HashiCorp

NORD/LB | CUSTOMER CASE STUDY

Under locks and keys

Leading German bank locks away vital secrets with Vault's encryption as a service feature.

About NORD/LB

NORD/LB is the leading commercial bank in northern Germany. Boasting locations in Hanover, Brunswick, Bremen, Oldenburg, and Hamburg, NORD/LB offers financing solutions for medium-sized companies nationwide. With over 3,900 employees, the bank is a leader in financing renewable energy and has special expertise in financing infrastructure projects, real estate, and aircraft.

$116B in total assets

3,900 employees

Eliminated risk of unplanned downtime

Established first centralized key repository

Reduced annual hours spent on secret rotation from 2,400 to 20

5 minutes instead of 4 days for management and rotation

> "HashiCorp Vault speaks several languages and interfaces effortlessly with containerized and non-containerized services alike. Now, anyone can connect any app or vital system simply and without hand-holding."
>
> JANNIK NOLTE
> INFORMATION TECHNOLOGY SECURITY SPECIALIST, NORD/LB

Critical infrastructure, critical security

Few industries are as critical to national and global economies as commercial banking. In Germany, it's even considered critical infrastructure alongside power, water, and transportation.

NORD/LB, one of the country's leading commercial banking entities, is well-known for its innovative lending solutions for the energy, aerospace, and real estate markets. But operating under the designation as one of the nationally system-relevant banks in Germany, the bank faces enormous pressure — from customers and the government alike — to protect highly sensitive data and systems at all costs.

"As a cloud-first bank operating with a hybrid infrastructure, we have our hands full with endpoint security, network security, and all points in between," says Jannik Nolte, NORD/LB's Information Technology Security Specialist. "We implemented HashiCorp Vault because effectively securing every point of potential vulnerability of today's IT environment is a true team effort that can no longer be done using yesterday's processes and technologies."

End-to-end encryption across environments

Part of a small, select team of security specialists, Nolte plays a prominent role in keeping essential data and core systems secure. As the bank's lead cryptographer, he's responsible for cryptography across the entire organization and consults on cybersecurity implementation protocols on a wide variety of projects.

"If an app developer wants to join our environment, the first thing we do is check to see if it's possible to deploy in Microsoft Azure, our public cloud of choice. If not, then we host the app on-premises," he explains. "In either case, we need to be able to encrypt it in both environments because as a critical infrastructure entity, we don't have the luxury of not complying with government data protection rules. Anything that risks exposing sensitive data also puts our ability to conduct business at risk."

In the past, delivering that level of security and protection was a major challenge because encryption practices were decentralized and highly manual. Every department and team member had their own version of encryption and key management that involved first coordinating among several people to determine the algorithm and encryption method used, then entering the key into the central database by hand.

The process showed room for improvement because certain systems could be overlooked and not perfectly secured. A miskeyed encryption could lead to applications becoming unexpectedly unavailable and there was no software available to audit security protocols.

"We had been planning to adopt a KMS (key management system) solution for a while to replace the manual processes," Nolte says. "The announcement of a new regulation requiring that all security keys be truly centrally managed accelerated that decision and made implementing a solution the top priority."

Challenges

Complying with stringent and evolving regulatory requirements

Centralizing key management for security and efficiency

Eliminating manual-based cryptography and security tasks

> "Vault has simultaneously lowered how much effort it takes to meet regulatory compliance goals and reduced our risk of both a breach and unplanned downtime. It's been amazing."
>
> JANNIK NOLTE
> INFORMATION TECHNOLOGY SECURITY SPECIALIST, NORD/LB

Automated encryption for superior control

NORD/LB selected HashiCorp Vault over other key management solutions because of its platform and environment-agnostic design. Operating multiple datacenters with a variety of development and production environments made features like Key Management Interoperability Protocol (KMIP), integration with Kubernetes, and centralized key management must-haves.

"We had to be able to connect all our systems, including microservices, at will. It didn't make sense to implement a key system if no one can actually connect to it," Nolte notes. "HashiCorp Vault speaks several languages and interfaces effortlessly with containerized and non-containerized services alike. Now, anyone can connect any app or vital system simply and without hand-holding."

As the bank's lead cryptographer, Nolte also appreciates Vault's encryption as a service option. The solution's transit secrets engine unburdens him from manually encrypting or decrypting data while also automating data verification and signatures and other cryptographic functions on data in transit from a single, secure location.

Nolte says that NORD/LB considers this data to be its crown jewels, the most sensitive information in its possession. So, if the bank wants to store or transfer that in a cloud environment, it's mandatory to keep complete control of the encryption material.

"Not only are we not legally permitted to store that in the cloud without having full control at each point of the encryption key journey, but we also have to be ready to respond at a moment's notice to audit requests from EU Central Bank regulators," he explains. "Vault's automated encryption eliminates the risk of key exposure or expiration and gives us a digital audit trail so we can provide them detailed information about the encryption algorithms on the spot."

Stronger posture, better business

Adopting HashiCorp Vault has helped NORD/LB not only improve its overall security posture, but also dramatically improve its cybersecurity operating efficiency. Nolte credits HashiCorp's services and support teams with keeping the bank on track to meet its stringent (and evolving) security burdens, noting that trouble tickets are frequently fully resolved within just a couple of hours.

Along with troubleshooting help, Vault's robust automation and intelligent design have also freed Nolte from time-consuming manual tasks so he can focus on higher-value, more strategic initiatives.

"Before Vault, I'd spend at least three or four full days per month manually managing and rotating keys, but now it takes less than five minutes," he says. "Vault has simultaneously lowered how much effort it takes to meet regulatory compliance goals and reduced our risk of both a breach and unplanned downtime. It's been amazing."

Outcomes

Established first centralized key repository

Reduced key management and rotation from 4 days per month to 5 minutes

Eliminated risk of unplanned downtime from expired or forgotten keys

Solution

NORD/LB uses HashiCorp Vault to centralize key management, automate encryption of highly sensitive data at rest and in transit across its hybrid IT environment, and comply with strict banking regulations that constantly evolve.

NORD/LB Partner

Jannik Nolte
Information Technology
Security Specialist,
NORD/LB

Jannik Nolte is currently an Information Technology Security Specialist at NORD/LB. A seasoned cryptography expert, Nolte brings more than a decade of cybersecurity and enterprise IT expertise. Nolte is a graduate of the Frankfurt School of Finance & Management and holds various industry-recognized enterprise IT certifications and licenses.

Technology Stack

- **Infrastructure:** Azure (31%), on-premises (69%)
- **Workload type:** Linux (63%), Windows (37%))
- **Security management:** HashiCorp Vault

www.hashicorp.com