eBook

Introduction to Secrets Management

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Introduction

Whether you are new to secrets management and being thrown into it because you work in DevOps, or you are well versed in the concept and just want to update your thinking, this resource is for you. This eBook, although not long enough to deep dive into all the details, will provide an understanding to start you on the right path to get you where you want to be.

In technology, we use the term secrets to cover a swath of credentials that are all key to security. It is an unfortunate reality that sensitive data and systems will always be targets for malicious conduct. Though some of the users that seek out secrets to break into a system or database may believe they have an innocuous intent, it is not likely harmless from your point of view. Rest assured, however, that the majority that are looking to uncover secrets have malicious intent or are willing to provide them to others that do. Let's learn more about secrets management and how a centralized management system will benefit you by decreasing risk of losing sensitive information.

61%

of all breaches involve hacked credentials.

Source: Verizon 2021 Data Breach Investigations Report

What are secrets?

Secrets, in the digital space or DevOps, have various forms and names, but their purpose is to grant privileged access to systems and data. Secrets include objects that authenticate identities, such as passwords, API keys, tokens, SSH keys, and certificates.

We are most familiar with passwords which let the machine/application know that this person is likely an authorized user. When we speak of secrets, however, we are more commonly talking about machine-to-machine access validation objects.

Secrets are to be kept secure. If the secret is compromised, attackers could gain access to sensitive data and/or systems and result in a data breach or other security incidents.

Some examples of secrets in use are as follows:

Data and Systems:

- Database credentials enabling a container to access a database server
- SSH keys used by a local administrator to connect to a database
- Authentication for secure transactions between complex hybrid and multi-cloud systems

Applications:

- API keys for third-party services
- Passwords for database access
- Containerized applications built as a combined set of microservices that use secrets for secure interactions

Automation:

- Credentials for a CI/CD pipeline
- Access token for a chatbot

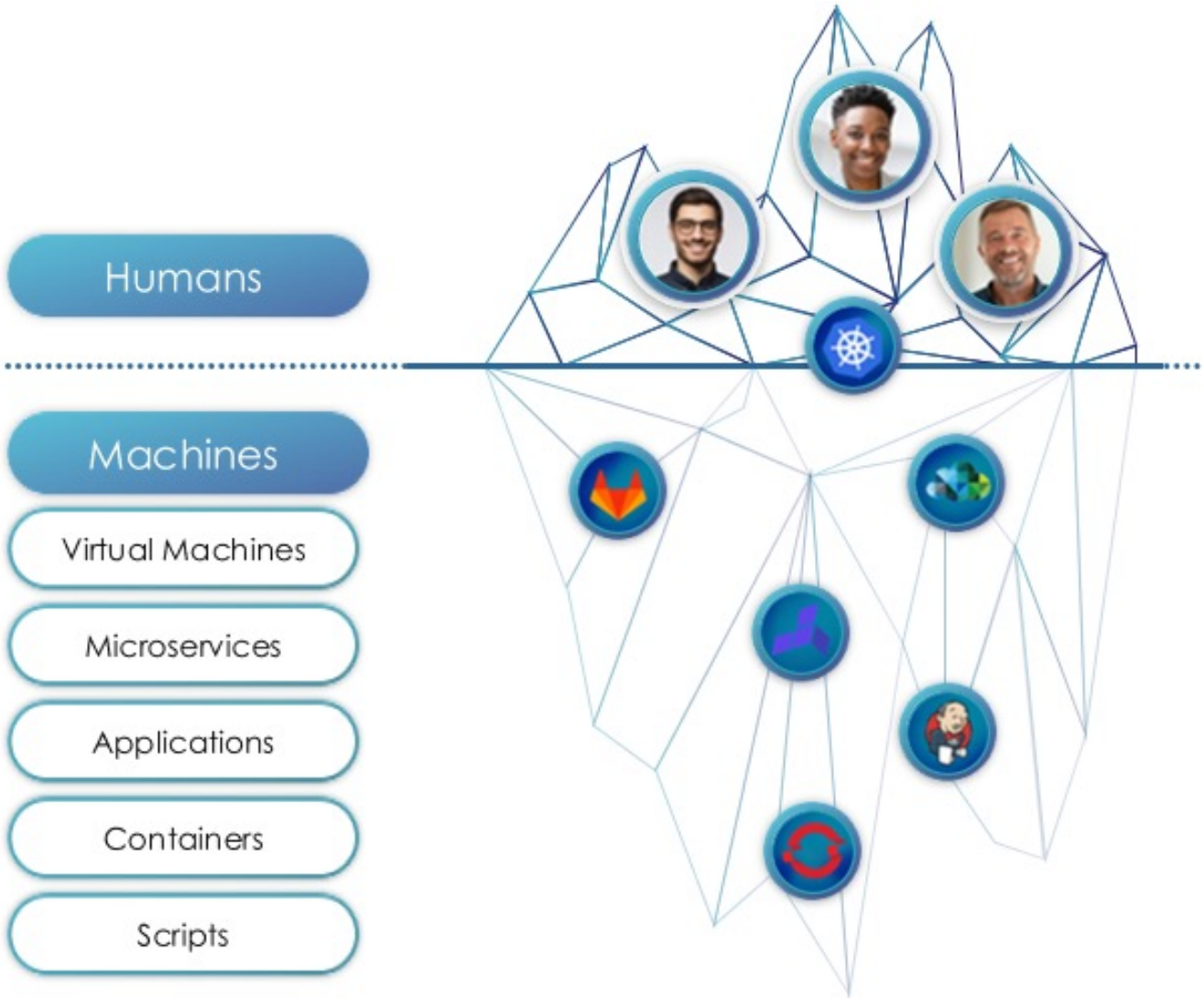
Why is secrets management important?

When the quantity of secrets within the organization is small, the secrets are the responsibility of the developer or admin for the application or service. That may work for a time, but as technology continues to be the answer to efficiencies and productivity, more systems and applications are deployed, leading to the need for DevOps to automate the interactions between them. Deploying and automating means more secrets are required to authenticate the users and applications.

At the rate of today's technology, it won't be long before your organization begins to lose track of all the secrets being created and what is termed "secrets sprawl" begins to take place. You may have heard about a breach or potential breach where a developer mismanaged a secret, and it was discovered in plain text within a public repository. Managing secrets in a centralized way, enables the following practices that mitigates the risks:

- Encrypts secrets rather than storing in plain text
- Stores secrets in a digital vault with security features in place
- Enables automatic rotation of secrets
- Ensures least privilege access so users and applications only have access needed to perform required tasks
- Tracks the use of secrets for auditing and compliance purposes

You can see from this list above how secrets management is a solid practice to elevate your security to a new level, especially with innovative product features like auto rotated or just-in-time secrets, or when the solution is secured with a Hardware Security Module (HSM). As you read the next section, think of the benefits this would bring to your organization.



The cost of poor secrets management versus the benefits of good secrets management

The cost of not implementing a secrets management solution can be significant especially when compared with effective secrets management.

Lacking secrets management, secrets are much more likely to be compromised, which could result in the following direct costs:

- **Data breaches** – Loss of sensitive data, such as customer PII, financial information, or intellectual property. This data could be used for identity theft, fraud, or other malicious purposes.
- **Unauthorized access** – Access to systems and applications by an unauthorized user. This could allow them to steal data, modify data, or disrupt operations.
- **Account takeover** – Accounts, such as email accounts, social media accounts, or cloud storage accounts could be infiltrated or seized. This could allow them to send phishing emails, post malicious content, or delete data.
- **DevOps disruption** – A disruption in DevOps operations could lead to delays in deployments, loss of productivity, and/or financial losses.

Not implementing a secrets management solution can result in the following issues:

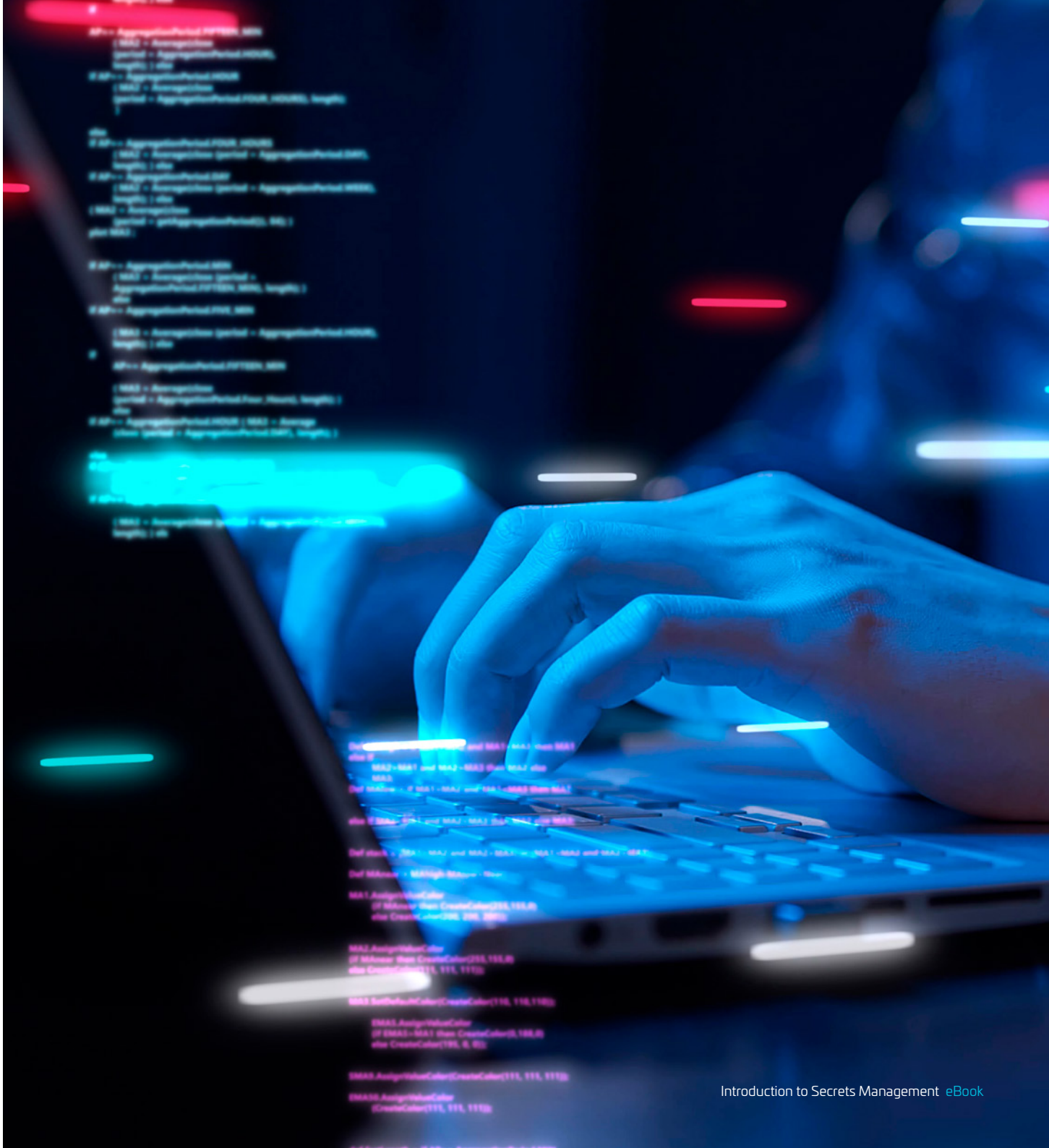
- **Credential leakage** – Storing credentials and secrets in an insecure manner, such as hardcoding them directly in source code or configuration files, increases the likelihood of accidental exposure. If an attacker gains access to these files, they can easily obtain the credentials and compromise the system.
- **Secrets can be reused** – Secrets that are reused across multiple systems and applications can make it easier for attackers to gain access to sensitive data. This is because once an attacker has compromised one secret, they can use it to gain access to other systems and applications.
- **It's difficult to manage secrets manually** – Managing secrets manually can be a complex and time-consuming task which can lead to errors and oversights. This greatly increases the risk of secrets being compromised.
- **Lack of auditability** – Without audit logs and access controls to track and monitor access to secrets, it becomes difficult to identify who accessed which secrets and when, hindering the ability to investigate security incidents.

By implementing a secrets management solution, organizations can help alleviate the above issues and mitigate risks of harm or loss of their sensitive data and systems. Secrets management solutions provide a secure way to store, manage, and access secrets as well as automate the rotation of secrets.

Implementing a secrets management solution leads to the following benefits:

- **Increased security** – Secrets management solutions increase the security of sensitive data and systems by providing a secure way to store, manage, and access secrets.
- **Reduced risk of compromise** – Automating the rotation of secrets and providing a secure way to store them greatly reduces the risk of secrets being compromised and thereby helps keep your data and systems safe. Using temporary, Just-in-Time secrets can go even further to prevent hacks by eliminating potentially vulnerable standing privileges.
- **Improved compliance** – Improve compliance with industry regulations by providing a secure way to store and manage secrets. Compliance is also aided by audit logging from the management system.
- **Increased efficiency** – DevOps operations are more efficient when the creation and rotation of secrets are automated and there is a centralized repository for storing secrets.
- **High availability and scaling** – A robust secrets management platform can auto-scale to meet the growing demands of modern DevOps environments and handle complex infrastructure and workloads.
- **Separation of duties** – Internal multi-tenancy of some secrets management solutions enable your organization a separation of duties without requiring you to deploy multiple instances for secrets storage. A proper solution can provide a completely isolated and autonomous secrets storage vault for each tenant, such as a business unit or a team, while enabling you to share objects between vaults as required.

If you are not already using a secrets management solution, keep reading for more about best practices so you can select a secrets management solution that best suits the needs of your organization.



Secrets Management **Best Practices**

Secrets are required by machines and people to interact securely with each other and to keep sensitive data and systems safe from abuse and misuse. With more and more systems, including microservices and automations, growing in popularity, secrets management is essential.

Often times, each developer is treating secrets as they learned how or sometimes "as long as it works." This often results in certificates and SSH keys stored in local files and servers, and API keys and passwords hardcoded into scripts, source code, or configuration files. Without the proper use of a good solution, secrets have been found in public repositories like GitHub and GitLab, in corporate messaging apps and shared drives.

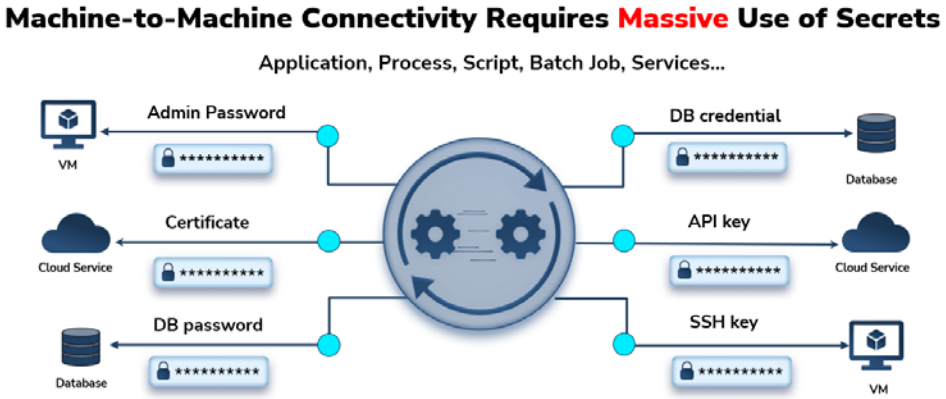
Security conscious organizations often implement policies regarding how secrets should be handled, but in documentation only, it is hard to get consistency on how they are used and stored, not to mention how often they should be rotated, versioned, or created.

Although individual DevOps platforms will have solutions to manage secrets, they are siloed and varied. Centralization of secrets enables consistency and security best practices.

1: Centralize secrets management

We've covered why secrets management increases security to some degree, but specifically having a central management solution provides the following benefits:

- Secrets are stored in a secure vault of sorts and not in plain text files, public repositories, shared drives, and other places that are not secure and where they can be discovered.
- Using a centralized system for automated generation of secrets reduces risk from users reusing secrets.
- Standardization whereby security minded professionals can set policies that align with the organization's risk and compliance ideals.
- Improved visibility through reporting and logs which aids in compliance and auditing.



> " Thousands of new, unique secrets are leaked every day"
>
> – **NCSU Report**

This phenomenon of secret sprawl has even gained attention of academics. In 2019, researches a North Carolina State University scanned GitHub over a six-month period and were easily able to get their hands on API keys from over 100,000 repositories.

Thier findings, presented in How Bad Can It Git? Characterizing Secret Leakage in Public GitHub Repositories, show that hundreds of thousands of API and cryptographic keys are leaked from GitHub repositores at a rate of thousands per day.

2: Use encrypted credentials

A secrets management solution will automatically encrypt all secrets according to the encryption standards set by the organization. Secrets are encrypted when they are first stored in the secrets management system. The encryption process uses a cryptographic algorithm to convert the secret into a format that cannot be read without the decryption key. The decryption key is stored securely, and a hardware security module (HSM) may be used for an even greater level of security.

Encrypted secrets are utilized when they are needed to access a system or application. The secrets management system will decrypt the secret and provide the plaintext version to the user or application to authenticate to the system or other application.

The encryption and decryption of secrets is done automatically by the secrets management system. Users and applications do not need to be aware of the encryption process.

3: Rotate secrets regularly

Secrets management solutions rotate secrets on a regular basis to help mitigate the risk of compromise. The frequency of rotation depends on the specific secrets management solution and the sensitivity of the secret, but it's recommended to rotate secrets at least every 90 days.

Secrets can be rotated manually, automatically, or based on a particular event. Centrally managed secrets can be set to either of these, depending on the use case:

- **Manual rotation** – In manual rotation, the user or administrator is responsible for rotating the secret. This can be a time-consuming and error-prone process.
- **Automatic rotation** – In automatic rotation, the secrets management solution automatically rotates the secret on a regular basis. This is the most common way to rotate secrets, as it is more secure and efficient than manual rotation.
- **Event-based rotation** – In event-based rotation, the secrets management solution rotates the secret when a specific event occurs, such as a server being decommissioned. This type of rotation can be used to ensure that secrets are rotated when they are no longer needed.

When a secret is rotated, the old secret is invalidated, and a new secret is generated. The new secret is then stored in the secrets management system and made available to the user or application that needs it.

4: Use dynamic Just-in-Time secrets

Secrets management solutions can allow the creation of temporary, Just-in-Time secrets which are only created when needed and expire after use. These short-lived secrets significantly enhance security by minimizing the timeframe for potential malicious activity and eliminating the standing privileges that can be a window of opportunity for hackers.

5: Train employees on secrets management

No system is going to be perfectly automated and work its wonders without the knowledge of your employees. In accordance with your secrets management system, develop a plan to educate employees about the benefits of using the solution and how best to interact with it, especially those in DevOps that may work with it the most.

6: Implement role-based access controls

Role-based access control (RBAC) within a secrets management solution can enable the organization to control who has access to secrets and what they can do with them. Best practice is to follow the least privilege principle to limit access rights for machines/human users to the bare minimum of permissions they need to perform their work. RBAC is another way that secrets management solutions can prevent unauthorized access to secrets and to ensure that secrets are only used by authorized users.

7: Monitor and audit secrets access

An enterprise grade secrets management solution will generate audit logs that track who accessed secrets, when they accessed them, and what they did with them. These logs can be used to track down security incidents and to ensure that secrets are being used properly.

Audit logs take note of just about every change\action within a qualified solution, providing a complete track record of your system operations. These logs are a valuable resource for admins and auditors who want to examine suspicious activities or to diagnose and troubleshoot issues.

Monitoring these audit logs can give an administrator invaluable insight into what behavior is normal and what behavior isn't. A log event, for example, will show what activity was attempted and whether it succeeded. This can be useful when identifying whether a system component is misconfigured or likely to fail.

Monitoring and auditing is important for cybersecurity professionals because it provides the insight and evidence in the event of a legal battle and can protect your business from liability.

Secrets Management **Solutions**

We've covered what secrets are and the benefits of managing all types of secrets in a central system, but how do you select a solution you will not regret? Of course, the answer is to select an option after having done some research and making sure you get the features that best fit your situation. Here are a few insights to kickstart your understanding of three categories of solutions.

SaaS solutions

Software as a Service solutions are very popular these days because they are quick to get up and running and easily scaled to fit your business as you grow.

Pricing – SaaS solutions are subscription based. Managed services can be subscriptions, but are more often based on, or combined with, some usage criteria pricing. Because SaaS solutions are managed by the solution provider, and don't require your own employee resources for installation and upgrade maintenance, they are often associated with a low Total Cost of Ownership (TCO).

Scalability – Secrets (certificates, SSH keys, API keys, and tokens) tend to increase in number rapidly so it's ideal to have a solution that can auto-scale. SaaS solutions are often best at scaling quickly.

High Availability and Disaster Recovery – See the SLA (Service Level Agreement), but in general, SaaS options handle high availability and disaster recovery out of the box, without the need to dedicate your company's resources. This can be a significant benefit for organizations with lean security teams.

Self-deployed or managed services

Although these two deployment types differ in who is doing the installation and management, the infrastructure decisions are often the same. Between the two, there's a trade-off between control and convenience.

Expertise needed – With a self-deployed solution, you have more control, but you also need to be more versed in the technical aspects especially if you are managing the infrastructure. For self-deployed systems, setup and management may be particularly onerous. Expertise required is less if using a managed service, but still greater than when selecting a SaaS solution.

Pricing – The price on these can vary greatly depending on the number of services and what you undertake yourself, along with the chosen feature set. Be sure to consider the TCO as you are likely doing more yourself and in the case of managed services, the fees may be difficult to track or predict if based on various usage parameters.

Open-source solutions

Open-source software is often where users first start because the need is low enough to manage without an enterprise grade solution and is legally obtained without a license fee. In addition, if you have real technical knowledge, it can be very customizable.

Expertise needed – For basic needs, you can set it up, but the more you grow and if you wish to customize it, the technical knowledge grows exponentially, making it difficult to keep up with the growth in secrets. This often results in the need for technical support which then adds a fee to what was otherwise free.

Feature set – Though open source is customizable if you have the technical expertise to do it, it often has fewer features or does not allow a full enterprise implementation in its free open-source version. Check if the primary sponsor has an enterprise or otherwise more fully featured version and compare the two.

Conclusion

In conclusion, we hope this eBook provides enough information to help you realize the benefits of a centralized secrets management solution and to get you thinking about how to take steps before secrets sprawl gets overwhelming and puts your organization at risk. Ultimately, the best secrets management solution for you will depend on your specific needs and requirements. However, what would an eBook be without a suggested solution?

Introducing CipherTrust Secrets Management, powered by Akeyless

CipherTrust Data Security Platform by Thales enables you to stay a step ahead of dynamic cybersecurity threats by discovering, protecting and controlling access to databases and files in cloud, virtual, and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements and prepares your organization to respond nimbly when the next security challenge or compliance requirement arises. You can see more at https://cpl.thalesgroup.com/encryption/data-seccurity-platform.

CipherTrust Secrets Management, powered by Akeyless, is a state-of-the-art enterprise secrets management solution which protects and automates access to secrets across DevOps tools and cloud workloads including credentials, certificates, API keys, and tokens. Find out more on our website at: https://cpl.thalesgroup.com/encryption/ciphertrust-secrets-management

Use Case: Cimpress, a global manufacturer of consumer goods, was already using a secrets management solution, but was able to reduce costs up to 70% while seeing adoption increase by 270% after switching! This is a testament to the ease of use, greater functionality and lower total cost of ownership.

About Thales

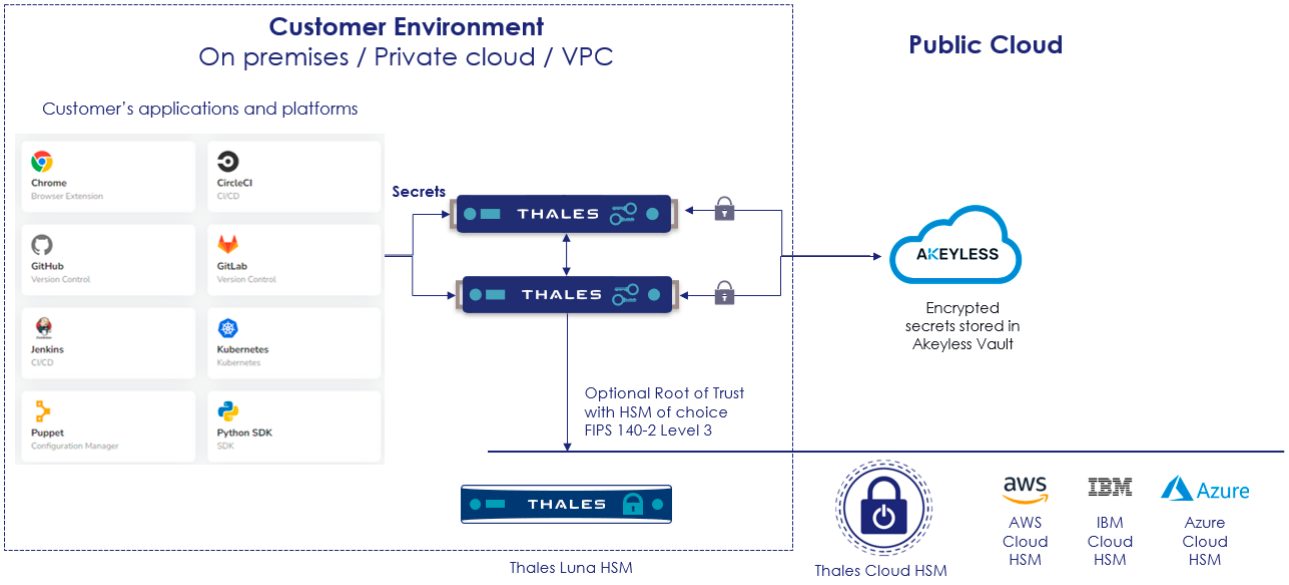
The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Call to action

Evaluate your growth in secrets, how they are managed, and determine how a Secrets Management solution will benefit your organization. Make a plan to improve how you are currently managing your secrets. Contact Thales for a free consultation: https://cpl.thalesgroup.com/encryption/contact-us

CipherTrust Secrets Management Deployment



THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com