SSH.COM

Tectia® SSH Server/Client Datasheet

What is Tectia SSH Server/Client?

The most trusted enterprise software for fast encrypted file transfers and secure access. Tectia is the proven market leader that combines enterprise-grade reliability with high performance. Save time, guarantee business continuity and get peace of mind with the leading 24/7 supported SSH (Secure Shell) solution.

Your secure file transfers could be up to 2.5x faster

The gold standard in secure access and encrypted file transfer.

Reliable. Compatible. Supported.

Tectia SSH is the leading mature, commercial SSH server and client 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.

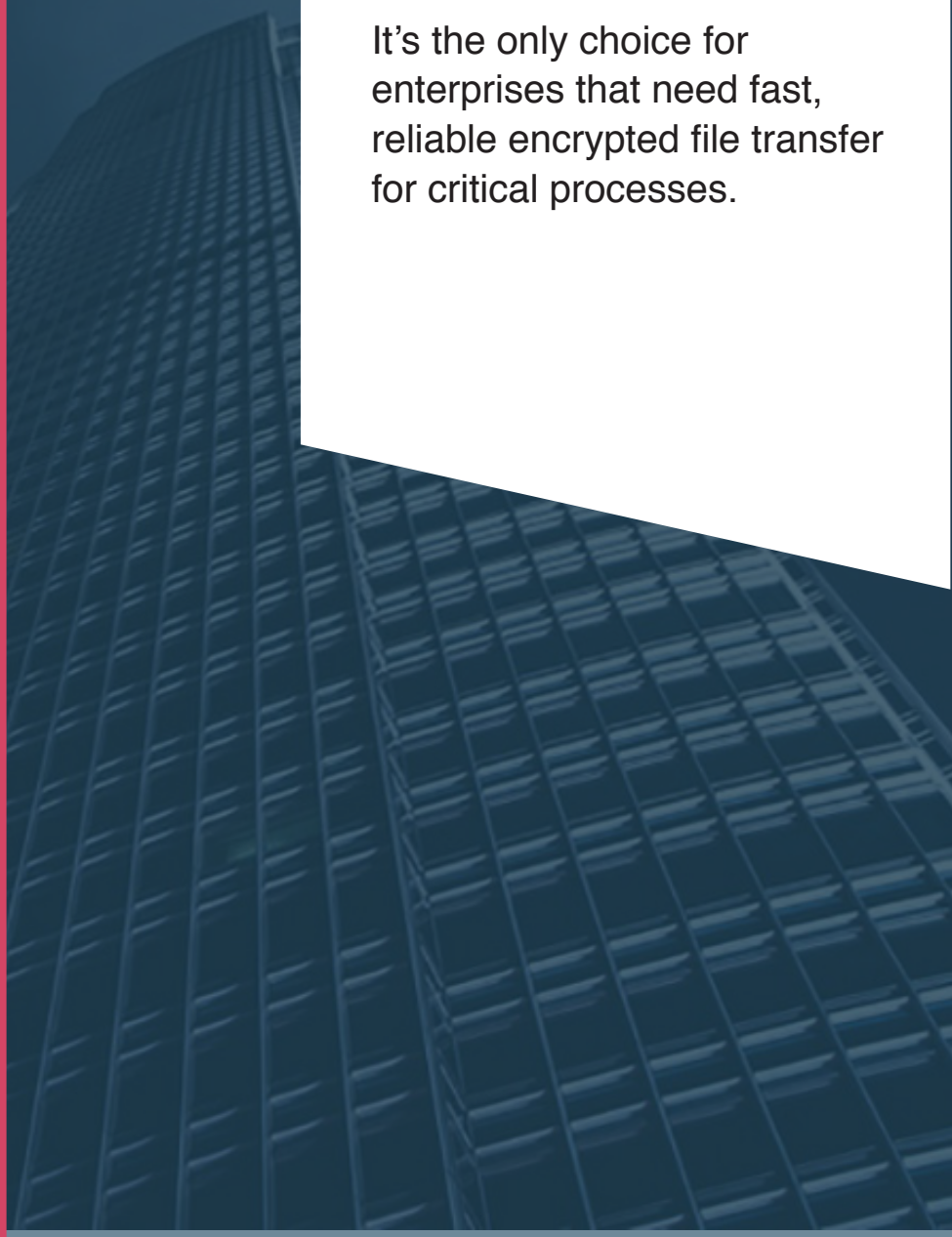
Tectia SSH is trusted by

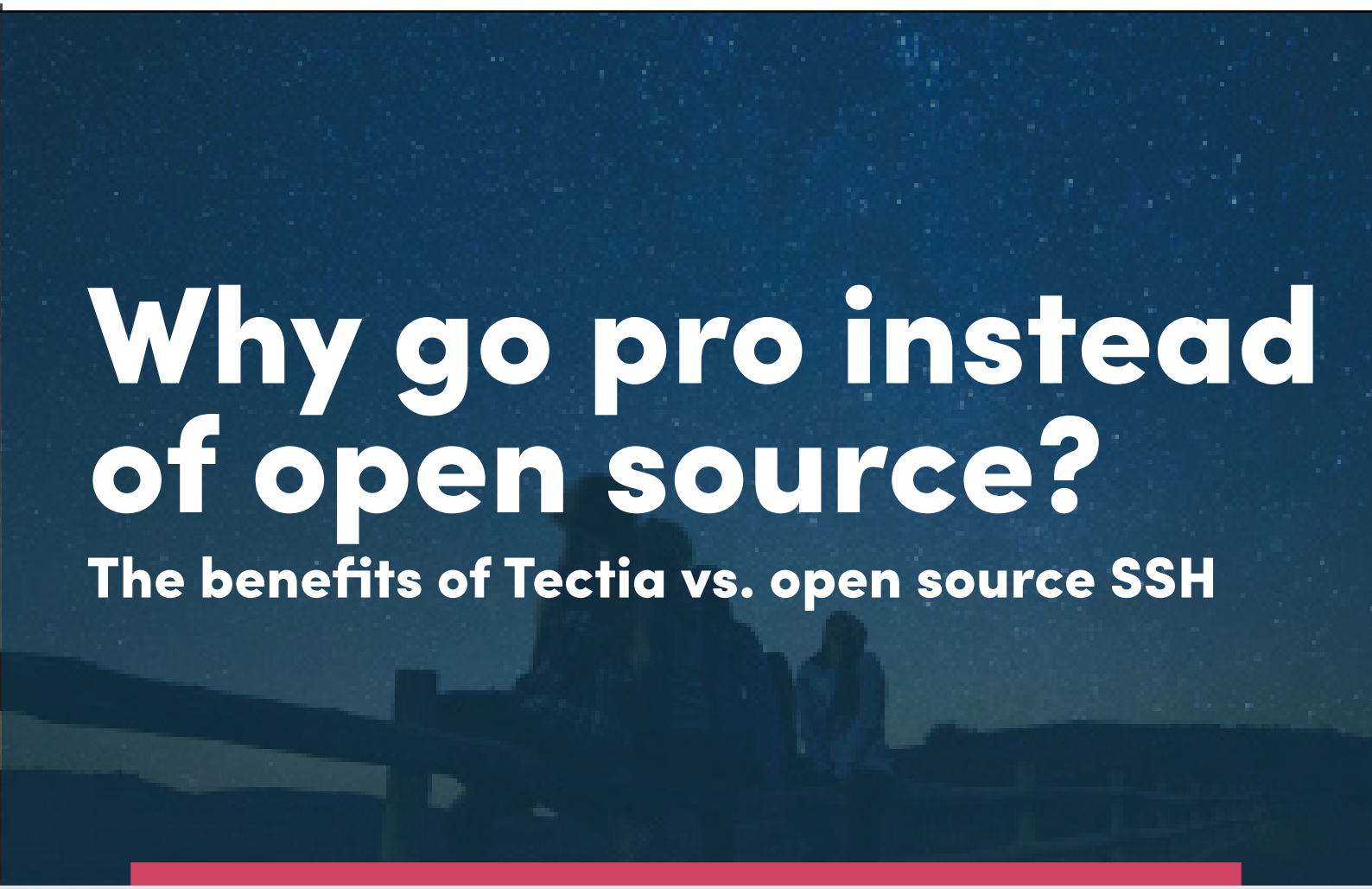
40%

of Fortune 500 companies and

4/5

of the world's largest banks.





Why go pro instead of open source?

The benefits of Tectia vs. open source SSH

SPEND YOUR TIME USING FILES, NOT MOVING THEM

Transfer large files up to **2.5x faster** against the best that open source SSH can deliver. Save time and admin resources by automating processes for remote commands and secure file transfer.

THE ONLY CHOICE FOR DEMANDING ENTERPRISES

Enjoy enterprise-class compatibility with: open source SSH; all popular platforms, including z/OS; a vast array of cryptographic algorithms; and PKI smartcards, including CAC for federal organizations. Enforce security policies with forced remote commands per user/group without giving root access to all users.

BUSINESS CONTINUITY FROM SUPPORTED, UPDATED SOFTWARE

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

NO NEEDLESS TRAFFIC WITH LARGE FILES

Tectia SSH Server/Client can handle massive TB files with configurable compression options to save time and money on every transfer. If there are interruptions, the checkpoint resume feature ensures that the file transfer picks up from the point it got interrupted.

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 keys.

Functional highlights.

- Encrypted streaming secure file transfer via SFTP and SCP command line tools.
- Automatic application tunneling and nested tunnel support.
- Fully interoperable with OpenSSH.
- Fully compliant with PKI standards.
- Smartcard authentication support, including CAC and PIV cards for federal agencies.
- Multi-platform support, including Linux, Unix, and Windows platforms, as well as IBM z/OS mainframes. For more information, see the Tectia SSH Server for z/OS mainframes datasheet.

FEATURES AND BENEFITS	
Compiled and tested packages for all key platforms, including IBM Mainframes	Saves systems administrators tasks of tracking and obtaining updates from multiple sources. Reduces test time as well.
Available long term support versions	Stay with one version of Secure Shell across the enterprise, even as OS versions change.
Smooth integration with AAA infrastructure	Support for multiple authentication systems: including X.509, SecurID, GSSAPI, CAC.
Mainframe support features	Easily convert legacy applications from FTP to SFTP.
Ease of use	Connection profiles.
Interoperable, multi-platform	Tectia SSH Client and Server are fully interoperable with OpenSSH and standard SSHv2-compliant third-party implementations. No issues creating secure connectivity with business partners or within mixed environments.
Premium support	Better business continuity – up to 24x7 available.
Secure File Transfer Protocol features	• Strong encryption • SFTP and SCP command line tools • Multi-gigabyte file size support • Streaming • Resume on re-transfer • Configurable compression
IBM z/OS support	For a complete feature list, see the Tectia SSH Server for IBM z/OS data sheet
Application Connectivity	• Automatic application tunneling • Nested tunnel support • Automated connection set-up • Fully interoperable with OpenSSH • TCP/IP port forwarding • Multiplexing – multiple SSH sessions over a single TCP/IP connection
Security	• IETF Compliant • Configurable rekeying policies • GSSAPI/Kerberos support • OpenSSH key support • Third-party authentication support • FIPS-certified cryptographic module
Supported cryptographic algorithms (partial list)	• DSA, RSA, ECDSA, ED25519 • AES • 3DES • HMAC (MD5, SHA-1,SHA-2) • Diffie-Hellman (SHA-1, SHA-2, Elliptic Curve)
Platform Support	• HP-UX (PA-RISC, IA-64) 11i v3 • IBM AXI (POWER) 6.1, 7.1 • Windows Vista, 7, 8, 8.1, 10 • Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 • Red Hat (x86, x86-64) 5, 6, 7 • Solaris (SPARC, X86-64) 10, 11 • SUSE Linux Enterprise Desktop (x86-64) 12 • SUSE Linux Enterprise Server (x86-64) 10, 11, 12 • IBM z/OS 2.1, 2.2
Authentication Support	• Microsoft CA • Windows Domain • RSA SecurID • Microsoft IAS through RADIUS • FreeRADIUS • PAM • Kerberos • In-built password cache on Windows

ssh®, PrivX®, Tectia®, Universal SSH Key Manager® and CryptoAuditor® are registered trademarks or trademarks of SSH Communications Security Corporation and are protected by the relevant jurisdiction-specific and international copyright laws and treaties. Other names and marks are the property of their respective owners. Copyright © 2019 SSH Communications Security Corporation. All rights reserved.

SSH Communications Security Oyj
Kornetintie 3
00380 Helsinki

+358 20 500 7000
info.fi@ssh.com