AI Product Launch

BrainStation Cybersecurity Capstone

Prepared by: Isabelle Jaber

Introduction

VISION is a leading tech firm in San Francisco that excels in computer vision technology. They help businesses build custom computer vision solutions with services including data management, annotation, and model libraries.

Their success is driven by data, talent, and technology. All data is securely managed in the U.S., and their team of 200+ employees, along with various contractors, ensures innovative solutions.

VISION is now partnering with a major healthcare provider to enhance medical imaging diagnostics through AI, aiming for increased accuracy and efficiency with secure data processing and careful result communication.

See more information here

Risk Assessment

Top 3 High Impact Risks

Adversarial Attacks

Intentionally crafting inputs designed to deceive AI models to produce incorrect results.

Data Breach

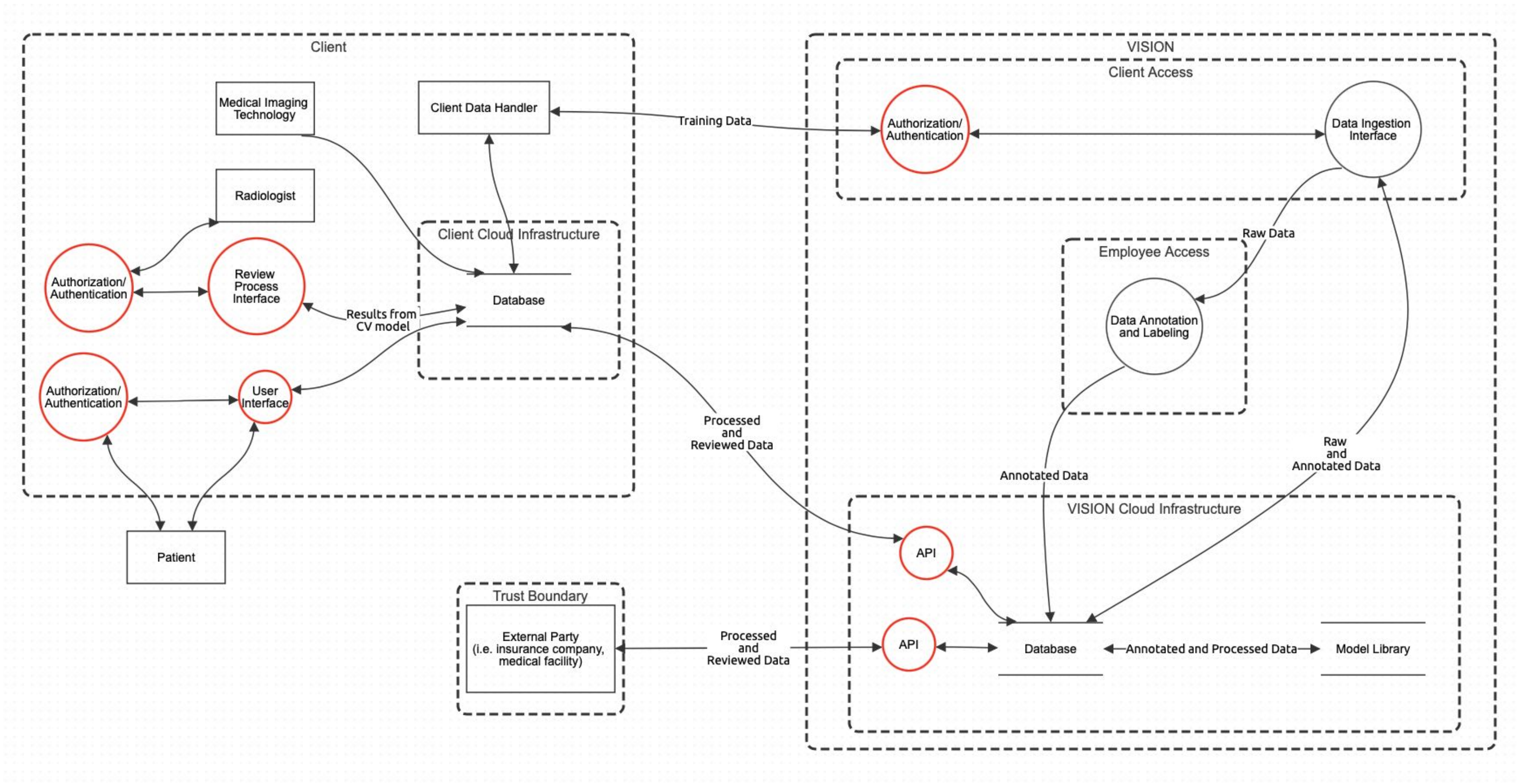
Exposure or exfiltration of sensitive health data.

Non-Compliance with Data Protection Policies

Violating HIPPA and other regulations could lead to penalties.

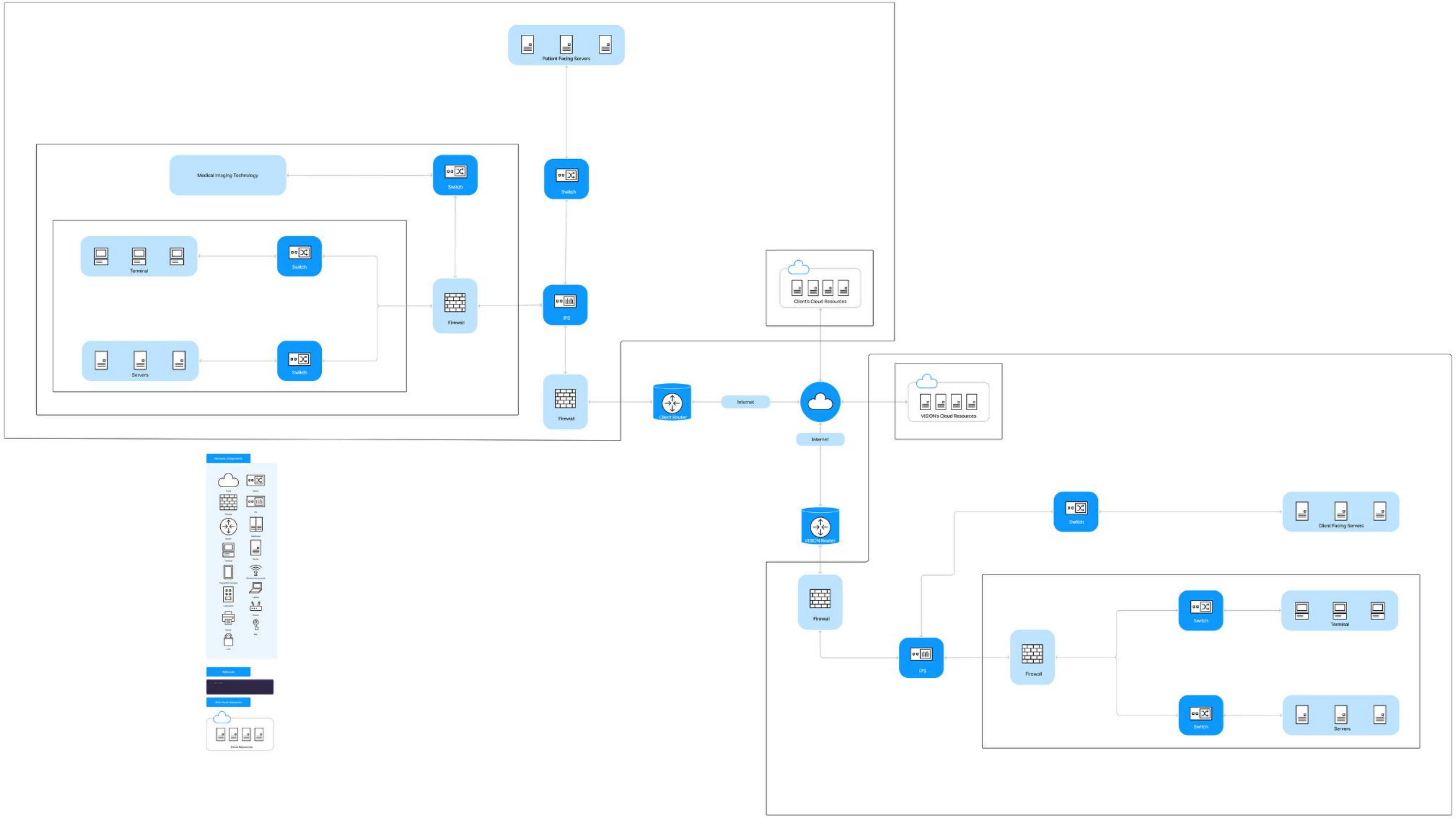
Threat Model

Threat Model


Client
Medical Imaging Technology
Client Data Handler
Training Data
Radiologist
Client Cloud Infrastructure
Authorization/ Authentication
Review Process Interface
Database
Results from CV model
Authorization/ Authentication
User Interface
Processed and Reviewed Data
Patient
Trust Boundary
External Party (i.e. insurance company, medical facility)
Processed and Reviewed Data
VISION
Client Access
Authorization/ Authentication
Data Ingestion Interface
Raw Data
Employee Access
Data Annotation and Labeling
Annotated Data
Raw and Annotated Data
VISION Cloud Infrastructure
API
API
Database
Annotated and Processed Data
Model Library

Network & Data Security

Network Architecture Diagram



Third-Party Risk Assessment

Third-Party Risks

Asset	Potential Impact	Likelihood	Mitigations
Cloud Service Providers (eg. AWS)	High	High	Encryption standards, monitoring of service level agreements (SLAs), and regular security audits.
Cybersecurity Monitoring Team (eg. contracted team in India)	High	Medium	Coordination with the team, clear security protocols, and continuous coverage and regular audits.
Data Annotation and Labeling Tools	High	Medium	Tools with strong security certifications, access controls, and regular security audits..
IT Vendors (eg. cleaning, office supplies/snacks)	Low	Low	Strict access controls and regular vendor security assessments.
Consultants and Contractors	Medium	Medium	Contracts with stringent security requirements and regular audits and compliance checks.

Incident Response Plan

Incident Response Plan Goals

Quick Identification

Rapid detection of ML threats to ensure a timely response.

Containment

Limit the spread of events affecting ML models or data pipelines.

Mitigation and Remediation

Mitigate vulnerabilities and remediate attacks to ensure ML model integrity.

Recovery

Restore ML systems with minimal downtime, ensuring data accuracy.

Compliance

Adhere to data protection regulations when responding to events.

Business Continuity Plan

Plans

Business Continuity

Redundancy, disaster recovery (DR) site, failover systems, vendor management, and testing and drills.

Backup and Recovery

Data backups and integrity checks, RTOs/RPOs, disaster recovery plan.

Communication

Internal, client, third-party, and regulatory authorities.

Thank You

Questions?

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

Appendices:

Risk Assessment

- Appendix A: Risk Assessment Report
- Appendix B: Client Onboarding Process
- Appendix C: Data Collection and Ingestion Process
- Appendix D: Asset List and Risk Register

Threat Modeling

- Appendix E: Threat Modeling Report
- Appendix F: Threat Model

Network & Data Security

- Appendix G: Network Architecture Diagram
- Appendix B: Network & Data Security Report

Third-Party Risk Assessment

- Appendix H: Third-Party Risk Assessment Report

Incident Response Plan

- Appendix I: Incident Response Plan

Business Continuity Plan

- Appendix J: Business Continuity Plan