SecurePro

Owner: G03
Reviewer: Dr Mamoona Humayun & Dr Touseef Tahir
Contributors:
Date Generated: Thu Oct 31 2024

Executive Summary

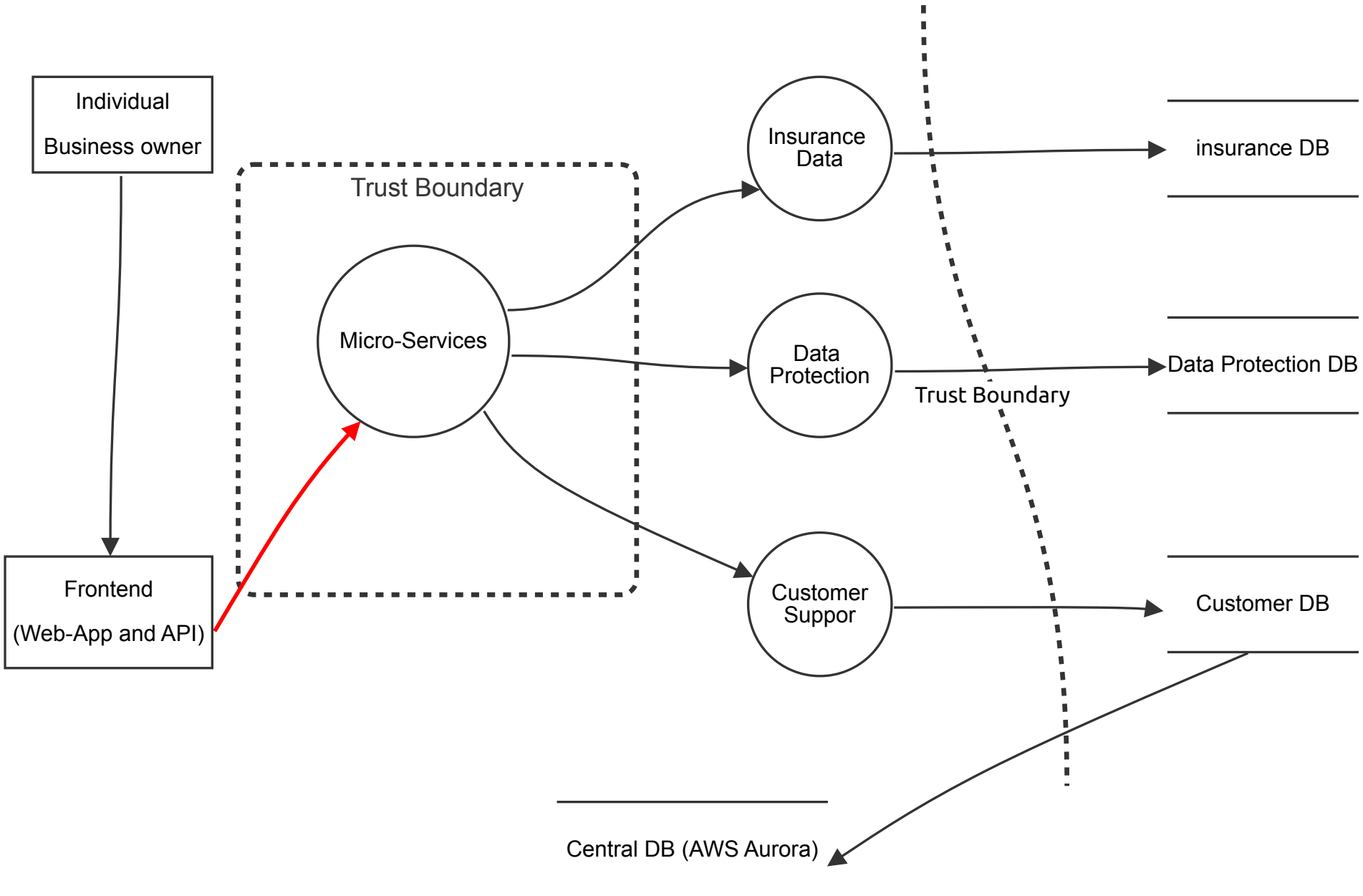
High level system description

SecurePro is a global leader in insurance services, providing comprehensive and secure solutions to individuals and businesses worldwide. With a strong focus on innovation and technology, we develop cutting-edge software and network connectivity systems to ensure seamless and trustworthy interactions with our clients.

Summary

Total Threats	34
Total Mitigated	33
Not Mitigated	1
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	1
Open / Unknown Priority	0

SecurePro


Individual
Business owner
Frontend
(Web-App and API)
Trust Boundary
Micro-Services
Insurance
Data
Data
Protection
Customer
Suppor
Trust Boundary
insurance DB
Data Protection DB
Customer DB
Central DB (AWS Aurora)

SecurePro

Individual

Business owner (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

insurance DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
31	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Unauthorized access to customer and policy data.	Use data encryption at rest and in transit to protect against disclosure.
32	New STRIDE threat	Tampering	Medium	Mitigated	7	Alterations of sensitive data, impacting data integrity.	Apply access controls and logging for any data modification actions.
33	New STRIDE threat	Denial of service	Medium	Mitigated	6	An attack could overwhelm the database.	Implement rate limiting and database-level firewalls to mitigate DoS attacks.

Data Protection DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
28	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Unauthorized access to customer and policy data.	Use data encryption at rest and in transit to protect against disclosure.
29	New STRIDE threat	Tampering	Medium	Mitigated	6	Alterations of sensitive data, impacting data integrity.	Apply access controls and logging for any data modification actions.
30	New STRIDE threat	Denial of service	Medium	Mitigated	6	An attack could overwhelm the database.	Implement rate limiting and database-level firewalls to mitigate DoS attacks.

Customer DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
25	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Unauthorized access to customer and policy data.	Use data encryption at rest and in transit to protect against disclosure.
26	New STRIDE threat	Tampering	Medium	Mitigated	5	Alterations of sensitive data, impacting data integrity.	Apply access controls and logging for any data modification actions.
27	New STRIDE threat	Denial of service	Medium	Mitigated	6	An attack could overwhelm the database.	Implement rate limiting and database-level firewalls to mitigate DoS attacks.

Central DB (AWS Aurora) (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
22	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Unauthorized access to customer and policy data.	Use data encryption at rest and in transit to protect against disclosure.
23	New STRIDE threat	Tampering	Medium	Mitigated	6	Alterations of sensitive data, impacting data integrity.	Apply access controls and logging for any data modification actions.
24	New STRIDE threat	Denial of service	High	Mitigated	8	An attack could overwhelm the database.	Implement rate limiting and database-level firewalls to mitigate DoS attacks.

Micro-Services (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
19	New STRIDE threat	Elevation of privilege	Medium	Mitigated	6	A compromised service gaining unauthorized access.	Limit role-based access control (RBAC) to prevent privilege elevation.
20	New STRIDE threat	Tampering	Medium	Mitigated	6	Malicious manipulation of data or services.	Implement service authentication within microservices and restrict network access with container security policies.
21	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Sensitive service data might be exposed.	Encrypt internal communications using mutual TLS.

Insurance Data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
39	New STRIDE threat	Tampering	Medium	Mitigated	6	Malicious manipulation of data or services.	Implement service authentication within micro-services and restrict network access with container security policies.
40	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Sensitive service data might be exposed	Encrypt internal communications using mutual TLS.

Data Protection (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
36	New STRIDE threat	Tampering	Medium	Mitigated	5	Malicious manipulation of data or services.	Implement service authentication within micro-services and restrict network access with container security policies.
38	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Sensitive service data might be exposed.	Encrypt internal communications using mutual TLS.

Customer Suppor (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	New STRIDE threat	Tampering	Medium	Mitigated	7	Malicious manipulation of data or services.	Implement service authentication within micro-services and restrict network access with container security policies.
35	New STRIDE threat	Information disclosure	Medium	Mitigated	6	Sensitive service data might be exposed.	Encrypt internal communications using mutual TLS.

Frontend

(Web-App and API) (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	New STRIDE threat	Spoofing	Medium	Mitigated	6	Attackers could impersonate legitimate users and access sensitive information.	Enforce multi-factor authentication (MFA) to prevent spoofing.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Spoofing	Tampering	Medium	Mitigated	6	Attackers might impersonate legitimate users to gain unauthorised access to customer or financial data.	Implement strong multi-factor authentication and session management to prevent unauthorised access.
4	Data Transmission	Information disclosure	Medium	Mitigated	7	Data transmitted between users and the frontend may be altered by attackers if not properly secured.	Apply strict access control en encrypt sensitive customer data in transit and at rest, ensuring that only authorised users have access.
9	DoS Attack	Denial of service	Low	Open	4	Temporary disruptions due to minor DoS attacks might occur without significantly impacting operations, especially if targeting non-critical components (e.g. seldom-used dashboard feature).	Periodically monitor performance metrics and re-evaluate the criticality of components if usage changes.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Unauthorised access to Personal information	Information disclosure	Medium	Mitigated	7	Weak access controls can result in unauthorised users accessing customer personal details, such as contact information or payment records.	Implement strong authentication methods, enable access logging, and conduct periodic access reviews.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Phishing Attacks on Customers accounts	Information disclosure	Medium	Mitigated	7	Attackers use phishing emails to trick customers into providing their login details, potentially compromising their accounts.	Educate customers on phishing prevention, implement email filtering, and monitor for unusual login behaviour with risk-based authentication.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Data Breach due to Misconfigured Access Controls	Information disclosure	Medium	Mitigated	7	Misconfigured access permissions could allow unauthorised individuals to view sensitive data.	Regularly audits permissions, implement least privilege access, and use identity and access management systems.
15	Insufficient Data Anonymisation	Information disclosure	Medium	Mitigated	5	Data that lacks anonymisation increases the risk of exposure of sensitive information if breached.	Apply data anonymisation techniques where possible and enforce strict access control on original data.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Unauthorised Access to Policy Data	Information disclosure	Medium	Mitigated	6	Unauthorised access to sensitive insurance policy details could result in data leaks or unauthorised alterations.	Use RBAC to limit access to policy data, conduct regular audits, and enable logging for all data access activities.
13	Tampering with Claim Data	Tampering	Medium	Mitigated	6	Attackers could alter claims data, leading to fraudulent claims processing or unauthorised claims approvals.	Implement input validation, data integrity checks, and maintain an audit trail for all changes to claims data.

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Unauthorised Database Modifications	Tampering	High	Mitigated	8	Attackers may attempt to modify database records without authorisation, altering stored data integrity.	Enforce database auditing and implement encrypted connections for all database operations, with regular integrity checks.
7	Sensitive Data Exposure	Information disclosure	Medium	Mitigated	7	Data could be disclosed due to weak access control policies, allowing unauthorised visibility.	Encrypt data at rest and limit data visibility to authorised users through access control.
8	Database Downtime through high query volume	Denial of service	Medium	Mitigated	5	Attackers could overload the database with intensive queries, causing service degradation or downtime.	Implement query limits, utilise read replicas for load distribution, and monitor for unusual database activity patterns.