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**

Cybersecurity

Shrinking the Cyberattack Threat Window: InfiniSafe® Automated Cyber Protection (ACP)

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 attacks, Cybersecurity, Storage, Immutable snapshots, Data, InfiniSafe Cyber Protection (ACP)
Paper type Research

Abstract

If enterprises are investing millions of pounds into their cyber protection armour and disaster recovery strategy, why are hackers still managing to profit from data disasters? Ask the author of this article, explaining that one of the big contributors to organizational vulnerability is the lack of integration between primary and secondary storage infrastructure and the data centre-wide cyber security software applications employed to spot suspicious activity.

Introduction

The threat of a cyberattack has become so pronounced that in the 2023 survey[1] of Fortune 500 CEOs, cybersecurity was cited as the #2 threat to their companies. These incidents are on the rise. As Professor Stuart Madnick from MIT wrote in a recent research paper, the number of data breaches between 2022 and 2023 rose by 20% and this frequency continues to increase[2]. It's not surprising because hackers want to wreak havoc and, in our data-driven society, breaches cause extensive damage and long-lasting suffering to enterprises and individuals alike.

If we assume that a cyberattack will take place at some point – this is a somewhat inevitable situation for enterprises to acknowledge – the question now for security

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**

administrators becomes less about attack prevention and one of attack recovery. How can storage experts shrink the window of threat to their organizations once security systems have been compromised? And how do they minimize the impact of a cyberattack both internally and externally? It's impossible to keep cyberattacks quiet. New laws and regulations for reporting cyber incidents for public companies in the USA and specific regulations pertaining to and written by the European Union, have made knowledge of these attacks highly visible to the public.

Part of the problem is that traditional storage backup methods using immutable snapshots are only effective to a point, because snapshot schedules are not automated. This means they are not running constantly and may even require manual intervention, which leaves dangerous gaps in data protection. Even replication means that data is available but not really protected, because once it is corrupted or encrypted, the compromised data can also be replicated, potentially causing even more havoc. Overcoming these problems is not a new challenge and has been part of the disaster recovery challenge for many years.

Enterprises have been trying to protect themselves from these threats, typically by employing teams of people to monitor and manage their cybersecurity. Despite this, it can still take hours to determine if someone should call a storage admin and say, "we detected something in server x, why don't you snapshot the data as soon as possible?" The reality is that this call often never happens, leaving the vulnerability window wide open for attackers to proliferate data corruption, encryption, or other attack vectors against enterprise data. For instance, if immutable snaps are taken four times a day, that means up to a six-hour RPO (recovery point objective). Today, the amount of data that could be compromised in that timeframe can ruin a 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**

To help ameliorate these issues Infinidat has developed a unique new solution to solve this longstanding problem and reduce the threat window. InfiniSafe® Automated Cyber Protection (ACP) is unique in allowing enterprises to regain control of the chaos that cyber attackers bring on, saving time, money and risks to reputation. It is available free for users of the new InfiniBox G4 family of InfiniBox® and InfiniBox™ SSA enterprise storage solutions and has been given rave reviews by storage and security industry analysts across the world.

According to Krista Macomber, Research Director at the Futurum Group, “Infinidat’s complete solutions have taken the lead by leveraging the syslog of security technologies, such as SIEM and SOAR to detect and respond to anomalies that belie potential threats.”

Storage analyst firm founder Chris Evans of Architecting IT, said, “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.”

Andrew Buss, Senior Research Director, EMEA Future of Digital Infrastructure at IDC commented that “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.”

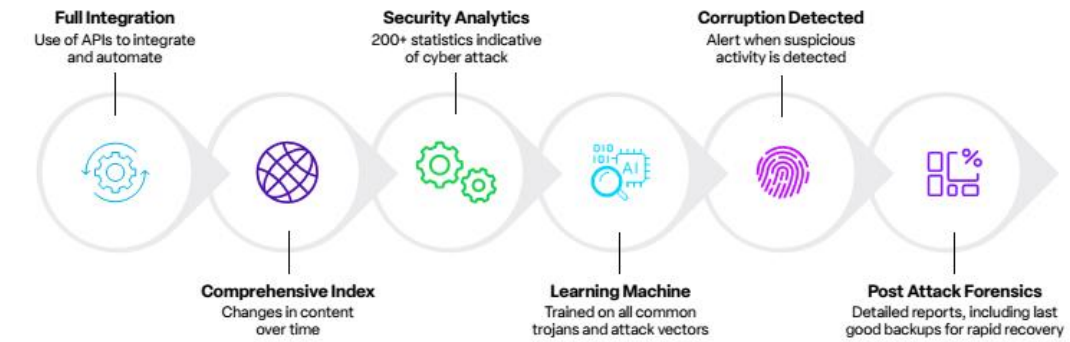
IT for CEOs & CFOs is published by House of Words Media Limited.

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

How does InfiniSafe ACP work?

InfiniSafe ACP works to reduce the cyberattack threat window to enterprise data at the speed of compute, by automatically triggering a protection scheme to create immutable snapshots of any data within the InfiniBox SSA and InfiniBox platforms. These requests come directly from the enterprises' cyber security software environments, the SOC, SIEM or SOAR, as soon as any concerning changes or events are detected. Application environments like these have extensible interfaces and so tying them together with the well-defined InfiniSafe reference architecture provides a fully automated set of seamless capabilities. These capabilities can be orchestrated to proactively and quickly create immutable snapshots to protect the most critical primary data assets.

Figure 1: Identify, Orchestrate, and Act



Source: Infinidat

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**

InfiniSafe Cyber Detection can be integrated with ACP to take the process to the next step. InfiniSafe Cyber Detection performs deep scanning of block, file, and database stores by presenting immutable snapshots to a powerful AI-based scanning engine. This validates the data integrity and through AI-based machine learning, can identify any malicious changes as a result of the cyberattack. More importantly, the scanning process uses more than 200 data points to determine which data may have been compromised, with 99.99% accuracy.

This ensures that any additional forensics are highly defined and easy to act on, by minimizing any possible false positives. You need to be fast and accurate when dealing with a cyber event. Such a rapid, automated response means that full recovery from an attack can be guaranteed for entire snapshots of data, regardless of volumes.

Being prepared for cyberattacks is everything today. It's not a matter of if cyber attackers will strike, it's a matter of when and how often. Bad actors will attempt to create chaos and gain leverage over your most critical data assets if you are not prepared. Knowing the state of your data by proactively keeping it protected beyond scheduled events, is a key component to reducing the threat window, gaining back leverage, and thwarting those looking to extort you by compromising your data. Now InfiniSafe ACP is making these goals easier for every enterprise to achieve.

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
3. Solution Brief: InfiniSafe® Automated Cyber Protection: Reducing the Threat. Infinidat. Available at: https://www.infinidat.com/en/resource-pdfs/infinisafe-automated-cyber-protection.pdf