Automate data security – APAC

Multicloud financial services applications

Red Hat | intel

Automate data security

Multicloud financial services applications

The cost of data breaches will rise from $3 trillion annually to over $5 trillion in 2024, or an average annual growth of 11%.[1]

Juniper Research

Managing security and compliance across multiple clouds means mitigating multiple risks

In recent years, benefits like agility and elasticity have driven rapid adoption of cloud-native applications in the financial services industry. However, moving to cloud and multicloud deployments brings security and compliance issues to the forefront, especially when it comes to customer data. Protecting data represents a critical concern for every business, but in financial services it can mean protecting the customer's money as well.

Banks, payment providers, and insurers along with other financial service firms must comply with a range of increasingly strict security and privacy standards. These include the Payment Card Industry Data Security Standard (PCI DSS) and the European Union's General Data Protection Regulation (GDPR). Although a European law, many global companies are raising the bar to comply with GDPR, which requires stringent tracking, reporting, and documentation to maintain compliance.

Many of these laws contain specific requirements regarding how organizations protect personally identifiable information (PII) data. They also require companies to prove that they have safeguarded customers' data in the event data gets lost or stolen. For example, California's Security Breach Information Act (SB-1386) – which other U.S. states have also adopted – was the first state law to require breach disclosure. It mandates organizations notify affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[2] However, it specifically offers a safe harbor if you can demonstrate that the compromised data was encrypted at the time of loss.

Managing security and compliance across multiple clouds means mitigating multiple risks

In recent years, benefits like agility and elasticity have driven rapid adoption of cloud-native applications in the financial services industry. However, moving to cloud and multicloud deployments brings security and compliance issues to the forefront, especially when it comes to customer data. Protecting data represents a critical concern for every business, but in financial services it can mean protecting the customer's money as well.

Banks, payment providers, and insurers along with other financial service firms must comply with a range of increasingly strict security and privacy standards. These include the Payment Card Industry Data Security Standard (PCI DSS) and the European Union's General Data Protection Regulation (GDPR). Although a European law, many global companies are raising the bar to comply with GDPR, which requires stringent tracking, reporting, and documentation to maintain compliance.