Media Company Uses Universal SSH Key Manager to Lower Risk and Gain Operational Efficiency

In order to meet thE challenges of a deadline driven environment, this leading news and media organization needed to streamline provisioning and access controls for application developers and IT staff.

The Challenge

Like many organizations, this company is a heavy user of Secure Shell as a secure access tool for systems administrators and application developers. These users are granted privileged access to servers, applications and data bases as they are responsible for updating and maintaining those systems. Some administrators are granted “super user” status. However, as the company expanded, the processes for provisioning and managing privileged user access had outgrown the needs of the business. Responsiveness to the needs of developers was going down while exposure to risk and compliance issues was going up.

> “Our process for granting authorizations was cumbersome and was creating risk and compliance headaches. Universal SSH Key Manager enabled us to gain control over our authorizations while improving the productivity of our IT staff”
>
> *- IT Project Manager*

Manual Processes Slowing the Pace of Business

The process for setting up Secure Shell authorizations was cumbersome and error prone. A user needing a new authorization would have to open a support ticket to make the request. Support required email confirmation from his/her manager before proceeding.

Quick Facts

Industry:
Online Media, Publishing and Education

The Challenge:
Streamline privileged user authorizations and improve identity and access governance

The Solution:
Universal SSH Key Manager from SSH Communications Security to automate provisioning, manage authorizations and monitor for compliance.

The user would then run a key generation utility on their workstation and email the public key to Support. Support would then copy and paste the public key to the correct directories on the target systems. Common errors encountered in this process included:

- Mistakes editing the configuration file on each server to which the key is authorized.
- Mistakes editing the client configuration file to add the private key as an identity key.
- Mistakes ensuring that privileges of public and private keys were properly set.
- Fully testing that the setup works.
- Forgetting to install keys and test on backup systems.

Even without errors the process generally took 1-2 business days.

Identity and Access Governance for Privileged Users

There was also a need to make improvements in identity and access governance for the Secure Shell environment. A scan of the environment revealed a significant number of undocumented authorizations as well as keys overdue for rotation. In addition to streamlining the process for granting privileged access, the company sought to achieve the following Secure Shell access management goals:

- Remediation of the Secure Shell environment. Removal of unneeded authorizations. Update old authorizations.
- Automated tracking of new authorizations.
- Central database of who had been granted access to what systems and with what privileges.
- Authorizations based on end user job role - need to know, need to do.
- Reduce number of administrators involved in granting authorizations.
- Central control over configurations and policy enforcement.

In short, the company saw an opportunity to lower overhead costs by streamlining operational procedures and at the same time reduce risk and compliance exposures.

Further Reading:

- SSH User Key Remediation: Getting Control of One of the Most Significant Hidden Threats to Your Enterprise Security

- SSH User Keys and Access Control in PCI-DSS Compliance Environments

- The Technical Complexities and Risks of Public Key Authentication

The Solution

After surveying various offerings on the market, the company selected SSH Communications Security as the solution provider. Universal SSH Key Manager (UKM) from SSH Communications Security proved to be the only product on the market that could meet their solution requirements (See Table 1). The company also needed professional services to tailor a solution design to meet the specific needs of their environment. SSH Communications Security demonstrated the expertise and experience to ensure a smooth transition from the manual, loosely managed process to a more automated process with sound identity and access governance.

SOLUTION REQUIREMENTS
Map collected user accounts from various sources into individual persons and groups
Import and sync users and other groups from LDAP
Organize collected hosts into host groups
Import and sync hosts and host groups from LDAP
Define authorization rules (which users/groups have access to which hosts/groups)
Compare defined authorization rules against the effective trust relationships
Enforce authorization rules (deploy and revoke keys according to these)
Setup an approval chain for authorizing a key deployment (web based interface)
Setup of key request interface process/ integration to existing approval process
Setup of creation of new private key on the client system
Setup of private key lifecycle and renewal management
Setup distribution of the public key to defined hosts
Setup of notification and email alerts
Activation of real time monitoring and maintenance of environment

Table 1: Solution Requirements

The Result

The customer first used the Discovery phase of implementation to identify the extent of public and private Secure Shell keys in their environment. They found and removed hundreds of authorization keys that should not have been there. They also found many more keys needing to be rotated and/or relocated. With the discovery and remediation phase complete, the customer then implemented the management and governance capabilities of UKM to centralize and automate key generation processes and integrate with Active Directory to apply role based authorizations to Secure Shell users. This provided a central, directory based system for managing user access based on "need to know/need to do" role definitions. Figure 2 summarizes how UKM was deployed. The results were higher productivity, lower risks and stronger compliance (Table 3).

Benefits of UKM Deployment
Reduced overhead of systems and support personnel
Improved productivity of application developers by reducing idle time
Improved security posture of organization, reduced risk of unauthorized access
Improved ability to meet SOX compliance, lowered reporting costs

Table 3: Deployment Benefits

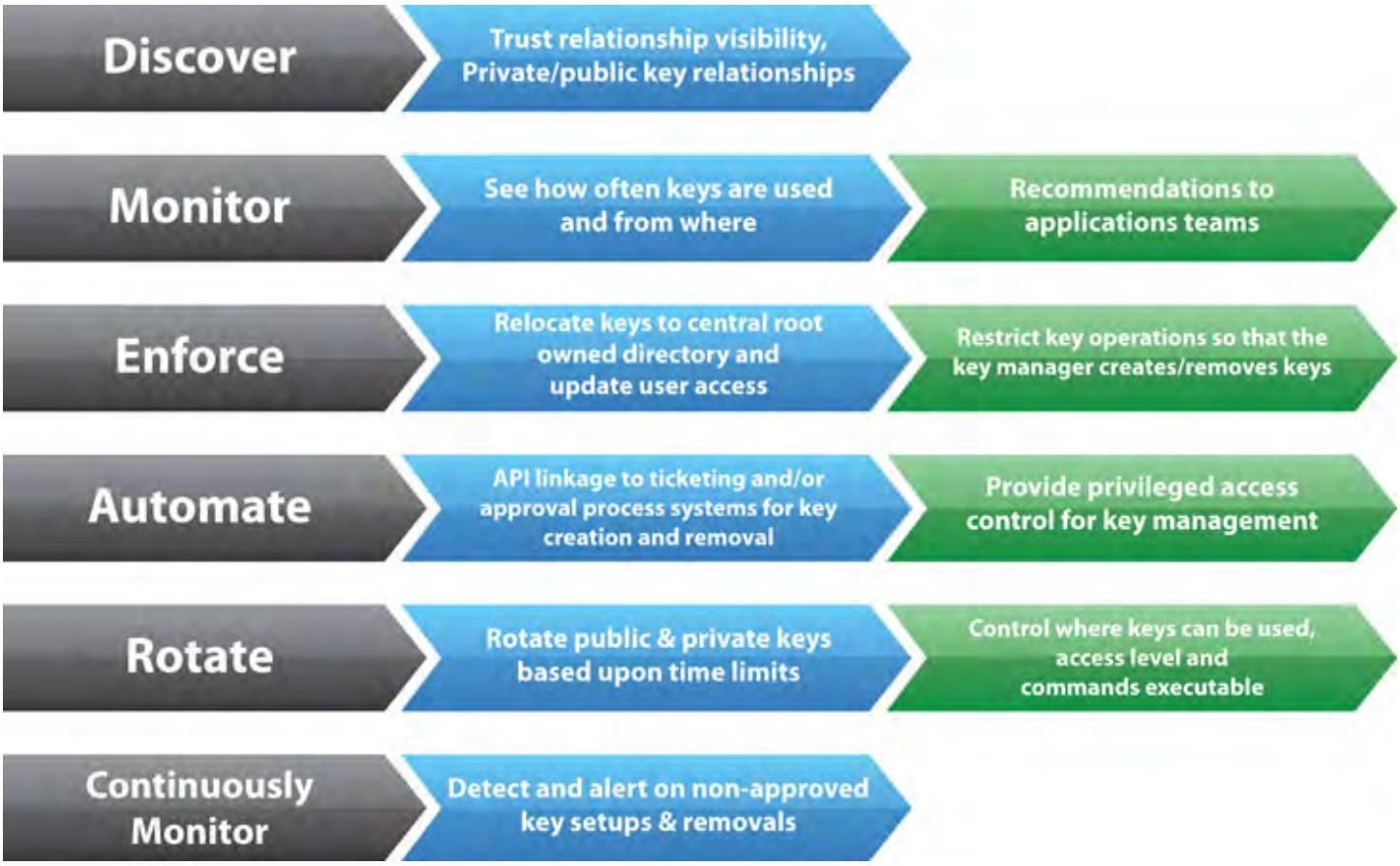

Figure 2: Deployment Outline

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