Three Secrets Management Customer Use Cases

THALES

Building a future we can all trust

CipherTrust Secrets Management (CSM) is a state-of-the-art secrets management solution, powered by Akeyless, which protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens. The features enhance the capabilities of the CipherTrust Data Security Platform to help security and governance teams reduce risks by streamlining security processes across their operations.

Enterprise-ready secrets management provides automatic processes for creating, storing, rotating, and removing secrets. This brief highlights how three customers in consumer goods manufacturing, Fintech, and business applications software industries utilized the secrets management component that is powered by Akeyless to consistently enforce security policies across their organizations.

Comprehensive Data Protection with Secrets Management in One Tool

Efficient Secrets Management at Enterprise Scale

The Organization

A multinational consumer goods manufacturer with 12,000 employees and 13 subsidiaries globally had quite the challenge before them. To support massive operations, the manufacturer needed a reliable, high-value service for secrets management that could be implemented by a small central team that provides security services to their globally distributed security teams. This central team's aim is to support local security teams as an MSSP, or a managed security provider. The MSSP team discovers, purchases, and provides services to the distributed security teams across the globe. By managing relations with vendors and providing support, their goal is to make it easy for these teams to get security done right.

The Challenge

However, the manufacturer was facing heavy licensing costs from their provider, on top of costs associated with spinning up and managing their own infrastructure. Additionally, they needed to set up monitoring, so they knew immediately if something was not working correctly. Also, having a team on call 24/7 when issues arise would be quite the cost and undertaking, all adding up to a high total cost of ownership (TCO).

Although teams worked hard at providing documentation and onboarding resources, they still struggled to understand and work with their secrets management tool. Frustration built with the current provider's reliability, availability, and assurance of the solution working as expected. With low adoption, questionable reliability, and an astronomically high TCO, it was time to look for a change.

The Solution

The manufacturer needed a secrets management solution with fast deployment and minimal maintenance. They were looking for a cloud native solution that had API driven capabilities allowing Out of the Box integrations no matter what their toolset.

The Benefits
- Fast deployment
- API driven capabilities
- Out of the Box integrations
- Enhanced security and risk mitigation

After nine months leveraging the secrets management component that is powered by Akeyless, the manufacturer benefited from:

Higher adoption

The MSSP team saw adoption rate by the regional security teams soar 270% compared with their previous provider. Teams were not mandated to use certain tools – they simply found it easier to use.

More functionality

They could use features that had been missing or difficult to implement with their previous provider, like the use of temporary credential for database users and rotating credentials for on-prem machines.

Lower TCO

Overall, they reduced costs by 70% compared to their previous provider, including both engineering and computing resources.

Engineer FTE

Savings:
70%
Cost Reduction

Computing Resources

Engineer FTE

Computing Resources

Licensing

Licensing
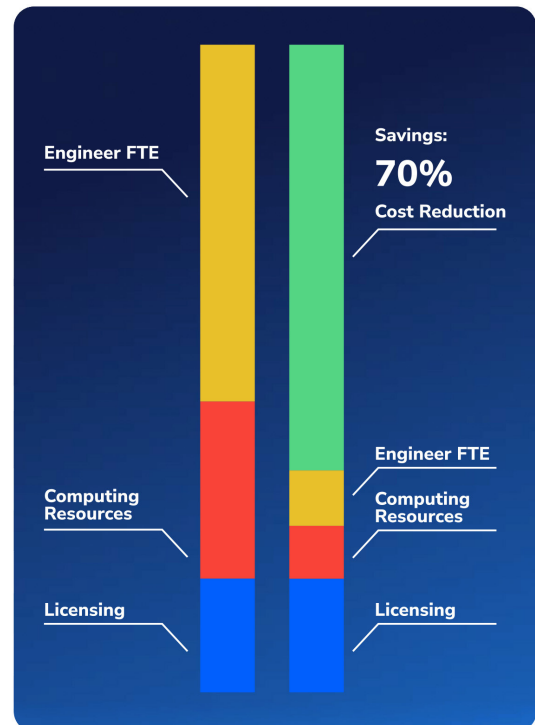
Actual before vs. after view

Uplevel Security and Accelerate DevOps Workflows

The Organization

A highly regulated, fast-paced Fintech company employs hundreds of developers and engineers to create innovative financial services that will maintain its competitive advantage. To help bring services to market faster using a cloud-first philosophy, they needed automated workload orchestration and continuous integration (CI) pipelines.

The Challenge

The challenge of ensuring they maintain compliance with many regulations, such as PCI-DSS was difficult. As the company's software developer and engineering teams grew, secrets within their Kubernetes environment grew exponentially. Secrets management is not something developers want to worry about; they want to focus on creating impactful solutions to help the company grow and stand out against competition.

Engineers   **Financial Services**   **Developers**
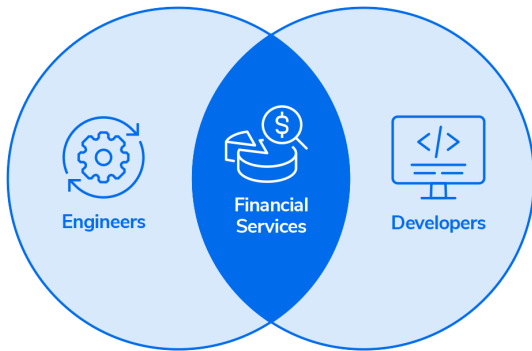
The Solution

To reduce risk and help with compliance efforts, they were looking to uplevel their secrets management solution, as well as their VPN remote access. They highly valued that the secrets management component that is powered by Akeyless takes a Zero-Knowledge approach to provide fully secure encryption key custody, so only the customer has access to their secured data. The solution enabled the customer to scale their engineering teams and make DevOps workflows more efficient by using Just-in-Time access scenarios.

The Benefits:

- Fully secure encryption key custody
- Out of the Box Kubernetes integration
- Simplified workflows

By using a SaaS-based secrets management solution, they eliminated the operational overhead associated with deploying and managing secrets management infrastructure, high availability, disaster recovery, and backups. The solution replaced their open source-based VPN solution and addressed the human-to-machine access use cases they had. With the solution's unified platform of comprehensive features, it was able to meet their needs for both secrets management and Privileged Access Management (PAM).

The Results:

- Compliant with strict privacy laws
- Seamless scale for 100s of engineers and developers
- Peace of mind for CISO
  - Disaster Recovery
  - High Availability
  - Backups

Support for Hybrid Multi-cloud Strategy

The Organization

A Business Applications Software company of 2,100 employees in 16 countries offers software for creating and deploying business applications. From an organizational perspective, the company is broken down into different divisions, which have individual responsibilities, including application and digital experience, as well as creating tools and/or modules for developers.

The Challenge

The developer teams were inundated with disparate tools due to a series of acquisitions and continued growth among the different divisions. This resulted in a rapid growth in secrets usage, needed access to APIs, and workloads. With that comes an increased risk of secret sprawl and exposed credentials. But their multi-cloud strategy required a central solution that the business teams could simply consume, without spending considerable time and money to run and maintain the tool.

The Solution

They needed a secrets management platform that could be easily adopted by the different teams, with a wide range of Out of the Box integrations for their existing cloud services and DevOps tools. They needed a solution that would:

- Enable the diverse developer teams to focus on innovation and developing software, as opposed to worrying about security.
- Allow teams to access a centralized secrets management system available wherever the staff and workloads are located, regardless of their use of AWS, Azure, or Google Cloud.
- Bring new confidence with a multi-cloud architecture, that is also multi-regional, while offering high availability, high performance, and scalability.

- Maintain exclusive ownership of their keys. Unlike cloud provider vaults or virtualized vault instances which require users to relinquish their master keys, the new secrets management solution enabled the organization to maintain ownership of their keys. This decreased risk because the keys, and the data they protect, cannot be accessed by rogue administrators, and hackers, or be handed over to the government through the CLOUD act.

The Results:
- **60%-70% savings on overhead**
- **Teams no longer wasting cycle on maintenance or patching software**
- **Increased developer workflows**

Leveraging the secrets management component that is powered by Akeyless, the organization:

- Saved 60%–70% of overhead and simplified the workflows associated with granting employees access to the resources they need to stay productive and drive the business forward.
- No longer wasted cycles on maintaining the complex underlying infrastructure and patching software that is common with traditional secrets management tools.
- Increased efficiency and security for developer workflows.

CipherTrust Secrets Management

CipherTrust Secrets Management, powered by Akeyless, is quick to deploy and enterprise-ready, so you can simplify secrets management and improve developer efficiency. CipherTrust Secrets Management is part of the CipherTrust Data Security Platform, an integrated suite of data-centric security products that help organizations discover, protect, and control their sensitive data across clouds, on-premise, and hybrid environments. The CipherTrust Platform enables you to address your urgent requirements and prepares your organization to respond nimbly when the next security challenge or compliance requirement arises. Learn more about the CipherTrust Platform.

Resources

Plan to improve how you are currently managing your secrets.

- Contact Thales for a free consultation
- Schedule a free demo/POC
- Start your 90-day free trial
- View demos
- **Learn** How to Choose a Secrets Management Solution

See The Difference:
- Centralized management for all secret types
- Easy to use with automated functionality for DevSecOps
- SaaS (Software as a Service) scalability for hybrid and multi-cloud environments

About Akeyless

Akeyless' unique combination of innovative technology and cloud-native architecture enables enterprises to quickly secure DevOps, cloud workloads, and legacy environments, while meeting compliance and regulations.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.