

REGAINING CONTROL OF TRUSTED ACCESS

Customer Success Story: A Global Financial Institution

A global financial giant was alerted to the unmanaged state of trusted access within their network. An internal audit revealed developers' unmanaged and uncontrolled Secure Shell (SSH) access to the thousands of Unix and Linux systems that run the online retail and investment services. The organization quickly ramped up their efforts to regain control of trusted access to remediate this clear violation of corporate security policy and the regulatory mandates.

Quick Facts on Customer

Size and Type of Environment

- Up to 35,000 managed hosts – for both retail and investment banking.
- Various Unix and Linux operating systems in various versions (HP-UX, AIX, Solaris, Linux, ...)
- Both agent and agentless SSH management solutions at servers.
- Requirements for reporting on the state of the environment and the changes in it.

Customer Drivers

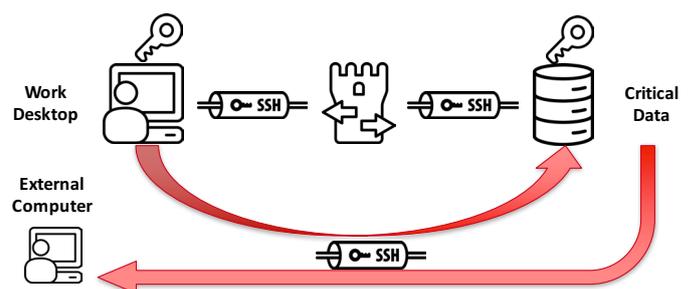
- A reaction to an internal security audit – conformance to corporate security policy.
- Development department users were discovered to be capable of self-provisioning SSH access across production systems.
- Regaining of control – readiness for audits and compliance regulations.

BRIEF BACKGROUND

The customer's brand is global and associates with trust and prosperity. The corporate risk management team is tasked with protecting the brand from being tarnished by undesired attention. Internal audits play an important role in this, and the control and visibility of trusted access of internal and external privileged users is essential. The management and control of trusted access with Secure Shell (SSH) was brought to spotlight when an internal audit revealed that developers were able to use SSH keys to bypass existing privileged access management solutions. Regaining control over SSH keys became a priority.

ACHIEVING COMPLIANCE BY REMEDIATION OF AUDIT FINDINGS

An internal security audit of the retail and investment IT revealed serious shortcomings in privileged access management – due to the unmanaged state of SSH keys, the developers were able to self-provision their own SSH access and bypass the PAM solutions altogether. As the SSH keys never expire, self-provisioned accesses to production servers have accumulated and proliferated over the years. These unmanaged SSH key-based accesses were quickly assessed to require remediation.



Bypassing a PAM solution with SSH

The corporate IT environment bears all the typical characteristics of the market – large server volumes, heterogeneous platforms, wide software and vendor diversity. These characteristics formulate the requirements for a strict and demanding SSH key management project – the discovery, monitoring, remediation, and management must be achieved in-line with existing operations and processes. The rollout of risk management solutions must be risk-free and non-disruptive.

SOLUTION SELECTION

The solution for controlling and managing trusted access must be able to cover the maximum environmental diversity with minimal disruption to existing processes and operations. Due to the complex technical and organizational structures, the selected vendor was required to contribute subject matter expertise, consultation, and assistance in the planning, deployment, and rollout of the selected solution.

SSH Communications Security is the original inventor of the SSH protocol that provides the secure trusted access to the entire server populace of the bank. When the bank was evaluating their options for SSH key management they also considered an in-house software development project. However, the sheer complexity of the effort as well as the identified shortcomings in subject matter expertise quickly turned the attention to the world's leading source of SSH expertise, SSH Communications Security.

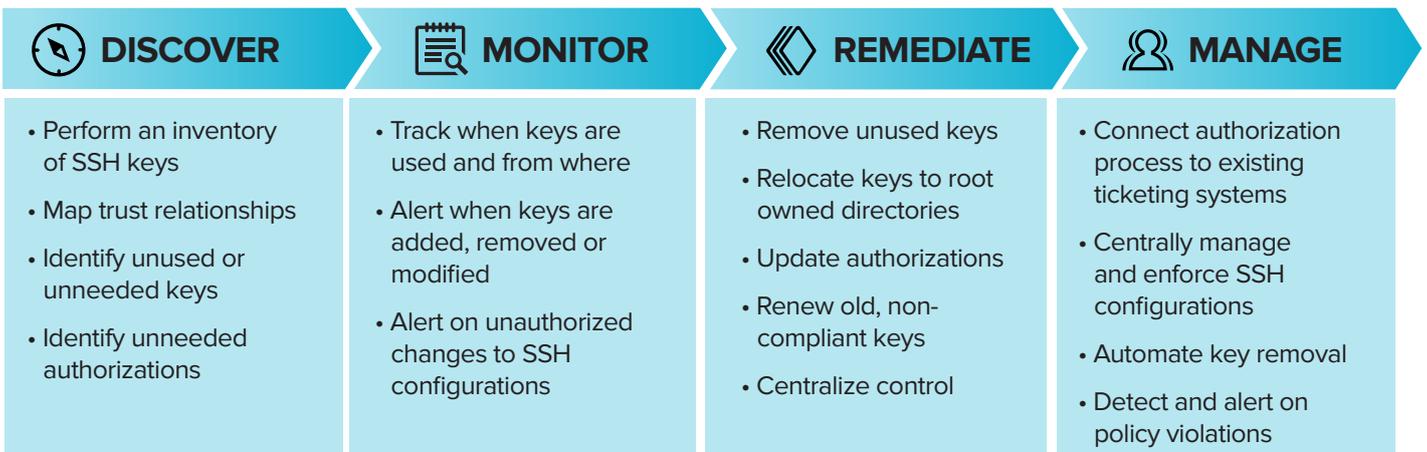
SOLUTION SUMMARY

SSH Communications Security offered the bank a mature, off-the-shelf key management platform (Universal SSH Key Manager®). The product addressed the SSH key management issues with a purpose-built solution that focuses on workflows for SSH key management, as opposed to some competing solutions that are based on certificate management systems retrofitted for SSH keys.

Universal SSH Key Manager handles the entire trusted access lifecycle at the bank - it discovers the trust relationships, monitors the SSH key usage, remediates the access to conform to policy, and manages the SSH-based trusted access centrally. Universal SSH Key Manager allowed the bank to regain control of trusted access in their critical infrastructure.

SSH Communications Security complemented the product offering with an extensive service and consultation package (Secure Shell HealthCheck) that ensured the coverage and smooth progress of the deployment project.

“ This case validates our approach of workflow-based SSH key management, and highlights the customer value we can add with our subject matter expertise on all things SSH. ” - Kalle Jääskeläinen, VP, SSH Communications Security



ssh®, Tectia®, Universal SSH Key Manager® and CryptoAuditor® are registered trademarks of SSH Communications Security Corporation in the United States and in certain other jurisdictions. SSH and Tectia logos and names of other SSH products and services are trademarks of SSH Communications Security Corporation and are protected by international copyright laws and treaties. Logos and names of the products may be registered in certain jurisdictions.

Copyright © 2016 SSH Communications Security Corporation. All rights reserved.