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**

IT Security

The Hot Trend − Security and Enterprise Storage Together

Eric Herzog

Eric Herzog
Chief Marketing Officer
Infinidat

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com). Prior to joining Infinidat, Herzog was Chief Marketing Office and Vice President of Global Storage Channels at IBM Storage Solutions.

His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division.

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

Keywords Cyber storage resilience, Cybersecurity, Data, Cybersecurity strategy, Ransomware, Malware, Automation
Paper type Reference

Abstract

Cybersecurity and cyber storage resilience are usually treated separately in the enterprise. This exposes a huge gap in creating a comprehensive enterprise cybersecurity strategy. But when they are trending together, they fill this critical gap that cyber attackers have been able to exploit. 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 warns the author of this article.

Introduction

Enterprises need to make sure they are fully securing their data, both at rest and in motion. With datastores moving between on-premises enterprise data centers and the public cloud in hybrid environments, security experts agree that it's vital to invest in creating secure datastores for both primary data sets and for backup datasets that use immutable snapshots and air-gapping.

Cyberattacks have become a matter of life and death because of the mission-critical nature of data in the 21st century – and this is not hyperbole or exaggeration. Among the first deaths directly linked to a ransomware attack was the death of a woman reported in Germany in 2020[1].

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**

Because of a ransomware attack, a hospital was locked out of its system. The result was that the medical staff were unable to treat their patients. A woman in need of immediate medical attention was brought to the Emergency Room but the doctors could not provide the urgent care she needed.

The patient had to be transported 20 miles away to another hospital that was still functioning. Unfortunately, she did not survive. Looking back, the realization was a hard wake-up call: the hospital did not have the cyber resilience that could have neutralized the ransomware attack and have the whole system up and running in minutes.

The impact may not always be so drastic, although it can be in mission-critical situations, which large enterprises usually have, whether a health system, a government body, a financial institution, a retailer, a utility, a large university, a pharmaceutical company, or countless other types of organizations. The result may be significant lost revenues for a company, or a damaged reputation, or massive recovery costs, or chaos, or loss of trust, which can devastate any organization.

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**

What's Hot

It's important to understand what is trending – and what you need to know to be successful.

Trending Number 1 – Baked-in Cyber Resilience

What's trending is enterprises and service providers more proactively deploying enterprise storage products that have baked-in 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.

Trending Number 2 – The Onslaught of Ransomware and Malware

What's trending is the expectation 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 once and then have years to recover. Hackers have become highly skilful at hiding malicious code. The attacks have


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**

become an onslaught that requires a different way of thinking about how both cybersecurity and enterprise storage are 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, have increased exponentially in recent years.

Trending Number 3 – The Automation

What's trending is the use of machine learning-based automation to hone enterprise security infrastructures, and CIOs and CISOs are increasingly looking to enterprise storage solutions that are not only AI/ML-friendly, but also have autonomous automation that makes the infrastructure smarter to nullify and/or recover from cyberattacks.

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

While ML-based automation is definitely an area where 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 versus criminal automation on the security front.

Where Infinidat fits in

The complementary 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 information technology team within an enterprise to bridge the two worlds of security and enterprise storage. Then the capabilities are 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 credibility in the enterprise and service provider markets.

We focus on those areas we're great at. These areas include cyber recovery, air-gapping, fenced forensic environments in which to perform data forensic analysis and immutable snapshots – all weaved together in a system that is empowered by autonomous automation.

In addition, 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 on primary storage.

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**

Enterprises and service providers don't have to worry if they don't have the in-house expertise to make enterprise storage and security come together in the perfect marriage. Our partners, which are some of the best IT solution providers on the planet, and our team of storage experts extraordinaire are here to help you figure all this complexity out 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. You may equate the InfiniBox®, InfiniBox™ SSA II, and the InfiniGuard®, all award-winning platforms, as the engines in three Ferraris, but figuratively speaking, it takes other pieces from other suppliers to make the whole car.

The key is integration, and you may be surprised how many other "parts" Infinidat integrates with through Application Programming Interface (APIs). Of course, the quality of the engine has an enormous effect on the whole driving experience. Add resilience to the "engine" and your data infrastructure will rev like a Ferrari.

You don't have to settle for the following headline trending on social media: *"Ransomware attack freezes and compromises the data of [insert your organization's name], forcing all operations to come to a halt."*

Help is on the way! Trending alert: #cybersecurity #cyberresilientstorage

Reference

[1] Eddy M. and Perlroth, N. (18 September 2020), Cyber Attack Suspected in German Woman's Death, New York Times. Available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html