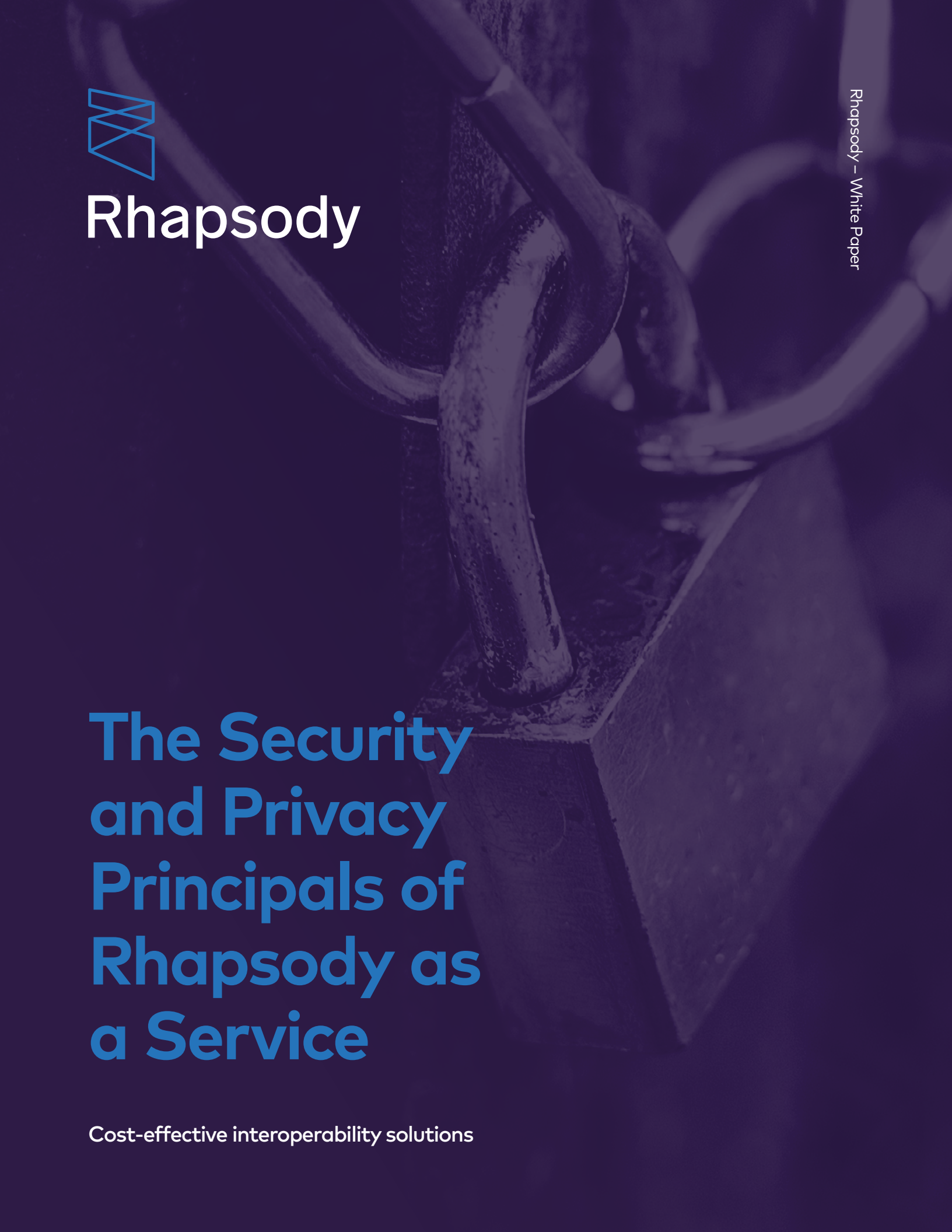


Rhapsody

Rhapsody – White Paper

The Security and Privacy Principals of Rhapsody as a Service

Cost-effective interoperability solutions

The Security and Privacy Principals of Rhapsody as a Service

Introduction

There are many well-documented advantages to utilizing managed services including higher availability, greater scalability, predictability of costs and the reduced complexity of managing systems. This report explores how Rhapsody as a Service (RaaS) benefit providers by relieving the burden of adhering to ever-evolving security frameworks and regulations (such as HIPAA and GDPR).

As there is a legal responsibility for all providers to manage their patients and customers privacy and data integrity it is essential that stakeholders understand all aspects of the solution, especially how it meets frameworks and regulations. This document provides a high-level overview of the security and privacy principles and techniques used in RaaS. The principals and techniques discussed include; encryption of protected health information (PHI) in transit and rest, VPN tunnelling, monitoring and alerting, etc.

Security and Privacy

The security and privacy practices of RaaS have been created as a result of working through the HITRUST certification process with other services. The development team has applied the lessons and learnings that have come from meeting HITRUST, HIPAA and GDPR requirements and have implemented them within RaaS from the ground-up.

To begin with, when a customer chooses to implement RaaS, a new account is created in Amazon Web Services (AWS). The service is then deployed within the closest AWS region to meet governance requirements and reduce service latency. Each account has its own virtual private cloud (VPC) to isolate it's network traffic (there is no multi-tenancy model).

A virtual private network (VPN) is also implemented for each customer, this enables their internal systems to privately exchange messages with RaaS. Encryption in transit has been applied throughout — not only in the external networking connections — using a robust VPN solution with AES-256/ SHA-256 encryption (if applicable).

RaaS uses firewalls to only allow traffic that is required in and out of the RaaS system and create audited events customers and the SOC.

SOC

A separated and autonomous security company known as the Security Operations Center (SOC) has been employed to act as RaaS's second eyes. The SOCs role is to summarise and view audited events and complete regular checks to ensure that RaaS is not vulnerable to any known security exploits,

The Center monitors RaaS 24/7 using a completely independent set of tools, processes and team members who run intrusion detection and numerous other security related activities.

Hands-off Principles

Rhapsody employs a hands-off approach to DevOps to create the optimal environment for data protection. Rhapsody Engineers do not have physical access to customers infrastructure and use automation to manage the service. The engineers develop, test, and productionise the software behind the automation, and use it for provision, support, maintenance, and for reacting to incidents.

All changes to the service create audit trails which grant healthcare providers the ability to review any interactions, these are also sent in real-time to the SOC. This enables Rhapsody to reduce the cost of support and maintenance, and enables scalability while removing the risk of accessing PHI/PII Data.

Development process

Rhapsody has a focus on continuous improvement, so the full development team meets twice a month to discuss, and plan, practice and process improvements for all customers. In the unlikely event of an incident or fault, the Rhapsody team will perform a post-incident review. This process collects everybody who was involved in the incident together to work through the timeline and establish a root cause. The goal of this process is to work out ways to prevent the incident happening again or to mitigate its impact, and create fixes so that all customers receive the benefit of the improvements.

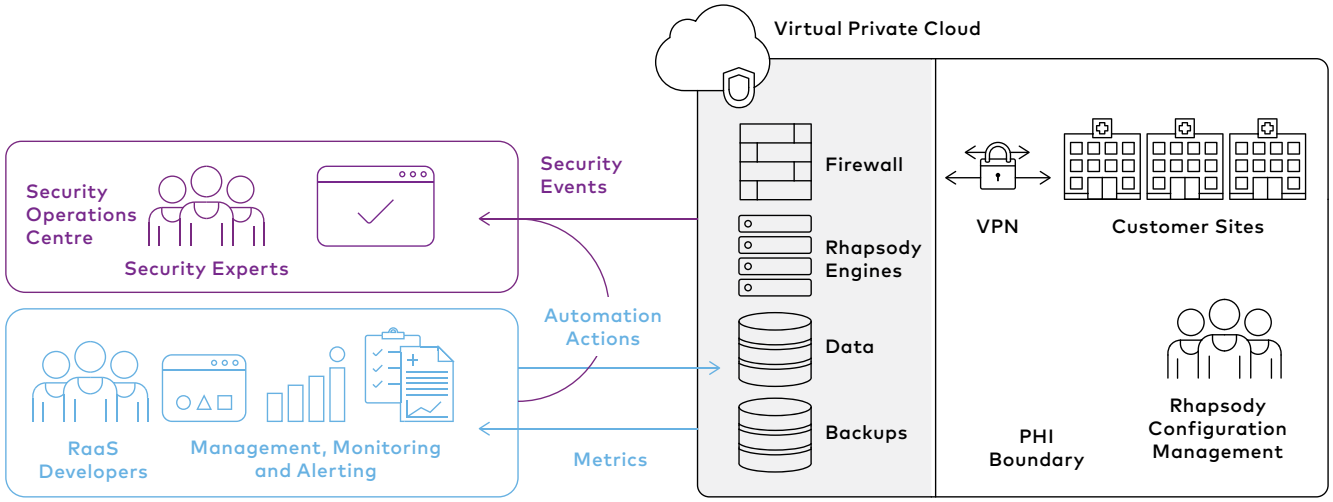
The Security and Privacy Principals of Rhapsody as a Service

Metrics by Default

Major performance and workload indicators are measured within RaaS. These can be compared and visualised over time to define impacts or improvements to the service after changes have been made. The metrics provide valuable information that can be used to detect abnormal conditions, which can be a precursor to major issues. Analysing this information helps the RaaS team to react to potential incidents before they become major incidents.

Conclusion

Both security and privacy are important parts of the Rhapsody company culture. All Rhapsody services have been developed with the principals in mind and automation is utilized throughout to further increase security, improve quality of service and reduce at the forefront costs. RaaS incorporates HIPAA and GDPR standards and is undergoing HITRUST certification to help offset the complexities of meeting regulations for healthcare providers.



Rhapsody

Rhapsody is now available as Rhapsody as a Service.

Find out more at www.rhapsody.health

—