Top 15 Global Bank Restores Compliance and Reduces Risk with Universal SSH Key Manager®
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.

At a Top 15 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", says Joe Scaff, Chief Sales Officer at SSH.COM.

"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."
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.COM.

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.

“SSH.COM’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.”

“SSH.COM 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.”
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