Network Fort

Strengthening Cloud Security with Network Fort

Introduction

The security of the cloud-based infrastructure is of paramount importance. As an organization store and process huge amount of data in the cloud, the risk of cyber threats looms large. To address these issues, businesses need comprehensive strategies to fortify the cloud infrastructure. From advanced encryption protocols to robust access controls, the most resilient cloud security framework empowers businesses to navigate the digital landscape with confidence.

Business Background

The large enterprise faced cloud security issues that included Data Loss/Leakage, Data Privacy/Confidentiality, and Legal and regulatory compliance. The enterprise was in dire need of implementing a strong defensive security system to counter the risks associated with it. With a vast amount of sensitive data stored in the cloud, ensuring robust security measures is crucial to maintaining the trust of their clients.

Customer Challenges

- There is no such thing as the completely isolated subnet
- Security groups are difficult and imperfect
- Network flow logs are too shallow
- Blackbox detection tools lack the context to triage alerts
- API logs are not exhaustive, voluminous/noisy, inconsistent
- Enabling forensic logging and easy integration of different systems with Network Fort.

Solutions Provided to the Customer

1. Cloud Security Assessment

NetworkFort performed a comprehensive audit of the cloud environment, analyzing access controls, data encryption protocols, and network configurations. This assessment identified existing security flaws and formed the foundation for developing a robust security framework.

2. Intrusion Detection and Prevention System (IDPS)

NetworkFort implemented a cutting-edge IDPS that constantly monitored network traffic and proactively identified and blocked suspicious activities. This helped prevent

unauthorized access attempts and potential data breaches, providing an additional layer of security to ABC Corp's cloud infrastructure.

3. Two-Factor Authentication (2FA)

NetworkFort implemented the 2FA across the client’s cloud platform to strengthen access control. This required users to provide two forms of verification, such as password generation, ensuring only authorized personnel could access critical systems and data.

4. Security Incident Response Plan

NetworkFort developed a comprehensive incident response plan for the client. This plan outlined all the necessary steps to be taken in the event of a security breach while ensuring a swift and effective response. This minimizes the potential damages and restores normal operations.

Security Flaws Detected

- Weak access control to sensitive data
- Outdated software risks that caused vulnerabilities
- Insufficient data encryption
- Inadequate monitoring and logging