



Securing A Financial IT Environment



A large Asian financial institution - one of the biggest financial institutions in the world, processes billions of financial transactions each day. Security is paramount in an organization of its size and that has such an oversized impact on global finance. But, with a complex IT environment that is accessed by both in-house staff and contracted third-parties, it's not easy to find secure solutions that offer the full range of functionality they need to manage IT projects, while also maintaining compliance with industry and global regulations.

A large Asian financial institution turns to SSH.COM for secure FTP and key management

Brief background

Each year, the company conducts an evaluation of its technology solutions to ensure it has the best solutions for each job. After a wide search that includes both traditional vendors and open source products, the company determined that two SSH.COM products - Universal SSH Key Manager (UKM) and Tectia SSH Client/Server were the right solutions for the job.

Complex problems require expert solutions

The customer relies on SSH keys to manage secure access to important IT resources and, like many enterprises, found itself overwhelmed by the sheer volume and variety of SSH keys in its IT environment. SSH keys are a convenient and efficient way to establish encrypted connections, and that's why they are widely used. At the same time, they are the only form of access a user can provision themselves without oversight or control. They also never expire by default or are not associated with an identity. In addition, SSH keys automate critical M2M connections that transfer a lot of sensitive information, like financial transactions or credit card information.

These keys were being created by both in-house IT staff as well as external third-party contractors who had been hired, sometimes on a temporary basis, to support with specific operational projects. Key mismanagement created several operational and administrative challenges. So, they needed a solution to help them regain control of their keys.

It would be important to find a secure file transfer protocol (SFTP) that it could rely on to protect sensitive information in transit without slowing down productivity

Separately, the customer's employees and partners rely heavily on file transfer solution to securely share information throughout the entire organization. As one would expect, security is of paramount concern to an organization that transfers sensitive files frequently, but the customer also needed a solution that enabled an agile way of working for its staff. So, it would be important to find a secure file transfer protocol (SFTP) that it could rely on to protect sensitive information in transit without slowing down productivity.

When the time came to reconsider its solutions for key management and file transfer protocol (FTP), the company's head of on-premises infrastructure cast a very wide net. Everyone was considered, from traditional vendors to open source products. Ultimately, the customer decided that nothing can replace deep industry expertise. So, they chose to bring in the originators of SSH keys, and the company that knows more about SSH key security than anyone else: SSH.COM.

UKM automatically scans an organization's IT infrastructure to identify and create an accurate inventory of SSH keys

The customer chose UKM to solve this challenge. UKM automatically scans an organization's IT infrastructure to identify and create an accurate inventory of SSH keys. The solution also analyzes and presents the trust relationships enabled by the found keys. That significantly cut down on oversight time and meant that additional manpower no longer had to be used on manually identifying keys and their relationships.



Improving compliance with secure key management

One of the major risks of misplaced or mismanaged SSH keys is that they can provide a backdoor to sensitive IT resources or data. That's a clear and significant risk to financial services companies like this customer, especially because regulations require stringent protection of their IT infrastructure and financial assets to prevent the likelihood of intrusion. Failure to comply could result in significant fines or reputational damage.

Privileged users would use SSH keys to access the customer's UNIX systems. The organization found that hundreds to thousands of public keys would be added to their servers every day. This large collection of keys – many of which were outdated or unused – was stored primarily in one folder. This process created an administrative nightmare: Every time users need to establish a connection, they would need to search for the right key among a pool of thousands. At the same time, the customer assigned additional team members to the task of manually sifting through thousands of keys so they could categorize them into new folders in the hopes of speeding up the search process for users.

UKM also helps organizations determine if their SSH keys are up to standard and comply with regulations

UKM also helps organizations determine if their SSH keys are up to standard and comply with regulations. For example, some regulations might require specific key lengths, and banks often face the strictest requirements in this area. If any keys are found that are not in compliance, UKM can bring the keys into compliance with one click. Unused or outdated keys can also be instantly removed.

The solution can also be configured to scan the infrastructure at regular intervals, including daily, weekly, or even smaller time intervals like every five minutes. Similarly, IT admins can set policies, alerts and reminders that govern the creation and sunsetting of SSH keys.

UKM provided centralized control and clarity to the customer's key management lifecycle. UKM manages keys for thousands of hosts, throughout the organization, drastically simplifying oversight of its entire IT environment.



Protecting important files with secure FTP

Much of the customer's daily workflow also required the use of secure FTP, which encrypts the tunnel that enables file transfer between two servers. These connections can be significant points of risk for organizations, especially in situations where they connect an internal server to a user that is outside of the company, as was the case when the customer needed to provide access to its third-party contractors.

Much of the customer's daily workflow also required the use of secure FTP, which encrypts the tunnel that enables file transfer between two servers.

In their search for an FTP solution, the customer also wanted something that could enable an agile development culture within their programming team. At first, OpenSSH seemed like a sensible solution. Besides the fact that it's a free tool, the customer thought using OpenSSH would promote higher code quality within its development team: if developers knew their source code was going to be published and subject to large-scale peer review, they would theoretically be much more careful about how they write it.

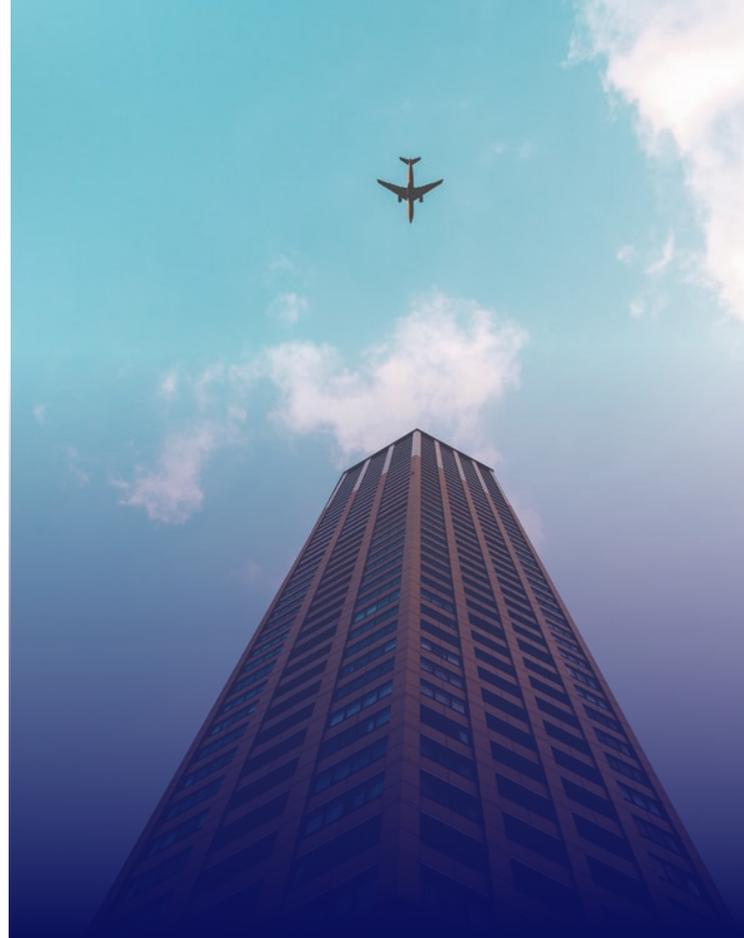
However, after further consideration they realized OpenSSH didn't make sense for several reasons. Firstly, it could potentially open the code for some of the customer's core banking systems to the public, a risky idea that could have made it easier for hackers to find ways to hack their systems in the future.

Secondly, the customer was wary that OpenSSH did not offer the ability to disable the creation of weak ciphers, or short encryption key strings. Longer key strings offer higher degrees of encryption, an important security consideration for financial services providers.

The customer had other practical concerns with OpenSSH. The company had SFTP automation scripts built deeply within their infrastructure, and a time-consuming migration to OpenSSH would simply be too costly and demanding for the team. Introducing a new solution could also disrupt day-to-day operations, requiring staff to take time out of their day to learn the new tool.

Finally, the customer felt it was important to have local support for its FTP solution. Knowing you can call up a solution engineer for instant support offered peace of mind.

Ultimately, Tectia SSH Client/Server proved to be the right solution for all these needs. The solution supports secure and compliant X.509 certificate-based authentication, and besides its robust security, it is also fast, transferring large files up to twice as fast as OpenSSH.



Tectia SSH Client/Server supports secure and compliant X.509 certificate-based authentication.

Tectia SSH is used by many of the world's largest banks, insurance companies, retailers, technology companies and more than 100 U.S. government agencies, including the IRS, NASA and U.S. Army.

Tectia SSH was deployed on the customer's Windows and UNIX systems. The company relies on expert support from the SSH.COM team to ensure smooth deployment and integration, and they now benefit from fast, secure file transfers throughout the organization.

The combination of UKM and Tectia, backed by decades of security expertise, made SSH.COM the right partner for the customer as it looked to secure its IT infrastructure now and into the future.





Finland

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

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com