



# Enterprise Security Solutions



Effective management of information security risks requires encryption and authentication controls that can protect mission-critical data flows against both external and internal security threats. These threats cannot be eliminated in the network perimeter with firewalls and VPNs alone.



# New Challenges for Information Security

While diversity of information systems and sophistication of attacks against data security continue to grow, protecting sensitive data is becoming increasingly challenging. Proactive management of information security is vital to ensure the integrity of data being accessed and exchanged in the enterprise networks.

Compliance with existing and emerging regulations such as HIPAA, SOX, and Basel II has recently become a top priority, not only for the corporate board, but anyone responsible for delivering IT services to the enterprise or government. Especially confidentiality of customer data such as patient records or consumer credit information is today a regulatory matter that needs to be addressed with necessary technical safeguards such as data encryption. Additionally, centralized auditing and authorization of network connections are among the key legislative requirements on IT.

## Diverse IT Environments Demand Adaptable Security Solutions

In recent years, enterprises have witnessed vast proliferation of employee remote access, integration with partner systems, and wireless network access to internal business applications. As a result, information security threats cannot be eliminated in the network perimeter with firewalls and VPNs alone.

This effect, now known as deperimeterization or disappearing perimeter, requires a more comprehensive, end-to-end approach for securing enterprise networks.

Another challenge for enterprise information security is the heterogeneous nature of today's IT environments. Therefore, enterprise security solutions need to integrate with a variety of third-party products and support multiple platforms, ranging from Windows to Unix/Linux and mainframe systems.



# End-to-End Communications Security

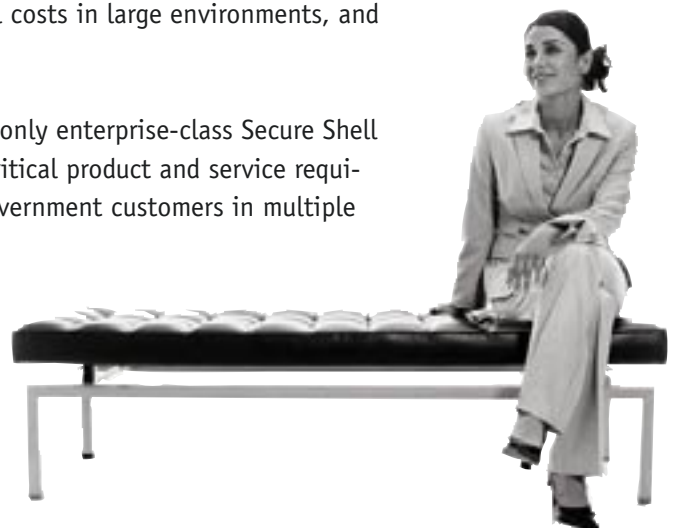
SSH Tectia™ is the leading end-to-end communications security solution for large enterprises, financial institutions, and government agencies. With SSH Tectia, organizations can ensure the confidentiality and integrity of their data communications throughout the network, enabling effective protection against both internal and external security risks.

## Finally, Enterprise-Class Secure Shell for IBM Mainframes

As a pure software solution with support for all major enterprise platforms including IBM mainframes, SSH Tectia adapts to diverse enterprise networks without the need to invest in additional hardware.

The management capabilities of SSH Tectia support centralized deployment, maintenance, and monitoring of communications security, enabling improved regulatory compliance, reduced total costs in large environments, and increased system security.

SSH Communications Security offers the only enterprise-class Secure Shell solution in the market that fulfills the critical product and service requirements of demanding enterprise and government customers in multiple application areas.



# One Solution – Multiple Applications

SSH Tectia solution can address a variety of communications security needs:

## Secure System Administration

- Provides system administrators the ability to remotely manage servers in heterogeneous operating system environments.
- Replaces Telnet, Rlogin, and other unsecured login and remote command execution methods with centrally managed enterprise-class Secure Shell tools.

## Secure File Transfer

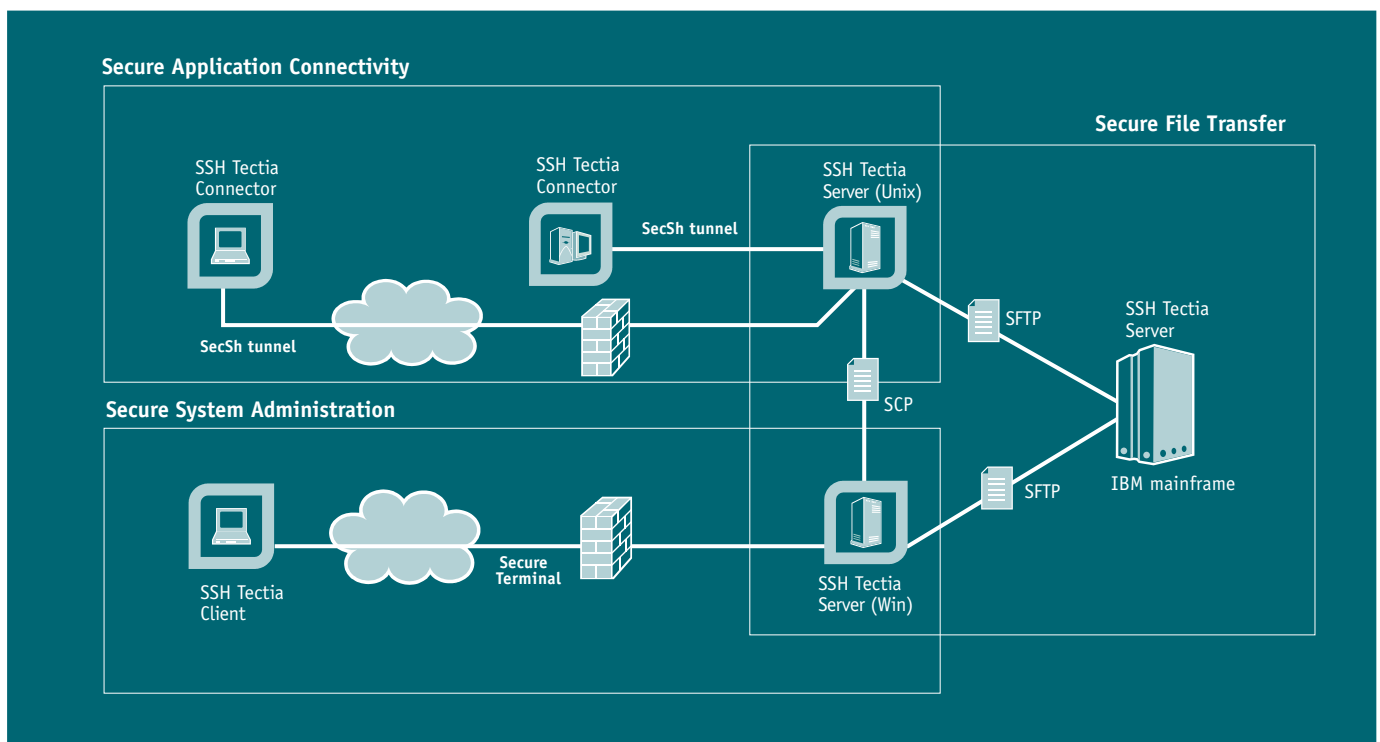
- Enables secure automated and interactive file transfers throughout the network, both for internal and remote file sharing.
- Provides a secure drop-in replacement for FTP (File Transfer Protocol) with application programming interfaces that facilitate effortless transition from legacy file transfers to strong file transfer security.

## Secure Application Connectivity

- Brings end-to-end confidentiality, data integrity, and authentication to application connections between workstations and servers.
- Protects transparently both in-house and commercial business applications without the need to modify the applications or the supporting IT infrastructure.

## What is Secure Shell?

Secure Shell is the standard security protocol used by millions worldwide for secure remote login, remote command execution, and file transfer over TCP/IP networks. Secure Shell was originally developed in 1995 by SSH Communications Security to provide a secure drop-in replacement for Telnet, Rlogin, and FTP.



# Designed for the Enterprise

## Centrally Managed for Reduced Costs

Enterprises can experience a considerable reduction in TCO (Total Cost of Ownership) by automating resource-consuming system management tasks. SSH Tectia allows centralized management of communications security including Secure Shell software deployment and maintenance, configuration management, and environment monitoring, to significantly reduce TCO. Centralized management features also enable fast reaction to new security threats and deviations from security policies, thus improving the overall system security.

## Easier Regulatory Compliance

SSH Tectia can help organizations in multiple industries to comply with existing and emerging regulations with privacy and data security implications. Improved compliance is met with end-to-end communications security, which eliminates the risks of unauthorized external or internal access to sensitive file transfers and other remote connections. Additionally, the monitoring features of SSH Tectia allow centralized logging and monitoring of secured connections including system administrator access – controls that have traditionally been extremely difficult to implement with third-party Secure Shell utilities.

## Effective Risk Management - Strong Encryption and Authentication

SSH Tectia can prevent common network attacks including password sniffing, data eavesdropping, and connection hijacking by implementing strong authentication and end-to-end encryption of remote connections. Incorporating the third generation, high performance Secure Shell architecture, SSH G3™, SSH Tectia is an ideal solution to secure even the most throughput-intensive file transfer and applications. The cryptographic libraries of SSH Tectia are FIPS 140-2 certified, satisfying the critical requirements of government and enterprise environments. Broad support for standards-based and commonly used authentication systems including passwords, digital certificates, and hardware-based authentication tokens provides organizations maximum flexibility with minimum integration effort.

## World-Class Technical Services

SSH Communications Security offers a choice of different support packages and services to help implement and maintain reliable communications security with SSH Tectia. Phone and e-mail support and web-based self-help are offered for prompt resolution of technical problems. A 24x7 support option is available to meet the support standards of even the most demanding environments. Furthermore, as the original developer of the Secure Shell technology, SSH has a comprehensive product roadmap with possibilities for customers to influence future functionality and features.

## Broad Platform Support

The SSH Tectia solution is available for the industry's broadest range of platforms including common Unix, Linux, Windows, and IBM mainframe operating systems. With SSH Tectia you can standardize on a single Secure Shell solution in large and heterogeneous IT environments and avoid the need to support implementations from multiple vendors.

## Strong Partnerships

To ensure seamless compatibility with third-party products and availability of supplementing services, SSH Communications Security has forged strong partnerships with industry-leading companies such as IBM, HP, RSA Security, and Entrust Technologies. These partnerships help customers implement integrated enterprise security solutions that combine best-of-breed technologies, products, and services. For a complete list of partners, please visit [www.ssh.com/partners/](http://www.ssh.com/partners/).



business partner





SSH | Original Secure Shell  
10 years – 2005

## Third Generation of Secure Shell – SSH G3™

In 1995 Tatu Ylönen, the founder of SSH Communications Security, developed the Secure Shell protocol and coded the first implementation. SSH developed and introduced in 1999 an improved version of the protocol, today the de-facto standard called SSH2. In 2005, 10 years since the original invention, SSH Communications Security continues to lead the development of the Secure Shell technology by completely rearchitecting and rewriting the protocol implementation for a second time, resulting in a third generation SSH G3™ architecture. SSH G3, based on and compatible with the standard SSH2, takes Secure Shell encryption and management performance to new heights, securing throughput-intensive file transfers and applications without causing processing bottlenecks. The SSH G3 architecture is incorporated in the SSH Tectia client/server solution 5.0 and later versions.

SSH Communications Security is a world-leading provider of enterprise security solutions and end-to-end communications security, and the original developer of the Secure Shell protocol. The company's SSH Tectia solution addresses the most critical needs of large enterprises, financial institutions, and government agencies. With SSH Tectia, organizations can cost-effectively secure their system administration, file transfers, and application connectivity against both internal and external security risks. As the original developer of the Secure Shell protocol and other key network security technologies, SSH has for 10 years developed end-to-end communications security solutions specifically for the enterprise. Currently more than 100 of the Global Fortune 500 companies are using SSH security solutions. SSH shares are quoted on the Helsinki Exchanges Main List. For more information, please visit [www.ssh.com](http://www.ssh.com).



### Americas

#### United States

20 William Street G35  
Wellesley, MA 02481  
Tel: +1 781 247 2100  
Fax: +1 781 431 0864  
[sales.americas@ssh.com](mailto:sales.americas@ssh.com)

### Europe

#### Finland

Valimotie 17  
FI-00380 Helsinki  
Tel: +358 20 500 7000  
Fax: +358 20 500 7001  
[sales.fi@ssh.com](mailto:sales.fi@ssh.com)

### Asia Pacific

#### Japan

Palazzo Girasole 6F  
2-9-2 Higashi-Shimbashi  
Minato-ku, Tokyo 105-0021  
Tel: +81 3 3459 6830  
Fax: +81 3 3459 6825  
[sales.jp@ssh.com](mailto:sales.jp@ssh.com)