



Cybersecurity

Fortifying Frontline Defences – Cutting-Edge Enterprise Data Storage Solutions are Revolutionizing Cybersecurity

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 Data breach, Cyberattacks, Cybersecurity monitoring, Storage, Data, InfiniSafe Cyber Protection (ACP)
Paper type Research

Abstract

Today, the threat of a cyberattack has become so pronounced that in a survey¹ of Fortune 500 CEOs in 2023, the #2 threat CEOs cited to their companies was cybersecurity. We live in a data-driven world and protecting data assets is a constant challenge for all enterprise organizations. As Professor Stuart Madnick from MIT wrote in his recent paper², there was a 20% increase in the number of data breaches between 2022 and 2023 and this frequency continues to increase dramatically year-after-year. In this article, the author discusses why storage can be considered one of the missing links to a comprehensive enterprise protection strategy.

Introduction

Cyberattacks are so prevalent today that most Chief Technology Officers (CTOs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs) will acknowledge that some form of 'cyber-incident' is likely to take place inside their organization at some point. This is an inevitable part of doing business. The question is not if an organization will suffer a cyberattack, but when and how often.



Cybersecurity

One issue behind the rise of incidents involving data breaches is that the connection between cyber security resilience and data storage systems tends to be overlooked by CTOs, CIOs, and CISOs. Enterprise storage is sometimes regarded as being at the more traditional and staid end of the technology stack compared with other newcomers, like Gen AI and EDGE computing. Yet, the type of storage in use within an organization plays a critical role in their ability to recover quickly from a cyberattack.



In addition to sub-optimal awareness of the vital connection between storage and cybersecurity, another contributor to organisational vulnerability is the lack of automated integration between the infrastructure where data is stored and cybersecurity monitoring systems employed. This is another enterprise security oversight. Cybersecurity monitoring systems like a SOC or SIEM and SOAR cyber security applications need a direct link to storage systems because this is the only way to ensure that immutable snapshotting of data – to enable a safe recovery – is automated. The goal for security administrators needs to shift towards: first, protecting the organization as effectively as possible; and secondly, ensuring that the recovery phase is seamless and creates minimal problems. How can they be fully confident that primary and back-up data is safe and can be restored in minutes, and what tools exist to enable storage admins to shrink the threat window and minimize the consequences of an attack?

Reaching this point calls for a brand new, more joined up approach to cyber security strategy development, employing strengthened enterprise storage security and automated cyber-scanning. Now, a unique new solution developed by enterprise storage specialists, Infinidat, does exactly this. It has already been given rave reviews by IT industry analysts because of its potential to transform cybersecurity recovery capabilities.



As several of the leading storage industry analysts have noted ...

“Infinidat has carved out a unique leadership position as the only storage vendor to offer an automated enterprise storage cyber protection solution that seamlessly integrates with cyber security software applications. Infinidat’s newly launched InfiniSafe Automated Cyber Protection (ACP) that easily meshes with the SIEM, SOAR or Security Operations Centres is exactly what enterprises need to include enterprise storage as a comprehensive approach to combat cyber threats. This proactive cyber protection technique is extremely valuable, as it enables taking immediate immutable snapshots of data at the first sign of a potential cyberattack. This provides a significant advancement to ensure enterprise cyber storage resilience and recovery are integral to an enterprise’s cybersecurity strategy. ACP enhances an enterprise’s overall cyber resilience by reducing the threat window and minimizing the impact of cyberattacks on enterprise storage environments.”

[Chris Evans, Principal Analyst, Architecting IT]

“The new InfiniBox G4 hybrid and all-flash arrays represent a significant generational advance in cost economics and ultimate performance for enterprise-class infrastructure solutions. In EMEA we’re seeing a rapid acceleration in the Digital Shift and IT is becoming responsible for customer experience and becoming the foundation of modern business models. In addition, the performance



Cybersecurity

demands of GenAI are pushing storage requirements to the limit. Infinidat has built on its proven and scalable storage platform to deliver a storage architecture that can deliver not only on today's demanding requirements, but also on future storage needs as application demands continue to inexorably increase."

[Andrew Buss, Senior Research Director, EMEA Future of Digital Infrastructure, IDC]

"Cyber resiliency is a complex process. To mitigate business impact, organizations require the ability to detect and recover from attacks as quickly as possible. The challenge is that IT and Security teams are inundated; they require both intelligence and automation, in order to control the threat window and limit the blast radius. Infinidat offers a unique solution that enterprises critically need as a core component of their cybersecurity strategy. I expect the new Infinidat InfiniSafe Automated Cyber Protection to gain fast traction among customers by providing an automated, end-to-end process that aggregates triggers from a standard syslog, SIEM and SOAR applications, and a Security Operations Centre. Also notable is its ability to orchestrate the use of InfiniSafe Cyber Detection to scan whether the data is clean or compromised, allowing IT Operations to more quickly pinpoint the point of compromise."

[Krista Macomber Research Director, The Futurum Group]

In conclusion

In a world where data breaches are increasingly frequent and sophisticated, the connection between data storage and cybersecurity can no longer be overlooked. A convergent approach is paramount and there is a real need for integrated, automated and intelligent data storage solutions that offer a robust defence mechanism with added data protection and recovery capabilities. By taking a more holistic approach to cybersecurity, where storage and security are working together, enterprises can mitigate the impacts of cyber incidents and safeguard their most valuable asset: data.

Reference

- ¹ '24th Annual CEO Survey: A leadership agenda to take on tomorrow' (2021). PWC. Available at: <https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf>
- ² Madnick, S. 'The Continued Threat to Personal data: Key Factors Behind the 2023 Increase', (December 2023). MIT Sloan School of Management. Available at: <https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf>