IDENTITY & ACCESS TRACK

Persistent Security

THIERRY MAISON, GET GROUP NA

IDENTITY & PAYMENTS
SUMMIT

The Tenets of Security

Confidentiality

Maintain privacy and safeguard sensitive information. Only authorized individuals may access the information.

Integrity

Prevent unauthorized modifications, deletions, or additions to the data.

Availability

Ensure accessibility to its authorized users at all times.

Procedural

Data Management lifecycle

Important principles may, and must, be inflexible. Abraham Lincoln

IDENTITY & PAYMENTS
SUMMIT

The amount of data to protect is vast.

Personally Identifiable Information (PII)

- Real name
- Alias
- Postal address
- Unique personal identifier

Online identifiers

- Internet Protocol address
- Email address
- Account name
- Social Security number
- Driver’s license number
- Passport number
- Other similar identifiers

Commercial Information

- Records of personal property
- Non-fungible tokens (NFTs)
- Monetary Transactions Information
- Products or services purchased, obtained, or considered
- Other purchasing or consuming histories or tendencies

Biometric information

Legal Hold Data

Digital Assets (i.e. digital images)

Internet/Electronic Network Activity — including, but not limited to:

- Browsing history
- Search History
- Information regarding a consumer’s interaction with an Internet Web site, application, or advertisement

IDENTITY & PAYMENTS SUMMIT

Security Compliance Regulations

- USA: NIST frameworks for Cybersecurity (CSF) and Privacy (PF)
- USA: The Health Insurance Portability and Accountability Act (HIPAA)
- USA: BCBS 239 is the Basel Committee on Banking Supervision’s standard number 239 (BCBS 239).
- USA: PCI Security Standards Council (PCI SSC)
- USA: Department of Defense Cybersecurity Maturity Model Certification (DoD CMMC)
- USA: Sarbanes-Oxley Act (SOX)
- USA: California Consumer Privacy Act (CCPA)
- Europe: General Data Protection Regulations (GDPR)
- ISO: 27001, 27002
- Canada: Personal Information Protection & Electronic Documents Act (PIPEDA)

The Mechanisms of Cybersecurity

- Login /password, 2FA, SSO, Biometrics
- Anti-Viruses, Anti-Malware, Anti-Spyware
- Identity and Access Management (IAM) – Least Privilege, Separation of Privileges
- Cryptography, Data Encryption, Digital Signatures
- Transport Encryption (SSL/TLS)
- Firewalls, Whitelisting, Packet filtering, Stateful Inspection
- Layering, Application Proxies, Failsafe Defaults
- Digital Notarization
- Upcoming Artificial Intelligence (AI) discovery and counter-attack (A better SIEM)

- As a resource: Cybersecurity Infrastructure Security Agency (cisa.gov)

The Threats to Security

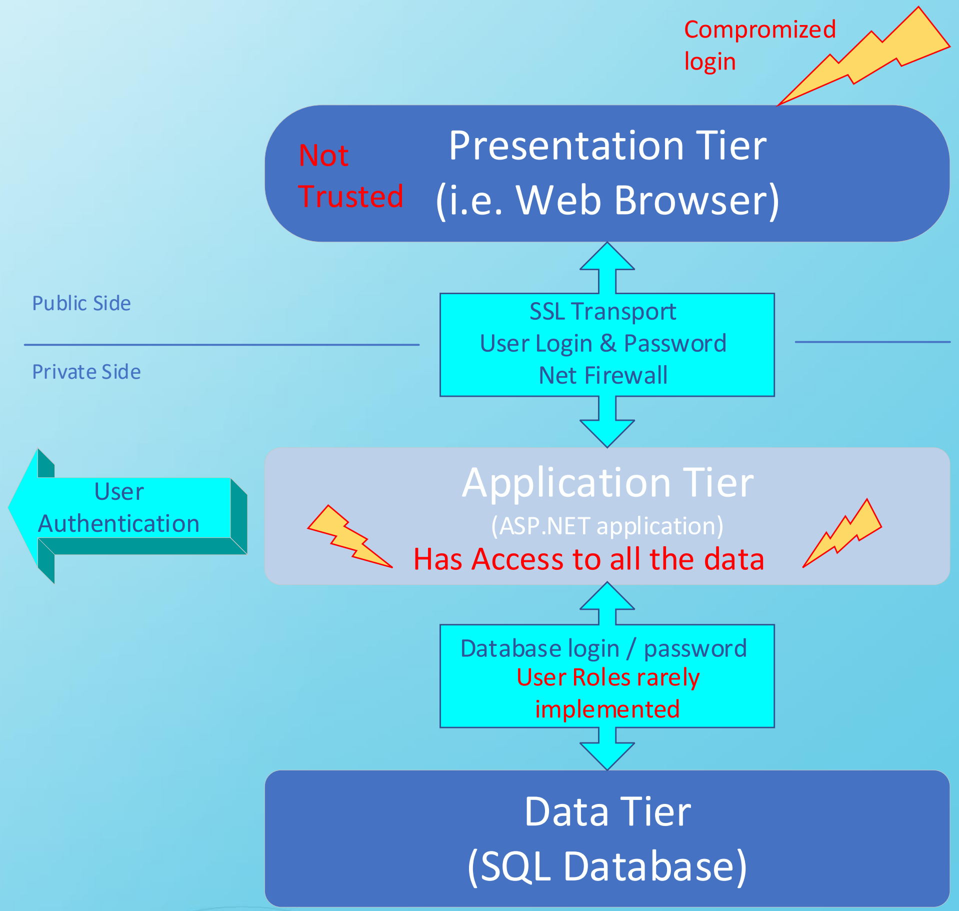
- Malware and Ransomware attacks
- Social engineering attacks
- Careless Users
- Software supply chain attacks
- Misconfigured and Unpatched Systems
- Man-in-the-middle attacks
- Distributed denial of service (DDoS)
- Internal bad actors
- Stale information

Well-known Data Architectures

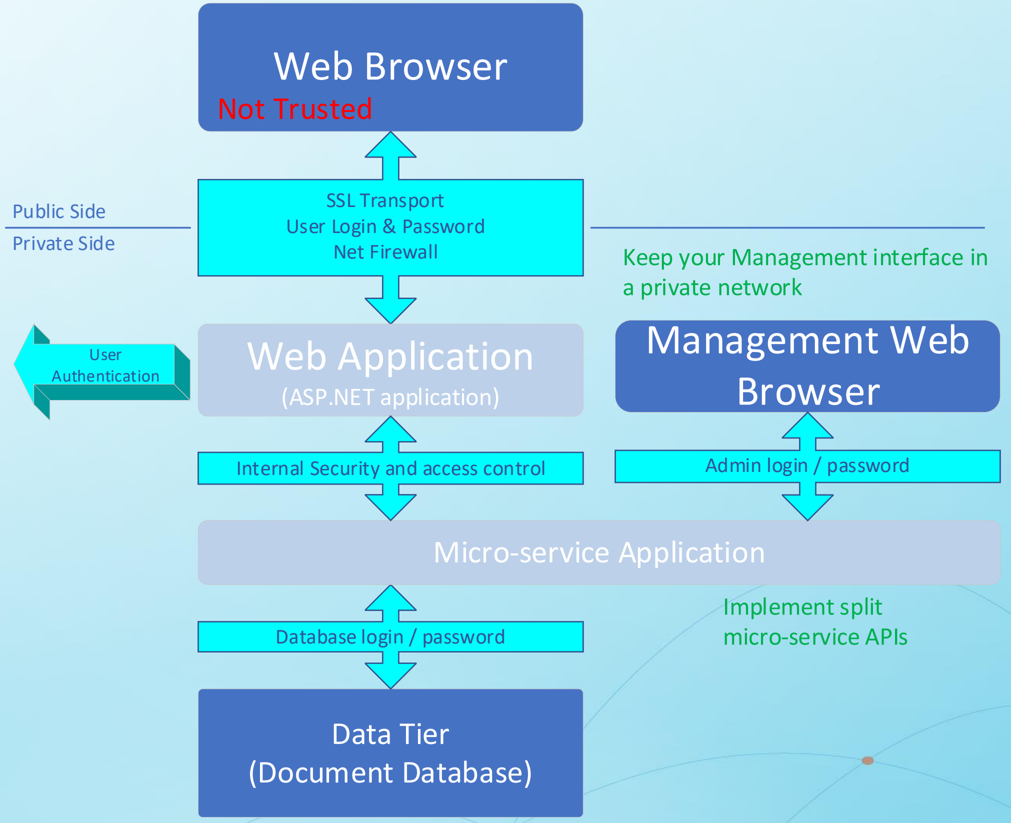
- Traditional 3-Tier
- Pipeline Process-based Systems (Queue-based)
- Service-Oriented Architectures (SOA)
- Micros-Services

3-Tier Architecture

- Because data is distributed in multiple SQL tables, it is very difficult to implement a role-based data store.
- An administrator compromised login/password can yield to the entire data store breach.
- SSL/TLS does not help it's insure confidentiality of the breacher.



Layer Architecture

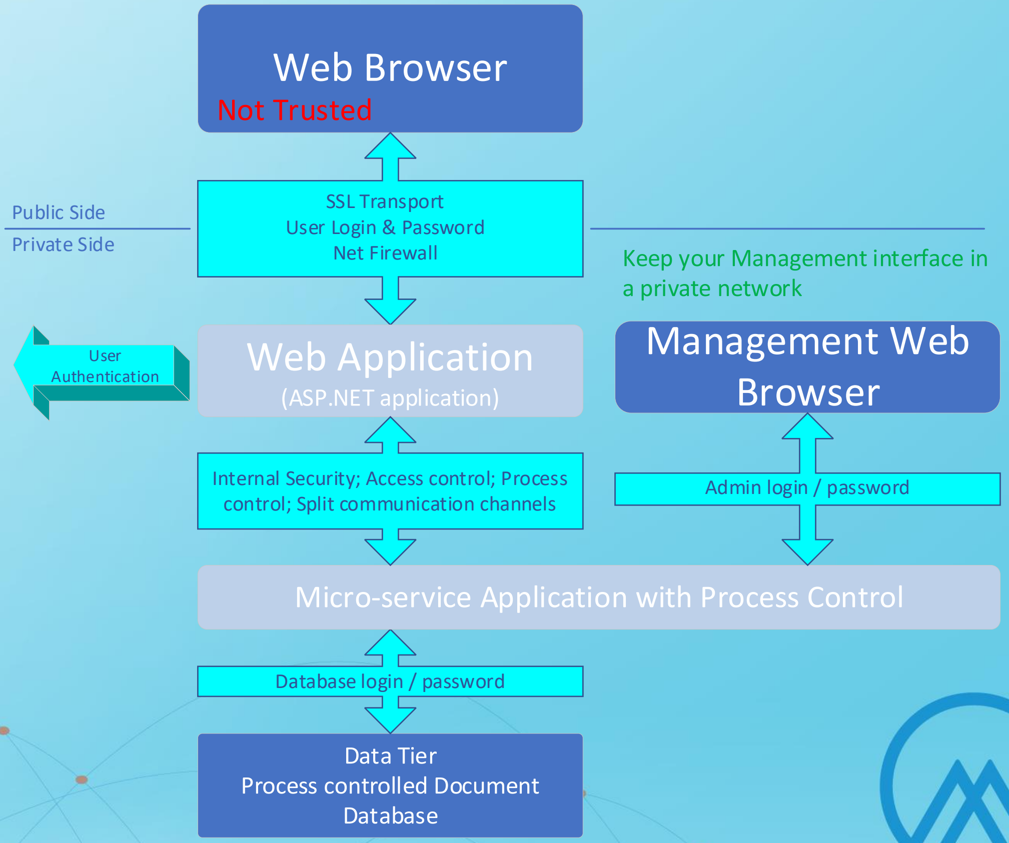


- Implement micro-service with different APIs for management and consumer users.
- Never expose management interfaces to the public network.
- Never expose the administrative credentials with the user credential mechanism.
- White-list the database to only the micro-service application.

Q

When Process Participates with Security

- Package user data for process-driven access control.
- Split the request from the data delivery under process control.
- Use a document database that minimizes exposing the entire dataset.
- Use internal private certificates for all internal data transport.
- Add message internal server authentication mechanism.
- Add server-to-server connection whitelisting.


Web Browser
Not Trusted
Public Side
Private Side
SSL Transport
User Login & Password
Net Firewall
Keep your Management interface in a private network
User Authentication
Web Application
(ASP.NET application)
Management Web Browser
Internal Security; Access control; Process control; Split communication channels
Admin login / password
Micro-service Application with Process Control
Database login / password
Data Tier
Process controlled Document Database

Core ID

The CoreID Applied Security

What is CoreID ?

- A highly secure platform for the creation of Secure Credential Document Issuance (ID/DL/CDL/mDL, Passports, Secure Access Documents, etc.)
- Flexible to adapt to government or corporate workflow requirements.
- Adaptable to various operational and hosting environments.
- Compliant with many biometric identification requirements.
- Applicable to government credentialing requirements.
- Applicable to stringent corporate requirements.

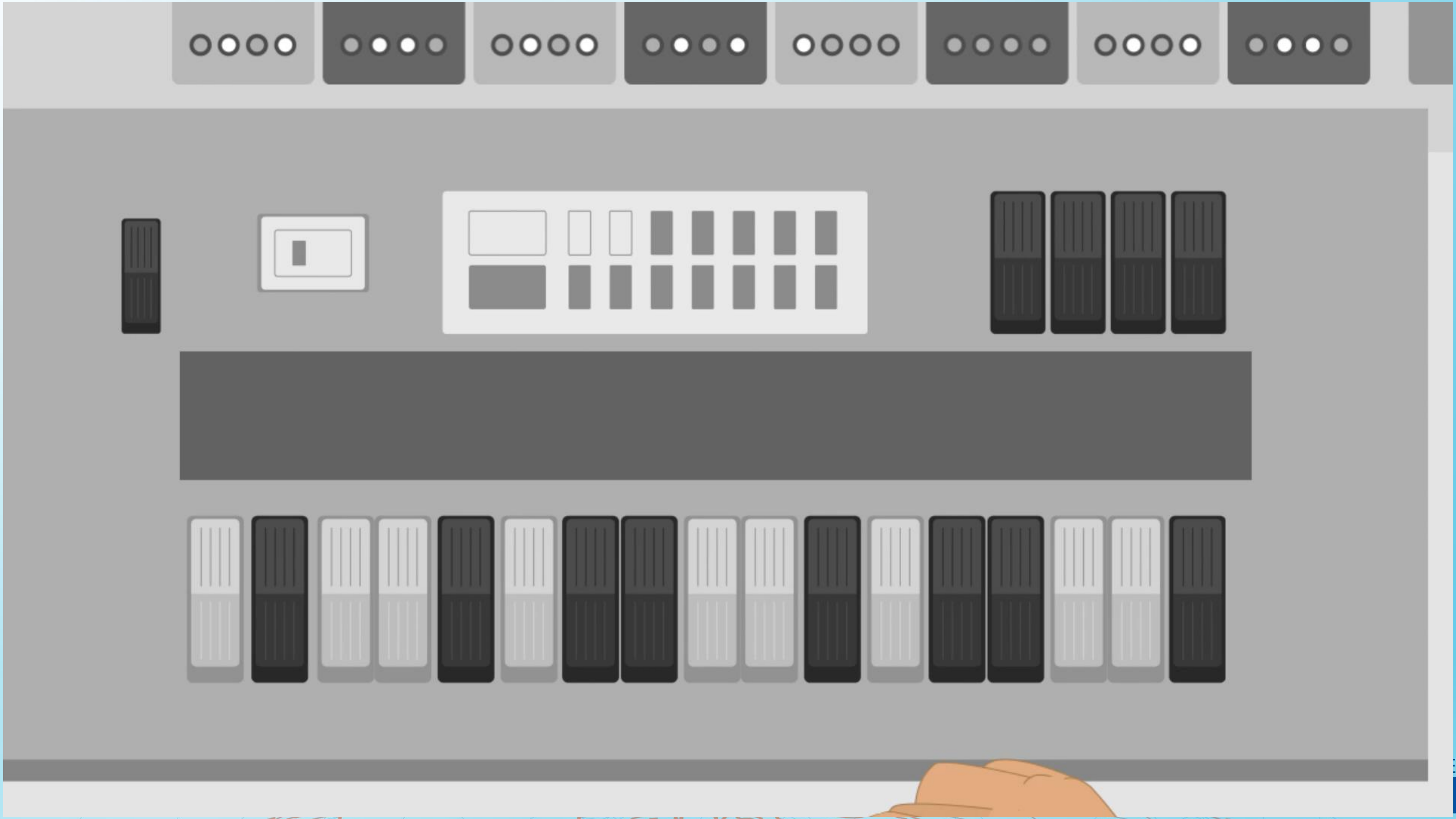
Let's Get Practical

- This is based on an existing framework created for GET Group NA called CoreID.
- We use Microsoft ASP.NET (Core 8) to develop our web applications.
- We encapsulated all the information pertinent to a user in a json/bson document stored in a MongoDB database
- You can use MongoDB community, MongoDB Atlas (in the cloud or on-premises) in Azure or AWS, Percona for MongoDB, or Azure CosmosDB.
- We queue messages using RabbitMQ (with queue persistence to aid recovery). You can use another queue server like IBM MQ or CloudAMQP.
- Our applications are deployed in High Availability (HA) and Disaster Recovery (DR) configurations.
- We package our applications for various hosting's to fit the security requirements of our customers (Windows, Linux, Docker, VM, etc.).
- We specially adapted the solution to existing business workflows by strategically using message queueing.

IDENTITY & PAYMENTS SUMMIT

Some Tenets of our Architectures

- Don’t let the data store touch any of the public-facing applications - PERIOD
- Use only one document (we call it the “Dossier”) per requested processing (we archive forever)
- Embed traceability (Audit Log) in the Dossier. Use revision information for each step of the dossier transaction.
- If our platform connects to external processing, we use “facades.”
- We use an internal standard for all our message queueing.
- We use internal Restful APIs.



La Fin

Q&A

Contact:

Dr. Thierry Maison
GET Group North America
tmaison@getgroupna.com