ManageEngine
Password Manager Pro

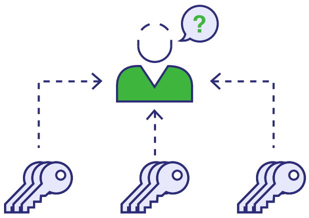
Are you securing your non-human privileged identities?

Learn more about potential security risks and the ways to mitigate them.

Privileged accounts are powerful accounts within an organization that information and communications teams use to set up the IT infrastructure, install new hardware and software, run critical services, and conduct maintenance operations. They serve as master keys for the organization's highly critical business assets housing sensitive information. Privileged account management solutions help IT administrators secure access to these mission critical assets by allowing them to store, share, manage, monitor, and audit the life cycle of all kinds of privileged accounts from a single, unified console.

However, most privileged account management solutions offer feature sets that are restricted to just securing and managing the passwords of privileged accounts like service accounts, application accounts and the like. Passwords, beyond a doubt, are noteworthy privileged access credentials. But the constant evolution of technology and expanding cybersecurity perimeter calls for enterprises to take a closer look at the other identities facilitating privileged access, especially cryptographic keys—which despite serving as access credentials for huge volumes of privileged accounts, are often ignored.

Here are some potential security risks posed to privileged assets within your IT ecosystem because of orphaning non-human access identities like SSH keys and SSL/TLS certificates.

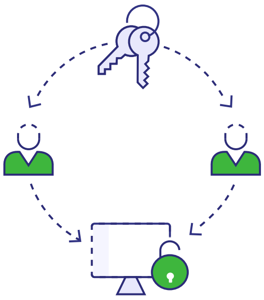


1. Uncontrolled numbers of SSH keys trigger trust-based attacks

A recent report, State of machine identity management, points out that 53% of organizations do not have a centralized SSH key management program, and 38% of organizations declare a likelihood of security incidents arising due to stolen SSH keys. Without a centralized key management approach, anybody in the network can create or duplicate any number of keys. These keys are often randomly generated as needed and are soon forgotten once the task they are associated with is done. Malicious insiders can take advantage of this massive ocean of orphaned SSH keys to impersonate admins, hide comfortably using encryption, and take complete control of target systems.

2. Static keys create permanent backdoors

Enterprises should periodically rotate their SSH keys to avoid privilege abuse, but huge volumes of unmanaged SSH keys make key rotation an intimidating task for IT administrators. Moreover, due to a lack of proper visibility on which keys can access what, there is widespread apprehension about rotating keys in fear of accidentally blocking access to critical systems. This leads to a surge of static SSH keys, which have the potential to function as permanent backdoors.

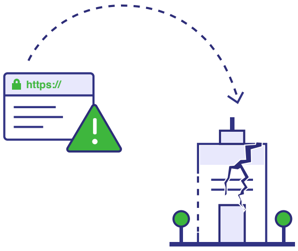


3. Unintentional key duplication increases the chance of privilege abuse

For the sake of efficiency, SSH keys are often duplicated and circulated among various employees in an organization. Such unintended key duplication creates a many-to-many key-user relationship, which highly increases the possibility of privilege abuse. This also makes remediation a challenge since administrators have to spend a good amount of time revoking keys to untangle the existing relationships before creating and deploying fresh, dedicated key pairs.

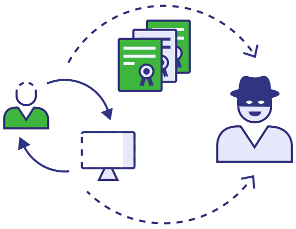
4. Failed SSL certificate renewals hurt your brand's credibility

SSL certificates, unlike keys, have a set expiration date. Failing to renew SSL certificates on time can have huge implications on website owners as well as end users. Browsers don't trust websites with expired SSL certificates; they throw security error messages when end users try to access such sites. One expired SSL certificate can drive away potential customers in an instant, or worse, lead to personal data theft for site visitors.



5. Improper SSL implementations put businesses at risk

Many businesses rely completely on SSL for internet security, but they often don't realize that a mere implementation of SSL in their network is not enough to eliminate security threats. SSL certificates need to be thoroughly examined for configuration vulnerabilities after they are installed. When ignored, these vulnerabilities act as security loopholes which cybercriminals exploit to manipulate SSL traffic and launch man-in-the-middle (MITM) attacks.



6. Weak certificate signatures go unheeded

The degree of security provided by any SSL certificate depends on the strength of the hashing algorithm used to sign the certificate. Weak certificate signatures make them vulnerable to collision attacks. Cybercriminals exploit such vulnerabilities to launch MITM attacks and eavesdrop on communication between users and web servers. Organizations need to isolate certificates that bear weak signatures and replace them with fresh certificates containing stronger signatures.

Incorporating an enterprise-wide crypto key management strategy

All the above scenarios highlight how important it is to widen the scope of your privileged access security strategy beyond password management. Even with a robust password manager in place, cybercriminals have plenty of room to circumvent security controls and gain access to superuser accounts by exploiting various unmanaged authentication identities, including SSH keys and SSL certificates. Discovering and bringing all such identities that are capable of granting privileged access, under one roof is one important step enterprises should take to bridge gaps in their privileged access security strategy.

Here are some best practices to begin with, that help your IT manage non-human identities effectively along with privileged passwords, to enforce complete governance over all kinds of privileged access within the corporate network.

☑ Discover

Discover SSH keys and SSL/TLS certificates deployed across heterogeneous environments.

☑ Consolidate

Consolidate the discovered keys and certificates in a secure, centralized repository.

☑ **Centralize**

Inhibit proliferation of SSH keys and SSL/TLS certificates by centralizing their creation and deployment.

☑ **Automate**

Streamline and automate the life cycle management of public certificates—right from CSR generation, provisioning, deployment, and renewal.

☑ **Rotate**

Enforce automated rotation of SSH keys at periodic time intervals via creation of scheduled tasks.

☑ **Scan**

Scan and remediate SSL configuration vulnerabilities regularly, after certificates have been deployed.

☑ **Monitor**

Set up the right type of alerting mechanism, paving the way for proactive certificate renewals well ahead of expiration.

Secure and govern your SSH and SSL/TLS ecosystem with Password Manager Pro

Password Manager Pro is an enterprise-grade privileged account management solution that helps organizations gain complete visibility and control over privileged credentials like passwords, SSH keys, and SSL certificates from a single roof without having to navigate between multiple consoles. Via a seamless integration with Key Manager Plus—ManageEngine's SSH key and SSL/TLS certificate management solution—Password Manager Pro enables IT teams stay on top of discovery, deployment, rotation, renewal, audit, and holistic management of all kinds of authentication credentials that facilitate privileged access.

Take control over your orphaned keys and certificates today

Schedule a personalized demo

www.passwordmanagerpro.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro