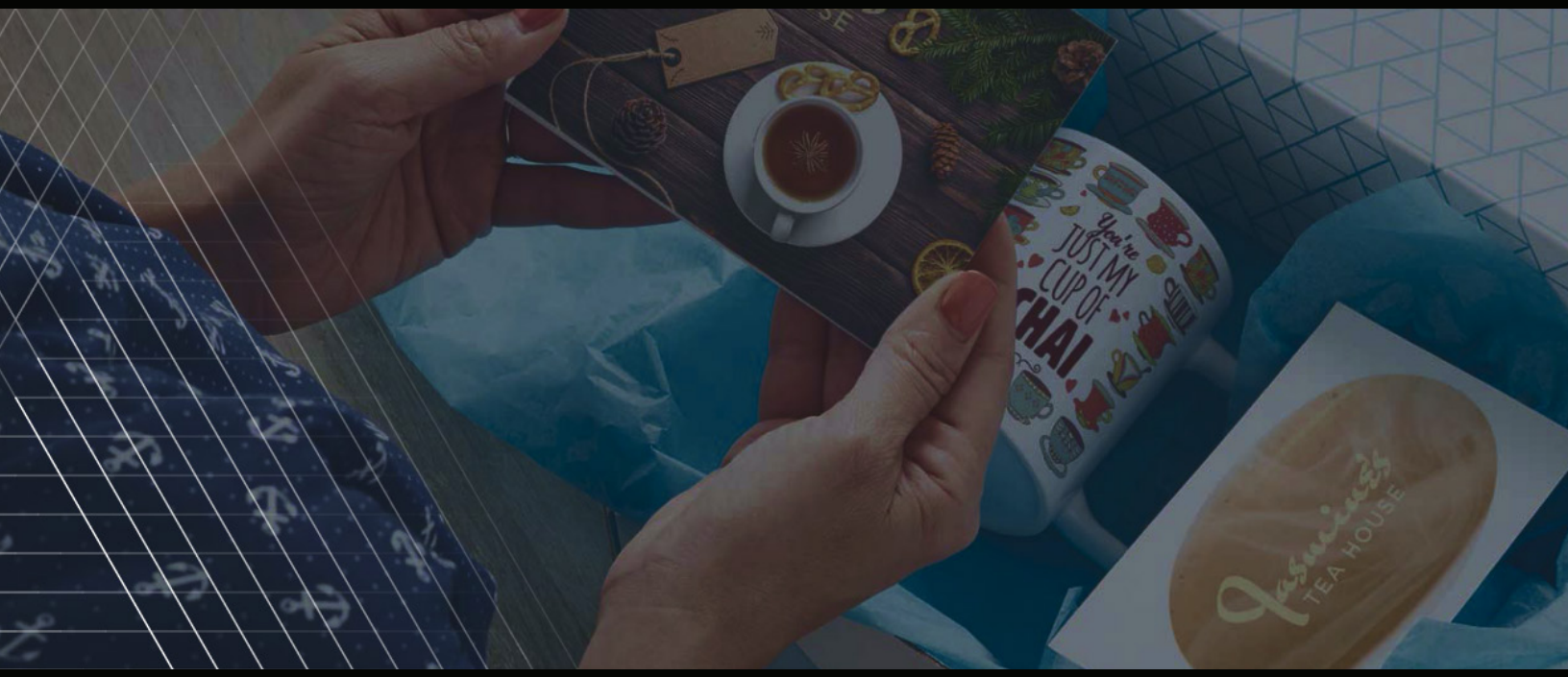
HashiCorp




cimpress | CUSTOMER CASE STUDY

# Secrets management made to order

Global leader in branding and promotional printing uses HashiCorp Vault to manage secrets for its 13 business units

// Infrastructure Enables Innovation

## Cimpress Summary

Cimpress plc (Nasdaq: CMPR) invests in and builds customer-focused, entrepreneurial, mass-customization businesses for the long term. Mass customization is a competitive strategy which seeks to produce goods and services to meet individual customer needs with near mass-production efficiency. Cimpress is a strategically focused group of more than a dozen businesses, each operating in a largely autonomous manner with a select few shared strategic and corporate activities that they maintain centrally.

CIMPRESS FAST FACTS

150,000+ tokens and credentials generated per day

Dozens of complete security namespaces

25+ manual work hours saved per week

46 million uniquely designed items

10+ million customers served per year

13 autonomous business units enabled by security-as-a-service model

## Promoting custom security-as-a-service

> " Vault is cloud agnostic and works well with a whole range of endpoints business users rely on, like LastPass, making it easy to roll out a comprehensive service that everyone can use with very little effort."

CHRISTOPHER TOM,
INFORMATION SECURITY ENGINEER

Companies of all stripes around the world can proudly display their logos on everything from letterhead to apparel, thanks to Cimpress and its family of companies. The global parent company of recognizable brands like Vistaprint, BuildASign, and nearly a dozen others provides innovative, mass customization of physical branding and promotional products for businesses competing in an increasingly digital world.

Providing a global customer base with an endless array of product possibilities means the company has to support a range of e-commerce, product-building, and cloud platforms. But the variety of applications and the broad range of data governance regulations in each market the company's business units operate created a host of new and complex challenges for securing the systems and the sensitive customer data they contained.

"Every business unit had its own best practices to support their individual objectives, but we were handling security for them as a single entity," says Dr. Conor Mancone, lead application security engineer at Cimpress. "We wanted to establish a general security standard for the enterprise and specialized security for each unit they could manage on their own. To do that, we needed to replace our existing on-premise secrets management tool with something more scalable and that we could bend to specific business and regulatory needs of the individual business units."

## One size fits all

In the past, the Cimpress app security team relied on a central private secrets server to securely store access credentials for the entire organization. It was an on-premise solution, integrated with Active Directory, and could only be reached via VPN or with direct admin access.

Each individual business had its own tech stack and as they began deploying more applications and systems in various clouds, it became increasingly difficult to keep up with the constantly changing steps for securing access to systems, applications, and databases.

Over time, the different servers and systems used by the company's 13 business units resulted in tens of thousands of nodes and virtual machines that needed access to other systems, usually managed through tokens and access secrets, but never integrated with systems from other lines of business.

"We didn't have a standardized method for updating secrets or changing passwords, so every time we changed a secret in one system, we had to change it on the secret server too," says Christopher Tom, an information security engineer at Cimpress. "And since our tools didn't integrate with GitLab, anytime we changed a password in the secrets server, we had to manually copy and paste into our repository to keep track of everything."

Beyond the sheer amount of time and effort it took to manage secrets manually, Mancone says that the risk of losing secrets and access to key systems was what really kept the team up at night. The frenetic pace and massive volume of changes overwhelmed the team to the point that they'd find ad hoc ways of keeping track — sometimes in code, config files, or occasionally on a sticky note on someone's desk — that could potentially expose sensitive information to the risk of falling into the wrong hands.

"In the app security space, it's an unforgivable sin to fail to secure customer data or for your app to go down because something broke between systems on the backend that really shouldn't have," he says. "Not only are you at risk for fines and penalties for violating data management regulations, but you also risk demolishing your brand's reputation virtually overnight if your business systems don't work and your end customers don't trust that you're keeping their information safe."

## Challenges

**Creating a security-as-a-service model for a global enterprise**

**Enabling security self-service capabilities for business unit staff**

**Efficiently managing hundreds of thousands of tokens and secrets**

> With Vault, we were able to create dozens of complete namespaces and automatically generate hundreds of thousands of security tokens each day for all of our business units to use in a fraction of the time it used to take."

DR CONOR MANCONE,
LEAD APPLICATION SECURITY ENGINEER

## Smart buy: bundled security

HashiCorp Vault makes it easy for the Cimpress team — Mancone and information security engineer Miguel Fernandez, along with Tom and his fellow senior information security engineer, Pablo de la Concepción — to establish foundational secrets management policies across the enterprise and then tailor specific data security parameters to the unique needs of each business unit.

"Vault is cloud agnostic and works well with a whole range of endpoints business users rely on, like LastPass, making it easy to roll out a comprehensive service that everyone can use with very little effort," Tom says. "More importantly, it's scalable, and has automation features that eliminate many of the most time-consuming aspects of protecting the business and our systems at every level."

The solution enables the small, but well-trained team to create a robust secrets-as-a-service model serving thousands of concurrent users across the enterprise to accelerate its adoption and improve the company's overall security posture. Along with HashiCorp Packer and Terraform to automate machine image construction and infrastructure provisioning, Vault enables Mancone's team to focus on securing the clusters and keeping secrets parameters up to date as new clusters are added instead of having to custom develop a new secrets management solution for each business unit.

Business unit teams are given their own individual namespaces that centrally store and distribute secrets like tokens, passwords, certificates, or encryption keys from a single location. Mancone's team then sets up additional barriers to keep everyone isolated into their own namespaces to ensure that different teams can only access their own secrets. They also provide ongoing support and documentation to quickly adapt to evolving business unit needs — an arrangement that minimizes issues caused by different configurations for teams with different regulatory needs.

This approach helps the company avoid resource and secrets sharing outside of each team or business unit, while still enabling security oversight by Mancone's team and more robust disaster recovery measures.

"Vault's integration with GitLab and AWS is an enormous benefit for us because it auto-generates some of our credentials, including temporary keys, which simplifies a lot of the more tedious processes we face each day," Mancone says. "More importantly, it alleviates a huge burden from our engineering and development teams, and allows them to focus much more on building profitable business solutions that keep customer data safe. This approach is really the only way that a team as small as ours could possibly manage secrets for a business of our size."

## On-demand security for an on-demand world

Mancone and Tom agree that Vault — along with other supporting HashiCorp solutions — is a great business and data security enabler for Cimpress and its various subsidiary brands. Since deploying the enterprise version of the multi-tenant security software, the team has also built a security-as-a-service model within its parent organization to enable each line of business to manage their own secrets and policies.

The solution brings a huge amount of configurability, integration options for every use case, and an enterprise-grade solution that Cimpress engineers can use with a very short learning curve, allowing them to build secure solutions with a lot less overhead.

According to Mancone, Vault makes it easy to manage policy rules and automate ingestion from AWS EC2 servers and can automatically generate more than 150,000 tokens and AWS credentials every day. At the same time, the team can leverage namespaces to be able to isolate each business into its own segment, complete with parameters and restrictions they require, in about 30 seconds.

"With Vault, we were able to create dozens of complete namespaces and automatically generate hundreds of thousands of security tokens each day for all of our business units to use in a fraction of the time it used to take," he says. "Manually copying and pasting passwords and secrets from one system to another is both terribly inefficient and an error-prone approach to managing secrets for a global enterprise. And with Vault, we thankfully no longer have to worry about that."

## Outcomes

**Created dozens of namespaces for business units and teams to securely store and manage secrets**

**Generated more than 150,000 tokens and AWS access credentials per day via Vault automation**

**Replaced previously manual token and secrets management processes with automated ones to save dozens of team work hours per week**

**Eliminated error-prone copy/paste tasks and reduced risk of unplanned downtime an unauthorized systems access**

## Solution

Cimpress uses HashiCorp Vault Enterprise to create dozens of namespaces that enable business units in the organization to create isolated environments within Vault Enterprise to define security policies and different authentication methods based on the unit's needs and environments, while leveraging secrets engines and tokens to secure secrets for a range of apps and systems.

## Cimpress Partners

Dr. Conor Mancone is a data scientist turned software developer and a lead application security engineer at Cimpress, responsible for developing and implementing security programs for each of the company's 13 business units. Mancone leads a team responsible for creating namespaces in Vault for internal business groups to use, answering any Vault-related questions, and providing general support across lines of business.

**Dr. Conor Mancone,**
Lead Application Security Engineer, Cimpress

# Cimpress Partners Continued

Christopher Tom is an information security engineer at Cimpress and brings more than a decade of experience in help desk, systems administration, and information security to the team. Prior to joining Cimpress, Tom spent seven years in support and systems administration roles in the financial services industry.

**Christopher Tom,**
Information Security Engineer, Cimpress

Pablo de la Concepcion is an information security engineer and AppSec lead at Cimpress and has experience in systems administration, web app development, and security management in the FinTech sector. Pablo led the process of converting Vault into a Cimpress service and a SaaS model. In addition to his work with Vault, he is also involved in the development of Cimpress's own secure software development life cycle, and managing their Static Application Security Testing and Software Configuration Architecture programs.

**Pablo de la Concepcion,**
Lead Application Security Engineer, Cimpress

Miguel Fernandez is an information security engineer at Cimpress and responsible for building and maintaining the infrastructure for Vault as a Service alongside his team members. As part of his role, Miguel works with customers to provide assistance and insightful feedback on secure code practices. Prior to joining Cimpress, Miguel worked in data engineering and brings years of experience in software development.

**Miguel Fernandez,**
Information Security Engineer, Cimpress

## Technology Stack

- Infrastructure: AWS EC2, ALB
- Workload type: Linux
- CI/CD: GitLab
- Storage: HashiCorp Consul
- Version Control: GitLab
- Provisioning: HashiCorp Terraform, HashiCorp Packer
- Security management: HashiCorp Vault


HashiCorp