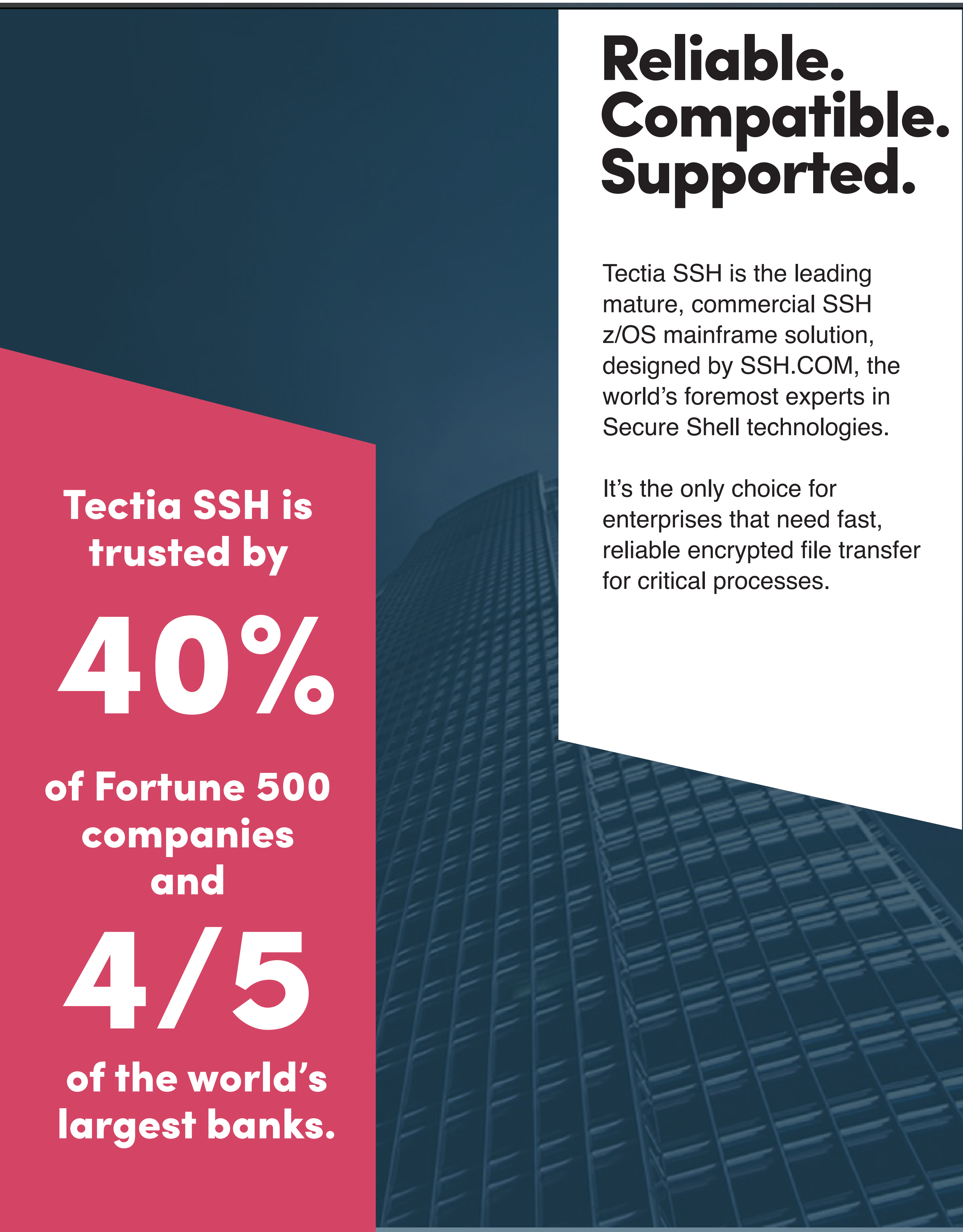
Tectia® SSH Server for IBM z/OS Datasheet

What is Tectia SSH Server for IBM z/OS?

Protect access to your mainframes and secure encrypted data flow with the most trusted software in the industry. Tectia is the proven market leader that combines enterprise-grade reliability with high performance.

Enterprise-grade security for big data in transit.



Reliable. Compatible. Supported.

Tectia SSH is the leading mature, commercial SSH z/OS mainframe solution, designed by SSH.COM, the world's foremost experts in Secure Shell technologies.

It's the only choice for enterprises that need fast, reliable encrypted file transfer for critical processes.

Tectia SSH is trusted by

40%

of Fortune 500 companies and

4/5

of the world's largest banks.

The easiest & safest way to put big data in motion

WORK NATIVELY WITH Z/OS DATA SETS

Out-of-the-box support for direct MVS data set access, interactive MVS data set listing, interfacing with JES, I/O streaming, configurable ASCII/EBCDIC code set conversions, ISPF application, and FTP compatibility commands, such as the SITE command.

ELIMINATE UNSECURE FTP FILE TRANSFERS

Here's a simple rule: never transfer sensitive business information over FTP. We provide automated FTP-SFTP conversion and transparent FTP tunneling which is the fastest way to transfer files securely. Risk mitigation should not cost you time and money.

AUDIT AND COMPLIANCE REQUIREMENTS MET

Tectia SSH Server for IBM z/OS helps organizations of all types and sizes meet internal and external compliance requirements including PCI-DSS, SOX, HIPAA, FIPS, FISMA, and many others.

BUSINESS CONTINUITY WITH UPDATES & SUPPORT

Lower lifecycle costs and mitigate the risk of your legacy open source SSH implementation. Let us worry about the latest updates, business platform requirements and accountability. Tectia is rigorously tested and offers the proven reliability demanded by enterprises that require up to 24/7 support and maintenance.

Is Tectia right for you?

Terabyte file transfers

Cut the costs of secure transfers in high-performance computing, global processing, biotech, genetics, experimental physics, chip design, large-scale simulation etc.

Governmental & federal agencies

Compliance with FIPS-certified cryptography regulations and PKI support with X.509 certificates.

Enterprise backups

Handle large file transfers for backups, disaster recovery, and data synchronization.

Infrastructure

Enjoy rapid, no-footprint deployment.

Open source users

Lower your lifecycle costs and mitigate the risk of your legacy open source SSH implementation.

Smartcards

Securely manage smartcards, SecureID or 2-factor authentication for SysAdmins.

Regulated organizations

Gain and remain compliant with PCI-DSS, Sarbanes-Oxley, HIPAA etc.

z/OS mainframes

Run processes and databases on z/OS that should be encrypted – replace FTP or Telnet, or securely tunnel FTP.

Take control of your SSH keys

Enforce restrictions, such as minimum key length, while gradually migrating from user-controlled to admin-controlled public key authentication using both OpenSSH and SSH2.

Functional highlights.

- Encrypted compressed secure file transfer via SFTP and SCP command line tools.
- Automatic application tunneling, nested tunnel support and transparent FTP tunneling
- Fully interoperable with OpenSSH
- Fully compliant with PKI standards
- Smartcard authentication support, including CAC and PIV cards for federal agencies

FEATURES AND BENEFITS	
Ease of use	• ISPF application for installation and configuration • Configurable FTP fallback option for controlled and phased deployment • System-wide and user-specific file transfer profiles • Listing of MVS data sets as files and folders for easy interactive command line
User and server authentication	• Authentication and access control through SAF calls to RACF, ACF2, and TSS • User authentication with passwords • User and server authentication with X.509 certificates • User and server authentication with public keys • Logging and auditing using SMF records and Syslogd facilities
Secure File Transfer Protocol	• Transparent, automatic FTP-SFTP conversion • Transparent FTP tunneling • Multi-terabyte file size support • Strong encryption of data • Strong packet-by-packet file integrity checking • SFTP and SCP command-line tools for interactive and unattended use • Logging and auditing using SMF records and Syslogd facilities • SFTP Extensions for SITE command support • Embedded file transfer advice strings in file names for third-party clients • Support for MVS and USS file systems • Automatic EBCDIC-ASCII character conversion • Interactive MVS data set listing capability • Interfacing z/OS Job Entry Subsystem (JES)
Security	• Automatic transparent encryption of data-in-transit, including user ID and password • Strong confidentiality and data integrity • Hardware acceleration of cryptographic operations • Support for U.S. NIST FIPS 140-2 Certified hardware acceleration • Firewall-friendly architecture • Multi-tier security architecture • Configurable re-keying policies • Multi-channel support - multiple secure sessions are multiplexed to a single TCP/IP connection • Compliance with the IETF Secure Shell standards
Secure application connectivity	• Automatic tunneling • TCP/IP port forwarding • Automatic encryption of data in transit • Transparent TN3270 security with Tectia Client
Platform Support	IBM z/OS versions 2.2, 2.3 and 2.4
Supported cryptographic algorithms by hardware	• AES (128 / 192 / 256 bit) • 3DES (168 bit) • SHA-1 and SHA-2 hash algorithm
Supported cryptographic algorithms by software	• AES (128 / 192 / 256 bit) • 3DES (168 bit) • DSA, RSA and ECDSA public-key algorithms • HMAC MD5, HMAC SHA1, HMAC SHA224, HMAC SHA256, • HMAC SHA384 and HMAC SHA512 data integrity algorithms • Diffie-Hellman (SHA-1, SHA-2 and ECDH methods) key exchange algorithms
Full utilization through ICSF for	• CCF • PCICA • PCICC • PCIXCC • CPACF • CryptoExpress
Supported Authentication Mechanism	• RACF • ACF2 • CA Top Secret

SSH.COM

Finland

SSH Communications Security Oyj
Karvaamokuja 2B
00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communications Security, Inc.
460 Totten Pond Road
Waltham, MA 02451
(781) 247-2100
info.us@ssh.com

Hong Kong

SSH Communications Security Ltd.
35/F Central Plaza
18 Harbour Road
Wan Chai, Hong Kong
+852 2593 1182
info.hk@ssh.com