Cyscale

CASE STUDY

Good Medicine: Securely Migrating a Medical Devices Leader from On-premises to the Cloud

Migrating a complex on-premises infrastructure to the public cloud without specialist resources is no easy feat. But this medical devices manufacturer was able to breathe easy and adapt their technical expertise to the new environment while keeping security at the forefront of the migration.

Challenges

- A complex on-premises infrastructure that needs to be migrated to the cloud
- A lack of cloud specialists within the technical team
- IAM (Identity and Access Management) visibility gaps when offboarding users and managing access control

Results

- A swift migration to a cloud infrastructure in AWS and Azure
- Integrated cloud security by design from the start
- Confidence in a secure cloud environment despite having no in-house cloud expertise

About the company

The medical device company is a leader in the pharmaceutical and medical devices production industry, with over 20 years of experience and millions of patients. The company has a strong reputation in the industry due to its dedication to producing high-quality medical devices and pharmaceutical products widely used and trusted by healthcare professionals and patients alike.

Problem

To take advantage of the scalability of the cloud, our customer aimed to migrate their applications, VMWare virtual machines, databases, and other components of their complex infrastructure to a multi-cloud environment. However, they faced challenges due to lack of cloud security expertise and a small infrastructure team, resulting in reduced confidence and slower progress.

They needed a plan to “start right”, to ensure maximum efficiency and security by migrating their resources securely from the beginning. Furthermore, in an environment with highly sensitive data, the customer had concerns regarding offboarding users and managing IAM (Identity and Access Management) permissions. They wanted to make sure that there would be no gaps in their security posture, such as former employees with active permissions after having left the company, or users with overly broad access rights.

Solutions

Cyscale recognised the customer’s need for cloud expertise and delivered a cloud security platform that automated the security assessment process, inspiring confidence in the new public cloud environment by enabling the team to do more with limited resources.

The company did not need to hire new personnel to achieve security in the cloud due to our platform, which highlighted any misconfigurations and vulnerabilities present in their infrastructure and helped them remediate the findings:

> **I have confidence that whatever we put in our cloud environments is properly configured.**
> says the Infrastructure Engineer

Besides this, Cyscale also helped them identify any resources left undeleted after being used to explore settings during this project. This allowed the team to explore the cloud environment within guardrails, gaining confidence and proficiency in managing cloud resources effectively.

Moreover, we promptly responded with excellent customer support with our team of cloud security specialists. We helped them with any questions and issues they had and informed them of best practices. An example of a best practice applied by the company due to our recommendations is assigning permissions to groups instead of users in the cloud.

Results

The company found that previous security tools created more work for the small team by bombarding them with dozens of security alerts that contained little context. Cyscale enabled the company to establish its own risk rules, so alerts were only sent out within defined parameters and contained all relevant context to remediate the issue quickly. With Cyscale, the company managed to securely and efficiently migrate their on-premises infrastructure to the cloud. **"I can't imagine being able to manage the project without Cyscale.”** says the Infrastructure Engineer.

Cyscale allowed the medical device manufacturer to migrate projects from legacy infrastructure to a multi-cloud architecture, providing increased confidence in the project and allowing the technical team to focus on adapting to the new environment rather than worrying about security. Using security controls that continuously checked the configurations applied, our customer consistently addressed security issues as they arose and kept alerts at zero. **“Cyscale gave me visibility and confidence in our cloud infrastructure”**, says the VP of Information Technology.

The technical team was eager to understand how the cloud and its many services work, and Cyscale enabled them to learn and build their multi-cloud infrastructure without worrying about vulnerabilities in their systems.
Finally, using Cyscale, the company managed to identify offboarded users that still had permissions to access resources, as well as improve access control policies.

Conclusion

Cyscale helped the customer migrate their on-premises infrastructure to the cloud, secure all cloud assets from the beginning, and manage IAM (Identity and Access Management) permissions. The company's confidence in its infrastructure in the cloud was enhanced drastically, while security and efficiency were top priorities.