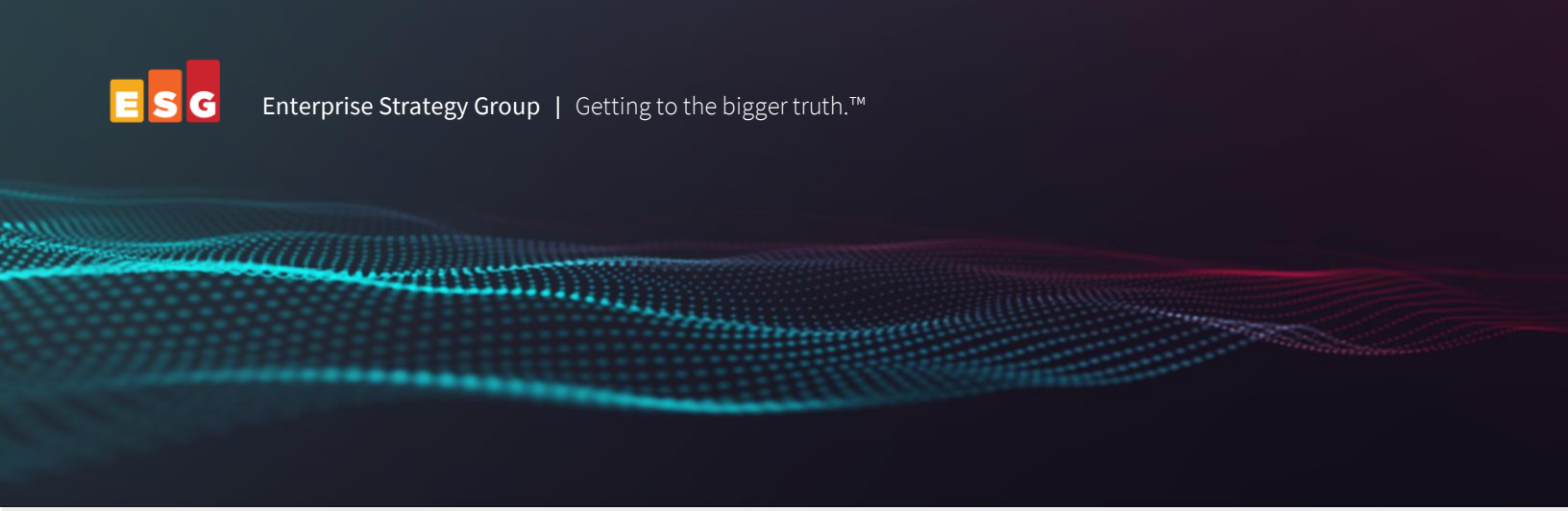


ESG WHITE PAPER

Enhancing End-to-end Cyber Resilience in IBM Z Environments with IBM Storage and Networking Solutions

By Jack Poller, ESG Senior Analyst

August 2020

This ESG White Paper was commissioned by Brocade and is distributed under license from ESG.

Contents

Introduction

Many of the world's leading industries rely on mainframes as the backbone of their IT and data processing infrastructure. Mainframes are a major driver of worldwide commerce, including banking, airlines, credit card processing, and retail operations. The mainframe processors themselves and the data storage systems that support them are key elements of these business environments, as are the networks that move data between these systems and around the world, which also play a crucial role. Developing and implementing secure and resilient end-to-end mainframe data processing environments is crucial to 21st century business.

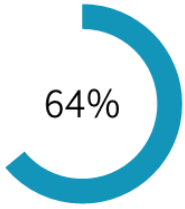
Until recently, cybersecurity was the primary focus to keep business systems operational. This domain encompasses the technology and processes that attempt to prevent attacks, data compromise, and data exfiltration. But even with the best security, data breaches—via attack or negligence—still occur, regardless of the amount of investment in preventative tools and techniques. When failures happen, sensitive data can be lost or exposed, and business operations will be impacted, often with disastrous results. The question of a cyberattack is not if one will occur—but when.

Cyber resilience represents the recent shift in thinking from attack prevention to preparing for the eventuality of failure. It focuses on ensuring organizations can continuously operate their businesses and deliver the intended outcomes despite adverse cyber events—whether malicious or inadvertent. A cyber resilient organization puts the infrastructure, tools, and processes in place to protect its core asset—its data—and can respond to and recover from attacks and failures, guaranteeing the continuity of operations before, during, and after any cyber event.

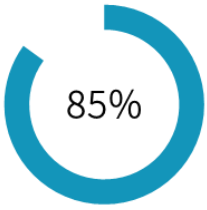
Developing and implementing secure and resilient end-to-end mainframe-driven business environments means addressing all the elements—the compute platform, storage arrays, and the network. But modern organizations face a number of basic challenges related to implementing and maintaining robust cyber resilience in mainframe environments.

Challenges

Cyber resilience strategies are being affected by the growing complexity of IT systems, which creates an ever-expanding surface of cyber exposure and complicates efforts to recover operations after a cyber incident. ESG research confirms that IT complexity is growing yearly, driven by higher data volumes and an ever-increasing cybersecurity threat landscape. Sixty-four percent of organizations say IT is more complex compared with two years ago.[1] Likewise, in another survey, 85% of respondents said network security has become more difficult than it was two years ago, and 45% believe the increased level of difficulty is driven primarily by an increase in the threat landscape.[2]



IT is more complex compared with two years ago.



Network security is more difficult compared with two years ago.

Three key challenges for IT environments include:

- Data security—organizations can ensure data is not compromised by securing data within the compute and storage platforms and in flight across the network.
- Data replication—organizations need to select methods of data replication to ensure they meet their business continuity and recovery requirements.
- Data recovery—continuity of business operations requires organizations to quickly recover their production environment from good copies of data.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

Security of data, both in flight and at rest, requires control of user access, which includes authentication of identities and authorization of rights to access. Another challenge, directly related to the network, is ensuring the integrity and confidentiality of data transferred between entities, and this is often addressed through encryption.

Identifying the right solution for data replication will be guided by recovery point objective (RPO) and recovery time objective (RTO), and the technologies involved can include array-based replication to multiple locations, virtual tape replication to multiple locations, or moving data to physical tape with an "air gap" protection.

Networks and cybersecurity exposure can compromise the business in a single data center or across multiple data centers. Ensuring secure, high-performance data transfer across both the storage area networks (SAN) within the data center and wide area networks (WAN) spanning thousands of miles introduces added complexity into an already complex environment.

Understanding where data is stored and where the latest valid copy of that data resides is critical to recovery from any type of cyberattack or failure. The host and storage tools used for tracking data will be a key element to recovery from valid copies.

Cyber Resilient Storage in IBM Z Mainframe Environments

The IBM DS8900F storage systems and TS7700 VTL solutions enjoy a unique relationship with IBM Z mainframes, which helps address these challenges. All three product lines exist within the same IBM Systems business group, fostering design and development coordination and collaboration. For example, as a result of concurrent innovation, the products jointly support both "pervasive encryption" of data at rest and encryption of data in flight using IBM Fibre Channel Endpoint Security. This end-to-end solution protects in-flight data, independent of the operating system, file system, or access method, by encrypting all data traversing FICON and Fibre Channel Protocol (FCP) links.

IBM DS8900F also includes additional data protection and cyber resilience capabilities such as IBM Safeguarded Copy, a feature that provides immutable point-in-time copies of production data with dual control security to protect and quickly recover business operations from user errors, malicious destruction, or ransomware attacks. When integrated with tape systems such as the IBM TS7700 Virtual Tape Library (VTL) with its offload capability to physical tape, the IT environment includes a critical "air gap" that isolates data from production networks and the internet, furnishing an effective safeguard against cyberattacks.

IBM Transparent Cloud Tiering (TCT) enables organizations to replicate data directly from an IBM DS8900F to the IBM TS7700 VTL with no IBM host intervention and no impact in performance. IBM TCT provides another method to protect data from cyberattacks by creating and protecting point-in-time backups in the cloud. Direct data transfer from DS800F to hybrid cloud environments simplifies archive and disaster recovery operations with no additional servers or gateways, improving business efficiency while reducing capital and operating expense. According to IBM, using TCT to secure data in the cloud can help reduce IBM Z CPU utilization by as much as 50%, and all data transfers are encrypted.

Data Recovery Management

Transparent Cloud Tiering ensures that backup copies of production data are secured in the cloud and are always available in case working copies are lost or corrupted. TCT uses dynamically adjustable policies to manage data migration to hybrid cloud repositories, providing the necessary flexibility for today's constantly changing environments. TCT extends the cyber resiliency capabilities of Safeguarded Copy by creating and storing full volume backups of production data in the cloud; these backups can be restored to any DS8900F system.

Similarly, TS7770 can safeguard data with backups stored in the cloud which can be restored to any empty TS7770 system outside TS7770 grids using Cloud Connect technology. Version retention is enabled ensuring previous copies can be retained for any duration to meet any RPO requirements. These new capabilities are supported in IBM Cloud, AWS S3, IBM Cloud Object Storage on-premises, and RStor.

Multi-factor Authentication

Access to data is also managed using various multi-factor authentication solutions. Dual control security authentication is offered on IBM enterprise and mainframe-oriented storage solutions—implemented with an innovative "maker" and "checker" approach to proactively reduce the risk of human error for accidental deletion and malicious damage.

Cyber resilience in IBM Z environments, ensuring continued operations no matter the cause, involves sophisticated networking that works in close harmony with mainframe processors and storage.

Cyber Resilient Networking in IBM Z Mainframe Environments

Networks play a critical role in modern IBM Z mainframe environments, providing fast and efficient movement of data both across the data center and around the globe. Data moves between the mainframe, storage, and backup systems using FICON and Fibre Channel (FC). These transports can be extended over IP links for global communications as well as for disaster recovery solutions.

Cyber resilient networks include features to provide:

- Encryption in flight and at rest—that protects the business by making data unreadable and unusable when data is exposed or exfiltrated.
- High availability—which ensures that data, the lifeblood of the business, can be used when networking components fail or are compromised.
- Data immutability—write-once-read-many-times (WORM) and tape air gaps protect data from logical corruption, both from malicious attacks such as ransomware and from inadvertent mishaps.
- Data transfer automation and management—that transparently enables the use of various cloud resources and IP networks, enabling multiple redundant data copies for disaster recovery.

IBM b-type Networking Solutions

IBM b-type networking solutions, provided through a partnership with Brocade stretching back more than three decades, are designed, developed, and tested in collaboration with the entire IBM Z family: mainframe processor, IBM storage for mainframe, and IBM tape systems to ensure interoperability.

The IBM b-type family provides storage networking solutions that are used to build highly resilient mainframe environments with emphasis on high availability, encryption, data transfer automation, and immutability. IBM b-type network offerings for the Z mainframe environment include FICON SAN solutions as well as FCIP and IP Extension (IPEX) technology that enables both the local and global movement of mainframe data. Some IBM b-type features that enable more resilient, efficient, and secure data movement in IBM Z environments include:

- Secure data transmission—encryption is applied to selected data across the WAN to achieve comprehensive encryption of data in flight.
- Data compression—maximizes network efficiency while reducing data transport costs.
- Load balancing and transparent failover—traffic is shared across all available logical network elements, removing any single points of network failure with self-healing systems to provide maximum protection and reliable data delivery.
- Network insights—advanced analytics help mainframe-driven enterprises monitor network operations, performance, and quality of service to reduce the time to problem resolution.
- Network validation and testing—increases confidence that mission-critical networks will support production environments with built-in traffic generator tests and other techniques to measure and verify network SLAs.

Advancements in Data Path Security

Over the past few years, innovation within all the data path elements has continued at a brisk pace. IBM has introduced a number of new networking features to enhance the cyber resilience of IBM Z environments, including Multi-Hop configuration supporting in-flight encryption, forward error correction, FICON Dynamic Routing, read diagnostics, and IBM Health Checker for z/OS. The IBM development work within the domains of encryption, high availability, and data immutability deserves a closer look.

Encryption

Beginning with the latest IBM Z models, IBM introduced the concept of "pervasive encryption." This approach offers the ability to encrypt data on storage media completely transparent to applications. It decouples encryption from data classification, reduces the risks associated with undiscovered or misclassified sensitive data, makes it more difficult for attackers to identify sensitive data, helps protect all of an organization's digital assets, and significantly reduces the cost of compliance.

Pervasive encryption leverages a suite of complementary technologies within IBM z/OS, IBM Storage for mainframe, and IBM b-type networking solutions to encrypt data at the host level, in flight across the network, and at rest in storage. IBM Z in concert with IBM DS8900F and TS7700 provide encryption capabilities within the processing and storage environments, and IBM b-type directors and switches encrypt data as it is transferred to production and backup solutions.

SANs are crucial to modern data processing, especially in mainframe environments. As mentioned previously, IBM has introduced Fibre Channel Endpoint Security, which ensures data is accessed only by authorized server and storage devices. This creates a trusted storage network that encrypts data both in flight and at rest without requiring application changes.

High Availability

Along with efficiency and processing power, enterprises choose mainframes because of their extremely high availability required for real-world mission-critical applications. IBM Z leverages a variety of internal and external strategies and technologies to increase its system availability, including ensuring isolation of workloads at scale, and Instant Recovery, which reduces the impact of planned and unplanned downtime.

Replicating data and workloads to remote nodes over the network remains a cornerstone of IBM Z high availability. Metro and Global Mirror technologies combined with b-type networking high availability features enable mainframe-driven organizations to build global fabrics that are highly resilient to both cyberattack and natural and manmade disasters.

Specifically, load balancing of all IP WAN circuits available, automatic failover and recovery of a single WAN failure, data compression, encryption, traffic generators for testing the network, and in-depth analysis tools to troubleshoot network issues enhance and increase b-type networking availability.

Cloud resources have become central to cyber resilience and high availability strategies, and IBM Transparent Cloud Tiering (TCT) enables hybrid multi-cloud storage architectures in IBM Z environments. TCT allows organizations to introduce hybrid cloud as a new storage tier for data archiving, long-term retention, and data protection in IBM Z environments. Without any performance impacts, TCT offloads data movement responsibilities for backup and archive operations from the mainframe to IBM storage DS8900F storage systems and/or IBM TS7700 virtual tape libraries, dramatically reducing mainframe CPU utilization and freeing resources for business applications.

Data Immutability

Backup, recovery, and archive strategies that incorporate points where data cannot be changed, and therefore corrupted, are becoming increasingly popular as a means to achieve cyber resiliency. Two of the most common options are write-once-read-many-times (WORM) data storage and systems that provide natural physical or logical barriers called "air gaps."

Mainframe-driven organizations can build cyber resilient topologies that incorporate air gap protection by replicating data copies across high-performance WANs built with IBM b-type networking devices. Data flows to IBM TS7700 VTL systems that are integrated with IBM tape storage. A logical air gap where the TS7700 is not connected to the internet and a physical air gap, created when valuable data copies are systematically removed and physically isolated from the TS7700, ensure that data is protected from malicious or inadvertent corruption.

The Bigger Truth

In modern organizations, a narrow focus on cybersecurity—identifying and preventing threats from malicious actors—is evolving into a broader approach known as *cyber resilience*, where organizations assume data breaches and failures occur, and plan for recovery and continued business operations.

Nowhere is cyber resilience receiving more attention than in mainframe-driven organizations. Mainframe utilization is as robust as ever, if not more so. Because mainframes are used in almost every sector of modern worldwide commerce, the network performance and the security of data in flight is crucial to 21st century business around the globe.

The b-type networking family—as a result of decades of collaboration between Brocade and IBM—provides a wide range of features and functionality that enable pervasive encryption and very high systems availability. IBM b-type networking components work closely with IBM Z, IBM DS8900F, and TS7700 elements to produce highly resilient data processing, storage, and network environments.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188