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 and Cloud Storage

Anchoring Your Cyber Secure Backup

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, Storage, Return on Investment (ROI), Capital expenditure (CAPEX), Cybersecurity, Cyberattacks
Paper type Opinion

Abstract

Daily data backups are standard for modern enterprises, but a critical dilemma has emerged: backup repositories have become primary targets for cybercriminals seeking to maximize extortion. Sophisticated, AI-enhanced threats, ransomware, and malware are increasingly targeting backup data to prevent recovery. According to Rubrik Zero Labs[1], 93% of ransomware attacks now target backups with 75% of these attempts succeed in compromising backup systems. With the focus shifting from simple data backup to a recovery-first, cyber-resilient strategy, the author of this article explains how organizations can anchor security with immutable and air-gapped technologies to ensure data integrity that provides nearly instant restoration capabilities.

Introduction

The smart enterprise is backing up its data every day. However, there's a dilemma. While you're backing up your business-critical data, cybercriminals have made backup environments into high-value targets for cyberattacks. As a result, highly available, cyber secure backup targets have become an absolute necessity for enterprises. In addition to continually servicing backups, backup targets need to perform forensic analysis and facilitate fast restores. A new world of cyber secure backup has emerged.

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**

Amid an ominous backdrop of highly sophisticated, AI-augmented cybercrimes, deepfakes and diversions, ransomware, malware and other cyberattacks are being increasingly launched against data backup repositories. More than 93% of ransomware attacks now target backup data to prevent data recovery and increase the pressure for enterprises to make significant “ransom” payments, with 75% of these attempts successfully compromising backups, according to Rubrik Zero Labs report[1].

Backup repositories are being breached. It’s a stark reality that CIOs, CISOs, IT security managers and backup administrators need to accept and address. You need to ask yourself a critical question – the answer to which may either save or sink your enterprise business. You cannot deny the inevitable. What if the way that your enterprise is backing up data is the weak link?

Therefore, you need to rethink your data protection strategies to counter the ways that cyberattacks work to encrypt, steal, cripple, and compromise your backup in secondary storage. World Backup Day 2026 is the perfect time to consider adopting new capabilities that will better protect your backups and accelerate cyber recovery.

The risky business of backups

The speed of cyberattacks has shifted from days or weeks to now hours or minutes. Cybercriminals are compressing the attack lifecycle. Although traditional backup is effective for standard restore, it’s not great for rapid recovery from such attacks. Restoring data to a point can happen rather quickly, but large-scale recovery of large environments of data is not optimal – even if the backup is not disabled. Traditional backups typically leave large gaps between points when data is protected. This increases risk of data loss and unwanted downtime. The threat window must be reduced.

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**

Cybercriminals attack backup environments in order to gain leverage. On average, it can take 22 days or more to determine affected data and then recover, according to various cybersecurity market reports. That's why it's best to protect data as close to the source as possible, with short-term retention, as well as many potential validated recovery points.

Cyber storage resilience and rapid recovery – guaranteed

Infinidat offers enterprises a next generation of data protection that is a cyber-focused, recovery-first strategy, enabling detection and providing near-instantaneous recovery of data in the event of a cyberattack. Through our industry acclaimed InfiniSafe® software, we give enterprises the capabilities to incorporate cyber storage resilience into their enterprise data infrastructure – both for primary storage and for backup workloads.

InfiniSafe is built on providing a simple, easy and very comprehensive set of capabilities to protect any data on our enterprise storage solutions, including our InfiniBox® G4 and InfiniGuard® platforms. Enterprises have successfully deployed a significant number of InfiniBox G4 and InfiniGuard systems as cyber secure backup targets. They have proven to be extremely reliable.

The InfiniBox is optimized for enterprise customers who choose to do data reduction with their backup software, while the InfiniGuard is optimized for customers who want to do data reduction in their storage layer.

We not only guarantee the immutability of our snapshots, but we also guarantee the recovery time (RTO) on our InfiniBox and InfiniBox™ SSA primary storage systems of one minute or less, regardless of dataset size. We guarantee the recovery time on our InfiniGuard® purpose-built backup appliance in 20 minutes or less, regardless of dataset size.

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**

The performance of Infinidat's systems as cyber secure backup targets is stellar, and our customers get great benefits from their Infinidat configurations. For example, one Global Fortune 500 customer deployed an InfiniGuard with InfiniSafe. That customer reduced the full backup window for one of their database workloads to only 30 minutes from 5 hours with their former backup target – a 10x improvement. They reduced the backup time for another workload to only 4.75 hours from 18 hours with the other vendors' product – nearly a 4x improvement. They also saw a reduction in recovery time of 97% for full copies.

Another Fortune 500 customer replaced 36 competitors' backup targets with 20 InfiniBox systems, using InfiniSafe for cyber storage resilience. The initial CAPEX was half of that of the competition, and in just their first year of deployment they saved more than $1.5 million in Operational expenditure (OPEX). All backup window SLAs and all recovery time SLAs were met or exceeded.

InfiniSafe includes truly immutable snapshots, logical and remote air-gapping, a fenced forensic environment, and near instantaneous recovery, guaranteed. As part of InfiniSafe's cyber storage resilience stack, we also offer the ability to detect data corruption, the fingerprints of latent data corruption attacks, and other cyber issues across your data with an accuracy of up to 99.99%, leveraging AI and ML technology. This is accomplished through our InfiniSafe Cyber Detection.

Data should be protected via immutable snapshots on a scheduled basis as a baseline. But schedules leave gaps, and data centre-wide cyber security software applications and the usual Security Operations Centre (SOC) leave your enterprise storage out of their scanning processes. Infinidat addresses this issue through our InfiniSafe Automated Cyber Protection (ACP) capability, which is a trigger that is provided as a fully enabled container leveraging our extensive API's and telemetry information.

InfiniSafe ACP seamlessly integrates with data centre-wide cyber security applications − SIEM, SOAR, a SOC and solutions from our technical alliance partners. The Infinidat storage infrastructure is automatically alerted whenever a customer deems a security event of interest and can immediately trigger immutable snapshots, helping to reduce the threat window.

Unlike traditional backup products that were engineered to primarily provide high ingest rates by utilizing inline deduplication techniques, Infinidat's cyber resilient storage solutions significantly speed up recovery, enabling an enterprise to bounce back from a cyberattack with little to no damage of any kind. It's the real power of next-generation data protection in action.

Reference

[1] Rubrik Zero Labs (18 April 2023) *The State of Data Security: The Hard Truths*. Available at: https://www.rubrik.com/content/dam/rubrik/en/resources/report-review/rpt-rubrik-zero-labs-global-report.pdf