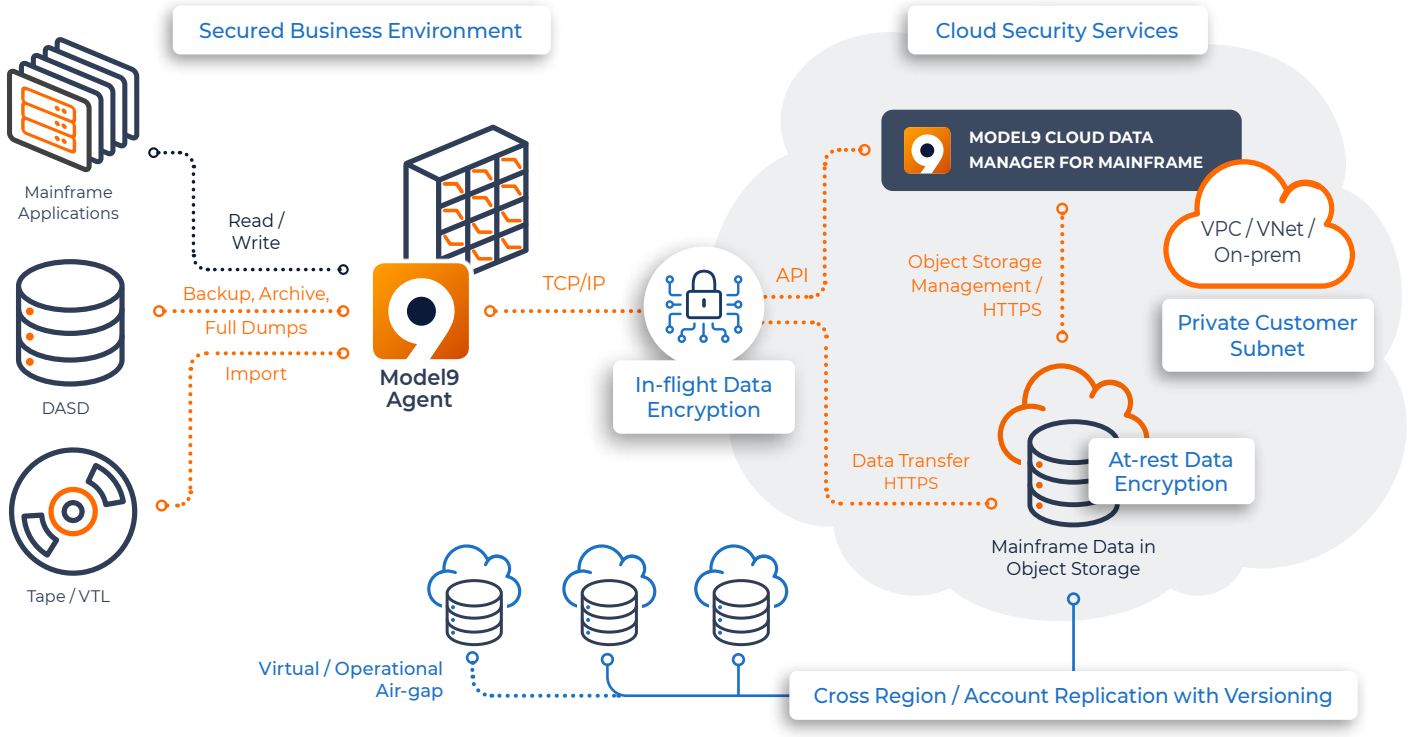
MODEL9 PROTECTS AND ENSURES YOUR MAINFRAME DATA IS ALWAYS ACCESSIBLE

The Model9 platform has strong cyber security measures, data resiliency and fast bare metal disaster recovery

OVERVIEW

Ensuring your mainframe data is protected and always accessible is a critical part of the Model9 platform architecture. Model9 replaces legacy mainframe data management tools with a modern and secure backup, archive, space management, and disaster recovery solution in either the private, public, or hybrid cloud.

MODEL9 ARCHITECTURE FLOW FOR CYBER RESILIENCY



Model9 has built-in security measures using pervasive immutable (WORM) storage to ensure all copies are protected. Data is also compressed, can be air gapped, and provides end-to-end encryption. Additionally, multiple copies can be maintained to preserve gold copies of backups. Should a disaster occur, Model9 makes it simple to prepare and use a stand-alone system so you can confidently perform a bare metal recovery of your data from anywhere.

A ROBUST APPROACH TO CYBER SECURITY

Model9 works with cyber security partners to provide protection from ransomware attacks by creating immutable copies either on-prem or in the cloud. When sent to cloud object storage, the mainframe data can also be air-gapped — which means an offline copy is maintained and can never be maliciously accessed.

Additional security measures include:

- Data transformation services can be used without access to a mainframe to convert the data and consume it on cloud platforms.
- Deploying the Model9 management server on a virtual private cloud (VPC) or locally in a secure on-premises environment.
- Uses mainframe security protocols when deploying the Model9 agent on the mainframe.
- Running periodic vulnerability scans.
- Protection from data loss by utilizing object storage capabilities such as versioning, immutability (WORM) and encryption.

HIGH MAINFRAME DATA RESILIENCY

Model9 ensures that your mainframe data is available, no matter what occurs. This is done using a combination of backups, encryption and access restrictions based on mainframe security protocols.

Model9 ensures data resiliency with:

- Secure backups of mainframe data in mainframe format on object storage, including full volumes or data sets both active and historical.
- End-to-end encryption for data in-flight and at-rest.
- Auditing capability provided in Model9 activity logs and z/OS SMF records.
- Standard mainframe security interfaces (SAF) control access and activity authorizations.
- Use of immutable (WORM) copies, versioning, and air-gap features on cloud object storage.
- Stand-alone restore directly from the cloud with no dependency on the compromised system.

FAST BARE METAL DISASTER RECOVERY

When a malicious attack or disaster strikes, Model9 makes it simple to use a stand-alone system so you can confidently recover the data from anywhere should a disaster strike. Model9 performs a bare metal recovery from cloud storage to a clean mainframe environment.

Model9 recovery includes the ability to:

- Recover quickly from full volume backups.
- Perform a bare metal recovery over TCP/IP.
- Utilize clean room recovery capabilities to examine data off the mainframe.
- Use simulate options to validate data before recovery.
- Easily initiate data set level recovery.
- Mitigate risk associated with recovery.

BENEFITS OF MODEL9 CYBER RESILIENCY

model 9 **FOR MORE INFORMATION:** CONTACT@MODEL9.IO, WWW.MODEL9.IO