SSH

Secure Data Communications for IBM z/OS Mainframe: Buyer's Guide

Index

How to Use this Guide

Mainframes are often the backbone of a large-scale organization's data infrastructure. Responsible for processing massive quantities of data and internet-based transactions simultaneously, mainframes are not typically the primary target for hackers. Their technology is considered to be rather esoteric and their security posture robust by default.

But many mainframes still use File Transfer Protocol (FTP) to transmit data. Information shared via FTP is generally unencrypted, untracked and in plain text format, making the mainframe's data communications highly susceptible to man-in-the-middle attacks.

All it takes is one malicious hacker to cause enterprise-wide outages, regulatory violations, confidentiality breaches, reputational damage, and much more, so investing in a solution to safeguard your data communications should be on every organization's list of priorities.

This white paper will serve as your guide to choosing a solution that will deliver robust secure data communications to your mainframe. We'll explore common challenges and suggest the ideal measures to resolve them so that you can choose a mainframe data communications solution robust enough for today's vulnerabilities and tomorrow's threats, even through the advent of Quantum Computers.

Challenge One: FTP Isn't Secure Enough

When it comes to mainframe data communications, FTP use is a liability and a risk. Not only does this protocol send sensitive data over the internet in clear text format, but it doesn't participate in any form of client-server authentication to validate who's receiving and sending this information. This can shield hackers from detection as they exploit confidential information, like transaction data.

If administrators wish to run integrity checks, they have to manually input command code to pull up diagnostic information, which, as one can imagine, can be an extremely time-consuming process. Manually converting FTP tasks to SFTP (or Secure File Transfer Protocol) is a laborious task that can be unfeasible for a large-scale organization, given how many different scripts they have. This reveals a need for a solution that will make this transformation quick and painless.

The Solution: Seamless Transitioning From FTP to SFTP

You'll want a mainframe data communications solution that prioritizes encryption and authentication protocols to transfer data and facilitates a smooth transition from FTP to SFTP. When selecting a solution, be sure it can:

- **Perform server authentication on its own**
- **Automatically conduct data integrity checks**
- **Provide closer integration with the mainframe for secure and comprehensive access to different data types**
- **Support SOCKS proxy for protected data conversion and transmission**
- **Engage in data compression to save network bandwidth**

Challenge Two: Complex Setup & Shortage of Experts

All SFTP solutions run on a UNIX command interface, which can be tricky to set up for those unfamiliar with UNIX's setup process. Many customers get frustrated because the setup requires them to reroute the traffic to use OpenSSH, and it can take months to rewrite all the Job Control Language (JCL) scripts to achieve this.

This process is made more challenging by a shortage of experts. To undertake the rerouting of traffic to use OpenSSH, organizations are likely to require expert support. Unfortunately, there aren't many mainframe security experts available to offer their expertise. With OpenSSH already integrated into various operating systems, demand for customer support on mainframe issues far outnumbers the supply of available professionals ready to help.

The Solution: Simple Setup & Ongoing Solution Support

Users are comfortable with the Interactive System Productivity Facility (ISPF) interface, which has been a pillar of mainframe navigation for many years.

Therefore, mainframe data communications solutions that mimic or incorporate this structure into their installation process will prove invaluable to your IT toolkit.

Specifically, you want a mainframe data communications solution that provides a seamless transition to secure data transfers, and does not require JCL modifications, break your existing file transfers, or need manual changes to scripts. You'll also want to look for solutions that can integrate with z/OS for compatibility with Resource Access Control Facility (RACF) features. This allows your mainframe to conduct:

- **Credential checks**
- **User-client authentication**
- **Asset classification**
- **Permission setting**
- **Privileged access user allocation**

To resolve the issue of a shortage of experts, make sure that your chosen solution:

- **Offers 24/7 support and professional services**
- **Possesses the capacity and capability to apply hotfixes to urgent matters**
- **Provides a clear-cut and detailed troubleshooting guide for minor disturbances**
- **Continues to evolve to account for industry updates and mainframe changes**

Challenge Three: Manual Effort & Disjointed Mainframe Communication with Distributed Platforms

In standard settings, data that needs to be moved between a mainframe and a distributed system has to be manually converted to a viable and actionable format — but it can be a convoluted process. Not only does it require configuring thousands or even millions of files by hand, but it also leads to data transformations that require further handling.

There are many components to keep track of as data is converted and transmitted from the mainframe to a distributed system and vice versa. Administrators might ask themselves: Who has the authority to manage this process? Where exactly are these data files going to be stored? What are the access privileges for each translated file?

With so many steps to consider, the manual effort associated with managing mainframe data communications can be daunting and potentially unmanageable. And this effort is made all the more challenging by the different coding languages at play, which can cause unwanted hiccups if data is not converted correctly.

Tools like SFTP help to seamlessly transmit and convert encrypted data from Linux-based, Windows, and z/OS environments, but what happens when data is lost in translation? Often, mainframe communication programs advise users to avoid complicated actions, leaving them to resolve roadblocks independently, requiring even more time and effort.

Manual management isn't a viable method for resolving communication errors or discrepancies, as administrators can't always carve out time to find alternative solutions. It's also not guaranteed that an administrator will securely and accurately resolve these issues as well as an appropriate mainframe data communications solution could.

The Solution: Reliable Automation & Universal Protocol Standards

To relieve your organization of the burden of manual tasks, look for a mainframe data communications solution that enables automation and speaks the same language across all operating systems. You'll want to look for the following:

- **Flexible cross-platform and mainframe-to-mainframe data conversion**
- **FTP/SFTP site command extensions**
- **Automatic conversion within user-set parameters**
- **Transparent and comprehensive conversion settings**
- **Debugging and the ability to add special fixes to code to work with specific servers**
- **Capable of working cooperatively with all SSH and SFTP tools and programs**
- **Interacts well with z/OS data**

Abiding by SSH's RFC protocol standards, including RFC 4251, RFC 4252, RFC 4253, and RFC 4254, also helps create uniformity in mainframe communications by keeping all SSH-reliant programs aligned with the same language guidelines. Choosing a mainframe data communications solution compliant with SSH RFCs is a step toward minimizing latency and miscommunication.

With these features at your disposal, you can streamline your workload while keeping all conversion channels safe and secure.

Challenge Four: Achieving Compliance

Enterprises are no strangers to compliance requirements, especially regarding data confidentiality. While there are a variety of regulations, internal company policies, and laws outlining what it means to safely handle and send data over the internet, all of them have one baseline requirement in common: encryption.

How your enterprise achieves encryption depends on the standards that apply to your country and the type of organization you're managing. For example, government entities in the US must transfer and store all data using algorithms that are compliant with the Federal Information Processing Service (FIPS) standard.

Another universal prerequisite for most businesses is a customer support service for around-the-clock assistance. This is particularly vital in cases where financial information has been compromised or transactions have been inaccurately performed.

Researching regional, national, and global cybersecurity requirements can quickly become overwhelming, but keep the above three baseline requirements in mind. You can also peruse guidebooks from NIST and ECSO, two of the world's leading cybersecurity organizations, to understand what's expected from all entities transmitting data online. Or, you can find a mainframe data communications solution that already checks off these boxes for you.

The Solution: Support For Compliance With Various Regulations

To maintain industry compliance, opt for a mainframe data communications solution that meets PCI-DSS, SOX, HIPAA, FISMA, and FIPS compliance, and offers 24/7 support from experienced IT professionals. Additionally, it helps to have a solution that, at a minimum:

- **Sends all information through an encrypted link**
- **Provides immediate, around-the-clock support for urgent issues**
- **Offers extensive consultancy for larger compliance projects**

Even with a highly compliant mainframe data communications solution in place, devote some time and resources to training your employees on basic security practices to minimize violations caused by improper data handling. Having administrators and IT teams regularly refresh their knowledge of compliance policies and updating them on new ones can mitigate the risk of accidental violations.

Challenge Five: High Financial Costs

Mainframes are crucial for organizations that function nationally and internationally, but the costs of maintaining them in the long term can add up rather quickly. Besides general licensing fees, customers are also billed for their CPU usage. This creates a constant challenge of balancing enterprise productivity with computational capacity.

To enhance mainframe performance, some organizations have begun adopting cryptographic accelerators — a type of co-processor designed to supplement CPU functionality by taking over computationally intensive processes. They're also more inherently secure than typical CPUs because of their embedded cryptographic structure, utilizing industry-recommended key algorithms to prevent brute force attacks. Nonetheless, not all cryptographic accelerators achieve much in terms of saving businesses money.

The Solution: Offloading

Discovering more effective ways to offload labor-intensive operations from CPUs will help eliminate inflated usage costs. Cryptographic accelerators aren't a bad idea for those wanting more robust computational security, but to cut costs, mainframe data communications solutions will need to:

- Run more extensive operations on parallel CPUs billed in a different way
- Support zIIP processing units in integration with cryptographic accelerators
- Keep keys invisible for harder detection by malicious actors
- Automatically allocate tasks to the appropriate hardware unit
- Offer user control over computational processes

Challenge Six: Minimal Support for Public Key Infrastructures (PKI)

Today, managing data securely over networks and between devices is largely accomplished through public key infrastructures, or PKIs. This form of encryption uses public and private keys to encrypt and decrypt sensitive data between two authorized users, applications, and devices. These key pairs are generated by algorithms that are extremely difficult to break through, making PKIs a strong tool for overall IT security.

The problem is that many solutions and applications don't fully support PKI integration. As mentioned, server authentication is often missing in many security applications, which is crucial in identifying where data is being transmitted to and received from.

Certificate validation is also missing in most mainframe data communications solutions that rely only on OpenSSH, which offers basic key-based encryption and data transmission. Metadata embedded in PKI certificates provides valuable ownership information. This information is divulged by certificate authorities (CA) working in tandem with third-party PKI providers, which many mainframe solutions don't properly support, producing a vulnerability where stronger public key authentication could be applied.

The Solution: Support for Enterprise PKI

Mainframe data communications solutions that support both server and user authentication with PKI should be on every organization's wishlist, but keep in mind that with PKI comes the responsibility of managing these certificates and keys. Standout solutions will come with a full range of PKI features, including:

- **Integration with RACF programs viable on z/OS to keep PKI certificates in RACF secure stores**
- **Complete inventories of PKI certificates across all different kinds of use cases**
- **Revocation privileges with the capacity to set automatic revocation seasons**
- **Key management capabilities that help administrators organize and monitor massive loads of credential and authentication data**

Challenge Seven: Preparing for the Quantum Threat

Quantum computers have all enterprises scurrying for a future-proof cybersecurity framework. Once unleashed, these devices will have the ability to break through safeguards relying on classical cryptography within mere seconds. Experts aren't sure when exactly these advanced tools will be available, but suggest that all infrastructures prepare for their arrival.

In fact, there's already a US law called the Quantum Computing Cybersecurity Preparedness Act, which will introduce requirements for federal agencies to migrate existing cryptographic environments into quantum-proof architectures.

However, experts suggest straying away from a complete overhaul of existing systems as this could cause latency issues, trigger enterprise-wide manual errors, and organization-wide disruptions. Instead, opt for a slow and natural transition by adopting elements of post-quantum cryptography into your enterprise's IT network.

The Solution: Choosing A Product With Post-Quantum Cryptography

To best safeguard your assets and data as the quantum age approaches, find a mainframe security solution to help your enterprise slowly ease into a quantum-proof environment. Look for features like:

- **Algorithms that include both quantum-resistant and traditional cryptography**
- **Scheduled updates to promptly enhance existing quantum-safe algorithms**
- **Compliance with quantum-related regulations, including emerging laws**
- **Quick and easy setup and assimilation**

What is Tectia Server For IBM z/OS? How Does it Overcome These Challenges?

Tectia z/OS Edition is SSH's answer to all of these challenges, protecting your organization with a suite of features that epitomize the best of high-speed, integrative, and future-proof mainframe security.

With support for Multiple Virtual Storage (MVS) and UNIX System Services (USS) file systems and automatic EBCDIC-ASCII character conversion, **cross-system communication** is as it should be: automated, quick, and stable. For mainframes that utilize IBM Crypto Express Cards (CEX), Tectia z/OS will direct or offload cipher functions to the co-processors in CEX through Integrated Cryptographic Service Facility (ICSF) software, **accelerating cryptographic operations**.

For further protection, Tectia z/OS eliminates manual steps with **automation capabilities** throughout its entire interface, greatly relieving businesses from the threat of human error. Additionally, Tectia z/OS allows **logging and auditing** using System Management Facility (SMF) records and Syslog tools for real-time performance metrics and security analytics. And for organizations looking to safeguard against future threats, Tectia comes in upgraded editions for **Zero Trust** and **Quantum-Safe** security.

Ready to try Tectia z/OS? Download our free 60-day trial or get in touch with SSH today to learn how Tectia z/OS can solve all your mainframe security needs.

SSH

We'd love to hear from you

Get in touch
with our experts
around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION

Karvaamokuja 2b, Suite 600

FI-00380 Helsinki

Finland

+358 20 500 7000

info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.

434 W 33rd Street, Suite 842

New York, NY, 10001

USA

Tel: +1 212 319 3191

info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.

35/F Central Plaza

18 Harbour Road

Wan Chai

Hong Kong

+852 2593 1182

info.hk@ssh.com

Let’s get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world? We’d love to hear from you.

Request a Demo