Secure Software Development (CMP020X306) Generated Case Study

Company name

OptiVision

Company profile

OptiVision is a technology-driven optician that offers cutting-edge eyewear solutions using software and network connectivity to revolutionize the way people see the world.

Product

OptiVue

Users

OptiVue Users OptiVue is designed for individuals seeking personalized eyewear solutions, including patients at OptiVision's physical stores and online customers.

Benefits of OptiVue:

- **Personalized Recommendations**: Based on a user's prescription, facial structure, and lifestyle, OptiVue provides tailored suggestions for frames and lenses.
- **Virtual Try-On**: Users can virtually try on different frames and see how they look without physically visiting the store.
- **Easy Prescription Management**: Customers can easily upload their prescriptions and track order status through the platform.

Benefits to OptiVision:

- **Enhanced Customer Experience**: By providing a user-friendly interface, OptiVision can offer a seamless shopping experience, increasing customer satisfaction.
- **Increased Sales**: With personalized recommendations, customers are more likely to purchase products that meet their specific needs, leading to increased sales.
- **Competitive Advantage**: OptiVue sets OptiVision apart from competitors by leveraging technology to enhance the overall shopping experience.

System architecture

System Architecture The OptiVue system consists of multiple components, each responsible for a specific function:

- **Frontend**: The user interface is built using web technologies (HTML5, CSS3, JavaScript) and a UI framework (React.js). Users interact with the platform through this layer.
- **Backend**: The server-side logic is implemented using Node.js with Express.js as the web application framework. This layer handles requests from the frontend, interacts with databases, and exposes APIs for third-party services.
- **Database**: A relational database management system (RDBMS) such as MySQL or PostgreSQL stores user data, prescription information, frame and lens details, and order history.
- **API Gateway**: An API gateway (e.g., NGINX or Amazon API Gateway) sits between the frontend and backend to manage incoming requests, authenticate users, and route traffic accordingly.
- **Cloud Services**: OptiVue leverages cloud services for scalability and reliability:
  - **Storage**: Object storage solutions like AWS S3 or Google Cloud Storage are used for storing user-uploaded files (e.g., prescriptions).
  - **Message Queue**: A message broker like RabbitMQ or Amazon SQS handles asynchronous tasks, such as sending notifications to users.
- **Network Connectivity**:
  - OptiVue uses a secure communication protocol (HTTPS) to encrypt data in transit between the frontend and backend.
  - The API gateway ensures that only authorized requests are processed by the backend.

This architecture enables OptiVue to provide a user-friendly interface, scalable performance, and robust security features. By leveraging cloud services and a microservices-based approach, OptiVision can adapt to changing demands and expand its offerings in the future.

Data

Data Stored by OptiVue OptiVue stores various types of data to provide personalized eyewear solutions:

- **User Information**: Customer data includes:
  - Personal details (name, email, phone number)
  - Prescription information (prescription numbers, lens requirements)
  - Frame and lens preferences
- **Order History**: Records of customer orders, including:
  - Order date and status
  - Product details (frame and lens selection)
  - Shipping and billing information

- **Product Catalogue**: Information about available frames and lenses, including:
  - Frame styles, colors, and sizes
  - Lens types, coatings, and prescriptions
  - Pricing and inventory levels
- **Staff Data**: Employee information includes:
  - Names and contact details (email, phone number)
  - Job roles and responsibilities

Note that OptiVue ensures the secure storage of personal data by adhering to industry standards for data protection, such as GDPR and HIPAA. The platform implements robust security measures to safeguard user and staff information.

Cyber risk appetite

OptiVision has a **low** cyber risk appetite. The CEO and CISO aim to minimize potential losses due to cyber incidents, prioritizing the safety of customer data and maintaining a secure environment. This approach reflects the organization's commitment to protecting sensitive information and preventing financial and reputational damage.

The low risk appetite is reflected in their willingness to invest in robust security measures and adhere to industry standards for data protection, such as GDPR and HIPAA. By taking a proactive stance on cyber security, OptiVision demonstrates its dedication to safeguarding customer trust and loyalty.

Employee awareness of cyber security

OptiVision's employees have **excellent** awareness of cyber security. This is due to:

- The organization's strong emphasis on employee education and training programs
- Regular workshops and online resources provided to enhance employees' knowledge about cyber threats, best practices, and data protection guidelines
- Leadership's commitment to promoting a culture of cyber security awareness throughout the company

As a result, OptiVision's employees are well-equipped to identify potential risks, report suspicious activities, and follow established protocols for handling sensitive information. This collective expertise contributes significantly to the organization's robust cyber security posture and minimizes the likelihood of cyber incidents.