USE CASE — ENTERPRISE SECRETS MANAGEMENT PROGRAM

HR Software Company Overhauls Secrets Management Program with Optiv’s HashiCorp Vault Services

**Business Drivers**
Many companies find themselves in possession of large amounts of sensitive data. Keeping that data secret and secure is essential to maintain compliance with legal requirements and earn their clients’ trust and satisfaction. This data is often spread across multiple systems throughout an organization, so developing a global security strategy is paramount.

**Business Problem**
A global payroll provider had very aggressive and ambitious plans for their digital transformation journey. Due to their size (supporting 36 million workers and more than 500,000 organizations globally), the organization had volumes of secrets sprawled across their technology ecosystem.

The sprawl of these secrets and dynamic identities was causing increased security risks, redundant costs from disparate third-party and home-grown secrets management applications, and operational inefficiencies. The disparity led to a lack of visibility and critical compliance and audit findings.

**Optiv’s Approach**
The engagement began with an all-hands kick-off to start the discovery process and initial assessment. The design and planning phase included multiple screencasts and points of contact to demonstrate Vault’s capabilities. It recommended a best-practice architecture that accounted for serverless and containerized compute platforms, VMs in existing data centers and a continuous integration and deployment (CI/CD) delivery pipeline with build tests. We also developed an enterprise-wide adoption program with a namespace design to automatically provision application teams. Automation and orchestration was used to integrated and deploy the client’s pilot use cases while tests and validation were performed throughout the process.

**Industry** Human Resources Management
**Software/Services**

**Desired Outcome** Consolidated secrets management program to reduce redundancies and security gaps created by disparate, third-party and home-grown applications.

**Use Case** Optiv enabled an HR management software and services organization to overhaul their secrets management program, thereby reducing risks and costs and improving their overall security posture.

**Client Benefits**
- Centralized secrets management capabilities for better visibility and security
- Reduced enterprise risk due to sunsetting legacy and home-grown applications
- Streamlined authentication processes resulting in improved operational efficiencies

**Proposed Roadmap**
- Optiv to continue partnering with the client to enable an enterprise-wide adoption program
- Integrating applications and services into Vault using multi-tenancy design
- Centralizing secrets management while providing teams the autonomy to control their users and access
Customer Deployment

Before the deployment, the client had multiple, overlapping secrets management solutions, including a mix of third-party and home-grown applications. Some of these apps had failed audits, left security and compliance gaps or were merely ineffective. They knew that, in order to make their digital transformation goals a reality, their current implementation was unsustainable.

Optiv worked with the client to deploy HashiCorp Vault technology through an automated and orchestrated Jenkins CI/CD pipeline. The clustered Vault environment enabled higher availability and improved resiliency of secrets as part of a unified secrets management program. Part of this unified program was integrating the client’s home-grown apps, the remediation of apps that failed audits and the elimination of ineffective tools. Optiv’s team also streamlined the client’s authentication methods through Kubernetes. Together, these processes and technologies led to an improved security posture, reduced costs and enhanced visibility, productivity and governance.

Implementation Breakdown

- Discovery and assessment of technical and business requirements
- Solution and architecture design
- Implementation of HashiCorp Vault technology, utilizing automation and orchestration, performing testing and validation throughout the engagement. The new secrets management program included use cases such as:
  - Dynamic database credentials
  - Token lifecycle auto-renewal
  - LDAP authentication method
  - Kubernetes authentication method
  - Approle authentication method
  - Deployment via Helm chart
  - Multi-cluster Terraform configuration
  - Vault agent templating
  - Integration of pilot use cases

Why Optiv?

Optiv is the only pure-play security services integrator (SSI) that can design, implement and manage an end-to-end cloud program focused on security and aligned to your business goals. Our certified experts can help you gain the agility, security, scale and control you need to stay ahead of the competition.

Secure your security.™

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.