

# ManageEngine KeyManager Plus

Une solution web de gestion des clés SSH et des certificats SSL pour les entreprises.

# Schéma d'une cyberattaque

## Reconnaissance:

L'attaquant effectue une recherche et identifie une cible potentielle et vulnérable.

1

## Établissement d'un point d'appui:

L'attaquant assure un contrôle continu des systèmes compromis en établissant des portes dérobées permanentes.

3

## Exfiltration de données :

L'attaquant prend le contrôle de comptes privilégiés et vole des données sensibles.

5

## Compromission initiale:

L'attaquant exploite une vulnérabilité de la cible et réussit à s'y introduire.

2

## Élévation des privilèges:

L'attaquant s'efforce d'exploiter des systèmes dotés de privilèges plus importants et étend son accès.

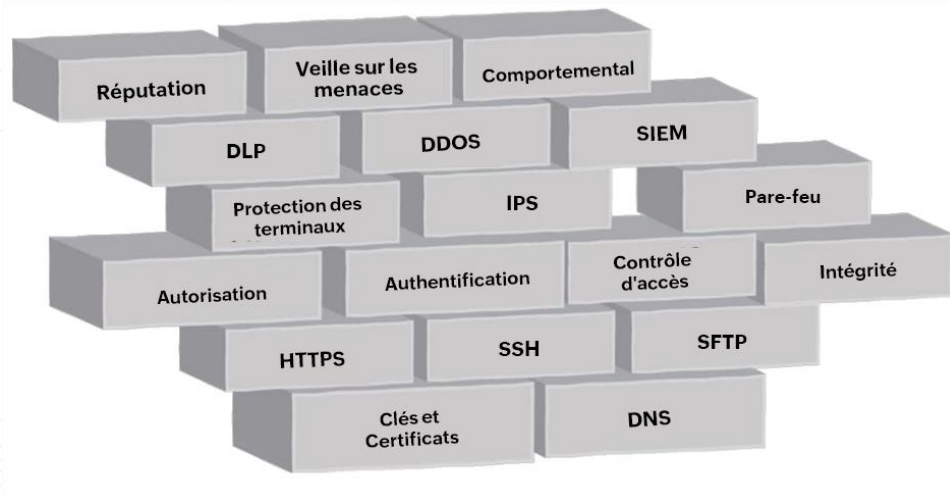
4

## Maintien de la présence:

L'attaquant s'assure un accès permanent au réseau par le biais de diverses portes dérobées.

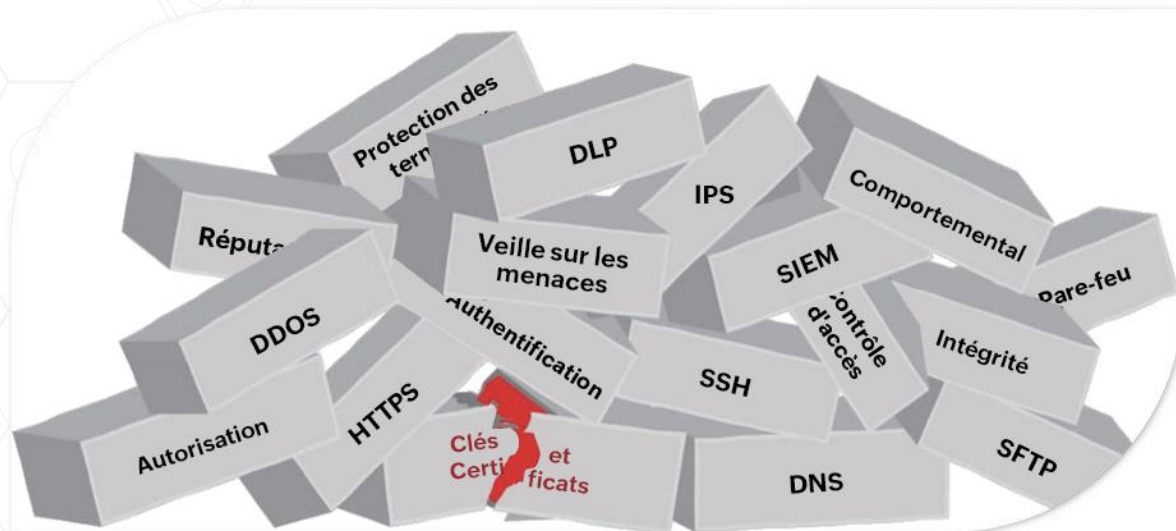
6

# Clés SSH et certificats SSL : La base d'une défense de sécurité en couches



Les organisations adoptent aujourd'hui une **approche par couches** de la sécurité de l'information, dont les clés et les certificats constituent la base.

# Lorsque la base n'est pas sécurisée





De nombreuses vulnérabilités très médiatisées dans le passé impliquaient la compromission de clés SSH et de certificats SSL mal gérés.

# Informations importantes

---

**23 922 clés et certificats**


En moyenne par entreprise



- Selon un [rapport](#) de recherche de Ponemon, une organisation moyenne possède plus de **23 000** clés et certificats.
- Les cybercriminels consacrent beaucoup de temps et d'efforts à voler les clés de chiffrement.
- Selon un [rapport de Gartner](#), plus de **50%** des attaques de réseau sont dues à l'abus de SSL.

# Problèmes de gestion et risques encourus

- Absence de gestion centralisée du cycle de vie
- Absence d'informations appropriées sur les liens de confiance
- Absence de contrôle d'accès précis ; aucune visibilité sur les activités des utilisateurs.
- La prolifération entraîne des accès non autorisés et des abus de privilèges.

The background features a dark blue diagonal section on the left containing a network of light blue nodes and lines. Three teal circles of varying shades are arranged vertically on the diagonal. Two teal icons are present: one of a certificate with a ribbon seal and another of a key with circular arrows. A hand is visible at the bottom right, pointing towards the circles.

**Que devez-vous faire pour  
renforcer la confiance dans  
vos clés et certificats?**

---

- **Découvrez et consolidez** toutes les clés et tous les certificats de votre organisation.
- **Centralisez** la création et le déploiement ; établissez des contrôles d'accès stricts.
- **Suivez** les relations de confiance ; identifiez qui accède à quoi.
- **Faites tourner les clés** périodiquement pour éviter les abus de confiance.
- **Suivez les renouvellements de certificats** pour éviter le risque de pannes inattendues.
- **Retirez** les clés inutilisées lorsque les utilisateurs quittent l'organisation.
- **Auditez** toutes les activités des utilisateurs.

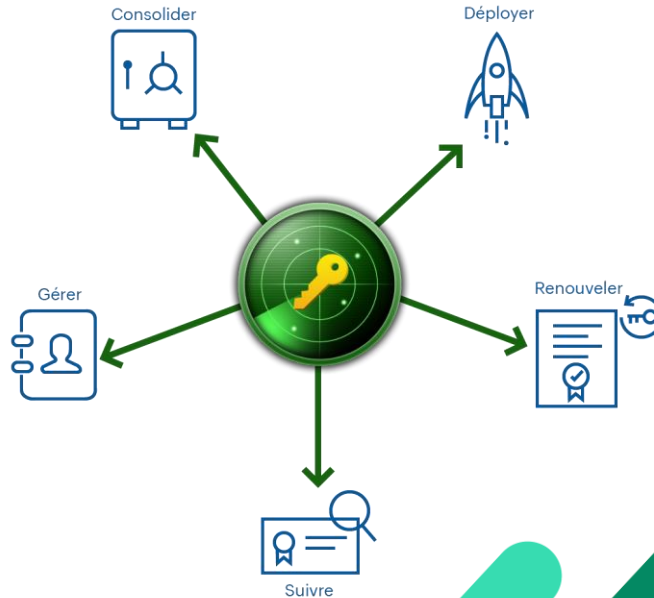


**Key Manager Plus centralise et automatise  
la gestion des cycles de vie des clés et des  
certificats.**

---

# Gestion des certificats SSL avec Key Manager Plus

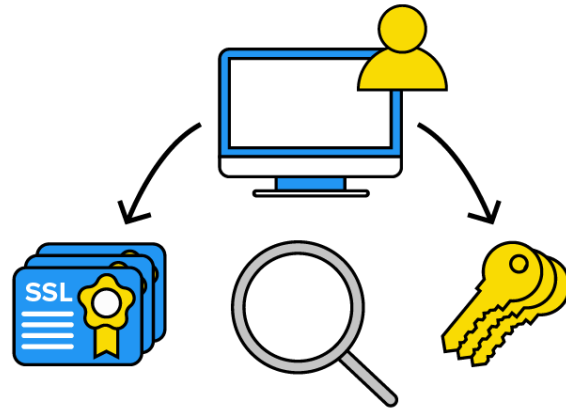
---



# Découvrez et consolidez

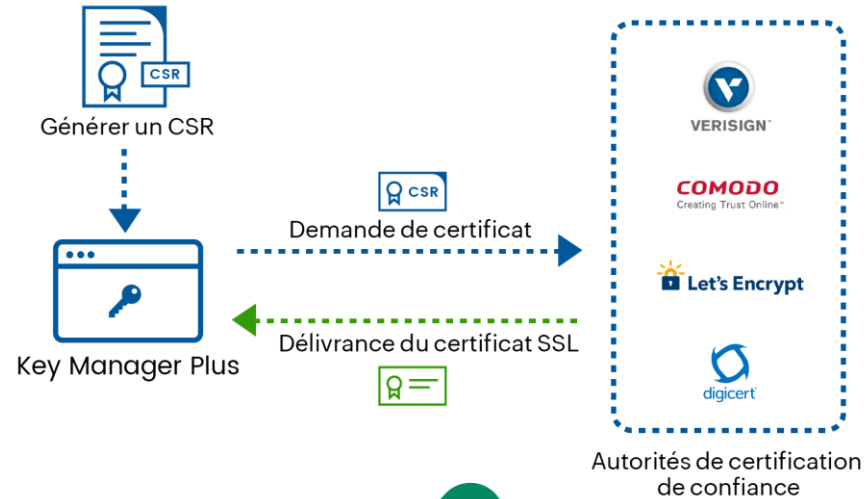
---

Key Manager Plus recherche les certificats SSL sur votre réseau et les consolide dans son référentiel centralisé sécurisé.



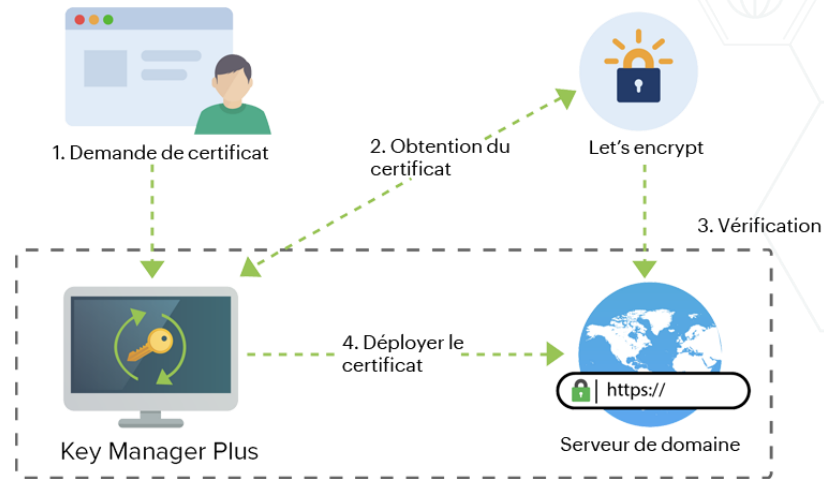
# Centralisez la demande, l'acquisition et le déploiement des certificats

Générez instantanément des CSR, demandez et obtenez des certificats auprès d'autorités de certification tierces fiables et déployez-les sur les serveurs finaux nécessaires grâce à un workflow de demande de certificats simplifié.



# Intégration avec Let's Encrypt

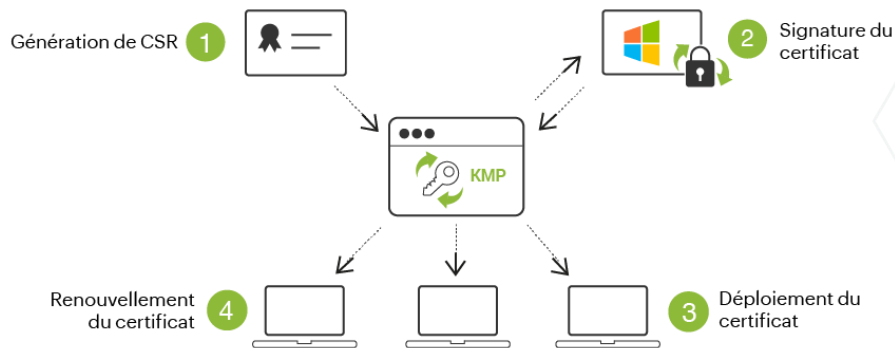
Tirez parti de notre intégration avec l'autorité de certification **Let's Encrypt** pour automatiser complètement la gestion de bout en bout du cycle de vie des certificats (acquisition, déploiement, suivi et renouvellement).




# Gérez les certificats d'Active Directory et de Microsoft Certificate Store

Découvrez, importez et gérez les certificats associés aux comptes d'utilisateurs dans Active Directory et les certificats présents dans Microsoft Certificate Store.

Automatisez complètement la gestion de leur cycle de vie grâce à une intégration avec votre autorité de certification Microsoft.





**Gestion des clés SSH  
avec [Key Manager Plus](#)**

- Découvre automatiquement toutes les ressources SSH au sein de votre réseau ; consolide les clés privées dans un référentiel sécurisé.
- Centralise la création et le déploiement des clés.
- Fait tourner les paires de clés périodiquement à des intervalles de temps spécifiés.
- Lance des sessions SSH directes avec les systèmes cibles.
- Audite et suit toutes les activités de l'utilisateur ; fournit des alertes en temps opportun lors de la détection d'activités inhabituelles.
- Fournit des rapports instantanés et complets sur toutes les activités de gestion des clés et des certificats.

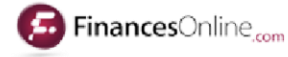


# FEUILLE DE ROUTE

- Gestion de bout en bout du cycle de vie des certificats grâce à une intégration avec des autorités de certification tierces de confiance.
- Génération et déploiement automatiques de certificats pour les utilisateurs AD et LDAP.
- Nouveaux rôles d'utilisateur pour fournir des autorisations granulaires pour le partage des ressources.
- Accès ininterrompu aux applications grâce à la haute disponibilité.
- Mécanisme d'approbation pour l'acquisition et le déploiement de clés et de certificats.
- Prise en charge de l'authentification à deux facteurs.
- Flux de travail actionnable sur la gestion des certificats à partir de ManageEngine ServiceDesk Plus.

# Les experts du secteur font confiance à Key Manager Plus

---



Key Manager plus de ManageEngine nous permet de rester au courant des certificats SSL pour tous nos sites Web. Avec Key Manager Plus, nous sommes en mesure de surveiller les certificats qui arrivent à expiration et de déployer de nouveaux certificats en temps voulu.

**Ken Odibe**  
Consultant Senior en Infrastructure Cloud,  
Sapphire systems.



# Merci de votre attention!

Si vous avez des questions, n'hésitez pas à nous écrire à **[helpdesk@pgsoftware.support](mailto:helpdesk@pgsoftware.support)**