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 Security of Enterprise Storage – A Call to Action for CISOs

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, Cyberattacks, Immutable snapshots, Ransomware, Forensic environments
Paper type Reference

Abstract

Cyber criminals can infiltrate an enterprise infrastructure and stay there, undetected, for months at a time. When a data infrastructure does not have the right level of cyber storage resilience, intruders can take advantage of the value of data by accessing critical enterprise storage resources and unleashing ransomware and malware, among other types of cyberattacks. But cyber criminals aren't only attacking primary storage; they also attack secondary storage. If you don't encrypt your data, don't replicate your data, and don't encrypt when you replicate, you are letting cyber criminals steal your back-up data, which is often close to your primary data, explains the author of this article.

Introduction

In the June 2023 Fortune 500 CEO survey[1], CEOs ranked cybersecurity as the second biggest threat to their corporations. The stakes continue to rise. The average number of days to identify and contain a data breach, according to security analysts, is almost 300 days.

All of this is indicative of a need in the enterprise market to modernize data protection capabilities to include a significant element of cyber storge resiliency.

Every piece of an organization’s storage estate must be cyber resilient to ensure business continuity in the face of a cyberattack.

An end-to-end approach needs to be taken to stay ahead of cybersecurity threats. Chief Information Security Officers (CISOs) and other IT leaders need to think of enterprise storage as a mission critical part of their overall enterprise cybersecurity strategy. But are they actually doing it?

To think or not to think about the security of enterprise storage

Typically, CISOs do not think about enterprise storage. The vast majority say they think about edge protection, network protection, application protection, and the threat of data theft. They are interested in trusted execution technology, rightfully so, considering zero-trust architectures for infrastructure assurance and assessments for root of trust, such as validating firmware updates for all the cards that are in an enterprise’s servers. Amid this backdrop of the multi-faceted nature of cybersecurity, many CISOs have never even thought about the security of enterprise storage.

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

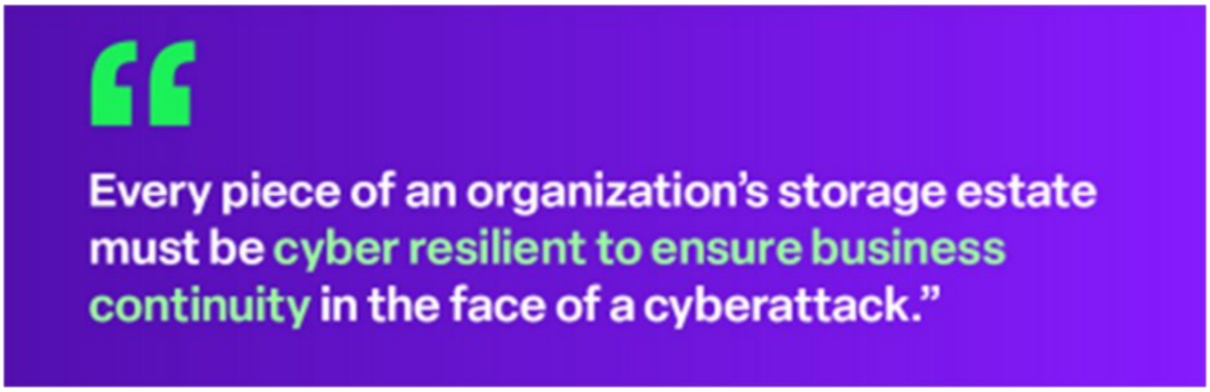
The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Enterprise storage is often left out of many cybersecurity corporate strategies –– much to the potential detriment for a comprehensive cybersecurity plan. But ignoring the security of enterprise storage is like leaving your house's doors wide open when you go on vacation with a sign over each open door that says, "Steal my possessions." A gap exists when cyber storage resilience, including cyber detection on primary storage, is not incorporated into a comprehensive cybersecurity strategy.

Ransomware and malware have become such an issue from an enterprise storage perspective. So much so, that both the US federal government and the European Union release extensive cyber security plans for enterprises and government agencies to follow in the first half of 2023. Enterprises have not done enough, in general, to secure their storage infrastructure, no matter whether they are using an all on-premises storage environment or a hybrid cloud approach with a mix of on-prem and public cloud. Cyberattacks are forcing CISOs, and broader IT teams, to reconsider the role of enterprise storage in the landscape that cyber criminals are attacking. The security of storage can no longer be overlooked.

When cyber storage resilience works

A cyber storage resilience solution is deemed effective when it provides guaranteed availability and a fully scaled data restoration for business continuity. Your cyber defence is only as good as the immutable nature of your data that can be recovered from a known good copy, how tight the air gapping is, how secure your forensic environment is, how fast the cyber recovery is, and the guarantees that should stand behind those recovery times.



"Every piece of an organization's storage estate must be cyber resilient to ensure business continuity in the face of a cyberattack."

Immutable snapshots ensure that the copies of the data cannot be changed. They cannot be altered or deleted. Therefore, the integrity of the data is preserved. Then the next step is logical air gapping, which creates a gap between the source storage's management capabilities and the immutable snapshots. Fenced forensic environments are needed to provide a safe location to conduct forensic analysis of immutable snapshots. In them, a copy of the data is identified, which is free from malware or ransomware. Only then should it be restored to your primary systems – once you know it's safe. Regardless of the size of the dataset, the data must be recovered.

Furthermore, cyber detection is a must-have. It can essentially be used in two ways. First, as an early warning system – where you scan the immutable snapshots to see if there are indications of a cyber intrusion. You can choose what you want to scan. You don't even have to scan the whole storage system. In addition, you can scan databases of all types. You can do files, volumes, workloads. It's your decision. After you do the scan, if something comes back that looks strange, the automated cyber detection capability sends an email and creates an alert. It provides this early warning signal.

Secondly, when an enterprise is attacked – in order to have a rapid recovery that will neutralize the effects of the cyberattack, you need a known good copy of the data. The last thing you want to do is recover immutable snapshots that have malware or ransomware hidden inside them. Before cyber detection, you would not necessarily know whether malware or ransomware was in there.

InfiniSafe® Cyber Detection solution

In May 2023, Infinidat introduced its new InfiniSafe® Cyber Detection solution[2], that adds new cyber resilience capabilities for enterprise primary storage to better resist and quickly recover from cyberattacks. InfiniSafe Cyber Detection provides highly intelligent deep scanning and indexing needed to identify potential issues. InfiniSafe Cyber Detection inspects the full breadth of files, applications, core storage infrastructure (such as volumes), and databases for signs of cyber threats for primary storage environments, helping ensure all data that needs to be recovered has integrity.

InfiniSafe Cyber Detection uses advanced machine-learning models that provide 99.5% confidence in detecting cyber threats. This helps dealing with false positive/ negatives and greatly reduces the effort in any additional forensics. Over 200 points of determination are included, using content-based analytics that inspect inside files for even subtle signs of attack. The post-attack dashboard (with forensic report) details the last known good copy of the data for rapid, intelligent recovery.

In a forensic fenced environment, you can undertake cyber detection of the immutable snapshots to identify the known good copy of data – and this is done on primary storage. You no longer need to call the Oracle team or the SAP team to have them take a look at the data in the fenced area. You can do the scanning yourself in the fenced forensic environment through the storage platform with cyber detection capabilities. You can better manage the process of ensuring a known good copy of data that is then recovered rapidly.

Enterprise storage needs to be considered as an essential part of a holistic corporate security strategy. This means that every possession in a company's enterprise storage estate needs to be cyber resilient, designed to thwart ransomware, malware, internal cyber threats, and other potential attacks. Cybersecurity must go hand-in-hand with storage cyber resilience.

Reference

[1] Murray, A., (2 June 2023) 'Fortune 500 CEOs aren't afraid of AI – but an impending recession is another story', Fortune. Available at: https://fortune.com/2023/06/02/fortune-500-ceo-survey-2023-ai/

[2] Infinidat (24 May 2023) 'Expands Support for Hybrid Cloud Storage Deployments with InfuzeOS™ Cloud Edition, Enhances Cyber Storage Resilience with InfiniSafe® Cyber Detection', Infinidat. Available at: https://www.infinidat.com/en/news/press-releases/infinidat-expands-support-hybrid-cloud-storage-deployments-infuzeostm-cloud