SECURITY OVERVIEW

Version 4.1 – March 2020

Introduction

As IoT based technology adoption expands beyond on premise Internet of Things Security Considerations in a hybrid / multi-cloud environment challenge a firms conventional infrastructure model and practices (Dugar A, IDC 2017). The introduction of external destinations for data and or opening corporate networks to external end points warrants thorough consideration and management of any new vulnerabilities introduced.

Purpose of this document

This document gives an overview of the security measures with the Cypernex IoT management platform. This solution incorporates IoT devices used to collect data and cloud technologies to ingest and present data within the designated applications.

About Cypernex

Cypernex is a provider of IoT fleet management solutions. Cypernex is both device and cloud platform agnostic. It ingests data from a variety of devices, passing through the nominated Cloud infrastructure where it is ingested, normalized and re-factored for Analysis and control. The platform architecture patterns were adapted from industry as represented in ”Industrial Internet Reference Architecture”, IIC 2017 and subsequent updates, and will as a consequence remain aligned with emerging security technologies and best practices as these evolve.

Data storage in IoT infrastructure

Each IoT device contains a proprietary operating systems and firmware developed by their respective manufacturers. Details of each device capabilities should be sought from its supplier.

The devices and the transmission relay junction (microservices) do not store Personally Identifiable Information such as names and addresses. The IoT device ecosystem uses services focus on circuit names and the capture of time-stamped telemetry data from the device fleet.

Data from devices are secured in the communications layer, using SSL encryption and by rejecting connections from unknown servers.

Equipment tamper protection

Tamper protected devices usually use printed circuit boards on which integrated circuits are mounted contains a single proprietary controller and logic arrays only available through its manufacturer. Devices deemed as providing sensitive information should be installed in a location that prevents physical access by non-approved personnel.

However if the building security was compromised attempts to hack an MCU based device would be pointless, providing at best access to the outgoing data already streaming through secure connections. No prior data would be on the device.

Some sensors installed in areas with poor communication or internet connection will store prior data on the device to buffer against outages. You should consult manufacturer specifications for details.

Platform Access

Cypernex is itself hosted on a Virtual instance residing in a Cloud providers platform. The security and access management for Cypernex is therefore one in the same as the cloud provider who hosts the Cypernex instance.

Monitor device API's and Hosting

Monitors use two encrypted channels to communicate with the external world. Firstly as stated each device channel is configured to only communicate with a single IP. These two channels have separate secret keys.

Maintenance and Support Channel

The first channel is used for installing firmware upgrades, and reconfiguring the device in cases where for example the size of the CT coil is changed or replaced to allow for a higher / lower loads.

The associated Services are Hosted in Tier 1 AWS facilities in Australia.

- Customer data is not stored within this platform, office premises, and remote access to the AWS server is through Secure Shell (SSH) certificate only.
- Amazon Web Services has obtained IRAP compliance for supply to Australia for Australian Government Information Services. The compliance process examines the controls of AWS' people, processes, and technology to ensure they address the needs of The Australian Signals Directorate Information Security Manual.

- Wattwatchers' hosting AWS complies with security standards including; ISO27001 - Information Security Management, ISO27017 - Code of Practice for Security Controls.

REST API's for Monitoring & Control which are secured with Authentication and encryption.

- To ensure Secure API connections token authentication OAuth is utilised.
- API traffic is secured using SSL encryption, and to reduce vulnerabilities we use the latest TLS1.2 certificates with 2,048 bit keys.
- Wattwatchers administers both user and device access based on commercial agreements. Authentication is via Username/Password.
- Passwords are hashed in the database and not stored as plain text. Logins for monitoring and control APIs are separated.
- To access individual devices Authorisation is via Roles-based Access Control (RBAC) or Access Control Lists (ACL). 128 Bit randomised API keys give access to device data.
- Leading AWS firewall services are utilised.

Wattwatchers Applications

Wattwatcher provides Simble with access through a web portal for configuration and diagnostic purposes.

- Wattwatchers administers user access to applications.
- Authentication and access to data from devices is controlled through the Wattwatchers API.
- User/password authentication is utilised for application login.
- SSL encryption is required for all production software applications. HTTP connection is not permitted for production applications.

- Personally identifiable information is not stored in Wattwatchers systems. In some cases our Enrollment Application is configured to capture location information however this is not stored by Wattwatchers. This information is passed directly into customer systems, and Wattwatchers stores a unique identifier such as a job number.

Third Party applications

Wattwatcher provides Simble with access through API to it's infrastructure for configuration and diagnostic purposes. The services provided allow Simble to notify the Wattwatcher platform when a CT device or monitor has changed, or to visualize status for diagnostic purposes.

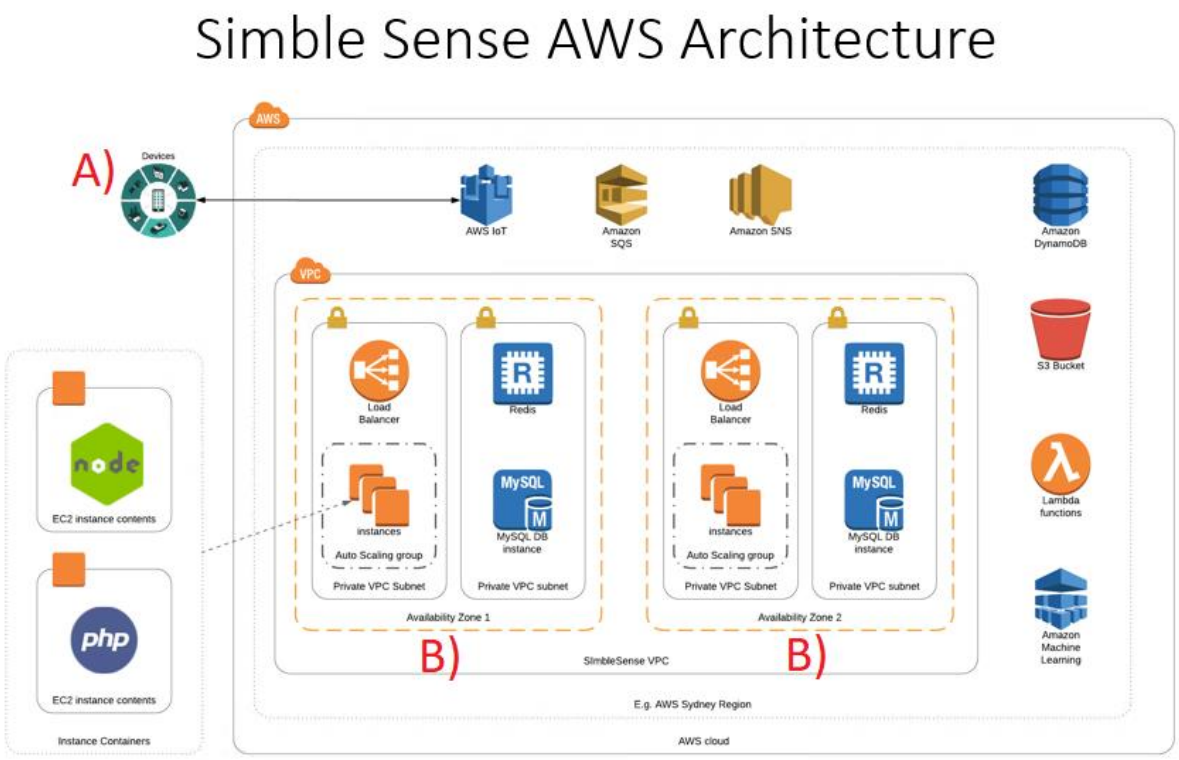
- Customers administer user device configuration.
- Authentication and access to data from devices is controlled through the Wattwatchers API.
- User/password authentication is utilised.
- SSL encryption is required for all software applications. Http connection is not permitted.

Data Streaming Channel

The second channel sends data to the Simble Sense platform.

Monitors stream data using <chris please give correct words> through the cellular network.

Simble Sense Platform



Operational characteristics.

A) Data streams ingested into the Simble platform flow from devices into the AWS IoT platform.

B) Data cleansing, normalization, categorization beings in the closest availability Zone, and for data sovereignty compliance remains with related customer information in the same geographical region. Each availability zone utilized load balancing and auto scaling.

C) Raw data is compressed and stored in the same region within S2 buckets to facilitate the building of data in support of new features as the software solution is enhanced.

D) Cookies where needed only use to store operational variables that are replaced when he UI is refreshed.

E) Login information for administrative systems are kept separate.

F) Leading AWS firewall services are utilised and our network heavily restricts inbound communication using these services.
Chris what does this mean ??

G) We also make use of AWS network anomaly detection services (chris)??) and IoT Device defender.

Security Process for API and Application Development

Simble applications utilize application and middleware API layers to perform their function. All information exchange with data storage is managed through the application system API protected from reverse engineer of API using oAuth2. Security within middleware centrally governs information access and data type in accordance with policies defined by user group, parent/child entity relationship.

Chris: do we do something like this ?
To overcome systematic API discovery (reverse engineering from authenticated user), API middleware makes use of Amazon Device defender to centrally manage and detect systematic infiltration attempts. In response this would send notifications and/or take remedial action.

This middleware also ensures that authenticated use API calls from the UI will only provide access to the tenants data, and more specifically the data that user of the tenant is entitled to access based on their credentials.

In alignment with (IIC 2017) (Amazon, Apr 2018) (IDC #US41695616, September 2016) security best practices application security source code is broken into encrypted libraries. For access developed follow proprietary CI/CD process that includes recording date/time/purpose of access and detailed explanation and approval of security changes made.

Securing the User Interface

Users access the system through both mobile and desktop applications after login which has the following characteristics:

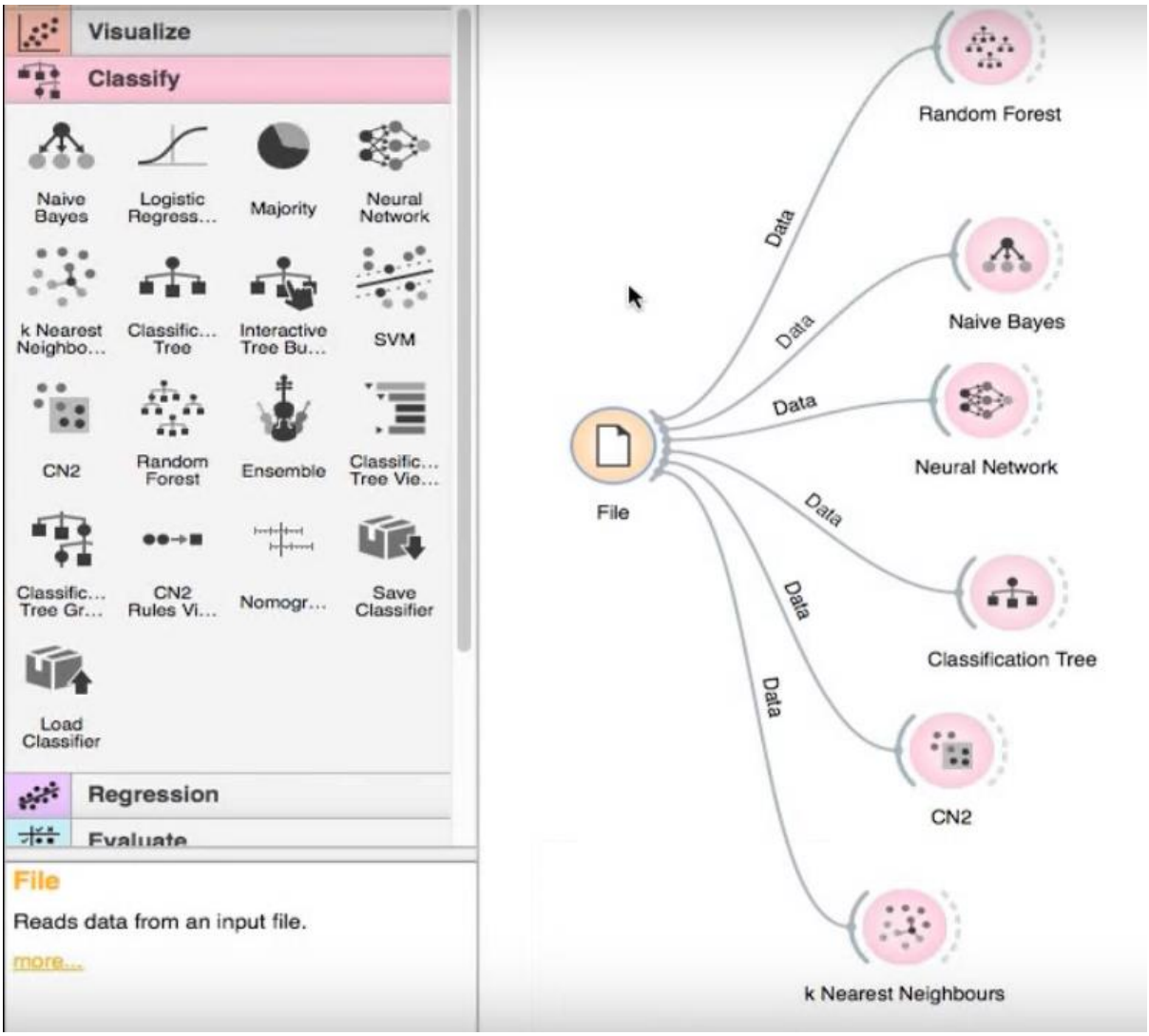
A) SSL encryption is required for all of our web based software application communications.
B) Unsecure connections such as HTTP or FTP are not permitted in our applications. All web traffic is secured using SSLv3 encryption with 2,048 bit keys.
C) User authentication is managed via username and password, the passwords are stored as hashes in the database and not as plain text.

Chris need some nice words here about why we do things the way we do, and why it helps security

Security third party tools

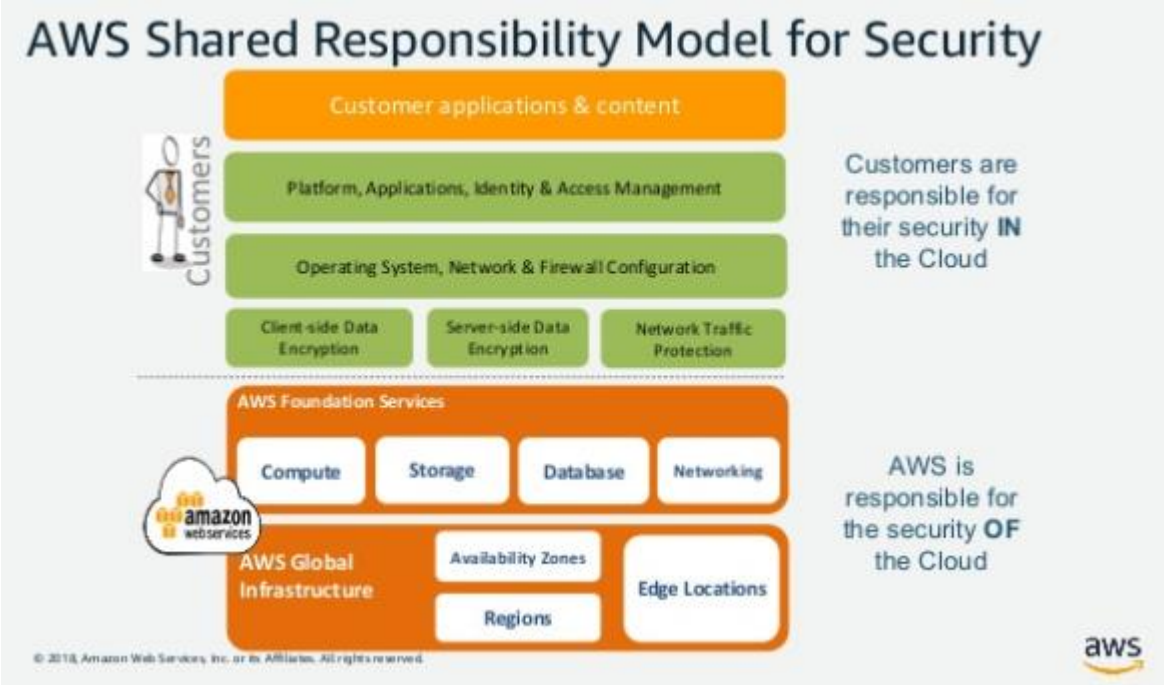
Third party tools such as productivity and Data Mining applications access the data through Rest based API calls. A single signon is required for each call authenticated through the user of <chris/Minh>???? .

Example: Data Mining with Orange3 uses API calls to examine access preassembled datasets to Orange3.



Amazon Security features

Simble has opted to follow AWS security best practices (Amazon, Apr 2018).



In particular the adoption of <chris> has provided the following benefits:

<benefit>

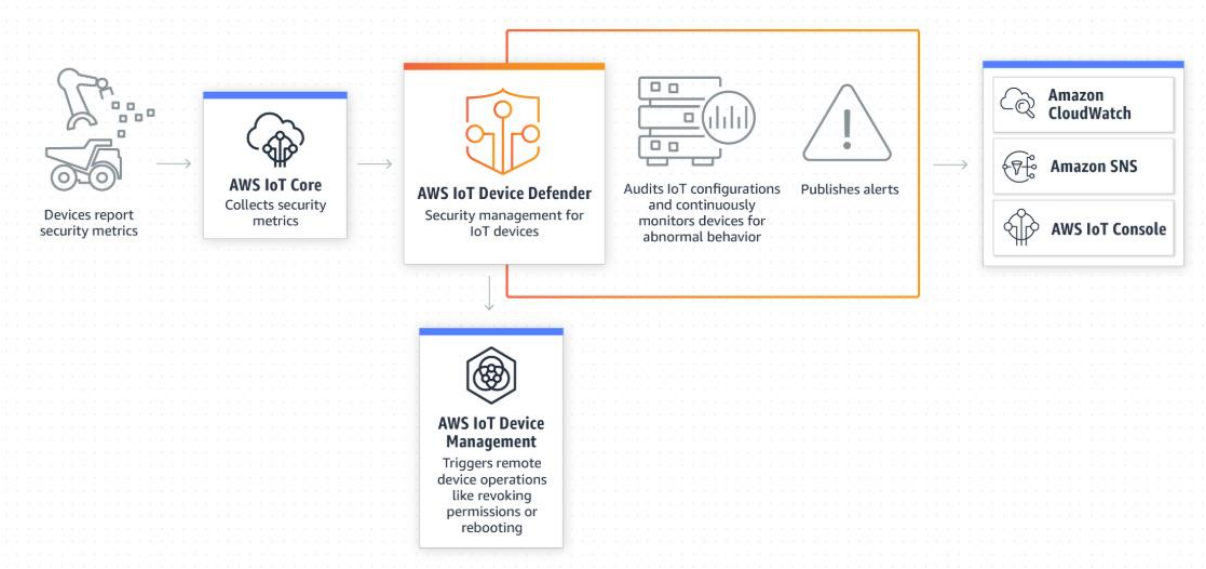
<benefit>

<benefit>

Insert conclusion <here>

AWS IoT Device Defender

AWS IoT Device Defender is a fully managed service used to secure a fleet of IoT devices. It does this by continuously auditing the IoT configurations for any deviation from security best practices.



A configuration is a set of technical controls used to keep information secure when devices are communicating with each other and the cloud. The effect is to maintain and enforce IoT designated configurations, ensuring device identity, authenticating and authorizing devices, and encrypting device data is maintained. Should the AWS IoT Device Defender uncover anomalies it may send messages or use pre-trained model to direct the Simble platform to isolate, control, shut down or sandbox processes or packets in readiness for further remedial action.

M2M Cellular Security Practices

M2M service provides the registration for the Monitor devices fitted with SIM cards. Each monitor is set to make the outbound call to the service passing encrypted data at designated intervals through M2M VPN Solution via the carriers (Vodaphone/Telstra) wireless telemetry services.

- IP protocols encrypt data from the device to the backend to create a more secure connection through the internet.
- Simble then extracts information packets through a secure VPN passing through Amazon IoT to the SImble for ingestion.
- Personally identifiable information is not stored in M2M.
- Any attempts at vulnerabilities introduced through source code would fail as the Monitor device initiates the connection to M2M.
- Device connection is SSLv3 encryption so any listeners are ineffective
- Any attempt to upload to IoT device reconfiguration packets are secured by SSLv3, proprietary (not public) hand shaking, encryption and secret key

Security Roadmap (C+C Idea: we can omit from this version of Doco)

1. Smart self healing platforms

   In consideration of the security challenges our company will face in the years ahead, Simble is building capabilities into the platform that can be used to combat new threats that come our way. One such threat can come from data tampering caused by equipment / infrastructure failure or attacks human aided scenario's.

   The platform is designed to manage very high volumes of 5 second data from millions of energy monitors and sensors. The multi-tenant database is designed to retain ingest and archive at scale whilst performing (or re-performing) transmission package tamper detection on incoming or previously ingested data packages. Simble is developing it's proprietary anomaly detection algorithms that would be trained to seek out, select, alert and/or counteract package abnormalities based on this capability.

References

- Dugar A, IDC, 2017. "Internet of Things Security Considerations in a Multicloud Environment.",(IDC PERSPECTIVE. 2017).
- Wattwatchers, "Wattwatchers Security Overview",v1, 2018, (IIC:PUB:G1:V1.80:20170131)
- IIC 2017,The Industrial Internet of Things ,"Industrial Internet Reference Architecture", Vol G1, January 2017
- Amazon, Apr 2018. "Amazon IoT Security Best Practices", Amazon Web Services ,https://www.slideshare.net/AmazonWebServices/aws-iot-security-best-practices, Apr 24,2018
- Advancing Industrial Internet Security: Convergence of IT with OT (IDC #US42020616, December 2016)
- Vendor Profile: Microsoft Azure — Focus on IoT Platform Security Solutions (IDC #US41695616, September 2016)
- Cloud Foundry Summit 2016: Momentum and Competition (IDC #US41447616, June 2016)
- Vendor Profile: Amazon Web Services — Focus on IoT Platform Security Solutions (IDC #US41085316, March 2016)