Identity and Access Management for Secure Shell Infrastructure

THE PROBLEM

There are large numbers of unmanaged access credentials in practically every enterprise network. Most of these credentials are SSH keys that are often self-provisioned by users. This is a serious security and compliance issue that poses an existential risk to many organizations around the world.

Enterprises rely on Secure Shell (SSH) for authentication and confidentiality (encryption) of business critical functions such as automated backups, day-to-day file transfers and interactive user access for systems administration. However, the process of generating, configuring and deploying SSH keys that enable these functions is often left to end users. The lack of a central authority to oversee the process of issuing these credentials means there is no way to track credential lifecycles nor to ensure they are created according to policies and regulatory requirements.

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.
THE SOLUTION

Universal SSH Key Manager (UKM) is an enterprise grade SSH user key management solution that uses a non-disruptive approach that enables enterprises to gain and retain control of the SSH infrastructure. Universal SSH Key Manager does not interfere with normal operations in production systems. There is no need to rip and replace how users get their work done or change the hundreds of automated processes or service accounts that manage daily business. UKM's non-disruptive approach is based on five principles:

- **Assess**: Define policies around SSH and validate your SSH environment against these policies.
- **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.

FEATURES AND BENEFITS

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agentless and script-based discovery</td>
<td>Gain visibility with a quick and non-invasive inventory process for SSH keys.</td>
</tr>
<tr>
<td>SSH policies and reports</td>
<td>Quickly report on compliance of the SSH key environment against defined policies.</td>
</tr>
<tr>
<td>Automation and integration interface</td>
<td>Leverage the in-place IAM infrastructure by extending it with UKM to cover also SSH access. UKM provides APIs for easy integration.</td>
</tr>
<tr>
<td>Real-time alerts</td>
<td>Improved and deepened security controls and leveraging existing SIEM solutions to detect and fix violations in real time.</td>
</tr>
<tr>
<td>Central management of SSH configurations</td>
<td>Policy control, improved situational awareness, and stronger security by using standard configurations. Reduced risk of manual errors.</td>
</tr>
<tr>
<td>User Portal</td>
<td>Streamline workflows by extending SSH key management to end users in the organization. Allow users to request access and provision keys centrally according to policies.</td>
</tr>
<tr>
<td>Compliance support</td>
<td>Enables compliance to current requirements and planned updates to PCI, NIST/FISMA, SOX, HIPAA, Basel III mandates.</td>
</tr>
</tbody>
</table>
## 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

## Supported Databases
- Oracle 11.2, 12, PostgreSQL 9.2

## High Availability
- Multiple UKM server support for high availability and scaling
- Non-intrusive – no point of failure to production operations

## Policy compliance and reporting
- Create policies on cryptographic properties, allowed trusts, shared private keys, unused keys and key sign-offs
- Validate the SSH key environment against defined policies
- Produce PDF reports on policy compliance and application remediation
- Schedule automatic sending of reports by email

## 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
- CLI, REST API, Web GUI (Recent & stable Firefox, Chrome, Internet Explorer 10, 11)

## 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 11.5, 2.0
- Tectia SSH 6.4
- Tectia Server for IBM z/OS 6.3, 6.4
- IBM ported tools for IBM z/OS: OpenSSH
- PuTTY Client
- Quest OpenSSH 4.x - 5.2
- Bitvise SSH Server 6.24, 6.45

### Supported Platforms for Managed Hosts

<table>
<thead>
<tr>
<th>Platform</th>
<th>Agentless</th>
<th>Agent-Based</th>
<th>Offline Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HP-UX 11iv2, 11iv3 (IA-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IBM AIX 5.3, 6.1, 7.1 (POWER)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IBM z/OS 1.13, 2.1, 2.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Microsoft Windows Vista, 7, 10, Server 2003, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Oracle Enterprise Linux 5</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Oracle Solaris 9, 10, 11 (SPARC)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Oracle Solaris 10, 11 (x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4, 5, 6, 7 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CentOS 4, 5, 6, 7 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Desktop 10, 11 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10, 11 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ubuntu Desktop 12.04, 14.04 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ubuntu Server 12.04, 14.04 (x86, x86-64)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>