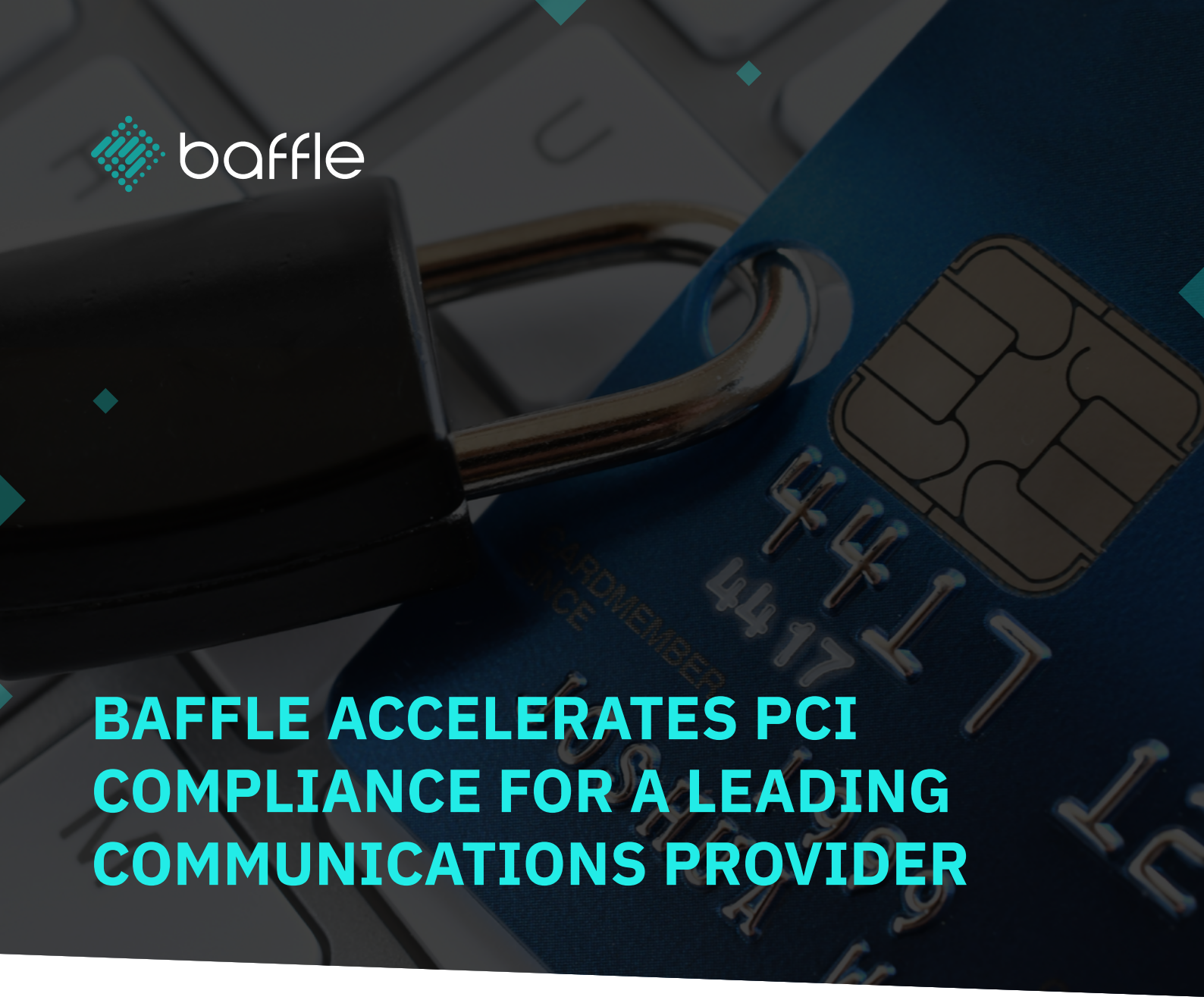


BAFFLE ACCELERATES PCI COMPLIANCE FOR A LEADING COMMUNICATIONS PROVIDER

A major provider of high-speed broadband internet, phone services, and digital TV packages was facing increasing pressure to meet the stringent requirements of PCI DSS 4.0. The company stores vast amounts of sensitive customer data, including credit card numbers and social security numbers, making it a prime target for data breaches.

PCI DSS 4.0 looms large

The company stores sensitive customer data such as credit card numbers for payments, and social security numbers for credit checks. As such, it is subject to PCI compliance and needed to meet both current as well as upcoming requirements for PCI DSS 4.0. Hence, they sought a solution to tokenize credit card and social security numbers quickly and efficiently.

Their infrastructure consists of J2EE applications running on top of relational databases in Oracle Cloud. Tens of millions of records subject to PCI compliance are stored in the databases. A multi-cloud architecture has their systems spanning across Microsoft Azure and Oracle Cloud. Their applications also run inside a centralized Kubernetes cluster.

Previously the organization had been using a legacy encryption solution that had reached end-of-life. They wanted to replace it with a modern data protection approach that was compatible with their cloud and container environments, but yet gave them full control and ownership over their data.

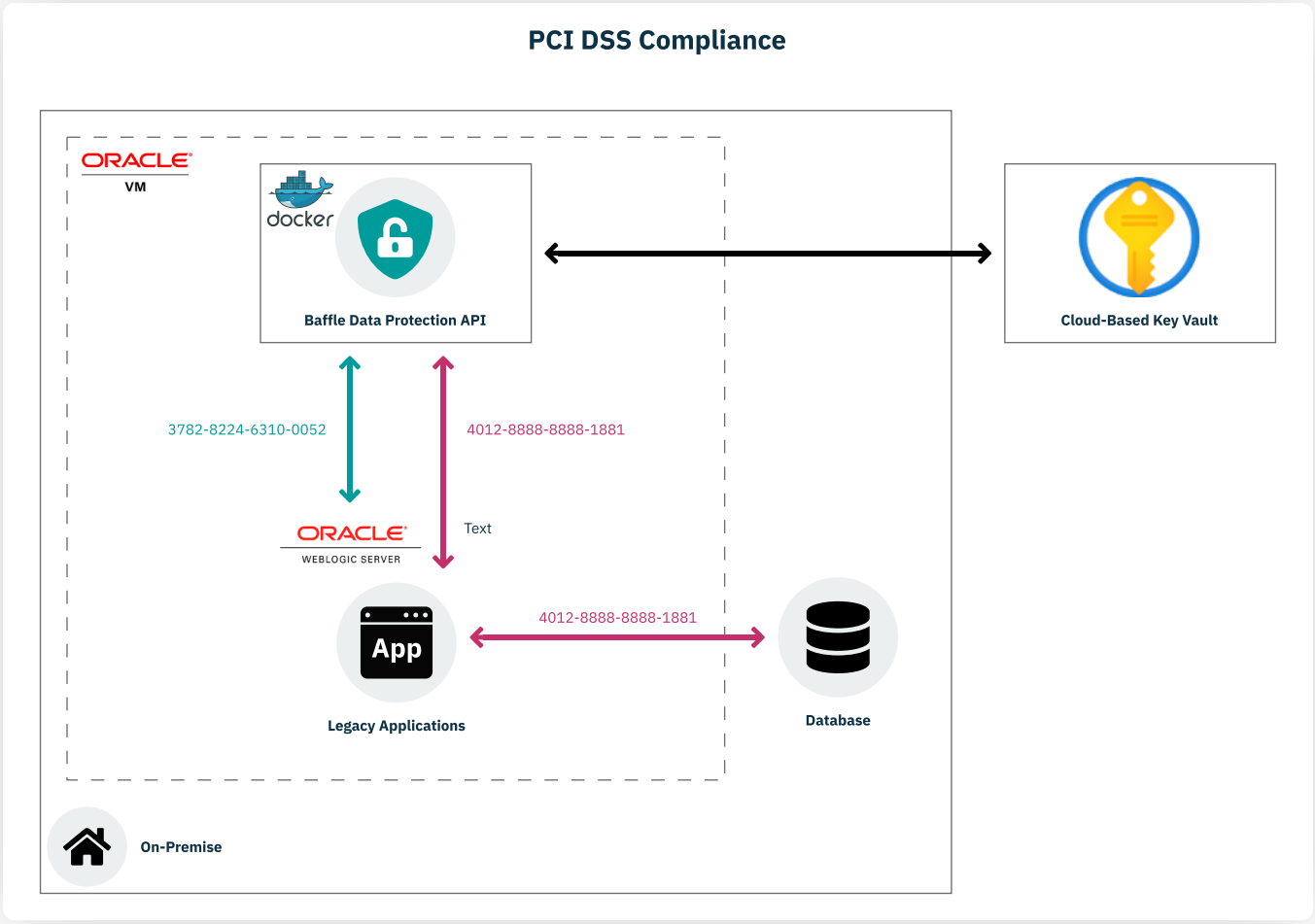
One approach the team considered was to rewrite large portions of their legacy application to meet these encryption and tokenization requirements. However, this would be extremely painstaking and costly. Hence, they sought an easier solution that would be faster and more affordable to implement.

Baffle's no-code approach enables simplified compliance

Baffle offered the company a significant advantage. They could easily encrypt data without having to make large scale changes to their application. APIs provided by Baffle's data protection service could tokenize credit card and social security numbers on the fly.

All of the policies associated with the encryption are defined centrally inside the Baffle solution which runs in the customer's own VPC environment. These policies are mapped to roles in their identity management system. When the application makes an API call, the user role is validated and passed via a JSON Web Token (JWT) token to Baffle. This is then used to apply the appropriate encryption or decryption for that role.

A leading cloud based Key Vault was used for simplified encryption key management which made the deployment even more streamlined.



The Results

The company was able to rapidly protect tens of millions of existing records in their database to meet PCI (including DSS 4.0) requirements. Any new data written by the application is seamlessly tokenized by Baffle before being written to the underlying database.

With Baffle, the company gained significant advantages in meeting PCI requirements, including:

Easy to Implement: Baffle's proxy based approach and an API made the implementation very easy with existing applications and databases.

Full Control: Since the Baffle software is fully deployed within their own environment, the customer never has to worry about sensitive data being transferred to any other party.

Highly Performant: The solution is able to scale to their needs easily and does not slow down existing applications.

Flexible: Baffle can work with multiple data formats including databases and semi-structured files.

Minimum Disruption: Migrating to Baffle was easy compared to other approaches, the initial data conversion took just a handful of hours ensuring minimal downtime.

Excellent Support: The customer really appreciated the very helpful and friendly customer success team at Baffle. In addition, extensive logging and easy troubleshooting made it very easy to resolve any issues.

info@baffle.io
https://baffle.io
3979 Freedom Circle, Suite 970
Santa Clara, CA 95054