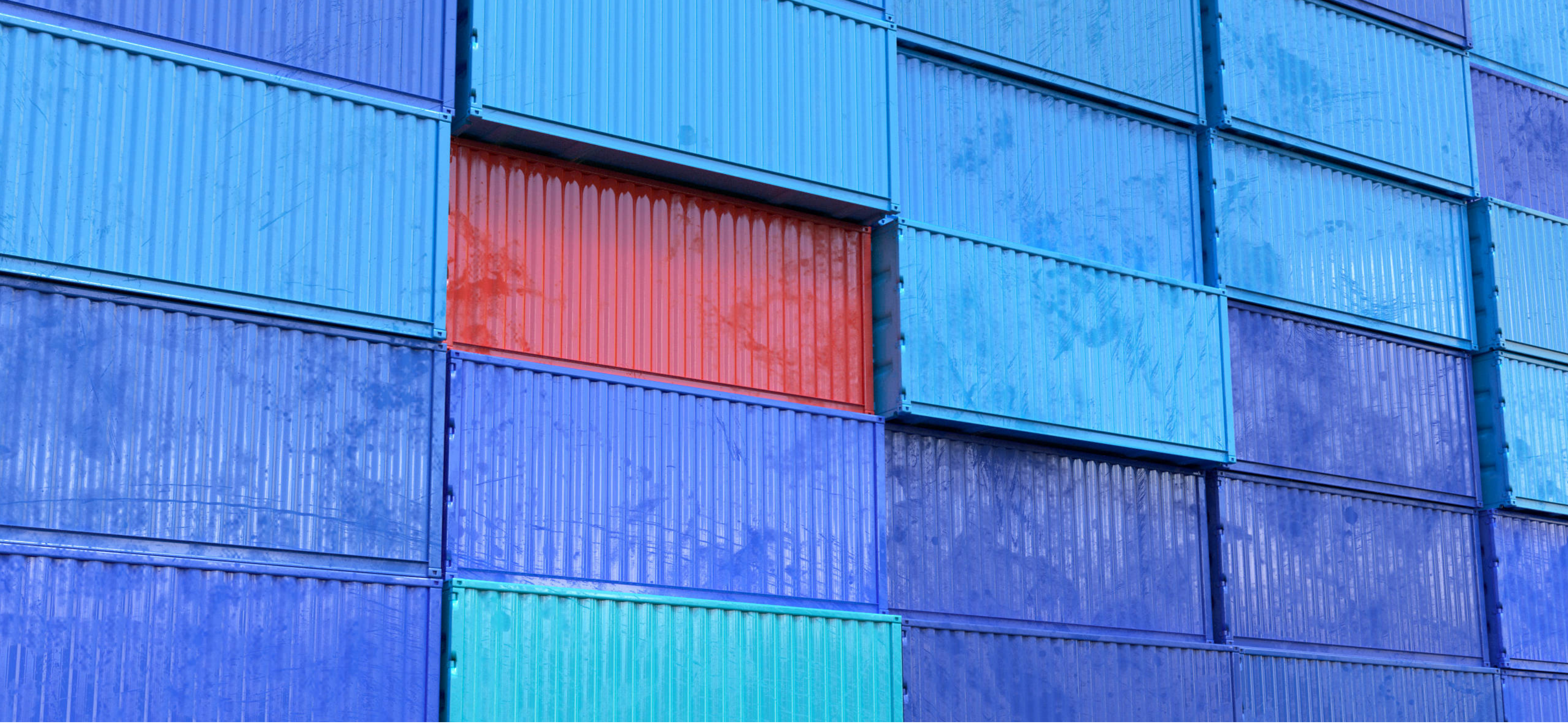
anchore

Hypothekarbank
Lenzburg

Anchore at Hypothekarbank Lenzburg

www.anchore.com
info@anchore.com



Hypothekarbank Lenzburg (HBL) was founded in 1868, and while the bank is deeply rooted in Swiss banking history, it is definitely not stuck there. HBL delivers cutting edge-products and services to its customers, from hybrid banking offices to block chain accounts. The bank's technology team also operates as a growing technology service provider in its own right, and is widely recognized as a pioneer of open banking within the Swiss financial sector.

HBL is constantly looking to support its development team, embracing technological progress and smoothing processes to increase the pace of innovation. One example is the adoption of a language agnostic approach, with multiple programming languages in use throughout its own infrastructure. And HBL has also jumped at the opportunities presented by containerization, implementing Red Hat's OpenShift platform to run containerized workloads in Kubernetes.

HBL has jumped at the opportunities presented by containerization

However, the bank's progressive attitude to technology has brought with it significant new challenges for the internal security team. In common with many banks, HBL formerly maintained a firm framework around the auditing, automation and scanning of servers for security issues. Aspects such as user permissions, service accounts and which software packages are installed, were all monitored and tightly controlled within the bank's traditional infrastructure.

Containerization can deliver massive benefits for any organization, dramatically speeding development, encouraging reuse and standardization, and often forming the core of an effective DevOps strategy. However, containers can also be challenging for organizations that have existing and mature processes around server management. The ease with which containers can be both built and distributed makes it impossible to manually keep track of what software is being introduced into your environment.

"More and more of our software, from both internal and external developers, is now delivered as containers. This made it very hard for our traditional vulnerability management solution to keep up because it couldn't scan containers efficiently," said Sascha Kaufmann, Head of IT Security at HBL. “We also needed a way to ensure a level of compliance on container deployment - such as enforcing certain base images or ensuring that no root user was allowed.”

> “More and more of our software, from both internal and external developers, is now delivered as containers”

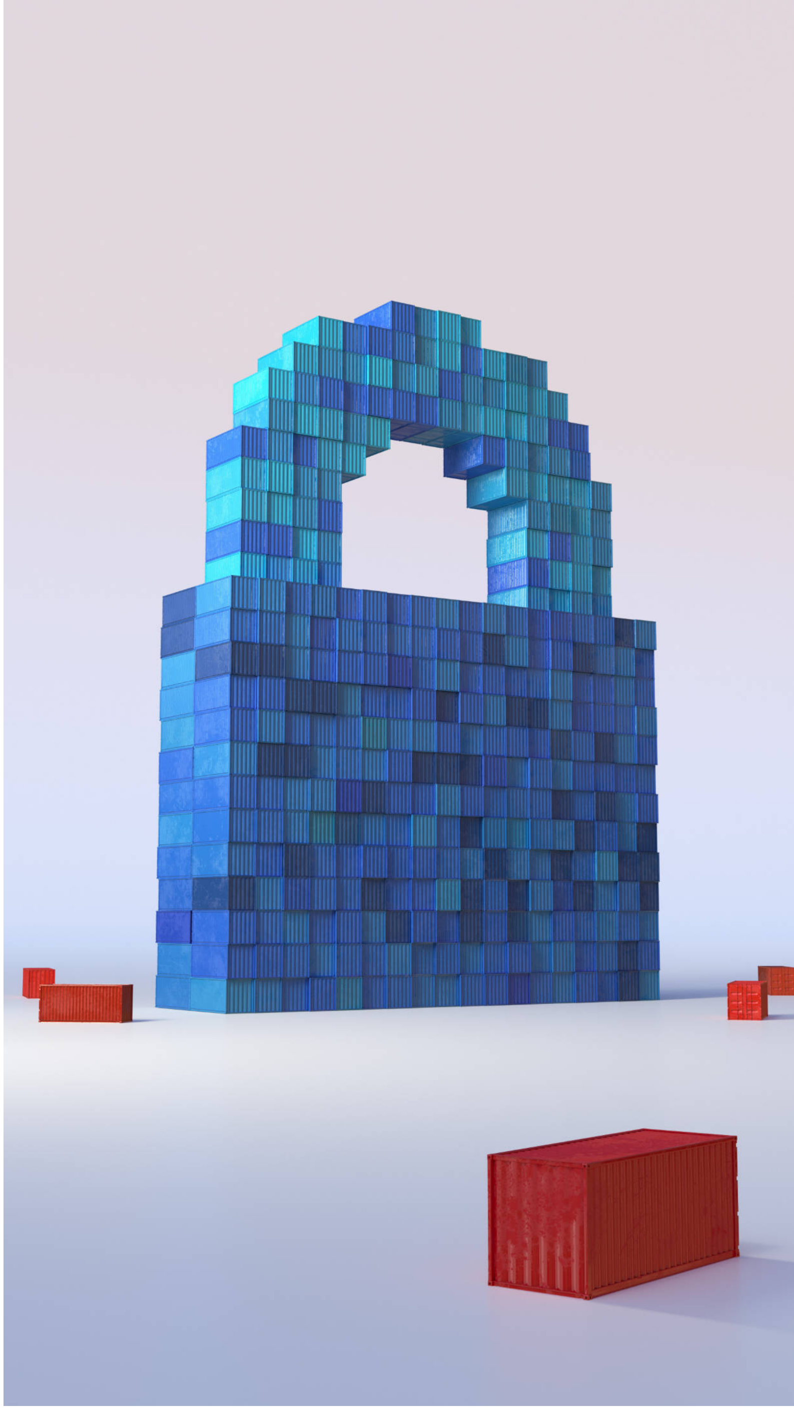
Traditional asset registries were built for a time of 'fixed' servers. They typically rely either on custom agents or, at least, an SSH connection to be present. And neither of these are likely to be available within a container. Even where teams have the considerable resources needed to manually audit containers with existing tools, most will struggle to keep pace with the rapid rate of change inherent in containerized workflows. This leads to these legacy systems delivering a view that is outdated at best, and at worst, wildly misleading.

Together, these challenges presented a major issue for HBL. Especially, since one of the many rules of the Swiss Financial Market Supervisory Authority (FINMA) requires regular, and accurate, security auditing of all software running in production.

It was obvious that HBL's existing software scanning tools and processes could no longer offer a secure solution, so the bank started by considering the larger security suites including Aquasec and Twistlock.

"At the beginning of our container journey, we were looking for a suite of tools that would cover firewalling, intrusion prevention, policy enforcement, and vulnerability management across our whole environment." Kaufmann explains, "But for a team like ours, the problem with this approach was human resourcing. Even where a vendor can offer you an all-in-one solution, it takes a lot of time to plan, deploy, maintain and monitor all these aspects."

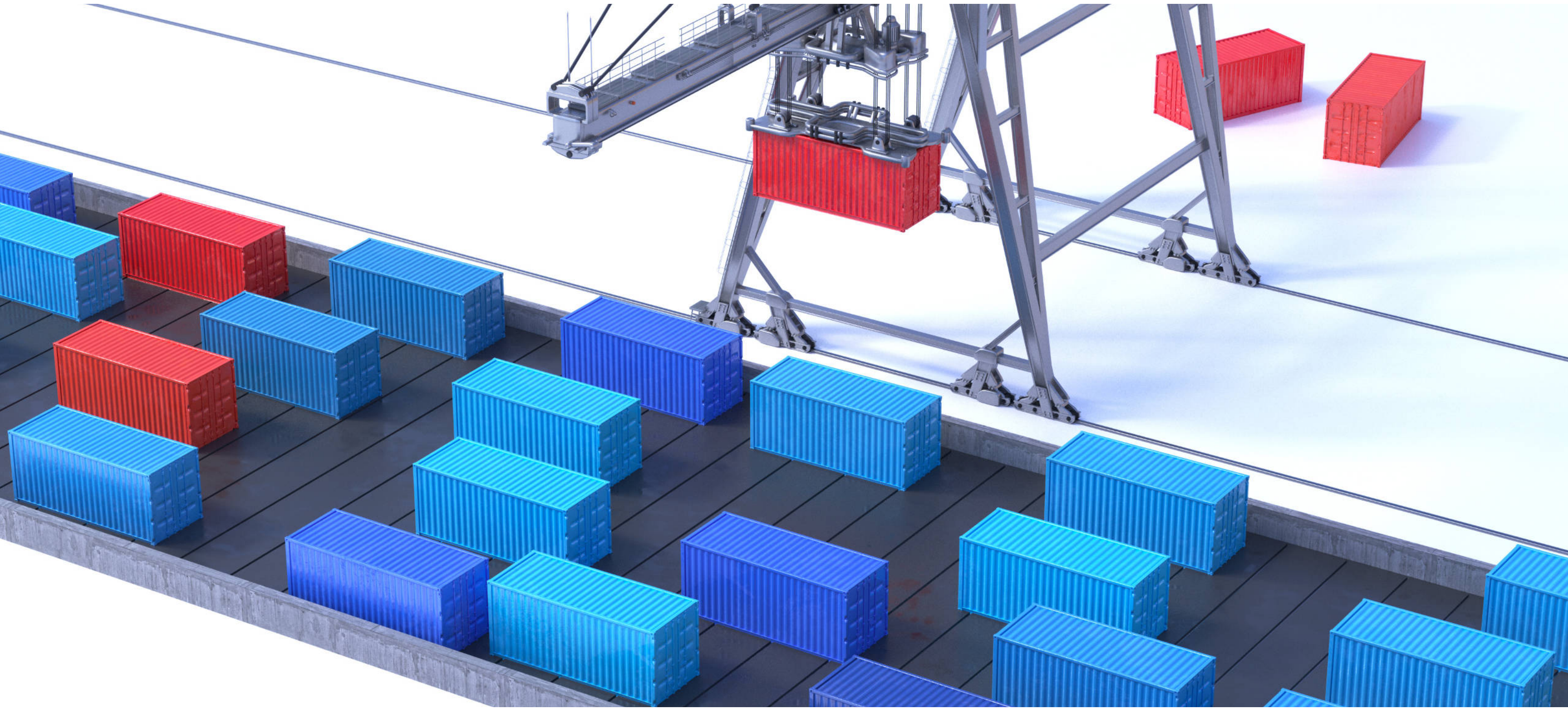
A search into newer, more agile, open source solutions led HBL to Anchore. This offered a focused solution for HBL's main concern: container security.



"Anchore didn't try to solve all of our security problems at once. It has a clear focus on a core aspect: vulnerability management and policy enforcement in containerized software," Kaufmann continues. “If you have a small team, pick your biggest pain point and then focus on fixing this. It's a lot faster and more straightforward to deploy a focused solution."

Anchore's focus on solving one core requirement allowed HBL to implement container scanning almost immediately.

After a short evaluation of Anchore's open source solution to get a feel for things, the team at HBL were convinced. The software offered a lot more than just a quick win, giving Kaufmann the missing visibility into any vulnerabilities within HBL's container environment. In contrast to other tools offering container scanning, Anchore seemed to be tailor made to fit a container-focused development workflow and to foster a workable DevSecOps process.



"Anchore is a real ally for our developers. With any security solution, it's important that we are not just 'shifting an additional burden left' and dumping it on them," explains Valeriano Piromalli, senior software engineer at HBL. "Our developers have always been responsible for resolving security issues. But with Anchore they are in control of the process and the timing. It removes the irritation."

"Security is no longer an afterthought: with a pile of vulnerabilities getting dumped on some developer who thought they had finished the job. Anchore makes security part of a smooth, ongoing DevSecOps process that starts from the earliest stages of design and development."

Impressed from the outset, HBL quickly realised the potential value of some of the additional features offered by Anchore Enterprise. These included the integration into the bank's existing authentication systems (LDAP), the intuitive enterprise UI and the enhanced vulnerability database.

But by far the biggest benefit of Anchore Enterprise was the dedicated policy interface for HBL's security team. This has allowed Kaufmann and his team to create policies that ensure compliance in the tightly regulated Swiss finance industry. It has allowed the team to create and implement a workable baseline for container security, from where they can iterate and advance policy over time towards an evolving best practice approach.

> "It is DevSecOps at work. Security is now a seamless part of our fast, smooth container-based development process"

As an implementation strategy, HBL took a two pronged approach. Firstly, Anchore has been pushed left to developers, allowing them to run ad-hoc, local scans on containers prior to deploying them. This now provides the developers with a view of any fixes needed without compelling instant action and interrupting the development process. It has helped turn security into a collaborative effort that both spreads the workload, and also engages developers to be part of the security efforts. The approach also provided the HBL security team with some immediate, valuable insights, while the work of amending the CI/CD pipelines took place in the background.

As a second part of the approach, HBL applied greater central control by adding Anchore into their CI/CD pipelines. HBL applied strict pass/fail gating to new containers as part of the publishing process. This gave developers instant feedback if their container had a high impact CVE.

"For the developers the major impact is the required change in mindset, to think of security from the outset as a part of our software development process. It is DevSecOps at work. Security is now a seamless part of our fast, smooth container-based development process," Piromalli reflects. "We are fostering a healthy attitude that security is an ongoing issue for everyone, not a problem that the security team dumps on developers as an afterthought."

For HBL, Anchore has been an invaluable tool on its container security journey. “Without Anchore we would still be completely in the dark about our container environment. We wouldn't know what kind of vulnerabilities we're facing or if a developer is running the container as root. Having a blind spot in an important part of our network wasn't a risk we were willing to take,” Kaufmann admits.

Anchore’s focused approach on delivering a solution around container scanning and compliance, has provided HBL with a rapid fix for what had initially seemed an almost overwhelming challenge. It also allowed Kaufmann to demonstrate the criticality of security to a wider audience.

“A more focused solution is a lot faster to deploy, you'll get your first wins, and you can show both management and developers that security in a container environment is as important as on a virtual machine in a datacenter.”

Moreover, Anchore has provided a security solution that is more in-tune with HBL’s development processes, delivering smooth, almost painless DevSecOps.

HBL is still at the start of its journey to create a full set of systems and policies around container security. Anchore has given them a running start, ensuring that the bank complies with legislation and guidance in one of the most tightly regulated industries. The work of Kaufmann and his team will underpin HBL’s container landscape for a considerable time to come, and provide them with a platform to progress their container security from compliance to industry-leading best practice.