

TOP 5 GLOBAL BANK RESTORES COMPLIANCE AND REDUCES RISK WITH UNIVERSAL SSH KEY MANAGER®

One of the largest banks in the world - with over \$2.5 trillion in assets - was alerted to a security and compliance issue during an external audit. The bank utilized OpenSSH to drive thousands of mission critical transactions every day but they needed to get a handle on their identity and access controls for application-to-application and privileged users in order to ensure the security of their Secure Shell environment.

BACKGROUND

Secure Shell (SSH) is an infrastructure-level security protocol that is widely used in enterprises, yet not widely understood. SSH performs critical IT functions such as automated file transfers, backups, disaster recovery readiness and system administration. SSH employs a public key based authentication system that in most enterprises operates completely outside of controls provided by RADIUS, AD and other centralized authentication and authorization mechanisms.

BANKING AND FINANCIAL SERVICES QUICK FACTS

Size & Type of Environment:

10,000+ hosts using OpenSSH

Number of User Accounts:

20,000+

Number of Applications:

500+

Number of Keys:

1.5 million

Compliance Issues:

SOX, Monetary Authority of Singapore

THE PROBLEM

At a Top 5 Global Bank*, a security audit raised attention to the risk and compliance issues stemming from lack of governance over SSH user keys – the keys that grant access to systems and enable functions critical to many banking operations. Auditors advised management that the existence of this unmanaged authentication system was in violation of compliance mandates (MAS & SOX) and even more serious, represented an existential threat to the organization itself.

The compromise of just one key granting root access to server infrastructure would expose the bank to information theft, tampering and loss – even including the loss of backups. Operations staff were charged with the task of bringing the SSH infrastructure under security compliance.

“During the discovery phase the scope and extent of the issue became clear: Over time the number of SSH keys had grown to an unmanageable level and with little to no visibility into what each key did. With over 85% of all SSH transactions being critical application-to-application data transfers, the first step was to lock down the environment and identify trust relationships. Then we were able to redeploy new keys - all without causing an outage.”

- Joe Scaff, SSH Director of Technical Services

CHOOSING A SOLUTION

The Bank needed a partner that could not only provide an SSH key management product but also the advice and expertise to design and implement a solution. The Bank realized that they simply did not have sufficient in-house SSH knowledge and expertise to deal with this problem that had been growing for years. After contacting several vendors, the Bank selected SSH Communications Security.

“One of the first things SSH Communications Security did was to demonstrate the scope of the problem. Their SSH Key Discovery tool showed us that the problem was even more widespread and serious than our auditors were saying. SSH’s technical deployment team found we had over 1.5 million SSH user keys distributed across our entire infrastructure, including over 150,000 user keys granting root access, with no records as to who was in possession of the corresponding private keys.”

“We found that some of our critical security safeguards such as those ensuring separation of test and production environments were easily circumvented via SSH. SSH Communications Security showed us how Universal SSH Key Manager combined with their professional services would enable us to take back control. No other vendor had the products or expertise to do this.”

- The Bank’s Project Manager

A STRUCTURED APPROACH

Key discovery is only the first step. Understanding key usage – identifying which keys are essential to automated processes – is an essential step towards remediation. Universal SSH Key Manager provides the monitoring capability to capture key usage. Unneeded keys are removed and actively used keys brought under administrative control. Universal SSH Key Manager provides central administration to ensure policy control over key usage, key lifetimes and authority over key creation. It also actively monitors the environment and alerts administrators on policy violations.

“Says the Project Manager: “SSH Communications has been a true partner in this endeavor. Their expertise and attention to detail have been invaluable in helping us address this major risk and compliance issue.”



Further Reading:

- [What You Need To Know About NIST Guidelines for Secure Shell \(SSH\)](#)
.....
- [Kuppingercole Report: Executive View on Universal SSH Key Manager](#)
.....
- [Achieving Effective Compliance: Hong Kong Monetary Authority’s General Principles for Technology Risk Management](#)

*The company has requested anonymity, but all the facts are accurate as stated.