Case study

# Centralized secrets management with regulatory compliance

## The motivation: the challenge of secret sprawl

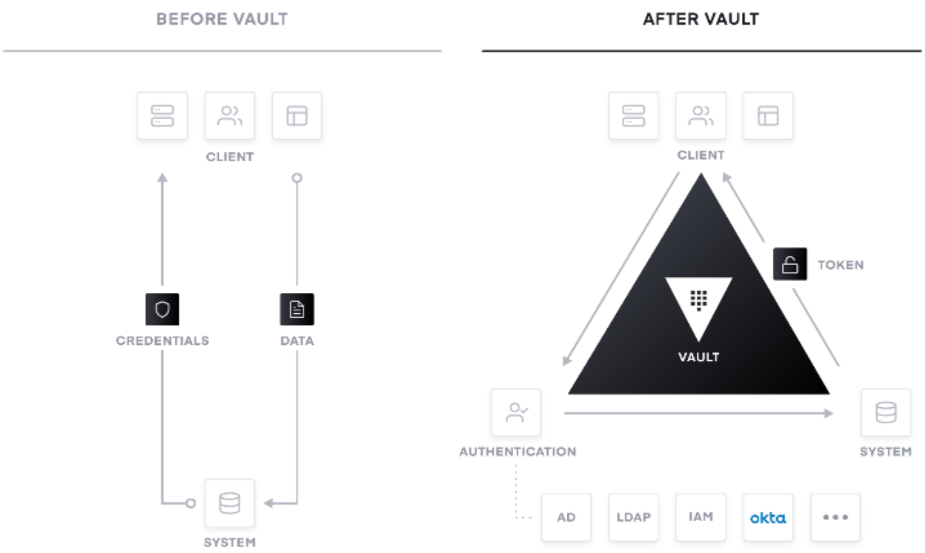
The shift away from legacy, on-premise environments to more dynamic, cloud-based environments has increased the number of secrets capable of authenticating access to various services, applications, and infrastructure. The conventional methods of using static usernames/passwords and perimeter-based security are no longer effective for these modern-day applications.

## The challenge: managing keys securely

To minimize the attack surface and adhere to security best practices, organizations should address security at the resource level, using dynamic secrets. Dynamic secrets enable users and services to gain fine-grained authorization to resource usage for finite and revocable duration of time. This can be implemented manually or scripted, but neither approach is scalable and could eventually be susceptible to being hacked. What is needed is a secure and automated way to distribute, manage, renew and revoke secrets.

## HashiCorp Vault centralizes secrets management across distributed application infrastructure

HashiCorp Vault is a security tool which centrally secures, stores, and tightly controls access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.

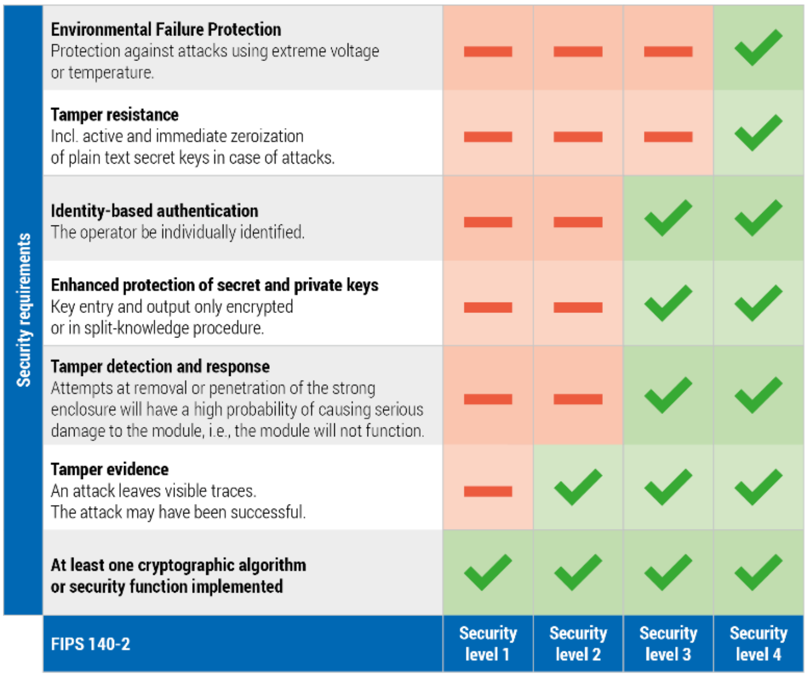


Vault can store existing secrets, dynamically generate new secrets to control access to third-party resources and provide time-limited credentials for your infrastructure. Any dynamically-generated secrets that Vault generates are associated with user-defined leases which are then automatically revoked after the lease period expires. Access control policies provide strict control over what users or applications can access what secrets or systems and all data is always encrypted both in-flight and at rest.

From API keys and sensitive data encryption to being a complete internal certificate authority, Vault is meant to be a solution for all secret management needs giving security operators certainty in when, where, and how secrets are being used across a system with a detailed audit log. To learn more about Vault refer to http://www.hashicorp.com/vault.html.

## Compliance and Regulatory Requirements

Many industries such as finance, healthcare, and telecommunications have strict compliance and regulatory requirements such as FIPS 140-2 overall level 3 or physical security level-4. To meet these compliance needs the use of a Hardware Security Module (HSM) is often necessary. An HSM is a hardware device that is meant to secure various secrets. These devices are designed to withstand any type of attack with the strongest security models in mind as defined by NIST (US National Institute for Standard Technology) and adhere to many compliance regulations.



Security requirements

| FIPS 140-2 | Security level 1 | Security level 2 | Security level 3 | Security level 4 |
|---|---|---|---|---|
| **Environmental Failure Protection**<br>Protection against attacks using extreme voltage or temperature. | — | — | — | ✓ |
| **Tamper resistance**<br>Incl. active and immediate zeroization of plain text secret keys in case of attacks. | — | — | — | ✓ |
| **Identity-based authentication**<br>The operator be individually identified. | — | — | ✓ | ✓ |
| **Enhanced protection of secret and private keys**<br>Key entry and output only encrypted or in split-knowledge procedure. | — | — | ✓ | ✓ |
| **Tamper detection and response**<br>Attempts at removal or penetration of the strong enclosure will have a high probability of causing serious damage to the module, i.e., the module will not function. | — | — | ✓ | ✓ |
| **Tamper evidence**<br>An attack leaves visible traces. The attack may have been successful. | — | ✓ | ✓ | ✓ |
| **At least one cryptographic algorithm or security function implemented** | ✓ | ✓ | ✓ | ✓ |

*FIPS 140-2 levels explained*

Utimaco HSM delivers a general-purpose hardware security module FIPS 140-2 level 3 or even physical security level-4 as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications like Vault.  Some of the key advantages of the Utimaco HSM include:

- FIPS 140-2 physical level-4
- Ease of use
- Best-in-class remote management
- Highly configurable
- Unmatched capacity/scalability
- Well-suited for dark data center deployments

## Solving the secret sprawl challenge with regulatory compliance

For some companies using an HSM may seem excessive and simply storing secrets in HashiCorp Vault might be sufficient. However, for companies that require a higher level of security – either for compliance reasons, or to further harden their security model, an HSM can be a relatively small investment that can eliminate all remaining attack surfaces. Utimaco HSMs integrate with HashiCorp Vault so as to provide the best of both worlds – a flexible tool to manage all your secrets for the modern-day applications, and a robust regulatory compliant way to store sensitive data in a hardware module.

It is worth clarifying that HashiCorp Vault doesn't replace the HSM, instead the HSM is used to augment the solution to make it more secure and compliant. Having both has the additional advantage of providing multiple audit logs – requests to Vault, as well as to the HSM.

## HashiCorp Vault + Utimaco HSM

HashiCorp and Utimaco have partnered to provide an integrated solution for customers looking for a comprehensive security solution to centralize secrets management with regulatory compliance in-mind. The partnership between HashiCorp and Utimaco provides customers with a full-tested, proven solution that customers can deploy seamlessly and with confidence.

## About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. For more information, visit https://www.hashicorp.com or follow HashiCorp on Twitter @HashiCorp

## About Utimaco

Utimaco is a leading manufacturer of HSMs that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services and the public sector. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovation and support the creation of new business by helping to secure critical business data and transactions.

Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 260 people, with sales offices in Germany, the US, the UK and Singapore.

For more information, visit https://hsm.utimaco.com