ssh
Securing the path to your information assets

Data Sheet

Universal SSH Key Manager

Identity and Access Management for Secure Shell Infrastructure

As the inventors of the Secure Shell protocol, SSH Communications Security is focused on helping IT organizations secure the path to their information assets. Our Universal SSH Key Manager is a multiplatform, scalable solution that brings compliance and control to Secure Shell environments. Universal SSH Key Manager reduces risk of unauthorized access from both internal and external actors, solves thorny compliance issues and reduces costs.

The Problem

The vast majority of large enterprises rely on Secure Shell (SSH) to provide secure authentication and confidentiality (encryption) for many business critical functions such as automated backups, day to day file transfers and interactive user access for systems administration. Many mission critical IT functions are enabled through SSH. However, most enterprises use manual processes for generating, configuring and deploying the SSH public and private keys that enable these functions.

Over time, this results in the uncontrolled proliferation of authentication keys. Security managers lose visibility and control over who has access to what servers and whether access rights previously granted should be revoked. It becomes nearly impossible to map the trust relationships between individual users, system accounts and application IDs with their respective destination servers.

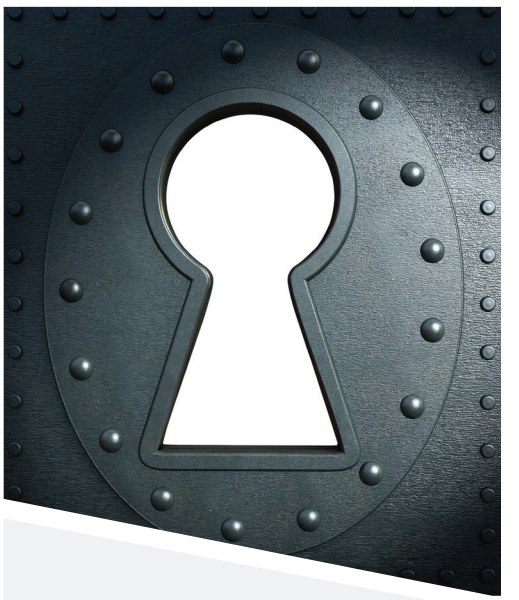
Standard identity and access management solutions that govern end user access typically do not encompass SSH key based access to systems and accounts. Lack of governance and control is exposing enterprises to elevated risk, compliance failures and the excess overhead of manual processes.

The Challenge

Traditional approaches to managing SSH user keys are time consuming and expensive, and there is little if any automation or auditability. Because so many business critical functions - many of them automated - rely on SSH, it is very difficult to bring SSH Key management under control without disrupting those functions. The problem is highlighted when there is need to revoke access when there are organizational changes, employee departures, mergers and acquisitions.

Enterprises generate significant overhead in the day to day activity of SSH user key setups, have increased risk from the lack of key renewals and removals, and face pressure from compliance initiatives.

Automated Access Control



Return on Security Investment

Lower Costs: Eliminate inefficient and error prone manual administration processes.

Reduce Risk: Protect against catastrophic loss - gain control and visibility over all privileged access.

Gain Compliance: A centralized, auditable solution ensures compliance to mandates.

A non-disruptive solution is needed to eliminate inefficient and error prone manual processes, dramatically reduce risk and address compliance exposures. Finally, processes and controls are needed to take care of the issues now and ensure they don't re-emerge in the future.

The Solution

SSH Communications Security's Universal SSH Key Manager (UKM) is an enterprise grade SSH user key management solution. UKM takes a non-disruptive approach that enables enterprises to gain and retain control of the SSH infrastructure without interfering with production systems. No need to rip and replace how users get their work done or change the hundreds of automated processes that are the lifeblood of ongoing business. UKM's non-disruptive approach is based on three principles:

Discover: Discover all SSH keys, map trust relationships and identify policy violations.
Remediate: Remove keys that should be revoked and bring valid keys under correct policy compliance.
Manage: Eliminate manual processes, centralize control, enforce compliance, audit all activity

UKM on average saves a typical Fortune 1000 organization $1 to $3 million per year in overhead costs while reducing the risk of serious security breach and resolving open compliance issues. Whether your environment uses OpenSSH or Tectia, UKM brings this complex problem under control.

Discover	Remediate	Manage
• Take inventory of SSH Keys • Map Trust Relationships • Track Key Activity • Identify unused/unneeded keys • Identify unneeded authorizations	• Remove Unused Keys • Relocate keys to root owned directories • Update authorizations • Renew old, non-compliant keys • Centralize control	• Connect authorization process to existing ticketing systems • Centrally manage and enforce SSH configurations • Automate key removal, link to AD/LDAP • Detect and alert on policy violations

Features	Benefits
Agentless discovery	Non-disruptive deployment
Multiple, redundant management instances	High scale, high availability
Multiplatform support – Unix, Linux, Windows, IBM z/OS	Deployable in vast majority of enterprises
RESTful API	Link to existing IAM infrastructure
Automated key creation, update, removal	Lower costs, fewer errors, faster turnaround
Central management and enforcement of SSH client and server configurations	Policy control, stronger security, fewer errors
Real time alerts	Fix violations in real time
Audit trail	Easier compliance reporting
Compliance support	Enables compliance to current requirements and planned updates to PCI, NIST/FISMA, SOX, HIPAA, Basel II mandates

Universal SSH Key Manager Technical Specifications

Supported Platforms for SSH Key Manager Server	• CentOS 6 (x86-64) • Red Hat Enterprise Linux 6 (x86-64) • SUSE Linux Enterprise Server 11 (x86-64)
High Availability	• Multiple UKM server support. • Non-intrusive – no point of failure to production operations
Key Discovery Features	• Public & private key discovery by size and type • Passphrase existence • Key owner by user or user group • Trust relationships per host & host groups • Rogue keys • Unauthorized trust relationships
Key Monitoring Features	• Detect manual changes to authorizations • Key activity (when key was used and from where) • Real-time email alerts of suspicious key activity
Key Enforcement Features	• Bring user keys under central admin control • Centralized management of authorization policies
Key Automation Features	• Automated key creation and deployment • Centralized SSH configuration management • Automate processes using the full-featured API
API Support	• RESTful API • Command-line client
Renewal/Rotation features	• Renew private and public keys per authorizations • Key lifetime tracking with automatic key rotation (in future versions)
Admin Authentication Methods	• Key Manager accounts • External accounts from Active Directory
Role Based Administration	• RBAC for Key Manager admins (for both on-box & LDAP admin accounts) • Customizable roles to fit the tasks of individual admins
Logging, Alerts, Alarms	• All management and admin actions are logged • Key activity • System alerts • Alerts of suspicious key activity per host
Management Methods	• Web GUI - Mozilla Firefox 12 or newer - Recent & stable Chrome - Internet Explorer 8, 9 • Remote command line client
Management Connection Types	• Support for agent-based and agentless host management.
Supported Managed Host Platforms	(The listed non-Windows platforms can be managed in either agentless or agent-based manner. The listed Windows platforms can be managed in an agent-based manner) • HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC) • HP-UX 11iv2, 11iv3 (IA-64) • IBM AIX 5.3, 6.1, 7.1 (POWER) • Microsoft Windows XP, Vista, 7 • Microsoft Windows Server 2003, Server 2008, Server 2008 R2 • Oracle Enterprise Linux 5.4, 5.5, 5.6, 5.7 • Oracle Solaris 9, 10, 11 (SPARC) • Oracle Solaris 10, 11 (x86-64) • Red Hat Enterprise Linux 4, 5, 6 (x86) • Red Hat Enterprise Linux 4, 5, 6 (x86-64) • SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64) • SUSE Linux Enterprise Server 10, 11 (x86, x86-64) • IBM z/OS 1.12 (in future versions)
Supported SSH versions	• Tectia 6.0 or newer • OpenSSH 4.0 or newer

Universal SSH Key Manager Architecture