ssh communications security

DATA SHEET

UNIVERSAL SSH KEY MANAGER™ 1.7

Identity and Access Management for Secure Shell Infrastructure

Universal SSH Key Manager is a scalable, multi-platform solution that provides visibility to SSH trust relationships and brings auditability and control into Secure Shell environments. It brings SSH keys into policy compliance, reduces risk of unauthorized access, and cuts 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. However, most enterprises leave the process of generating, configuring and deploying the SSH public and private keys that enable these functions in the hands of end users. The lack of a central authority to oversee the process of issuing these credentials means there is no tracking of their lifecycle or ability to ensure that they are created according to policies.

Over time, this results in uncontrolled proliferation of authentication keys. Security managers lose visibility and control over who has access to what servers and whether previously granted access rights 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 removal of a wrong key can result in a costly disruption of an operational process. The problem is highlighted when there is need to revoke access because of organizational changes, employee departures, mergers and acquisitions.

Supported Secure Shell versions

ssh communications security

Centrify

Attachmate

ORACLE SOLARIS

bitvise

TOP SECRET

UNIVERSAL SSH KEY MANAGER

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 operations in 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 five principles:

- **Assess:** Define policies around SSH and validate your SSH environment against those.
- **Discover:** Discover all SSH keys, map trust relationships and identify policy violations.
- **Monitor:** Track key usage to determine which keys can be safely removed without affecting operations.
- **Remediate:** Remove keys that should be revoked and bring valid keys under policy compliance.
- **Manage:** Eliminate manual processes, centralize control, enforce compliance and audit all activity.

With the optional user portal component UKM enables the delegation of key remediation actions to the users that are ultimately responsible for the applications and users to which the keys belong. In addition, user portal provides a simple way to request and provision SSH-based access from a central point in line with security policies and with a full audit trail from start to finish.

UKM saves a typical Fortune 1000 organization on average $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, Tectia, or other common SSH implementations, UKM brings this complex problem under control.

ASSESS	DISCOVER	MONITOR	REMEDIATE	MANAGE
Assess the state of your SSH environment • Define policies around SSH keys and authorizations • Report on policy compliance of your SSH environment	*Identify who has access to where* • Use a script-based scan to quickly perform an inventory of SSH keys across thousands of hosts or use agentless/agent connections • Map trust relationships and evaluate against defined policies • Identify unused or unneeded keys and authorizations	*Ongoing monitoring to identify and react to unauthorized changes and policy violations* • Track when keys are used and from where • Alert when keys are added, removed or modified • Alert on unauthorized changes to SSH configurations	*Perform changes to SSH keys in order to achieve policy and regulatory compliance* • Remove unused keys • Relocate keys to root owned directories • Update and restrict authorizations • Renew old, non-compliant keys • Centralize control	*Integrate and automate the full access lifecycle and remain compliant* • Connect authorization processes to existing ticketing systems • Centrally manage and enforce SSH configurations • Automate key provisioning and removal • Detect and alert on policy violations

FEATURES AND BENEFITS

Features	Benefits
Agentless and script-based discovery	Perform a quick and non-invasive inventory of SSH keys.
SSH policies and reports	Quickly report on compliance of the SSH key environment against defined policies.
Automation and integration interface	REST API and CLI to link to existing IAM infrastructure and workflows.
Real-time alerts	Send alerts to SIEM tools and fix violations in real time.
Central management of SSH configurations	Policy control, stronger security by using standard configurations, fewer errors.
User Portal	Extend key management to end users in the organization. Allow users to request access and provision keys centrally according to policies.
Compliance support	Enables compliance to current requirements and planned updates to PCI, NIST/FISMA, SOX, HIPAA, Basel III mandates.

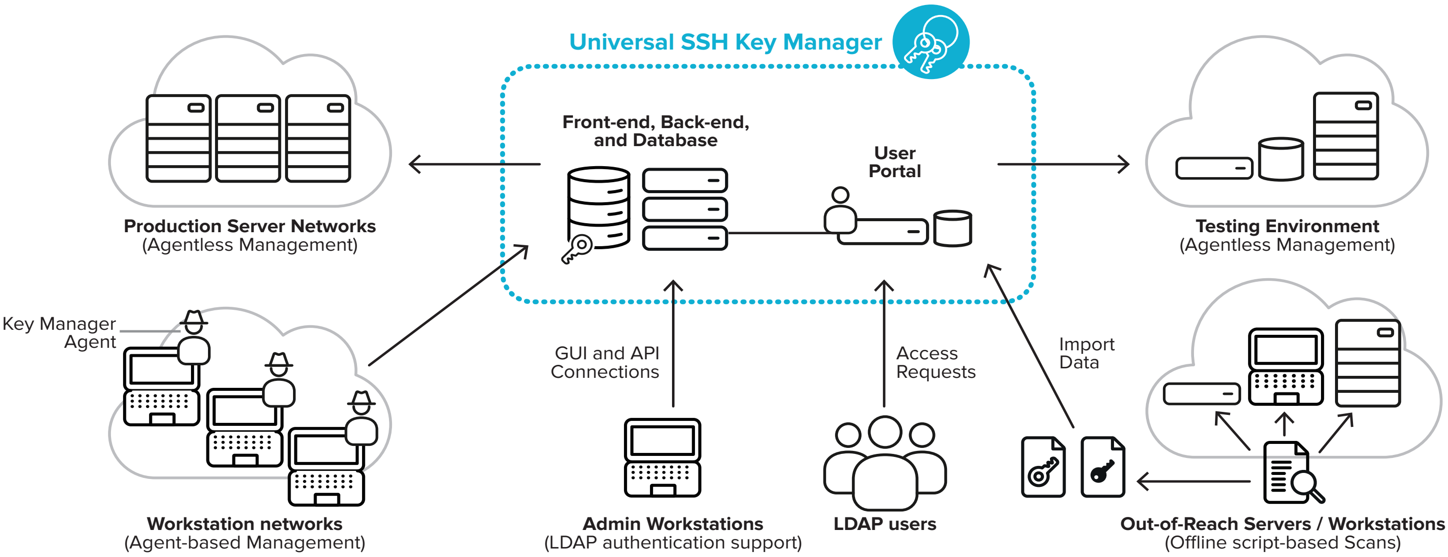
TECHNICAL SPECIFICATIONS

Supported Platforms for SSH Key Manager Server and SSH User Portal	• Virtual appliance for VMWare ESX 5.5 and other hypervisors • Red Hat Enterprise Linux / CentOS 6.5 and newer 6.x versions
Supported Databases for SSH Key Manager Server	• Oracle 11.2 and 12 • PostgreSQL 9.2
High Availability	• Multiple UKM server support for high availability and scaling • Non-intrusive – no point of failure to production operations
Discovery	• Public & private key discovery by size and type • Passphrase existence • Rogue keys • Key owner and other key attributes (including location, permissions, key comment) • Trust relationships per host & host groups • Host keys
Monitoring	• Detects unauthorized changes to SSH configurations • Detects unauthorized additions, removals and changes to user keys • Detection and tracking of SSH key-based logins • Configurable, real-time email alerts
Key Enforcement	• Brings user keys under central admin control (Relocate keys to root owned directories on host) • Creation of passphrase-protected keys and enforcement of adherence to passphrase policies • Centralized management of authorization policies • Managing key restrictions (such as command and allow-from restrictions)
Automation	• Key generation, deployment, renewal, update and removal • Centralized SSH software configuration management • Automate processes using command line integration • Provision temporary access (keys automatically removed after expiration)
Admin Authentication	• Local authentication • External accounts from Active Directory • Password and certificate based authentication
Role Based Administration	• RBAC for Key Manager admins (for both local & Active Directory administrator accounts) • Customizable roles to fit the tasks of individual administrators
Logging, Alerts, Alarms	• Comprehensive audit trail for changes to SSH keys and SSH configurations both initiated by Key Manager administrators as well as unauthorized changes done locally on the managed hosts • Email and syslog alerts for changes to SSH keys and configurations • Alerts of suspicious key activity per host (keys removed after use)
Management Methods	• Web GUI - Recent & stable Firefox - Recent & stable Chrome - Internet Explorer 10, 11 • CLI • REST API
Management Connection Types	• Support for agent-based and agentless host management • Support for script-based key discovery. Perform scans using existing orchestration tools (e.g. Chef, Puppet, Ansible) and import results. Management actions require agent/agentless connections.
Supported Key Algorithms	• RSA, DSA, ECC/ECDSA, Ed25519
Supported HSM products	• SafeNet Luna SA 5.4 (used for storing keys for agentless connections)

UNIVERSAL SSH KEY MANAGER TECHNICAL SPECIFICATIONS

Supported SSH versions	• Attachmate RSIT 6.1, 7.1, 8.1 • Centrify SSH 2013 • OpenSSH 4.x - 6.x • SunSSH 1.1.5, 2.0 • Tectia SSH 6.4 • Tectia Server for IBM z/OS 6.3, 6.4 • Quest OpenSSH 4.x - 5.2 • Bitvise SSH Server 6.24

Supported Platforms for Managed Hosts	Platform	Agentless	Agent-Based
	HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)	•	•
	HP-UX 11iv2, 11iv3 (IA-64)	•	•
	IBM AIX 5.3, 6.1, 7.1 (POWER)	•	•
	IBM z/OS 1.13, 2.1	•	
	Microsoft Windows Vista, 7, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2		•
	Oracle Enterprise Linux 5	•	•
	Oracle Solaris 9, 10, 11 (SPARC)	•	•
	Oracle Solaris 10, 11 (x86-64)	•	•
	Red Hat Enterprise Linux 4, 5, 6, 7 (x86, x86-64)	•	•
	CentOS 4, 5, 6, 7 (x86, x86-64)	•	•
	SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)	•	•
	SUSE Linux Enterprise Server 10, 11 (x86, x86-64)	•	•
	Ubuntu Desktop 12.04, 14.04 (x86, x86-64)	•	
	Ubuntu Server 12.04, 14.04 (x86, x86-64)	•	


Universal SSH Key Manager
Front-end, Back-end, and Database
User Portal
Production Server Networks
(Agentless Management)
Testing Environment
(Agentless Management)
Key Manager Agent
GUI and API Connections
Access Requests
Import Data
Workstation networks
(Agent-based Management)
Admin Workstations
(LDAP authentication support)
LDAP users
Out-of-Reach Servers / Workstations
(Offline script-based Scans)