



VinID | CUSTOMER CASE STUDY

Securing 10 Million Personalized Promotions

Vietnamese consumer retail app provider uses HashiCorp Vault to automate secrets management and reduce time required to protect sensitive data by 90%.

// Infrastructure Enables Innovation

VinID Summary

VinID by One Mount Consumer (part of One Mount Group) is the country's largest loyalty and customer engagement platform. The company serves nearly 7 million members with a comprehensive online ecosystem that connects everyday customers with thousands of discount codes from reputable and familiar brands through multi-channel merchandising and integrated pay-on-app via e-wallet. The platform is not just a hub for supporting daily shopping and online payments, but is also a high-value database powering new consumer research and artificial intelligence initiatives designed to incrementally but substantially improve the online shopping experience for millions of consumers every day.

VINID FAST FACTS



Billions of dollars in financial transactions per year



90% reduction in time spent on secrets management processes



10x increase in secrets management storage capacity



7 million+ registered users



Automation-driven self-service secrets management solution



Significant improvement in security posture

“ The open source-to-enterprise transition with Vault was critical for us, as it gave us the chance to re-engineer our secrets management practices with little or no financial investment and then strategically begin paying for the tools and capabilities we actually needed instead of buying into a one-size-fits-all solution like many Vault competitors offer.”

LIEM PHAM
DIRECTOR OF CYBER SECURITY, ONE MOUNT GROUP, VINID

Evolving from Retail Checkout to the Bank Account

Vietnam has undergone a monumental transformation in the last several decades and now has one of the fastest growing economies on the planet — thanks in part to companies like One Mount and Vingroup.

The latter, which started as a dried foods producer in the early 1990s has blossomed into a sweeping conglomerate comprising 48 subsidiaries spanning every market from real estate and health care to education, retail, and financial services. Vingroup’s financial services arm operates under the VinID banner, a customer loyalty and daily discount app that facilitates billions of dollars in financial transactions each year for more than seven million registered users.

While the app found instant popularity and has grown by leaps and bounds since its launch, doing so didn’t come with its share of challenges and risks. “The sheer volume and sensitivity of the information exchanged on the app makes ensuring the safety and security of every bit of data that it processes our top priority,” says Liem Pham, director of cybersecurity for One Mount Group, the subsidiary that manages VinID. “Our previous methods and strategies were inefficient and not robust enough to help us secure the various systems, connections, and data stores spread across our organization and needed to be enhanced or replaced with something scalable and ready to take on the challenges we face in today’s cyber landscape.”

Massive Footprint Needs Smarter Way to Address Potential Vulnerabilities

Since its launch, millions of users have flocked to VinID for instant, reliable access to thousands of discount codes from reputable and familiar brands and to facilitate purchases across various shopping channels with pay-on-app capabilities via an e-wallet.

Tracking individual users’ buying habits enables the company to better target new discount offers and

promotional opportunities to customers, execute the transactions directly within the app, and keep all that data within a single ecosystem. VinID relies on an extensive mix of cloud and on-premises systems to manage this massive volume of information and to deliver a consistently excellent digital customer experience. But securing the platforms, connections between systems and databases, and the private personal information of its users became increasingly challenging because of the company's mostly manual controls.

"An ecosystem this big isn't just a matter of securing user logins and bank information from unauthorized access, it's also about ensuring that non-human connections between different clouds, databases, and the frontend are reliably secure as well," Liem explains. "We historically managed all the secrets for these different transactions manually across multiple teams, but as our environment continued to grow, it became nearly impossible to keep rotating keys and digital passcodes to keep it all safe and prevent a domino effect if one system happens to be breached."

Liem says that manually managing thousands of secrets by hand was not only inefficient and time-consuming for an already overwhelmed support team, but also error-prone. And it increased the risk of breaches and potential impact on the app's overall performance.

"We needed a standardized way of managing secrets across the organization and our different properties," Liem says. "Every new feature release or version update required the DevOps team to take time away from their primary job to focus on one-off secrets management issues. It often impacted the app's performance, inhibited our ability to deliver new features to users faster, and unnecessarily increased the cost of doing business," as fast as our customers wanted."

Challenges



Improving security of backend systems and individual records for more than 7 million users



Eliminating time-consuming and error-prone secrets management processes



Automated secrets management process across a hybrid IT environment to support scale and expansion

“ With Vault, my whole team gets more time to do what really matters to drive our product forward and continue delivering the seamless, secure, and engaging user experience our customers have come to expect.”

LIEM PHAM
DIRECTOR OF CYBER SECURITY, ONE MOUNT GROUP, VINID

Simple security, bigger scale, less effort

As part of a group-wide data protection and privacy initiative, Liem’s team set out to find a more comprehensive, automated secrets management solution capable of tightly controlling tokens, passwords, certificates, and encryption keys for protecting secrets and other sensitive data across a sprawling, multi-platform environment.

After evaluating multiple third-party solutions and native tools from their cloud providers, VinID deployed HashiCorp Vault because of the product’s broad support for both cloud and on-prem systems, centralized key management for simpler data encryption, and easy ability to scale to match the company’s evolving security needs. Alongside HashiCorp Terraform and Consul to automate infrastructure deployment and service discovery, VinID uses Vault to centrally manage and enforce access to secrets and systems based on trusted sources of application and user identity.

Unlike static IP-based solutions that can’t scale in dynamic environments with frequently changing applications and machines, Vault automatically limits how long ephemeral credentials and secrets can live by creating time-based tokens for automated revocation and management. At the same time, the solution provides detailed audit logs that supply the VinID team with detailed histories of client interactions — authentication, token creation, secret access and revocation — to help detect security breaches or attempted access to systems, and enable the company to quickly respond by implementing new policy updates or manual interventions to mitigate risk further.

Liem says that Vault’s open source version made adopting a new secrets management solution more attainable and cost-effective while covering approximately 90% of their secret management needs. And as the company’s budget and security requirements permitted, it transitioned to paying for Vault Enterprise to cover the rest of the ever-growing environment.

“The open source-to-enterprise transition with Vault was critical for us, as it gave us the chance to re-engineer our secrets management practices with little or no financial investment and then strategically begin paying for the tools and capabilities we actually needed instead of buying into a one-size-fits-all solution like many Vault

competitors offer,” he says. “More importantly, it gave us a centralized and secure secrets management platform capable of supporting multiple cloud regions throughout Asia on Google Cloud Platform for better resilience, easier scale, and effortless secrets management.”

Liem credits the HashiCorp team with providing the constant support, insight, and advice his team needed to configure its secrets management operations and deliver the exact features and capabilities the company needs now and in the future. “With HashiCorp’s help, we were able to reduce the time we spent worrying about and trying to configure our secrets management systems by as much as 90% and increase the speed and number of secrets we can store by a factor of ten,” he says. “With Vault, my whole team gets more time to do what really matters to drive our product forward and continue delivering the seamless, secure, and engaging user experience our customers have come to expect.”

Outcomes



Reduced time spent on secrets management by 90%



Tenfold increase in secrets management speed and storage



Frees DevOps teams for higher value tasks



Automated secret management positions VinID to scale to a multi-region deployment across Asia using Google Cloud Platform

Solution

VinID is using HashiCorp Vault to automate dynamic secrets management across various cloud and on-premises systems and networks, enabling a richer, more secure, and engaging user experience.

Interviewee Profile



Liem Pham

Director of
Cybersecurity for One
Mount Group, VinID

Liem Pham is the Director of Cybersecurity for One Mount Group, the subsidiary that manages VinID. Liem brings more than ten years' experience in technology consulting, cyber security management and team leadership along with extensive experience in architecting and integrating enterprise infrastructure and security solutions. Prior to joining VinID's cybersecurity unit, Liem spent several years working as a security solutions consultant and technical consultant with an emphasis on improving clients' risk postures and developing solution roadmaps to address their most pressing challenges.

Technology Stack

- **Infrastructure:** On-premises (30%), GCP (70%)
- **Workload type:** Linux (90%), Windows (10%)
- **Container Runtime:** Docker
- **Orchestrator:** Kubernetes
- **CI/CD:** GitLab
- **Data Service:** SQL, NoSQL, Hadoop, BigQuery
- **Storage:** SAN, GCS
- **Version Control:** GitLab
- **Networking:** SDN
- **Provisioning:** Ansible, HashiCorp Terraform

