ermetic | Case Study

BILFINGER

A global industrial services provider based in Mannheim, Germany, Bilfinger has 30,000 employees and covers the entire value chain from consulting, engineering, manufacturing, assembly, maintenance and plant expansion to turnarounds, as well as environmental technologies and digital applications.

In 2019, Bilfinger undertook a major migration from their central data center to Microsoft Azure cloud, with AWS as a secondary environment. Today, the Bilfinger IT infrastructure is 60-70% cloud based, with all main applications running in the cloud or on IaaS. "We see ourselves as a global platform provider that everybody at Bilfinger – and that means a lot of business areas – can use for their cloud applications and services," explained Andreas Pfau, Tribe Lead Business Solutions, Bilfinger.*

> Ermetic gets more out of the raw data than the others can – the Ermetic platform is very, very good at analyzing, at giving insights... providing information we can act on. For me, that was key.

Andreas Pfau
Tribe Lead Business Solutions, Bilfinger

The Challenge

Bilfinger understood that securing their rapid growth Azure and AWS environments required an approach different from the on prem security they were familiar with. According to Pfau, they wanted to "...avoid the same mistakes as 10 years ago. We wanted to build unified cloud security from day one – to do it right from the start."

About one and a half years into their major migration, Bilfinger realized they needed to improve security around their identities and entitlements. Said Pfau, "Our cloud infrastructure was getting more and more complex – we wanted to understand our identities better. Due to tight schedules, we were over-provisioning permissions and not always later revoking them; we knew we had overprivileged accounts, some hidden." They also sought to better secure their growing number of Azure subscriptions, avoid manual hours they were spending on certain cloud risk detection processes and achieve transparency into their global multicloud operation.

*Andreas leads Bilfinger's Digital Solutions, Engineering Workplace Services and Business Applications & Operations. He explained his innovative title: "Last year Bilfinger underwent a major organizational transformation to optimize agility, regrouping our siloed structure into tribes and squads. The new order says a lot about how we work, how we structure work, and what work is about."

A key goal was to automate least privilege access; compliance requirements -- GDPR in particular -- were another concern. At a strategic level, Bilfinger wanted an independent view into risk to complement their internal risk assessment efforts.

Thomas Lützel, Service Owner of Identity & Authentication Services at Bilfinger [whose LinkedIn motto states: "Identity securely holds the cloud together"], recalls: "I learned of Ermetic and told Andreas we should do a PoC." Added Pfau: "Security was top of mind for our IAM team - they felt they could secure IAM more successfully with a tool like Ermetic."

Pfau continued: "Our team evaluated several vendors. We found an array of marketing material, and it was obvious some vendors don't know what CIEM means, and how it should be done. Also, assessing and comparing a CIEM solution is difficult because it's a new technology, a new way of thinking. All competing products, including cloud provider native tools, are using the same raw data from the API. On the other hand, this levels the playing field because you're comparing what each solution produces from the same data. Ermetic showed it gets more out of the raw data than the others can – the Ermetic platform is very, very good at analyzing, at giving insights. For me, that was key."

> We will be integrating Ermetic much more into our operational day to day processes... using Ermetic as a platform for change.
>
> Andreas Pfau
> Tribe Lead Business Solutions, Bilfinger

The Solution

Today, three different teams at Bilfinger are using Ermetic on a day-to-day basis:

- **IAM team** (manages identities & access, including cloud)
- **Cloud Center of Excellence** (handles cloud services operationally & architecturally, and lends cloud expertise to the business units)
- **IT Security** (responsible for cloud security posture & compliance overall)

Explained Pfau, "From my perspective, these three Bilfinger teams reflect the three pillars of cloud security that Ermetic is providing: IAM security, cloud expertise as a main asset, and overall cloud posture security and compliance. Ermetic is an independent tool giving us overall transparency and deep, unified insight into our cloud architecture across both Azure and AWS, into the accounts of multiple tenants, subscriptions and whatever is in their identities.

"Ermetic sees across our entire cloud infrastructure and generates an inventory of all our cloud assets," said Pfau. "We also found the platform to be much farther along in development and usefulness than comparable products. The Ermetic risk analysis engine doesn't just collect data; it analyzes the data and gives us information we can act on.

"Ermetic is providing a very clean, straightforward view into access usage – not just at the permissions level but actual use. With Ermetic we can easily see when a permission is "over the top" – maybe we were correct at the time in thinking a certain account or group needed it but Ermetic shows it's not needed because, for example, a permission hasn't been used in six months."

How Bilfinger is using Ermetic - Use cases

- Multicloud asset management and visibility
- Risk insight into identities and permissions including 3rd party
- Remediation of excessive privileges
- Cloud governance process for cloud identities
- Continuous monitoring of network security, Internet exposure, misconfigurations
- Reporting and compliance audit
- Least privilege enforcement for zero trust (soon)
- Threat detection (soon)

Bilfinger's cloud infrastructure

- Microsoft Azure (hundreds of subscriptions), for main business applications and services, with Azure Active Directory as IdP
- AWS for virtual CAD workloads and others
- Security audit by internal team and 3rd party vendor
- Internal team performing compliance audit and addressing findings/security gaps
- SIEM
- ServiceNow

ROI and next steps

"Ermetic is important in giving us a different angle, an outside-in view, acting as an independent advisor that gives insights into what we're doing," said Pfau. "The platform is adapting all the time, so it teaches us about current situations in the cloud, use cases and threats. While we were initially focused on solving our cloud identities and identity governance needs, Ermetic's cloud security posture management is a bonus and fits well with our strategy of how to go forward.

"Our immediate goal is to standardize on Ermetic for security scanning and acting more on its findings. We will be integrating Ermetic much more into our

operational day to day processes. Specifically, we will be integrating its policy remediation recommendations through more ticketing – to drive Ermetic as a platform for change. We want to ticket to different teams, SOC and others, so each manages security in their own area.

"We also seek to implement Ermetic insights into a PDCA circuit (Plan-Do-Check-Act continuous improvement, now a requirement of ISO 27001:2013). That is, we will use Ermetic to reduce privileges and rein in overprivileged provisioning and then check that it's been done. When you close a privileged account or even split roles because one role is overprivileged, you've effected change – we will put this complete PDCA chain in place and use Ermetic to execute on it."

Closing thoughts

"My advice," summed up Pfau, "is to not be afraid when Ermetic finds mistakes or tells you something is not done well or is a high risk. A tool like Ermetic can help speed up iterations so you learn faster and get a different perspective. In the fast-changing cloud platform world you need feedback loops that are internal and external – mirrors reflecting what you're doing. Ermetic provides an external feedback loop with fast insight that you can use to accelerate remediation and make incremental security improvements.

"At the end of the day, Ermetic is giving us transparency that informs us about our cloud infrastructure and risks to our resources, and what to do about it. In Ermetic, we're just two clicks away from seeing and acting on what is really going on – and that's creating a lot of value for us."

About Ermetic. Ermetic reveals and prioritizes security gaps in AWS, Azure and GCP, and enables immediate remediation. The Ermetic cloud-native application protection platform (CNAPP) uses an identity-first approach to unify and automate cloud infrastructure entitlement management, cloud security posture management, cloud workload protection and Kubernetes security posture management. It unifies full asset discovery, deep risk analysis, runtime threat detection and compliance reporting, combined with pinpoint visualization and step-by-step guidance.

www.ermetic.com

Contact us