ManageEngine
Key Manager Plus

Gain visibility and control over your SSH and SSL environments

www.keymanagerplus.com

How unmanaged keys and certificates impair your layered security defenses

Over the years technology has been constantly growing and evolving—as have cyberthreats and security breaches. Enterprises are meticulously working with various solutions and strategies to strengthen their security infrastructure. But, there's no silver bullet when it comes to security. A highly-recommended and widely-adopted technique among enterprises today is following a layered approach to information security. This technique combines multiple security strategies that offset one another's capabilities to prevent malicious intrusions, ensuring tighter security.

SSH keys and SSL certificates are at the heart of this comprehensive layered security framework. These digital identities serve as the foundation of trust, over which all the other security strategies unfold and operate.

As a result, encryption keys have also become the prime target for cybercriminals, who exploit them to create loopholes in your layered security infrastructure. Once hackers break into your organization's SSH and SSL environment, they constantly work to expand their access, steal identities of higher privileges, and establish permanent backdoors.

Failing to protect your keys and certificates completely ends up impairing your layered security defenses that blindly rely on the trust provided by keys and certificates.
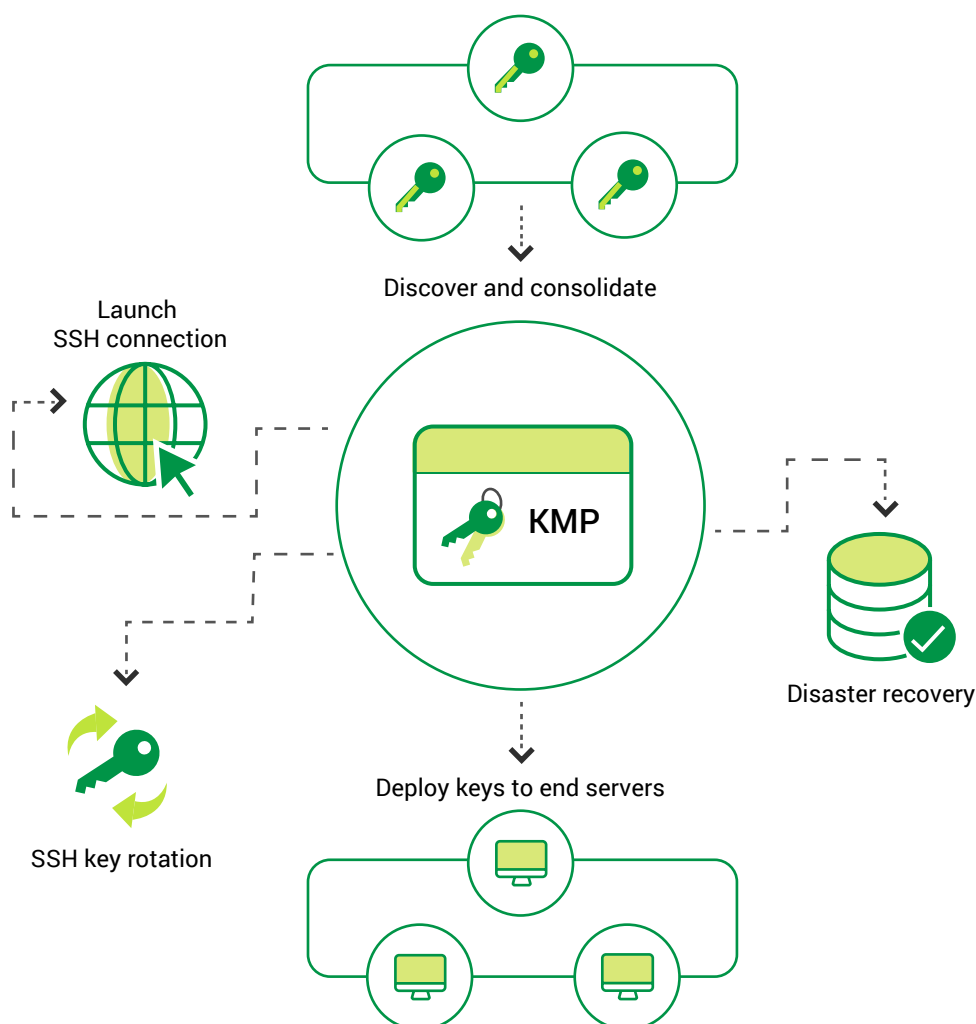
Here's what you have to do to reinforce trust in your SSH keys and SSL certificates:

- Gain complete visibility over your SSH and SSL environments.
- Centralize all key and certificate management operations.
- Enforce policies for creating keys and certificates.
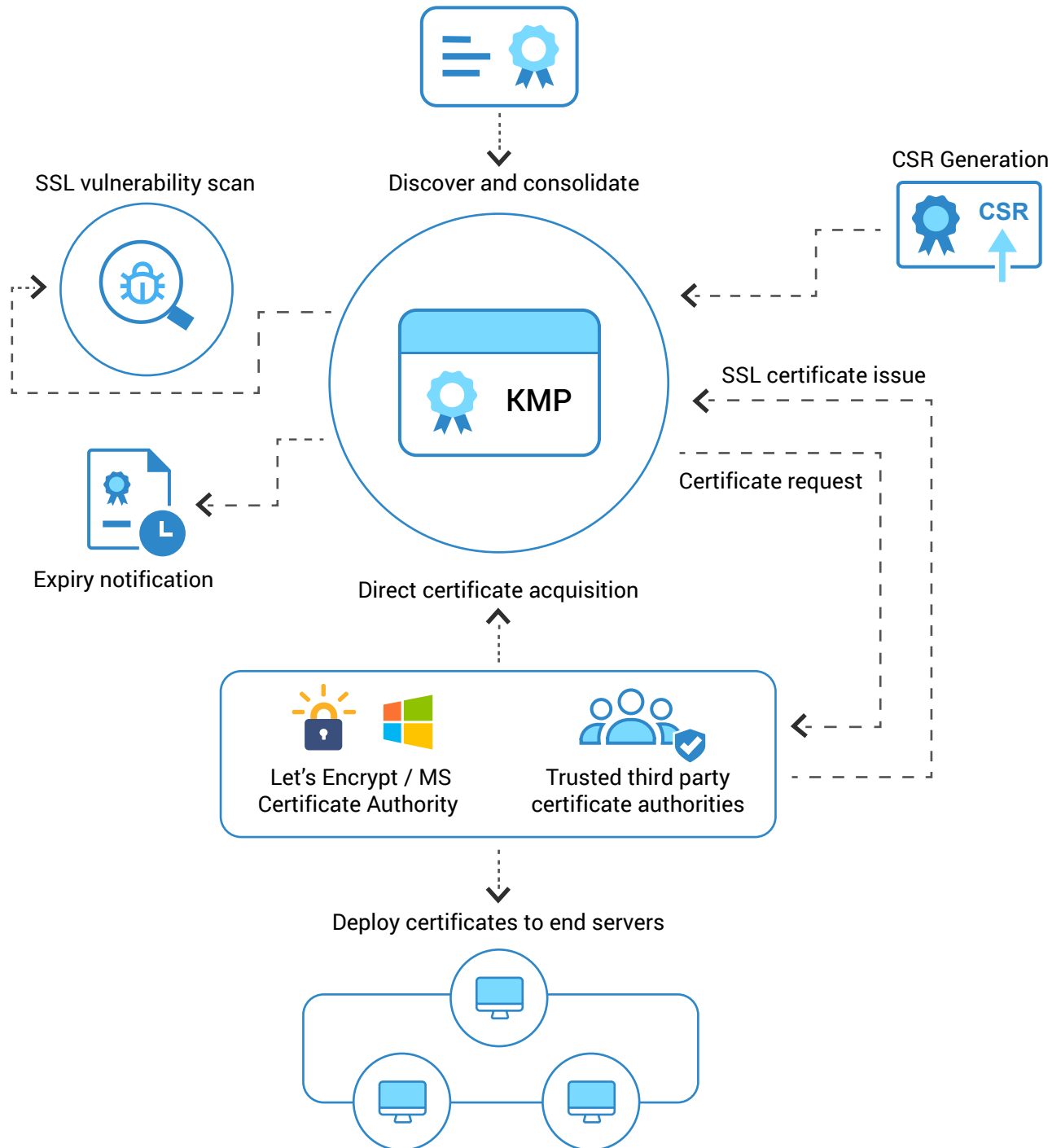- Create fined-grained access control regulations and log all user activity.

Key Manager Plus helps you effectively take control over your SSH and SSL environments

The average organization houses over 23,000 keys and certificates. Without an automated way to streamline key and certificate life cycle management, it's almost impossible to achieve the required level of visibility and control over your SSH and SSL environments. Key Manager Plus, our web-based key and certificate management solution, helps you discover, consolidate, deploy, renew, track, and manage the entire life cycle of SSH keys and SSL certificates. It helps you take total control over your encryption keys to preempt breaches and compliance issues.

SSH Key Life cycle Management

Discover and consolidate

Launch SSH connection

KMP

Disaster recovery

SSH key rotation

Deploy keys to end servers

SSL Certificate Life cycle Management

SSL vulnerability scan

Discover and consolidate

CSR Generation

CSR

SSL certificate issue

Certificate request

Expiry notification

Direct certificate acquisition

Let's Encrypt / MS Certificate Authority

Trusted third party certificate authorities

KMP

Deploy certificates to end servers

Highlights of Key Manager Plus

SSH key management

Key Manager Plus automatically discovers SSH keys present in your network and consolidates them in its secure, centralized repository. You can centrally launch remote SSH sessions, perform scheduled key rotations, create and deploy new keys, delete unwanted keys, and obtain instant, comprehensive reports on all key management activity.

SSL certificate management

Managing an SSL environment can be daunting if your organization uses a large number of SSL certificates from various vendors with different expiration dates. Key Manager Plus discovers and consolidates all SSL certificates within your network, tracks their usage, centralizes certificate requests and deployment, scans and remediates configuration vulnerabilities, and provides prompt alerts well ahead of certificate expiration.

Discover

Automatically discover all SSH resources within your network and add users and their respective private keys.

Consolidate, create, and deploy

Consolidate all discovered keys in Key Manager Plus' secure, centralized repository. Centrally create new SSH key pairs and deploy them to target servers.

Key-user mapping

Get a holistic, graphical representation of key-user relationships across your organization.

Discover and consolidate

Discover all SSL certificates within your network regardless of vendor, encryption algorithm, etc., and consolidate them in a secure, centralized repository.

Centralized deployment

Centralize deployment of newly acquired or renewed certificates to their respective end-servers.

Expiration alerts

Receive periodic, customized alerts on certificate expiration well in advance.

Launch SSH sessions

Launch direct SSH sessions with target systems from one location and capture the sessions for your records.

Configure key management policies

Enforce strict policies for key creation. Remove all existing keys for a fresh start or create and append new keys.

Active Directory integration

Leverage our integration with Active Directory to directly import users and user groups into Key Manager Plus.

Disaster recovery

Schedule automated backups of the entire database for disaster recovery.

Audits and reports

Generate instant, comprehensive reports on various key and certificate management operations with tamper-proof audit records of all user activity and provisions.

CSR generation and certificate request workflow

Generate CSRs instantly and request and obtain certificates from trusted third-party certificate authorities with a hassle-free certificate request workflow.

Let's Encrypt integration

Leverage our integration with the certificate authority Let's Encrypt to completely automate end-to-end management of the certificate life cycle, including certificate acquisition, deployment, tracking, and renewal.

Manage certificates from Active Directory and the MS certificate store

Discover, import, and manage certificates mapped to user accounts in Active Directory and certificates present in the MS certificate store. Completely automate their life cycle management through an integration with your Microsoft Certificate Authority.

SSL vulnerability scan

Scan SSL certificates and end-servers after deployment for configuration vulnerabilities such as Heartbleed, POODLE, certificate revocations, and weak cipher suites, and remediate them instantly.

> ManageEngine Key Manager Plus is an efficient and surprisingly user-friendly tool that can potentially help network administrators anticipate and block security breaches and bypass annoying compliance processes by providing all the necessary tools for monitoring and controlling SSH keys and SSL certificates.

SOFTPEDIA®
www.softpedia.com

> We were quite impressed by this product that simplifies even complex processes of key management, where most organizations fail, leaving themselves vulnerable to cyber attacks.

The Hacker News
Security in a serious way
www.thehackernews.com

> ...serves a one-stop solution for managing all digital identities.
>
> Users are treated with total visibility into the SSH and SSL environments.
>
> Administrators gain absolute control of the keys preventing instances and the likelihood of breaches and ensure adherence to compliance policies.

FinancesOnline.com
www.reviews.financesonline.com

> A web-based tool that can help to consolidate, control, manage, monitor and audit the entire life cycle of SSH keys and SSL certificates is ManageEngine Key Manager Plus.

TechTarget
www.techtarget.com

"

ManageEngine's Key Manager Plus enables us to stay on top of SSL certificates for all of our websites. With Key Manager Plus, we're able to monitor which certificates are nearing expiration and roll out new certificates in a timely manner.

Ken Odibe

Senior cloud infrastructure consultant,
Sapphire systems.

Download

Get Quote

Zoho Corporation Pvt. Ltd.
4141 Hacienda Drive Pleasanton,
CA 94588, USA
Phone: +1-925-924-9500
Fax: +1-925-924-9600
Email: sales@manageengine.com

Over **180,000+** companies around the world trust

ManageEngine