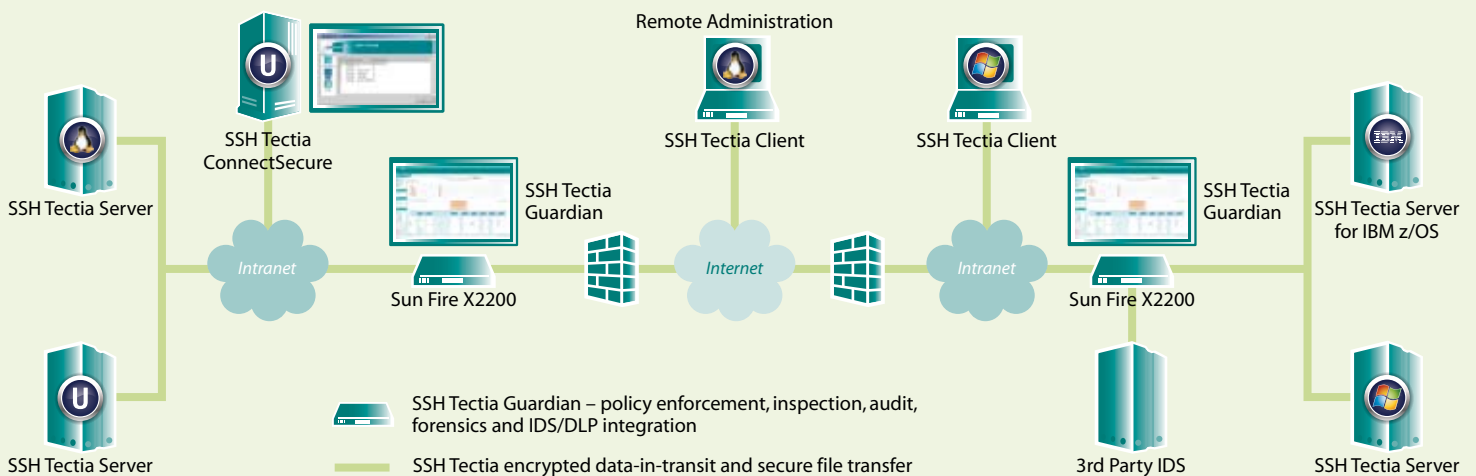




# SSH Tectia® Guardian 1.1

## Enabling the Next Level of Governance and Auditing



SSH Tectia Guardian is specifically designed to control, monitor, audit and inspect access to servers and networking devices – including the encrypted channels used by power and administrative users. It is a tool to oversee and to inspect SSH, Telnet and RDP traffic to meet the most demanding compliance, governance and auditing requirements. SSH Tectia Guardian adds an additional layer of security by inspecting the actions of secure protocol users and deterring internal malicious threats.

### Layered Security Approach

SSH Tectia Guardian is a unique governance tool that fully integrates into IDS solutions for a layered security approach by adding an additional audit and control point, independent of the client and server hosts. Packet inspection of the SSH, Telnet and RDP protocols ensure meeting data security compliance for SOX, PCI DSS, FISMA, DoD directives and other mandates requiring encrypted traffic to be inspected, audited and controlled, and providing accountability of root access.

### Auditing Functionality

SSH Tectia Guardian is the only solution to log and record every session and performs a step by step inspection and auditing of the encrypted and unencrypted traffic to resolve any potential threats to the internal network. Accountability of file transfers and remote access with detailed access reports eases the burden of internal and external auditing.

SSH Tectia Guardian logs all administrative traffic (including configuration changes, executed commands, etc.) into audit trails. All data is stored in digitally encrypted files, preventing any modification or manipulation. If an issue may arise (server misconfiguration, database manipulation, unexpected shutdown), the circumstances of the event are readily available in the audit trails, enabling the cause of the incident to be easily identified. The recorded audit trails can be displayed like a movie – recreating all actions of the host access by the users or server administrators. All audit trails are indexed, enabling fast forwarding, searching the texts seen by the administrator, searching for events (e.g. mouse clicks, pressing the Enter key), and more.

This full playback and archiving of sessions creates a valuable auditing and forensic tool eliminating any potential security threats that may be perceived or implied. SSH Tectia Guardian allows real-time response to true malicious threats by applying a proactive set of security controls on the most critical channels in the environment, minimizing the risk of breaches.

### Cost-effective Solution

SSH Tectia Guardian makes data security compliance easy and cost-effective with detailed reporting, logging and helps to maintain control of service-level-agreements (SLAs). Using these features, enterprises and government agencies can now effectively balance their valuable IT resources by reducing auditing times and drastically reducing the burden of maintaining governance and compliance.

# SSH Tectia® Guardian 1.1

## Features

- Transparent control and inspection over the entire SSH, RDP (Remote Desktop Protocol), and Telnet traffic
- Trusted and controlled man-in-the-middle-based technology
- Control remote access over different sub-channels
  - Agent-forwarding, port-forwarding, SCP and SFTP sub-systems, etc.
  - Printer, disk sharing, etc.
- Enforce strong authentication and encryption
- Archive complete sessions
  - Records complete workflow sessions
  - Compress and encrypt audit-trails
  - Search and replay sessions like a movie
- Real-time auditing
  - Oversee tunneled and forwarded communications
  - Relay selected sessions for real-time auditing (provides real-time response)
  - Forward decrypted traffic to IDS sensors (integrates with existing infrastructure)
- Ease of use
  - Web based management interface
  - Separation of duties for administration
  - Audit terminal server sessions
  - Automatic activity reporting
  - Automatic backup/archival
- Seamless integration
  - Support for different network topologies (router, bridge, bastion mode)
  - Dedicated management interface
  - Encrypted central logging (with syslog-ng)
  - HA support (mirrored partitions)
- Integration with user directories
  - Support for Active Directory and LDAP
  - Check user information in LDAP for user public-key authentication
- Runs on Sun Fire X2200 hardware



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

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

UK/IRELAND  
SoanePoint, 6-8 Market Place  
Reading, Berkshire  
RG1 2EG  
Tel.: +44 (0) 1189 255 580  
Fax: +44 (0) 1189 255 586  
sales.uk@ssh.com  
[www.ssh.com](http://www.ssh.com)

GERMANY/AUSTRIA/  
SWITZERLAND/BENELUX  
Lintorfer Str. 7  
De-40878 Ratingen  
Tel: +49 2102 30979 0  
Fax: +49 2102 30979 20  
sales.de@ssh.com  
[www.de.ssh.com](http://www.de.ssh.com)

JAPAN  
sales.jp@ssh.com  
[www.ssh.com/jp](http://www.ssh.com/jp)

ASIA-PACIFIC  
Valimotie 17  
FI-00380 Helsinki  
Tel: +358 20 500 7000  
Fax: +358 20 500 7001  
sales.asiapac@ssh.com  
[www.ssh.com](http://www.ssh.com)