E-Commerce Cloud Infrastructure

Group 8 (Andy, Syahir, Zaki, Zell)

BACKGROUND

- Medium-sized apparel enterprise based in Singapore, which aims to transition from on-premise to cloud-based infrastructure due to its scalability and suitability.

- Meet current demand and facilitate regional expansion. Struggles with managing high traffic during peak periods.

- Has faced security breaches, including credit card fraud and identity theft.

PROBLEMS ENCOUNTERED

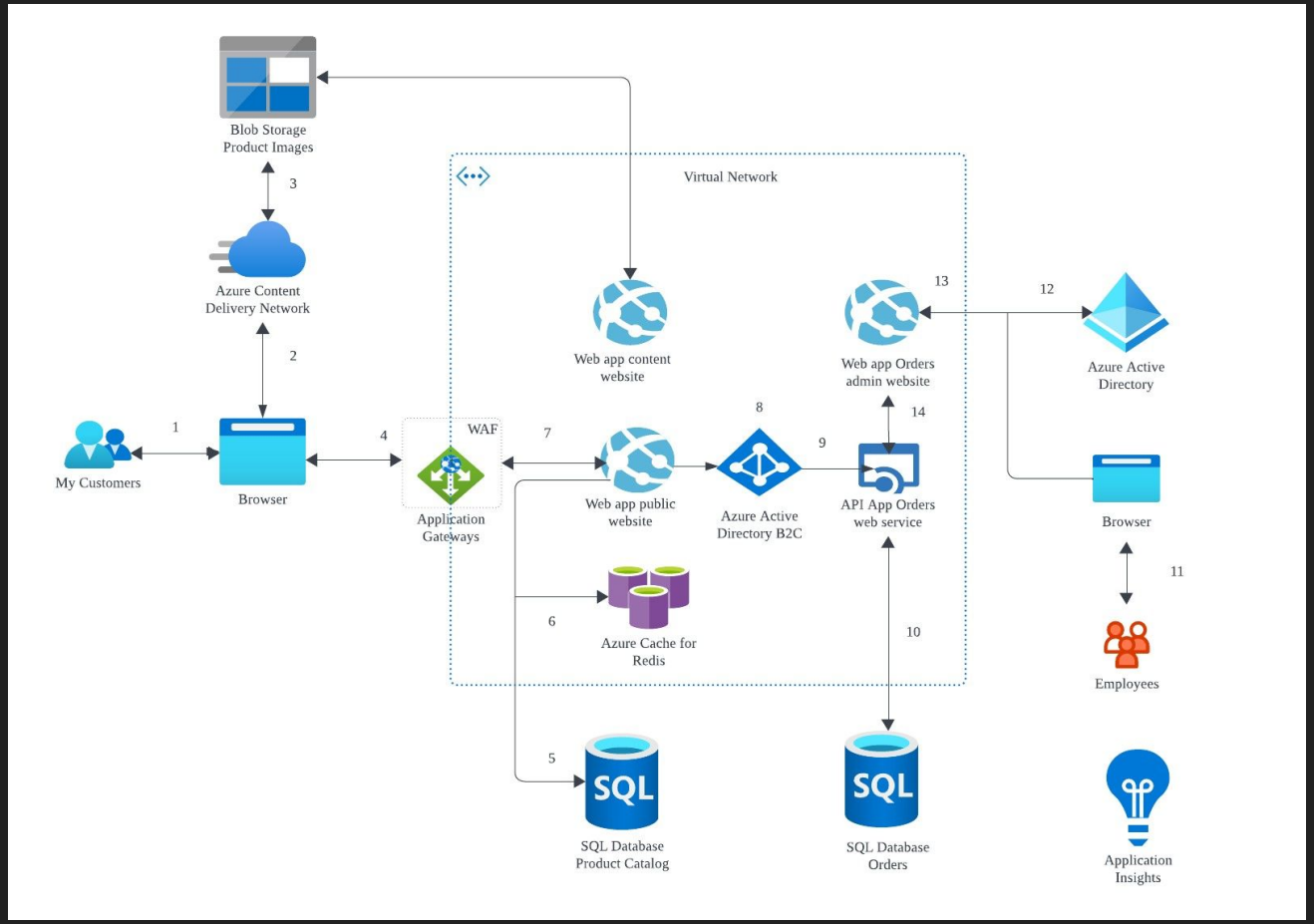
- Web Traffic Overload: Coping with abrupt surges in web traffic became overwhelming, leading to website crashes and decreased performance.

- Compromised Security: The existence of security vulnerabilities resulted in instances of personal data breaches, undermining customer confidence and trust.

- Financial Strain: The substantial expenses tied to establishing and managing on-premise infrastructure imposed a significant financial burden.

- Feature Constraints: Shortcomings encompassed the absence of advanced functionalities like real-time analytics, automated marketing, and efficient customer support.

PROJECT ARCHITECTURE OVERVIEW



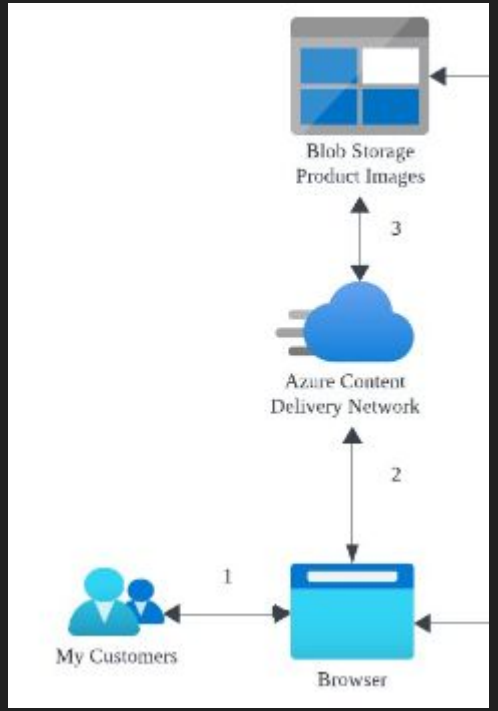
WHY WE CHOSE THESE SERVICES

Azure Content Delivery Network

- Cache product images from blob storage to POP locations closer to customer to improve performance and help reduce latency

Azure Blob Storage

- Set up a single blob storage account which will be used to store the product images for the e-commerce business
- Offers security features such as encryption and access control



WHY WE CHOSE THESE SERVICES

Azure Application Gateway

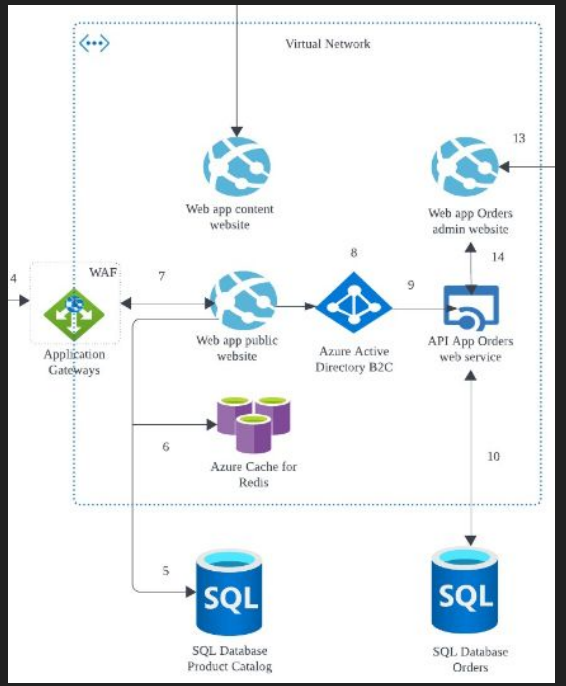
- A load balancer that will manage the traffic to the web applications
- Built-in WAF that helps to protect the web app from common attacks such as SQL injection and cross-site scripting (XSS)

Azure App Service

- Virtual Network: A isolated environment where each resources can securely communicate with each other while prevent data leakage, unauthorised access and network attacks
- Public website: Enables interactive browsing of products and making payment
- Content website: Manage and presenting of product content that the public will be able see
- Admin website: A back-end system to handle payment, tracking of orders, customer service and administration

API App (Orders web service)

- Managing, processing and tracking of orders
- Integrate with third-party services such as payment gateways and shipping providers



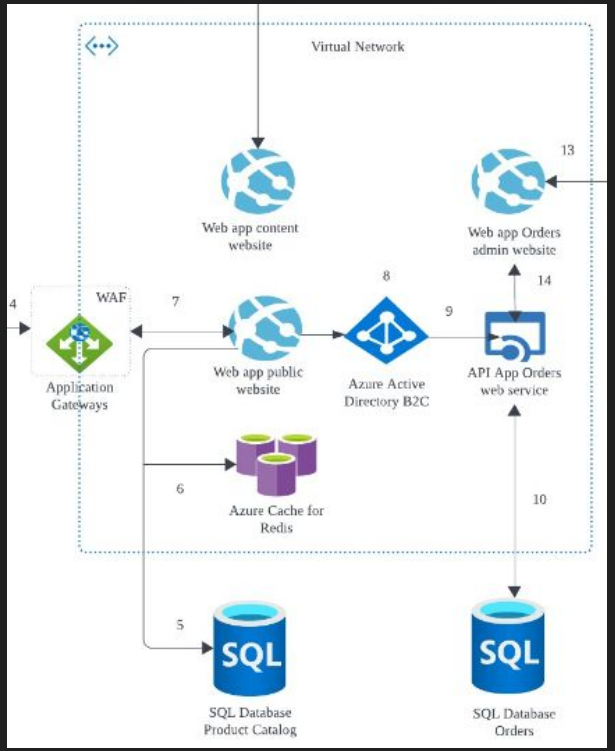
WHY WE CHOSE THESE SERVICES

Azure Cache for Redis

- Cache web output allowing users to access and load the web page faster
- Reducing workload on the backend databases or services

Azure SQL Database

- Product Catalogue database:
  Store product information such as the description, pricing and the stock status
- Orders database:
  Store information such as customers address and credit card information



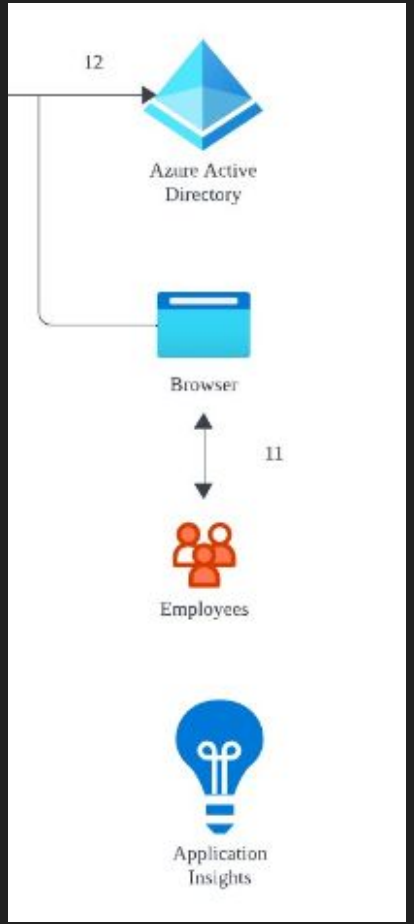
WHY WE CHOSE THESE SERVICES

Azure Active Directory

- Enhance security using multi-factor authentication

Azure Application Insights

- Monitor and improve using collected data and provide insights on how the application is performing
- Diagnose and troubleshoot issues to prevent performance degradation



Azure Active Directory B2C

- Stores all users' credentials, profile data, password and application registrations
- Control sign-in , Sign-up options, set permission rights and set conditional access if necessary

- AD B2C Key feature - Customers use either local account or their preferred social, enterprise identities to get single sign-on access to the Web App and APIs.
- Federate with identity providers that support OAuth 1.0, OAuth 2.0, OpenID Connect, and SAML (Security Assertion Markup Language) protocols
- Azure AD B2C defines several types of user accounts. Both Azure Active Directory and Azure Active Directory B2C share these account types.

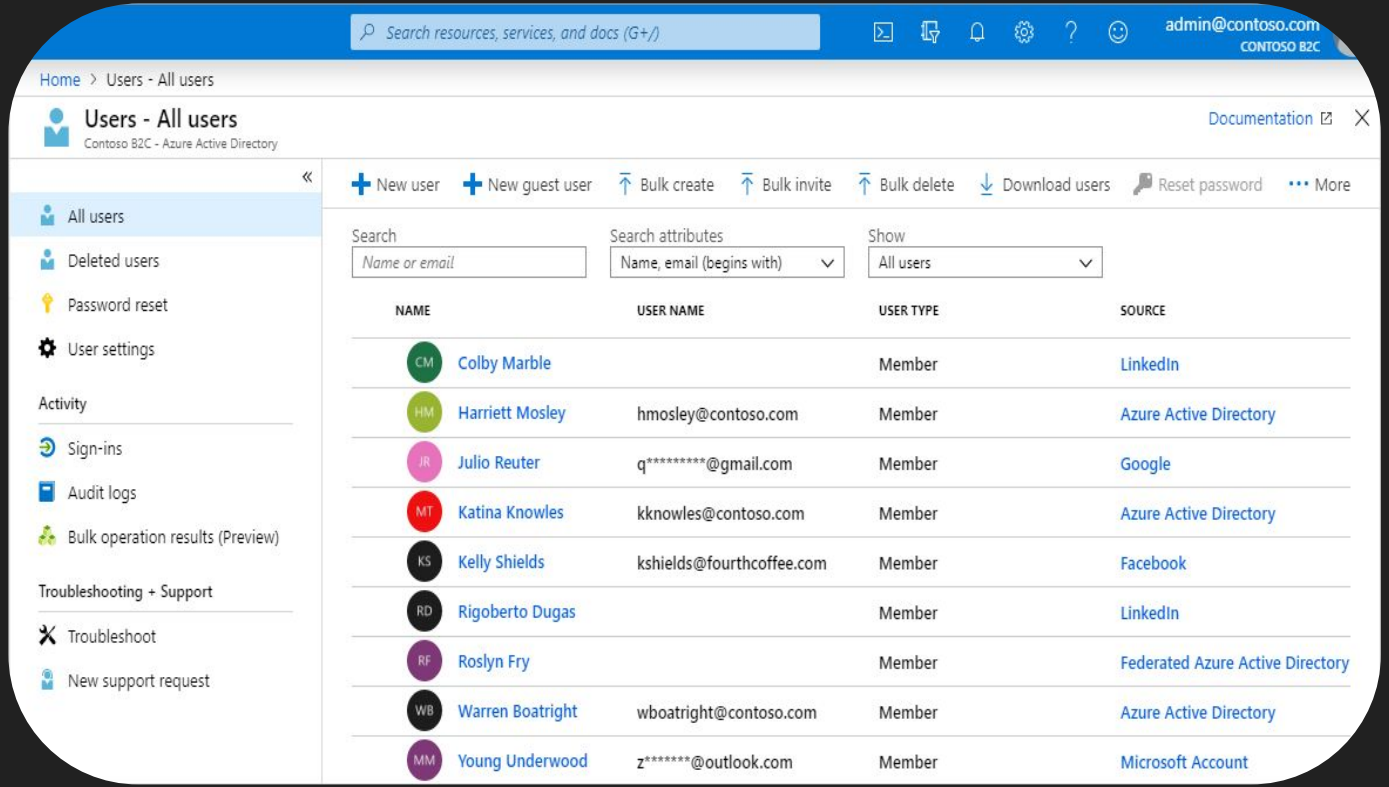
Tenant (Client's Organisation)

Work accounts

Guest accounts

Consumer accounts

Back End



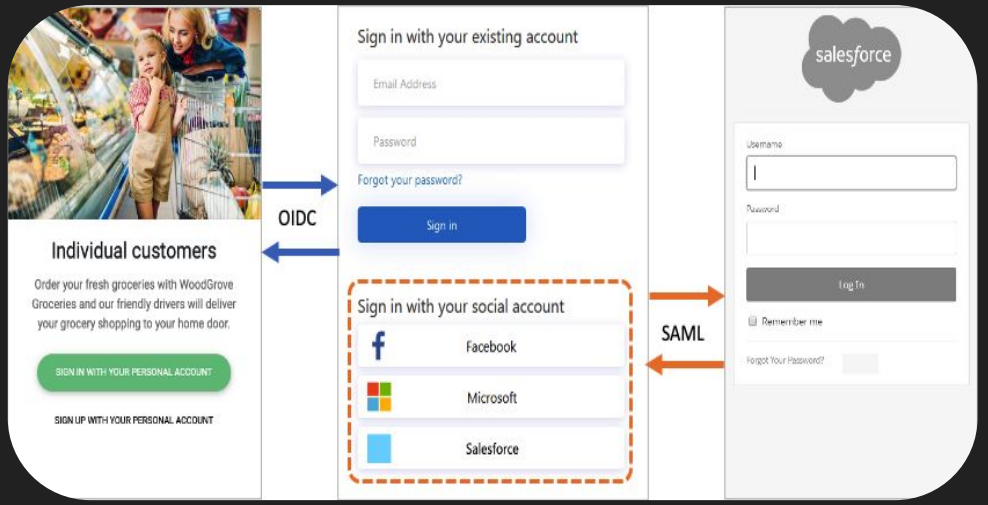
<u>Users with Work accounts</u>

-Have administrator role, and manage resources in a tenant

-Can create new consumer accounts, reset passwords, block/unblock accounts

-Set permissions or assign an account to a security group.

SECURITY FEATURES



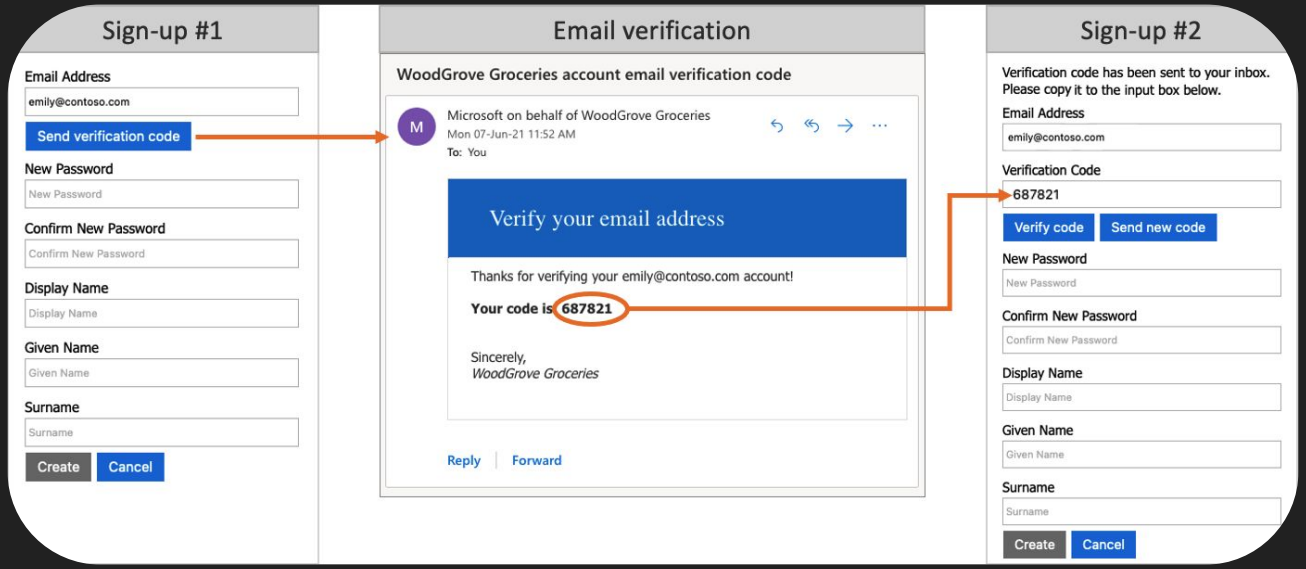
- Azure AD B2C provides various ways in which you can authenticate a user
- Allow users to sign in to the web application with local account or using credentials from social and enterprise identity providers

---

Employee Account

- Logged in using Azure AD registered username & password
- Additional Multi-factor authentication (MFA)

Sign up option - Email & OTP Verification



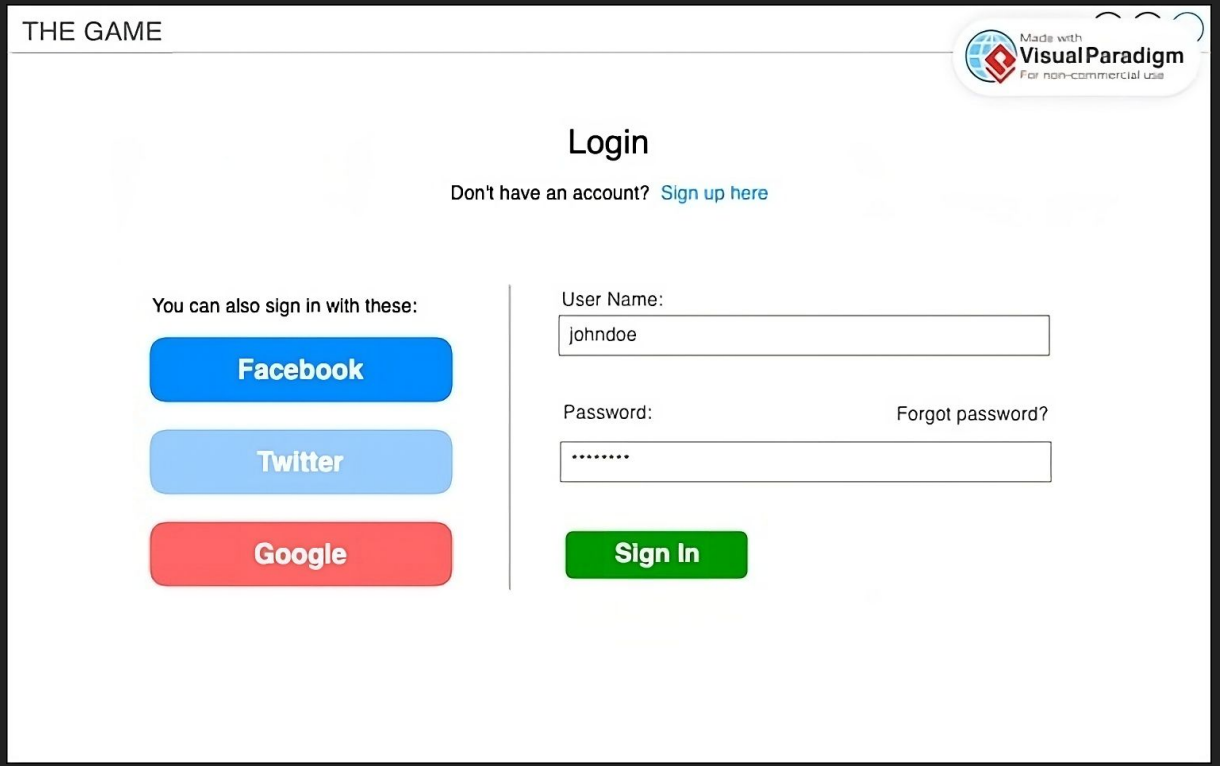
Azure AD B2C ensures valid email addresses by requiring customers to verify them during the sign-up, and password reset.

Prevents malicious actors from using automated processes to generate fraudulent accounts in the applications.

PROOF OF CONCEPT

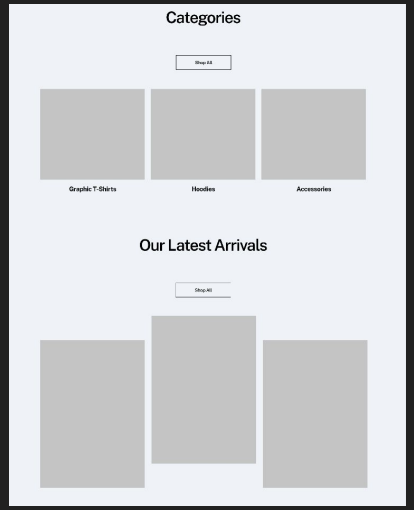
- Login Page
  - Customers: Azure AD B2C
  - Employees: Azure AD with MFA enabled
- Web App
  - Public/Content Website
  - Admin Website
- Database
  - Integrated with Web App

LOGIN PAGE FOR CUSTOMERS

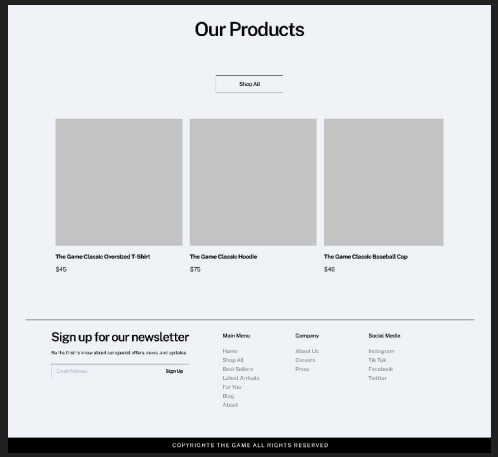


WEB APP - HOME PAGE

Header

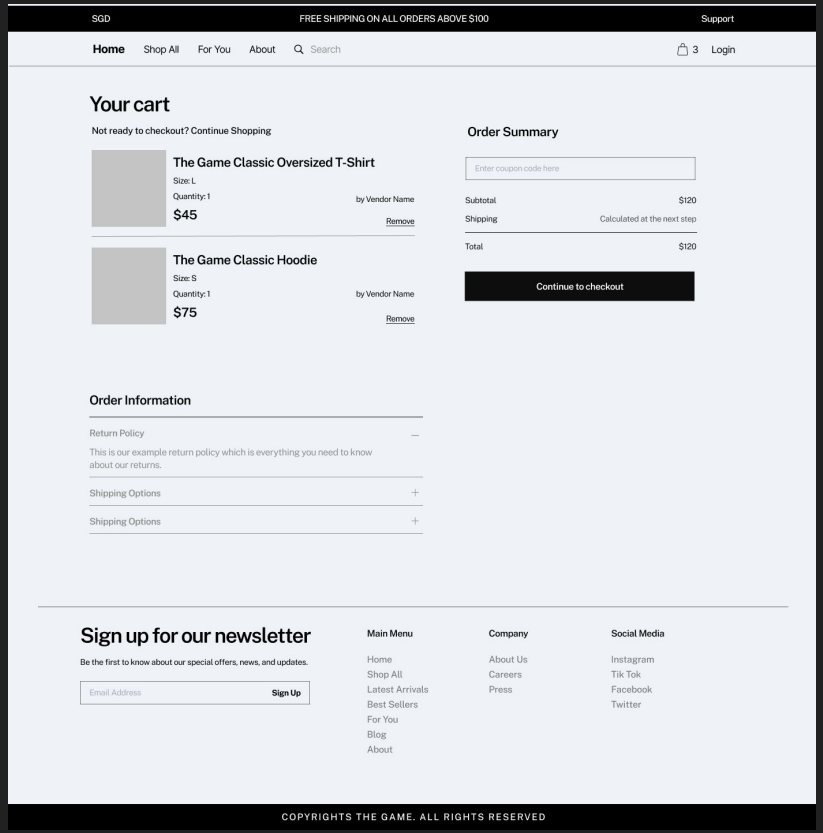


Body

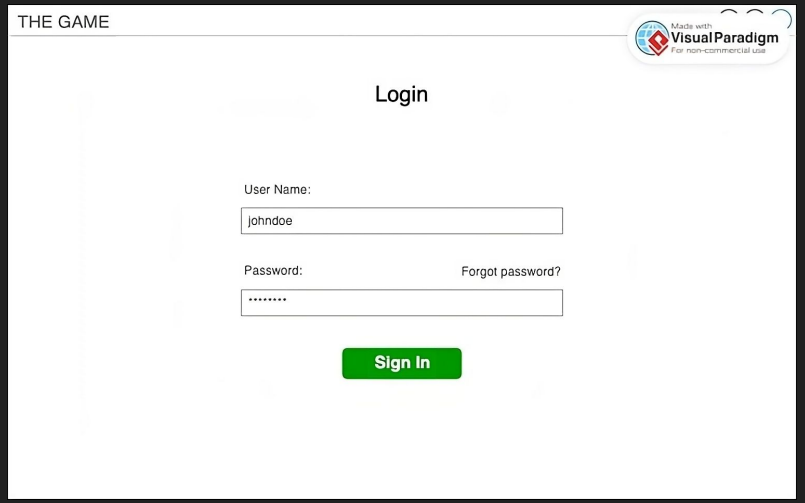


Footer

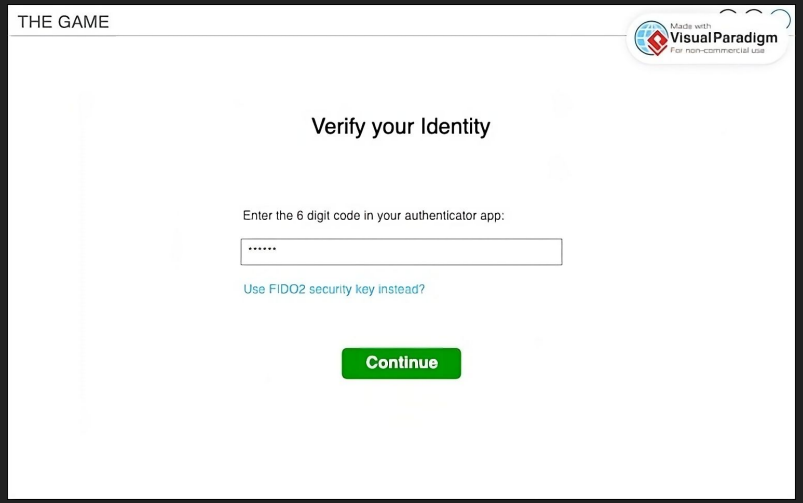
WEB APP - CART PAGE



LOGIN PAGE FOR EMPLOYEES

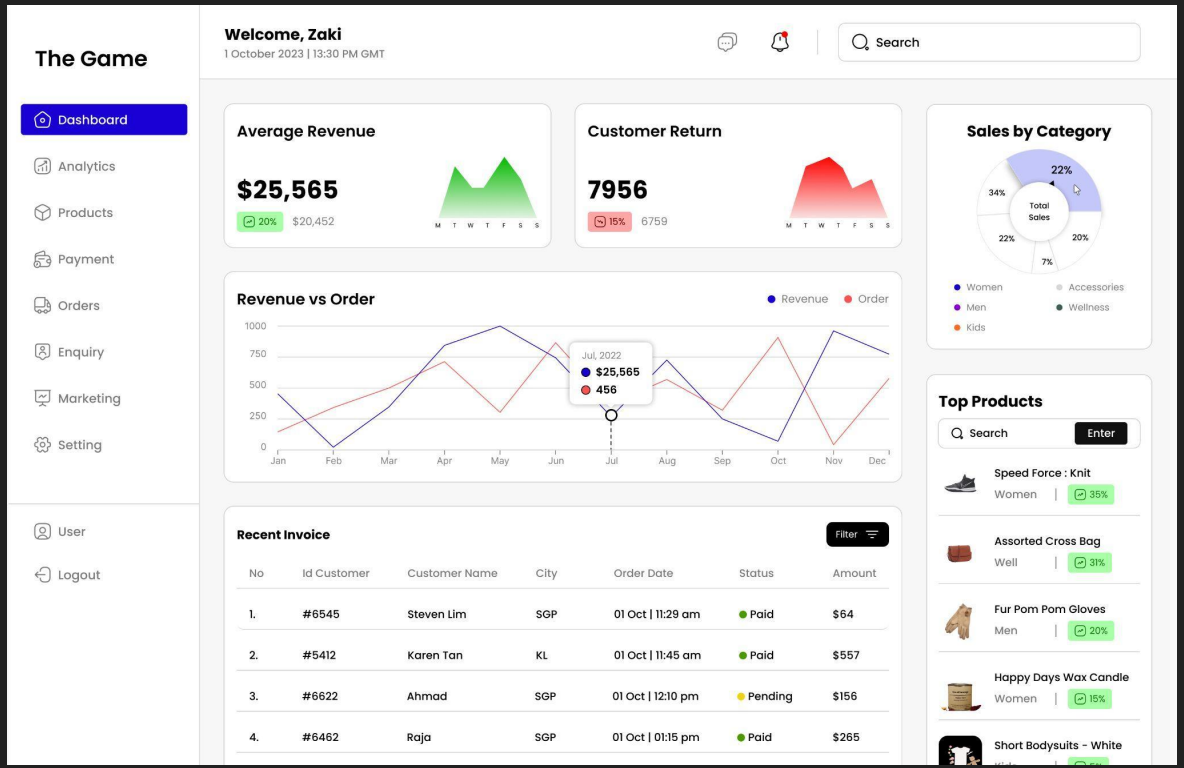


Log in using Azure AD account



Complete the MFA process

WEB APP - ORDERS ADMIN WEBSITE



Dashboard

THANK YOU

Q&A