Case Study: Fortifying cloud security and HIPAA compliance for a global health services company

Industry: Health services

Challenge

A global health services company faced significant security and compliance hurdles after migrating its critical health applications to a multi-cloud environment, leveraging both AWS and Azure. Their manual firewall management processes were slow, error-prone, and introduced substantial risk, particularly concerning the vast amounts of Protected Health Information (PHI) they handled. This outdated approach made it exceptionally difficult to achieve and maintain compliance with stringent regulations like **HIPAA (Health Insurance Portability and Accountability Act)**, jeopardizing patient privacy and data integrity. While they also managed payment card data and thus had obligations under PCI DSS, their primary focus for health data security was HIPAA.

Solution

The company implemented a robust security policy management platform to automate and centralize their security operations. This solution provided crucial visibility into application connectivity and data flows, enabling a clear understanding of potential vulnerabilities within their hybrid cloud infrastructure, especially where PHI resided. It streamlined their security policy change workflows, replacing cumbersome manual processes with an efficient, automated system. A key benefit was the platform's ability to ensure continuous regulatory compliance, specifically for **HIPAA**, by providing comprehensive audit trails, real-time policy enforcement, and granular access controls tailored for sensitive health data. A key aspect of this automation involved the centralized management of security groups within both AWS and Azure. The platform provided granular control and visibility over security group configurations, ensuring that network access to applications handling PHI was strictly controlled and compliant with HIPAA requirements. This eliminated the manual, error-prone process of managing security group rules across disparate cloud environments. The solution also supported their adherence to PCI DSS for payment processing, by reinforcing overall security best practices.

Key Benefits & Results

By adopting this automated solution, the health services company achieved significant improvements across several key areas:

Centralized policy visibility for audit & compliance (with a focus on HIPAA)

The platform offered a unified view of security policies across their multi-vendor, hybrid cloud environment (AWS and Azure). This centralized visibility was instrumental in simplifying policy management and ensuring consistency, which is crucial for accurate **HIPAA** audit reporting and demonstrating compliance with data privacy and security regulations. The clear documentation and change tracking features streamlined their audit processes, reducing the challenges associated with disparate, home-growntools.

- **50% faster audit preparation:** The automated reporting and simplified policy management drastically cut down the time and effort required for audit readiness, particularly for **HIPAA.**
- **Improved visibility and control over security policies for audit purposes:** The centralized platform provided a comprehensive and easily auditable record of all security policies impacting PHI.

Application-Centric visibility for risk assessment and compliance

The solution took an application-centric approach, discovering and visualizing application connectivity and dependencies. This was critical for understanding the risk exposure of their sensitive health applications and ensuring compliance with data protection regulations, especially related to PHI. The visualization of application flows highlighted potential security risks and vulnerabilities, supporting comprehensive risk assessments and audit reviews.

- **Enhanced visibility into application-specific risks:** The ability to see application flows provided a deeper understanding of potential threats to patient data.
- **Improved risk assessment for critical business applications:** Risk assessments were more accurate and relevant due to the application-contextualized view, ensuring that PHI security was prioritized.

Proactive risk mitigation and continuous compliance

The platform automated risk assessments and compliance checks, shifting the company to a proactive security posture. This automation reduced manual effort and improved the accuracy of compliance reporting. Features like risk checks integrated with their development lifecycle, identifying and preventing security issues early on, minimizing the likelihood of HIPAA violations and other data breaches.

- **65% fewer security misconfigurations:** Automated checks and enforcement significantly reduced human error in security configurations, bolstering PHI protection. This included a significant reduction in misconfigured security groups, which are often a common source of unauthorized access and data breaches in cloud environments.
- **Early detection and prevention of security vulnerabilities, minimizing compliance risks:** Proactive identification of issues prevented potential breaches of sensitive health data and compliance failures.

Strengthened security posture with application context for reduced risk

By providing application context to network security policies, the solution enabled more precise risk assessment and targeted compliance efforts for PHI. It helped prioritize remediation based on application criticality, ensuring that compliance resources were focused on the most vital assets and the highest-risk data.

- **80% faster security policy changes:** Automation and streamlined workflows drastically accelerated policy updates, improving the agility of their security response.
- **40% faster application deployment:** Proactive profiling of connectivity changes minimized risks and ensured compliance, leading to quicker rollouts of new health applications and services.

Conclusion

By implementing an automated and intelligent security policy management platform, this global health services company successfully overcame its cloud security and compliance challenges. They not only accelerated their operations and significantly reduced security risks associated with PHI but also streamlined their **HIPAA** audit preparation, demonstrating a strong commitment to protecting sensitive patient data in their multi-cloud environment.