage and they take lots of time typically unbeknownst to you that it's already happening.

Our expertise in combatting ransomware and malware, among a variety of cyberattacks, through both primary storage and secondary storage is second to none – and, to top it off, we provide industry-first guarantees for cyber resilience[3] on primary storage.

Enterprises and service providers don't have to worry if they don't have the requisite in-house expertise to make enterprise storage and security come together. Our partners, which are some of the best IT solution providers on the planet, and our team of storage experts are here to help you figure out all this complexity and to navigate the large ecosystem of solution providers that each offer different pieces of the puzzle.

Infinidat has a broad set of partnerships with complementary, state-of-the-art solution providers, spanning the enterprise data infrastructure. Envision the InfiniBox, InfiniBox SSA II, and the InfiniGuard®, all award-winning platforms, as the engines that drive the cyber storage solutions. The key is integration, and you may be surprised at how many other "parts" Infinidat integrates with through APIs. Of course, the quality of the "engine" has an enormous effect on the whole driving experience. Add cyber resilience to that and your data infrastructure can thwart the toughest cyberattack. If you don't want your organization to be the next cybersecurity breach headline, invite Infinidat to a Cybersecurity discussion.

Reference

1 Cybercrime Damages To Cost The World $8 Trillion USD in 2023 (15 December 2022), Cybersecurity Ventures. Available at: https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023)

2 Cybersecurity Awareness Month Champion Organizations (27 July 2023). National Cybersecurity Alliance. Available at: https://staysafeonline.org/programs/cybersecurity-awareness-month/cam-champion-organizations/

3 Herzog, E. (10 August 2022), The Industry's First Cyber Storage Guarantee on Primary Storage. Infinidat. Available at: https://www.infinidat.com/en/blog/first-cyber-storage-guarantee-on-primary-storage