



CASE STUDY

Major Enterprise Security Software Supplier Secures Critical Development Data

A MAJOR ENTERPRISE SECURITY SOFTWARE COMPANY AND ONE OF THE WORLD'S 20 LARGEST SOFTWARE COMPANIES (FORTUNE 1000) WITH OPERATIONS IN OVER 30 COUNTRIES NEEDED A WAY TO PROTECT CRITICAL AND CONFIDENTIAL PRODUCT DEVELOPMENT DATA IN ITS INTERNAL GLOBAL IT NETWORK.



THE PROBLEM

The company was faced with finding an ideal data security solution that could be easily implemented and maintained on a variety of computing platforms throughout the organization's multi-site internal network. The key requirements for the solution were providing secure remote access to development servers, replacing unsecured telnet sessions, and eliminating unencrypted FTP file transfers of source code and other intellectual property between development desktops and servers. The implementation was large-scale, including over 1,000 servers and over 500 client systems. The IT group needed to conform to their two-factor authentication policy using RSA SecurID® hardware tokens authenticated to an RSA ACE/Server®. The solution had to be easy to deploy and manage, dependable, cost-effective and ideally require no additional resources or modifications to the infrastructure or the applications. Finally, 24x7 technical support was also needed, since the solution would be implemented worldwide.

THE SOLUTION

After thorough analysis and evaluation, the company chose SSH Tectia® Client and Server software along with SSH Tectia Manager to protect its mission-critical development data. By using SSH Tectia Manager to deploy and configure the SSH Tectia Client/Server software, the company was able to perform this mass deployment in a fraction of the time it would have taken with other solutions. SSH Tectia Manager eased the burden on valuable IT resources and created an attractive ROI for the solution overall. The centralized management solution also helped enforce the security policies of the company and provide key access control and logging information for security compliance audits for over 1,000 servers and 500 client systems worldwide, from one central location.

SSH Tectia eliminated unsecured telnet sessions with secure remote access and replaced unsecured FTP file transfers with secure, encrypted SFTP file transfers, ensuring secure end-to-end communications in their internal network. The standards-based SSH Tectia was able to meet their authentication policy with its built-in support for the RSA SecurID hardware token.

SSH Tectia enabled the company to secure their business-critical SUN/Solaris and Linux servers accessed by both Windows and Unix clients. The SSH Tectia solution required no modifications to the existing infrastructure or applications, enabling a fast and easy deployment, and reducing on-going support costs significantly.



THE REQUIREMENTS

The decision to standardize the company's security program with SSH Tectia was based on a number of factors, including:

Performance

Compared with other solutions, SSH Tectia was found to outperform the competition on speed.

Multi-session Support

The company's employees frequently have multiple sessions open on their workstations. SSH Tectia's ability to support multiple sessions without user revalidation adds to worker efficiency.

Centralized Management

With such a large deployment of the product, the ability to centrally manage the software updates and to ensure policy enforcement was a key advantage. The product's ability to provide centralized logging and auditing capabilities helped reduce the security audit costs.

Easy Integration

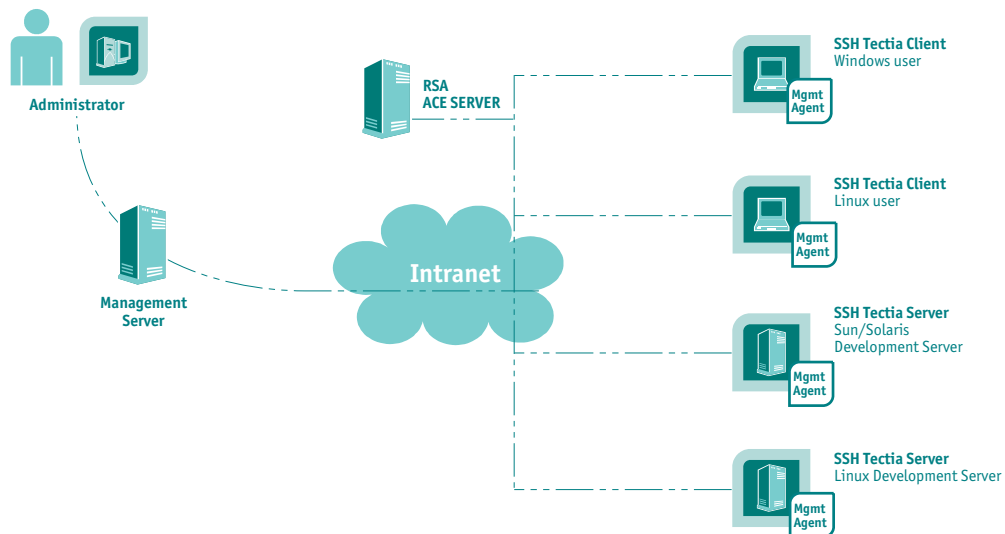
The company found that its flexibility was maximized by using SSH Tectia thanks to its built-in support for enterprise software from other vendors. This was important to the company as they are considering deploying SOCKS and HTTP proxy servers in their infrastructure.

Support For All Needed Platforms

Since the company uses a variety of platforms for both its servers and workstations, having a single product supporting Unix, Linux, and Windows greatly simplified the project for the IT support staff.

Technical Support

Finally, it was important to the company to have access to 24x7 technical support, and when needed, get timely in-depth assistance from the vendor's technical global support teams.



MISSION ACCOMPLISHED

The implementation of SSH Tectia has allowed the company to accomplish its goals and provide ultimate security for its proprietary product development data during remote terminal sessions and data transfers across its internal networks. The company has also streamlined the considerable task of managing the security for over 1,000 servers and 500 client systems by using SSH Tectia Manager to oversee the operations from a central location.

For more information, please visit www.ssh.com