Secure Patient Data Platform on Google Cloud

A Solution for UN SDG 3: Good Health and Well-being

Presented by: Pranith Jain

The Problem: Healthcare at High Risk

Vulnerable Infrastructure

Outdated on-premise systems are costly and difficult to secure against modern threats.

Escalating Cyber Threats

Healthcare is a prime target for ransomware, data breaches, and unauthorized access, compromising patient safety and privacy.

Stringent Compliance Demands

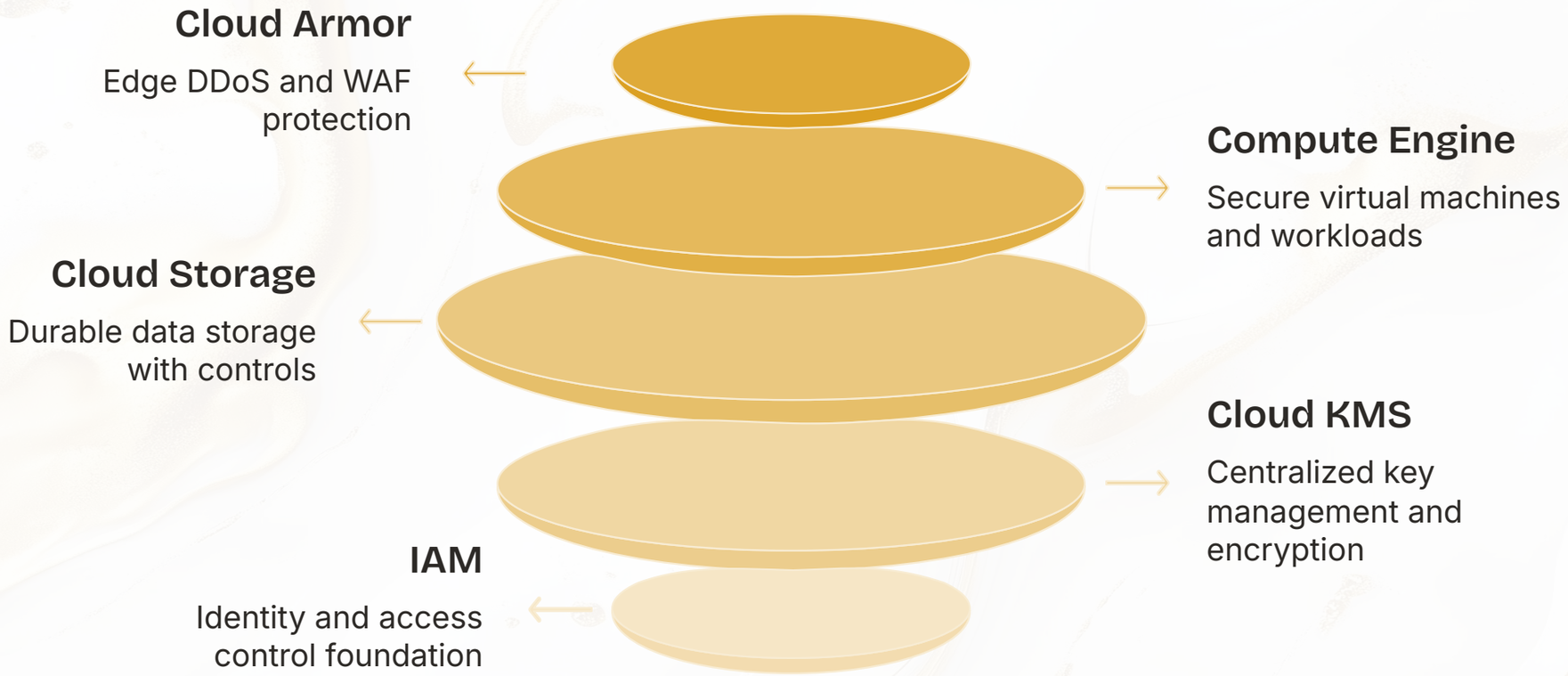
Navigating complex regulations like HIPAA, GDPR, and others imposes significant burden and risk of non-compliance.

Severe Impact

Breaches lead to financial penalties, erosion of patient trust, and critical disruptions to care delivery.

MY Solution: A Defense-in-Depth Approach on Google Cloud

A multi-layered security architecture designed for scalability, cost-effectiveness, and robust protection.



Leveraging key Google Cloud services:

- **Compute Engine:** Secure hosting for the web application.
- **Cloud Storage:** Encrypted, durable storage for patient data.
- **Cloud KMS:** Centralized key management for data encryption.
- **IAM:** Fine-grained access control to prevent unauthorized access.
- **Cloud Armor:** Web Application Firewall (WAF) for DDoS and application-layer protection.

Aligned with UN SDG 3: Good Health and Well-being

Our project directly supports **UN Sustainable Development Goal 3**, particularly **Target 3.c**, which aims to:

> "Increase health financing and the recruitment, development, training and retention of the health workforce in developing countries, especially in least developed countries and small island developing States."

A secure digital foundation is paramount for achieving these objectives.

Our Contribution:

- Protects Patient Privacy: Building trust and ensuring ethical handling of sensitive health information.
- Enables Operational Reliability: Allowing clinics to focus on patient care without fear of cyber disruption.
- Fosters Resilient Health Systems: Contributing to stable and secure healthcare infrastructure globally.

Implementation & Key Takeaways

01

Secure VPC Network

Provisioned a Virtual Private Cloud (VPC) with isolated subnets for enhanced network security.

02

Encrypted Cloud Storage

Set up Cloud Storage buckets with Customer-Managed Encryption Keys (CMEK) for data at rest.

03

Fine-Grained IAM Roles

Configured granular Identity and Access Management (IAM) roles to enforce the principle of least privilege.

04

Web Application Deployment

Deployed the patient data web application within the secure environment, ensuring secure communication channels.

05

Logging & Monitoring

Integrated robust logging and monitoring solutions (Cloud Logging, Cloud Monitoring) for continuous security oversight and incident response.

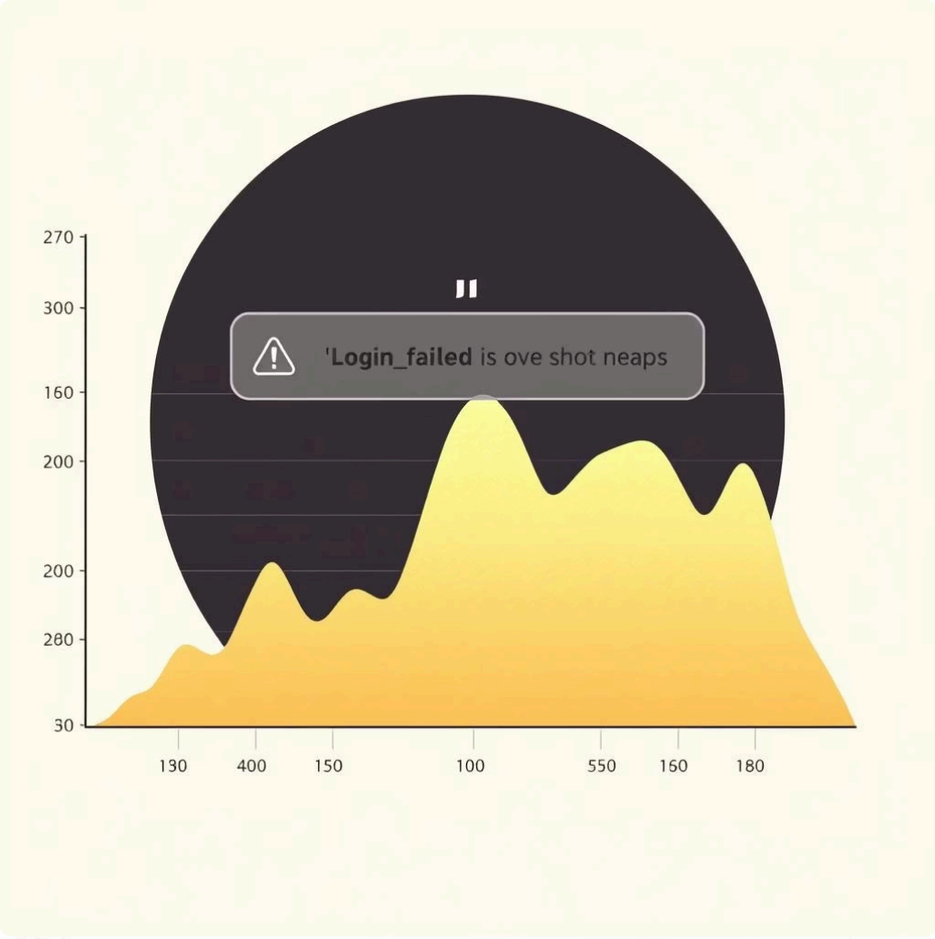
Key Learning:

Hands-on experience with **gcloud CLI**, applying **DFIR** (Digital Forensics and Incident Response) principles, and building a fully functional, secure system from the ground up.

Validated Outcomes & Demonstrations

1. Proactive Threat Detection

Successfully monitored and generated alerts for simulated login failures, demonstrating immediate detection capabilities. This showcased my ability to perform as a Security Operations Center (SOC) analyst, identifying and responding to potential threats in real-time.



2. Strict Access Control

Demonstrated how precisely configured IAM roles effectively prevent unauthorized users from accessing sensitive patient data, upholding strict data confidentiality.

3. Compliance Readiness

Highlighted the automatic generation of detailed audit trails, crucial for regulatory reporting and forensic analysis. Verified the implementation of **data encryption at rest**, ensuring compliance with industry standards and legal requirements.

Future Enhancements & Scalability

Our platform is designed with future growth and evolving security needs in mind.

Planned Enhancements:

- **SIEM Integration:** Implement an audit log sink to a Security Information and Event Management (SIEM) system for centralized, advanced threat analysis and correlation.
- **Google Cloud Healthcare API:** Integrate Google Cloud's Healthcare API for seamless, compliant management and interoperability of patient data, aligning with industry standards.
- **CI/CD Pipeline:** Establish a Continuous Integration/Continuous Deployment (CI/CD) pipeline to automate secure application updates and deployments, ensuring rapid and safe feature delivery.

Scalability:

The current architecture supports inherent scalability. We can easily scale to handle increased patient traffic by adding more Compute Engine instances behind a load balancer, ensuring high availability and performance even under peak loads.

Conclusion

A Secure Future for Healthcare Data

This capstone project successfully integrates my expertise in **DFIR** and **SOC analysis** with Google Cloud's robust security services.

> "I have built a secure, scalable, and compliant patient data platform that directly contributes to UN SDG 3: Good Health and Well-being."

Thank You. Questions?

Key Takeaways from the Project

Holistic Security Mindset

Security isn't an add-on; it's fundamental to every layer of cloud architecture.

Compliance is Achievable

With the right tools and design, stringent regulatory requirements can be met and maintained.

Cloud Empowers Healthcare

Secure cloud platforms enable healthcare providers to innovate and deliver better care.

This project demonstrates a practical, real-world application of cloud security principles for critical infrastructure.

About the Presenter

Pranith Jain

Cloud Security Enthusiast & Analyst

With a strong foundation in Digital Forensics and Incident Response (DFIR) and Security Operations Center (SOC) methodologies, I specialize in building secure, resilient cloud infrastructures.

- Passionate about leveraging cloud technologies to solve real-world security challenges.
- Committed to continuous learning and staying ahead of evolving cyber threats.
- Dedicated to contributing to a safer digital environment, especially in sensitive sectors like healthcare.

Contact: zyrenic@cc.cc