



# Enterprise and Cloud Storage

## Financial Institutions' Rising Interest in Solving New Cyber Threats, Data Centre Space Constraints, and the Cloud Paradox

Tony DeLisio



**Tony DeLisio**  
Vice President –  
Financial Accounts  
Infinidat

### Biography

*Tony DeLisio is Vice President – Financial Accounts at Infinidat (<https://www.infinidat.com>). His career has encompassed long tenures at HPE, Citi, EMC, and Hitachi Data Systems, among others.*

*With over 35 years of management experience in business, Tony is a senior leader within the world banking technology, helping to bridge the needs of the banking clients with their own technology teams through the use of Infinidat solutions providing petabyte-scale data protection and unrivalled reliability. Having worked on both the vendor side and the client side, Tony has become the “go to” expert for banks seeking to upgrade, secure, and consolidate their storage infrastructure.*

*Tony blogs at <https://www.infinidat.com/en/blog/>*

**Keywords** Enterprise storage, Ransomware, Data integrity, Critical asset protection, Cyberattacks, Cyber resilience, Immutable snapshots, Frictionless business infrastructure, Cyber recovery

**Paper type** Opinion

### Abstract

*The recent Strategic Technology Analysis Centre (STAC) Summit in New York City was the perfect venue to be teeming with discussions and shared insights about how to solve the infrastructure-related problems facing the financial community. As a featured speaker at the event, the author of this article outlines some of the strategies and insights he shared about enterprise storage for financial institutions at the event.*

### Introduction

Financial institutions have significant infrastructure challenges. On the one hand, the threat of cyberattacks against enterprise data infrastructure continues to escalate, and financial institutions need to build more cyber resilience into their infrastructure to minimize the impact of attacks by cyber criminals. On the other hand, their data centres are running out of space, but they don't really want to build new data centres. They go to the public cloud, but they then find out it's more expensive than anticipated, and there are trade-offs that create risk.



---

*Enterprise and Cloud Storage*

These challenges call for a combination of new strategies, deep insights, and advanced technological solutions suited for financial institutions, including banks, brokerages, asset management companies, credit card companies, and financial service providers, among others.



### **Ransomware attacks against financial institutions are on the rise**

Cyber resilience is critical for a financial institution's storage infrastructure, both to protect and defend its data against cyberattacks, but also to rapidly recover its data in the event of a ransomware attack. According to Statista, from 2021 to 2024, the share of financial institutions worldwide experiencing ransomware attacks has increased significantly. In 2024, roughly 65% of financial organizations worldwide reported<sup>1</sup> experiencing a ransomware attack, compared to 64% in 2023 and 34% in 2021.

To ensure the integrity of the data they collect and process – including bank account information, credit card information, client data and personal consumer information – banking and finance leaders must navigate a challenging security landscape.

The key to fighting off a cyberattack is having a known clean copy of data that can be recovered before the cyberattack has any significant impact. This is supported by cyber detection, automated cyber protection, encryption, access management controls, capacity consumption thresholds, guaranteed recovery time objectives (RTO) and data testing. At the same time, the strategy must satisfy financial regulatory requirements.



At Infinidat, we have gained this insight from our hands-on experience with financial institutions that have the most stringent requirements. Infinidat provides compliance-optimized, cyber resilient and cyber recovery storage solutions ideally suited for banks and other large financial institutions.

Already used by many large banks in multi-tiered strategies for further protecting their most critical assets, our award-winning InfiniSafe® solution for cyber resilience in primary storage includes a variety of vital elements:

- **Immutable snapshots:** Whether automated, scheduled or manually created, InfiniSafe's immutable snapshots are secure and unchangeable, point-in-time copies.
- **Logical remote air-gapping:** InfiniSafe provides a simple way to logically separate immutable data copies from network access, either locally, remotely, or both.
- **Fenced forensic environment:** InfiniSafe enables you to create a completely private network that is isolated for data validation, testing, and recovery.
- **Cyber detection:** InfiniSafe Cyber Detection validates the integrity of your immutable snapshots using powerful, AI-based scanning engines.
- **Automated cyber protection:** InfiniSafe Automated Cyber Protection reduces the threat window for cyberattacks, enabling integration into your SOC, SIEM, or SOAR applications.
- **Near-instantaneous cyber recovery:** Get all your known good and validated data back and available for restore in minutes, regardless of the data set size, supported by guaranteed recovery SLAs.

These elements all come together to build and enhance the cyber resilience of a financial institution's data infrastructure. By being one of the few enterprise storage solution providers with such a broad set of cyber capabilities specifically for primary storage as well as secondary storage, Infinidat has vastly improved the way financial institutions combat ransomware and malware.





## Data centre constraints versus the public cloud paradox

Financial institutions are understandably reluctant to build new data centres due to high costs and technological shifts. They want to get the most out of the space of their existing data centres. Simultaneously, they want to leverage the public cloud, but they must maintain a certain level of control of data.

What we have learned is that providing large storage capacity in a fraction of the size of traditional storage arrays is greatly helping a variety of financial institutions, including large banks, make more efficient use of space.

Furthermore, they can now also have a cloud experience in a private data centre, making the private cloud and public cloud appear as seamless in an end-to-end hybrid multi-cloud experience.

Infinidat enables customers to have an end-to-end experience that makes their business infrastructures consistent and easy to manage as well as providing them with storage management standardization from on-premises to the cloud.

InfuzeOS™ Cloud Edition is powered by the same enterprise-class InfuzeOS that powers our InfiniBox® G4, InfiniBox™ SSA G4, and InfiniGuard® platforms, reducing the OPEX costs to manage the storage estate. InfuzeOS Cloud Edition is currently available for Microsoft Azure and AWS environments.

If your financial institution is dealing with these challenges of cyberattacks, data centre space constraints, and how to leverage hybrid multi-cloud more effectively, reach out to me at [adelisio@infinidat.com](mailto:adelisio@infinidat.com).

### Reference

- <sup>1</sup> Petrosyan, A. (10 July 2024), 'Rate of ransomware attacks in financial institutions worldwide 2021-2024'. Statista. Available: <https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global>