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**

Data Centre and Virtualization

Five Enterprise Storage Trends for 2023: Vendors Must Rise to the Challenge

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 Resilience, Storage, Solid State Array (SSA), Hybrid cloud, Cyberattacks, Flexible consumption
Paper type Opinion

Abstract

Looking ahead, 2023 will be a very exciting year for enterprise storage. In this article, the author looks at five emerging trends. In each case vendors will need to respond quickly with the right solutions, but do they have the right foundations in place to do so?

Introduction

Market trends are dynamic, not static. Since Infinidat continues to expand its presence in the enterprise market as a leader in high-end enterprise storage, we have visibility into evolving customer expectations, changing dynamics and new developments across the world. Looking ahead, 2023 will be a very exciting year for enterprise storage, in particular we are expecting to see the following trends:

1. **Convergence of cybersecurity and storage as a cornerstone of an enterprise IT strategy**

   Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) continue to increasingly realize that, if they don't combine storage with cybersecurity, they are leaving a gap in their corporate cybersecurity strategy. IT leaders are accustomed to protecting the network and endpoints, deploying firewalls and looking at the application layer. However, all their data

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**

ends up on storage. The great awakening in the enterprise market, heading into the new year, is that, if an enterprise storage solution does not have the capabilities to help combat a cyberattack, the C-suite and the IT team are leaving the organization severely exposed. The trend emerging is for storage that is buoyed by cyber resilience to be part of the overall comprehensive cybersecurity strategy in every large organization.

This means vendors must – if they don't already – offer storage solutions that perfectly align with cybersecurity solutions and strategies commonly used to protect enterprises, as well as cloud hosting providers, managed hosting providers and managed service providers. It will require a vendor and its partners to work closely with CIOs and CISOs, along with other IT leaders and administrators, to make cyber resilient storage a key part of a comprehensive cybersecurity strategy, plugging vulnerable gaps and securing the data against cyberattacks.

2. Boosting the ability to make a near-instantaneous recovery from a cyberattack with the highest level of trust in the data

The question is not "if" your organization is going to be hit with a cyberattack; it's a question of "when" and "how often". Your organization will get attacked, and it could get attacked multiple times. At that point, it's a matter of how you respond to that attack. Cyber resilience is among the most important and highly demanded requirements of enterprises today to combat cyberattacks across the entire storage estate and data infrastructure.

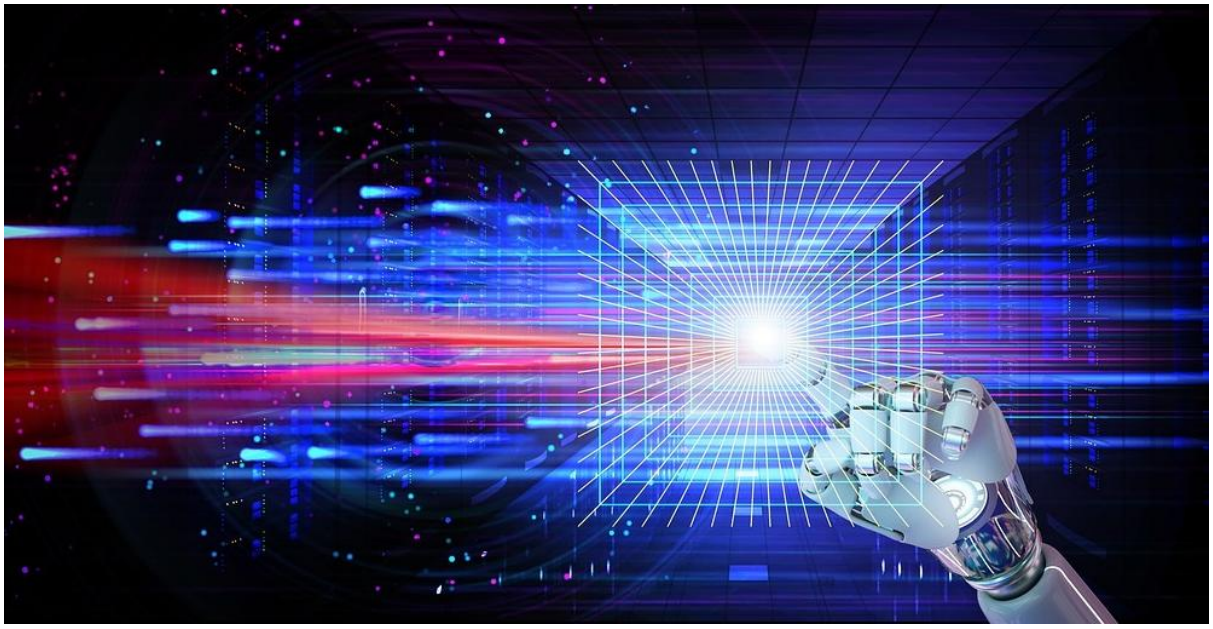
Even if your endpoint or your network security keeps the cyber criminals out once or twice, there will surely be times when they get through. When that happens, one of the critical things for an IT team is to get a known good copy


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**

of the data and make a speedy recovery. It is crucial to use an immutable snapshot of the data to ensure that the data has not been compromised. In other words, the data can be trusted. Finding a known good copy is done by curating the potential candidates to restore in a fenced forensic environment. The last thing you want to do is just start restoring data that has malware or ransomware infiltrated within it.

Vendors will need to offer solutions that combine immutable snapshots of data, a fenced forensic environment, logical air gapping, and virtually instantaneous data recovery – ideally with a rock-solid cyber storage guaranteed Service Level Agreement (SLA). Once a cybercriminal gets through an enterprise's line of defence, it's all about resilience and recoverability of the data, building on a known good copy of the data. A cyber resilient storage infrastructure helps you more easily identify threats with automation and put data into a safe, fenced forensic environment. The cyberattack is nullified.



3. Harnessing the capability of anomalous pattern detection to do cyber scanning on secondary storage

We're seeing a trend emerging more broadly in 2023 around cyber scanning with the ability to do anomalous pattern detection, particularly on secondary storage. In the longer term, we see an expansion onto primary storage over the next two to three years. This cyber scanning is another tool in the storage admin's tool bag, along with cyber resilience, to be proactively strengthening the data infrastructure to handle the ever-increasing sophistication and deceptiveness of cyberattacks. Whether for money, power or perverse entertainment, these attacks are designed to take down your business.

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**

Vendors will need to provide anomalous pattern detection capability, possibly through partnerships with backup vendors as part of a wider ecosystem. This is an evolving area of technology, and it gives customers the ability to do scanning on secondary storage, adding further value for enterprise customers and partners.

4. **Growing demand for ease of deploying cyber storage, resilience, and advanced security technologies**

Enterprises and service providers are increasingly seeking easy-to-deploy and easy-to-use solutions that meet their needs for cyber storage resilience and integrated security technologies. They want not only automation, but also the next level up with autonomous automation. End-users don't want complex set-ups anymore. They want to be able to quickly and efficiently access forensic environments, and when it comes to recovery of data, they expect two or three clicks, and then be done with it.

Vendors will need to respond with a 'set-it-and-forget-it' approach to cyber storage, offering advanced technology that is also easy to deploy and use.

5. **Cyber resilience is being recognized as necessary for both primary and secondary storage as a safeguard against cyberattacks and internal threats**

People often think that cyber storage resilience is only about backing up data. That's not true. Cyber storage resilience is more than backup. This is an important distinction that speaks to a trend for the next year because smart cyber criminals won't only attack your secondary datasets, like backup, but also attack your primary datasets. In recognition of this reality, enterprises


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**

and service providers are heading into the new year injecting new levels of cyber storage resilience into both their primary and secondary storage environments.

There is a shift in the enterprise market starting to happen from being reactive – waiting for the cyber criminals to attack and then doing something about it – to proactively prepare for recovery, likened to disaster recovery. Companies usually have elaborate disaster recovery plans and business continuity measures. There is a growing awareness that "cyber disaster plans" need to be put in place with the right set of capabilities to initiate and execute rapid recovery.

Vendors need to help customers rethink their approaches to cyber storage resilience, shifting approach reactive to proactive. Cyber storage resilience enables an enterprise to nullify a ransomware attack, as if the attack didn't even happen. No ransom, no disruption and full protection against attacks.

In conclusion

This year is shaping up to be a year of more uncertainty than the world has seen in years. To meet and exceed customer expectations for performance, cyber resilience, availability, and efficiency, Infinidat offers a broad set of guaranteed SLAs for its storage and cyber resilience platforms. The company recently added two new guarantees for the InfiniGuard solution: guaranteed recoverability of InfiniSafe immutable snapshots, and guaranteed recovery time of those immutable snapshots in 20 minutes or less on secondary storage, regardless of the size of the snapshot.

These guarantees build on Infinidat's already strong track record of the 100% availability guarantee and a cyber recovery guarantee on primary storage. Infinidat is now widely recognized for offering a comprehensive suite of guarantees that provide significant value-add to enterprise customers and service providers.