HashiCorp

ABN·AMRO | CUSTOMER CASE STUDY

On Account of Cloud Security

How a leading financial institution uses HashiCorp Vault to automate secrets management and deliver huge gains for its growing product portfolio

// Infrastructure Enables Innovation

About ABN AMRO

ABN AMRO Bank N.V. is the third-largest bank in the Netherlands, with headquarters in Amsterdam. ABN AMRO offers a full range of financial products and solutions for retail, corporate, and private banking clients. Their focus is on Northwest Europe. The bank serves around 6 million clients and employs just under 18,000 people. In 2008 ABN AMRO Bank was nationalized by the Dutch government along with Fortis Bank Nederland. It became a public company in 2015.

ABN AMRO FAST FACTS

$

$446+ billion in managed assets

25 new platforms implemented

2,600 business applications

25,000 associates

19 countries and territories

Significant decrease in time spent onboarding applications

Secrets here today, disappear tomorrow

> " Vault's dynamic secrets and API encryption capabilities, coupled with its secrets injector and secure communications, make it possible to confidently onboard apps to our container platform with a fraction of the time and effort as before."

TON VAN DIJK,
AGILE PRODUCT OWNER, ABN AMRO

Few industries require the level of privacy and security as banking. And few banks have as extensive security demands as ABN AMRO.

The bank provides a comprehensive line of products and services for its customers. But securing the systems, applications, and data that enable those services is a daunting task for the company's 400-person Corporate Information Security Office (CISO).

"Executing the access and identity governance across our various customer and backend business applications has been challenging but manageable with our existing security solutions, even as we've added thousands of new accounts and users," says Ton van Dijk, the bank's agile product owner in the identity and access space. "However, our legacy system required an additional module and hands-on monitoring to manage the ephemeral backend secrets and keys among our internal apps and infrastructure, so we decided to look for a more seamless, automated way to address such a critical element of our business."

Preventing a domino effect

Though the financial services industry has a reputation for requiring proven technologies that often makes early technology adoption challenging, ABN AMRO embraced a digital transformation to modernize and future-proof its business. Yet, while the multi-cloud IT strategy and containerized development environment provided a much-needed efficiency boost for its growing product portfolio, it also created a new set of complexities and challenges for the CISO team.

"Secrets management is a business-critical element of our work because if any of the secrets are compromised, they'll have a huge downstream effect," Van Dijk says. "Even a single compromised signing certificate can take an entire system offline, which means possibly losing access to online apps or exposing them to the risk of someone maliciously injecting something into the apps. There's really no room for error."

The bank's previous secrets management solution featured a number of out-of-the-box systems connectors that still required a good amount of programming to set up a new application. Worse, the self-managed platform didn't integrate well with the team's Kubernetes instance, which meant one of the team's engineers had to create a custom connector for new applications or containers that could take several days to reach a test-ready stage.

Additionally, ABN AMRO knew that they needed to prevent secrets sprawl. As many applications and platforms come with their own secrets engines, having that central oversight is critical to be able to quickly revoke secrets in case a serious compromise would happen. When secrets are spread across a multitude of solutions, that is going to be difficult to control.

"The whole process revealed to us that having an on-premise, self-managed secrets system that required third-party support for any type of change was a time-consuming and inefficient way to manage a crucial piece of our operations," Van Dijk explains. More broadly, "it became clearer by the minute that we needed a cloud-native environment that supported containerized development and emphasized automation — without having to undertake a complete and expensive replatforming or technology refresh."

Challenges

Securely managing ephemeral secrets

Reducing reliance on manual secrets management processes

Onboarding consumer and internal applications to a secrets server

> Data and systems security underpins every aspect of our operation. With Vault we have the agility, transparency, and world-class support to confidently build out solutions for today's and tomorrow's needs without having to constantly worry about one mismanaged secret wreaking havoc on all our hard work.

TON VAN DIJK,
AGILE PRODUCT OWNER, ABN AMRO

Central, dynamic secrets management for a booming business

Eager to improve its secrets management practices by eliminating hardcoded credentials from internally developed applications and scripts, the ABN AMRO CISO team adopted HashiCorp Vault after running a proof of concept involving the team's software development and security specialists.

With Vault, the CISO team has implemented a central secrets management repository and eliminates human operators having to manually apply secrets policies to new applications and hosts. The cloud-agnostic platform dramatically simplifies shared credentials and secrets management by automating many of the most time-consuming and laborious processes.

"Vault's dynamic secrets and API encryption capabilities, coupled with its secrets injector and secure communications, make it possible to confidently onboard apps to our container platform with a fraction of the time and effort as before," Van Dijk says. "We're now able to manage ephemeral secrets in AWS and Azure in ways we couldn't before without adding headcount, cost, or unnecessarily long learning curves."

Outcomes

Eliminated costly ephemeral secrets modules to reduce cost and complexity

Dynamic secrets enabled onboarding of two dozen new platforms

Established a foundation for an encryption-as-a-service model

Solution

ABN AMRO is using HashiCorp Vault to create a centralized secrets management system spanning its AWS, Azure, and other internal applications that automates secrets injection and API encryption for greater efficiency and fewer critical secrets errors.

About Ton van Dijk

Ton van Dijk is the agile product owner for ABN AMRO Bank. Ton is responsible for privileged access management and secrets management. Ton is a 30-year veteran of the financial services industry, spending virtually all of those years in a cyber security role.

Technology Stack

- Infrastructure: Microsoft Azure, IBM and Cisco clouds on-premises, mainframe
- Platform: Windows server, Linux, Z-OS
- Load balancers: Windows
- API gateway: Apigee, APIM
- CA: CGI managed service (internal certs) plus a few commercial cert providers
- IAM: Sailpoint, Ping Identity (customers IAM), Ping Federate (SSO)
- APM (Application Performance Mgt): Splunk, Tivoli (on-premises), Log analytics (Azure)
- Provisioning: ServiceNow, Azure devops
- Security management: HashiCorp Vault


HashiCorp