MODEL 9

PROTECTING MAINFRAME DATA FROM CYBER THREATS

BACKGROUND

Over 70% of the world's corporate data is stored on mainframes and most Fortune 500 companies still rely on the mainframe platform to generate and process their core business data. For this reason, the mainframe is a critical platform to protect from cyber attacks.

The mainframe is a highly secured platform due to its centralized architecture, authorization controls, audit tools and encryption capabilities. However, the mainframe is not invulnerable. The modern mainframe runs Linux, Java and web applications, and is serving transactions and data using APIs over TCP/IP. **Modern workloads enable the mainframe to remain a core component of business data processing, but also expose it to modern threats and vulnerabilities.**

One of the increasingly popular types of cyber threat in recent years is the ransomware attack. The cost of global ransomware damages reached $5B in 2017 and made data inaccessible for 2 or more days in most cases[1]. With hundreds of variants, ransomware attacks are becoming more sophisticated as they expand to more and more platforms. **The mainframe's massive batch processing capabilities and powerful encryption features, make it a perfect target for ransomware attacks.** Recent public reports[2] of security breaches in US government agencies, airlines and financial institutions, all mainframe-based organizations, stress the importance of mainframe data protection and recovery capabilities in case of an attack.

KEY FEATURES

Create secured backup copies, directly to any storage attached to the network, either on-premise or in the cloud

Isolate backup copies off-platform, or use immutable (WORM) storage, for enhanced protection

Improve RPO with multiple, consistent recovery points, without having to expand existing DASD capacity

Recover and restore data quickly, directly from any storage attached to the network, either on-premise or in the cloud

Avoid vendor lock-in, via a software-only, hardware-agnostic solution

Optimize MSU consumption, by utilizing zIIP engines to create protected backup copies

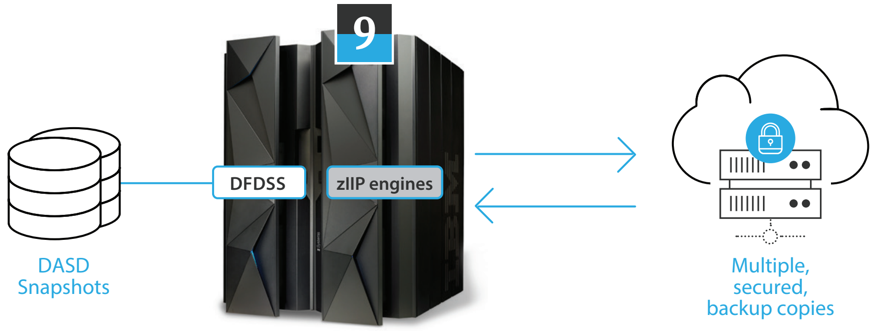
Enhance data protection, with end-to-end encryption

REQUIRED CAPABILITIES

Ideally, companies should be **making frequent data backups** to ensure compliance with Recovery Point Objectives (RPO) in case of data corruption. Backup copies should be **encrypted**, to make sure data is not tampered with over the network, and **stored on isolated, offsite storage platforms.** The use of **immutable storage** for backup copies is also recommended for improved protection against cyber corruption. Companies should **regularly test their ability to recover** their data from such backup copies **via bare metal recovery** procedures and without relying on the integrity of any compromised system. Finally, the backup storage system should **offer the right economics** to enable the required frequency of secured backup copies.

PROTECTING YOUR MAINFRAME WITH MODEL9

Model9 provides an industry-first solution for mainframe cyber threat protection and business resumption, enabling z/OS customers to create highly secured, off-platform backup copies and quickly recover mainframe data in case of an attack – all at minimal cost. When combined with storage snapshot technologies (such as Flashcopy), Model9 also improves RPO by enabling multiple, consistent recovery points without having to expand existing mainframe DASD storage capacity.



Model9's patented technology uses DFDSS as the data mover to create data-set backups and full-volume dumps directly on any storage attached to the network, either on-premise or in the cloud. Using pervasive immutable (WORM) storage solutions as the target for backups ensures that all copies are protected and cannot be tampered with. While all data are compressed before leaving the mainframe, end-to-end encryption can be applied for even more enhanced data protection. In addition, Model9 supports stand-alone restore directly from any storage attached to the network, both on-premise or in the cloud, providing fast data recovery at any location – without relying on an existing mainframe operating system.

CERTIFIED STORAGE SOLUTIONS

aws Microsoft Azure NetApp Hitachi Vantara DELLEMC IBM Cloud