SWITCH AUTOMATION

SECURITY OVERVIEW

Agenda

Platform Overview

Security Features

Appendix

Platform Overview

The Platform

CONTROL

LOGIC ANALYTICS
FDD, Alerts

BUILT-IN USER INTERFACE
Charts, Graphical Analysis, Dashboards

DATA MANAGEMENT
Historical files, Live device Integration, API, Historian, Tagging

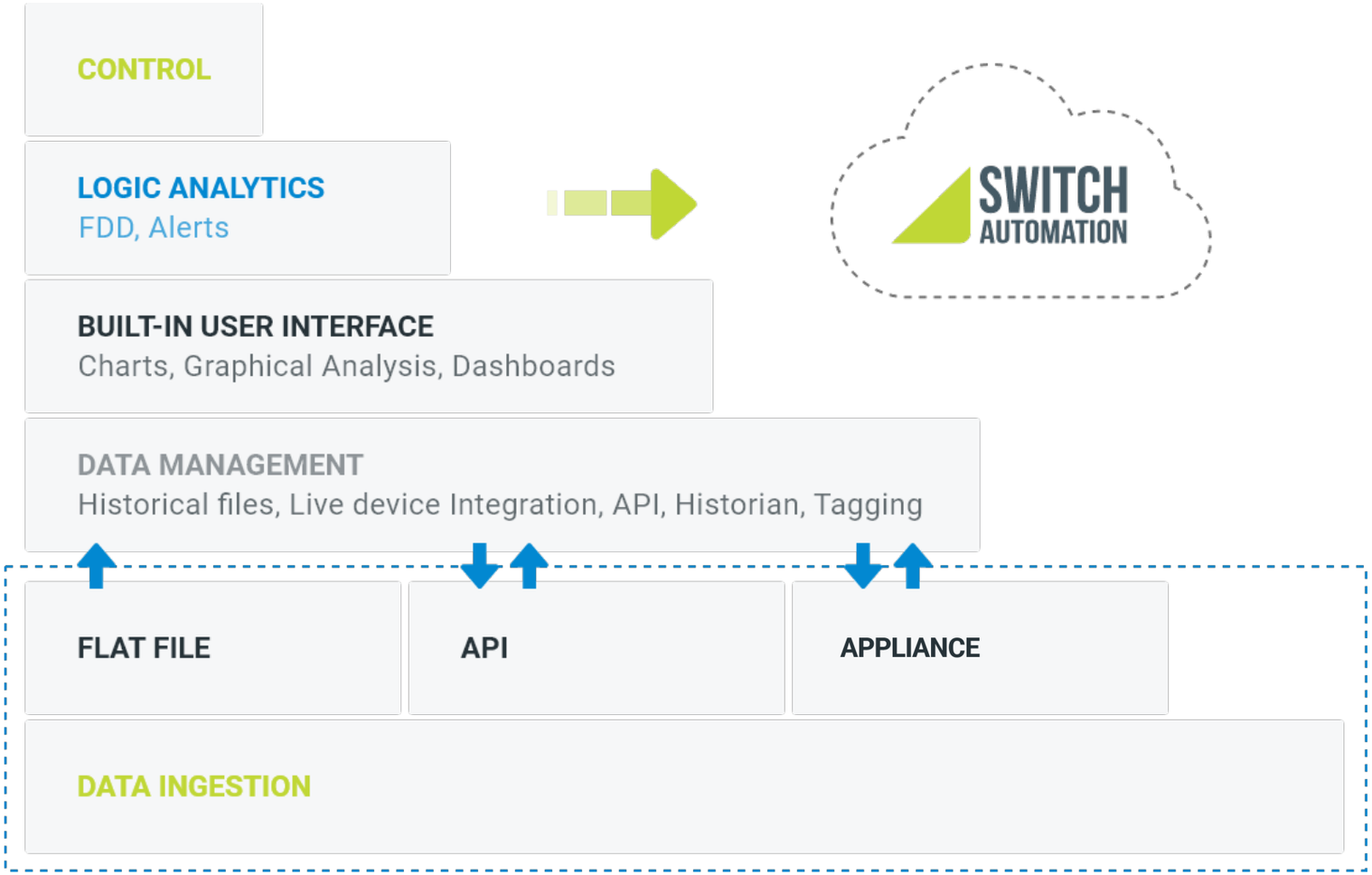
FLAT FILE | **API** | **APPLIANCE**

DATA INGESTION

- Switch is not a traditional BMS offering
- Switch Platform is hardware agnostic
- It ties together data and controls from disparate edge devices and systems
- The Switch Platform is built and hosted on Microsoft Azure, and Switch OS runs on Linux appliances
- The Switch Platform permanently stores all data
- Switch's simple, flexible architecture can accommodate various network setups
- Switch can be accessed by users from any modern web browser
- Users can control local devices remotely
- Logical analytics and control sequences can be configured in the Platform and run automatically in the background
- The Switch IoT appliance maintains continuity during an internet outage
- SSL Labs Rating of 'A'

Data Sources and Communication

The Platform can communicate via 3 primary sources



File Ingestion Engine

- Can receive files from secure FTP or email (dataimports@...)
- Users can create custom file mappings to automate repeated files imports

APIs

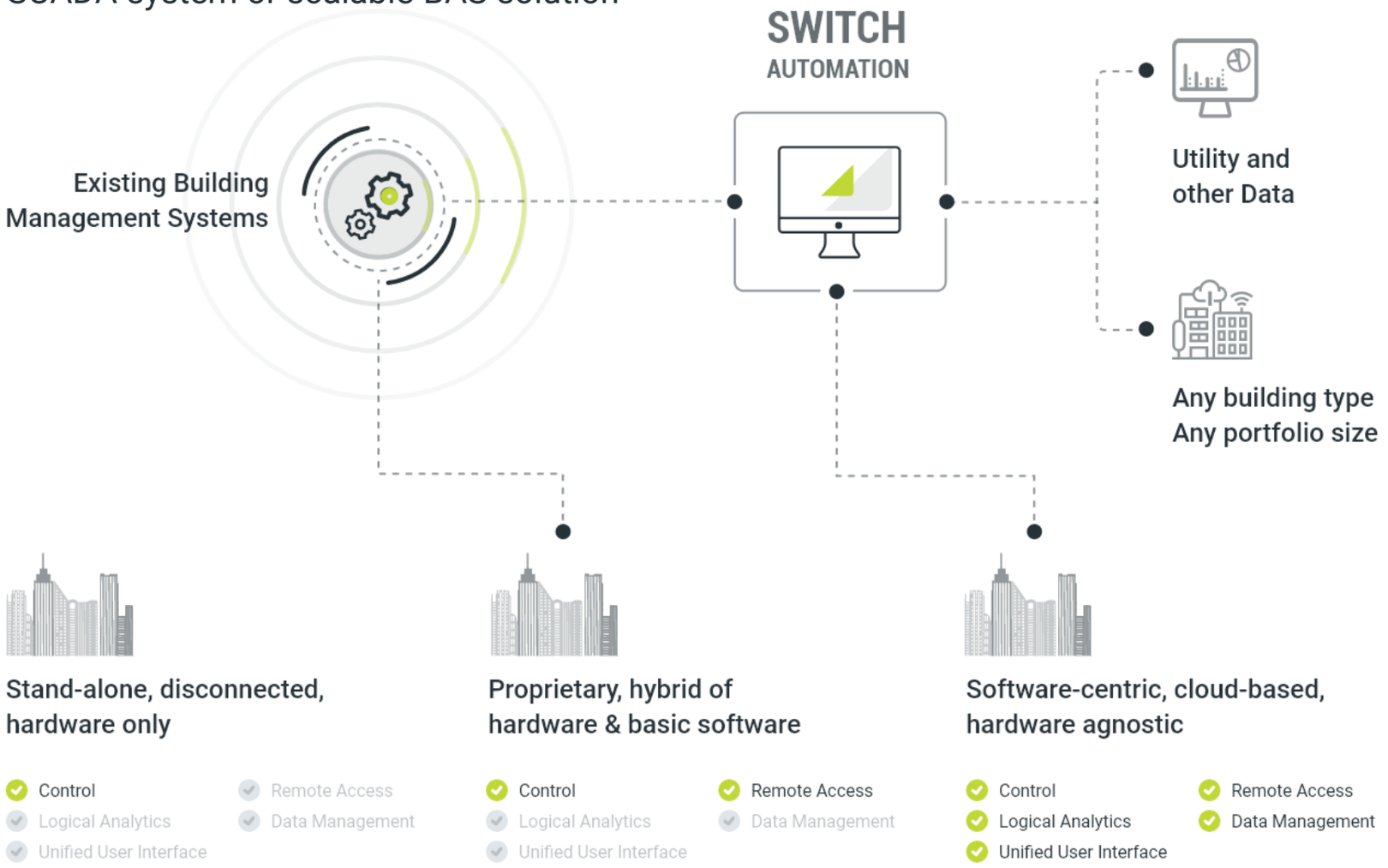
- REST based API is served over encrypted HTTPS, requires API keys
- Offers programmatic read, write, update and delete access
- Currently support Installations (Sites), Devices, Sensors, Readings (live data), Events and Search
- Several OEM hardware lines push to Switch API (e.g. Obvius AquiSuite and eGauge)

Appliance

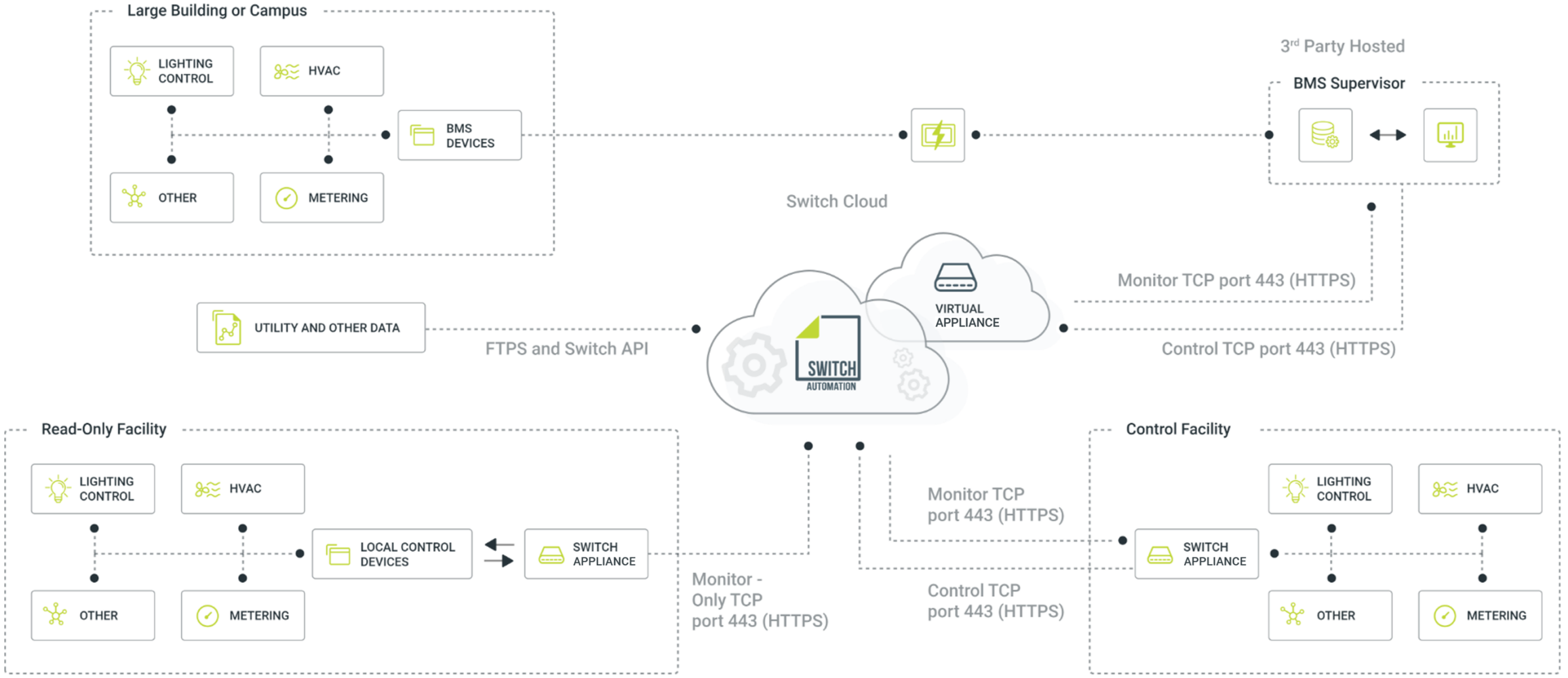
- Dell 3003 embedded device
- Embedded devices communicate securely in real-time with Switch cloud via outbound HTTPS (port 443)

Central platform for building data

But can also serve as a SCADA system or scalable BAS solution

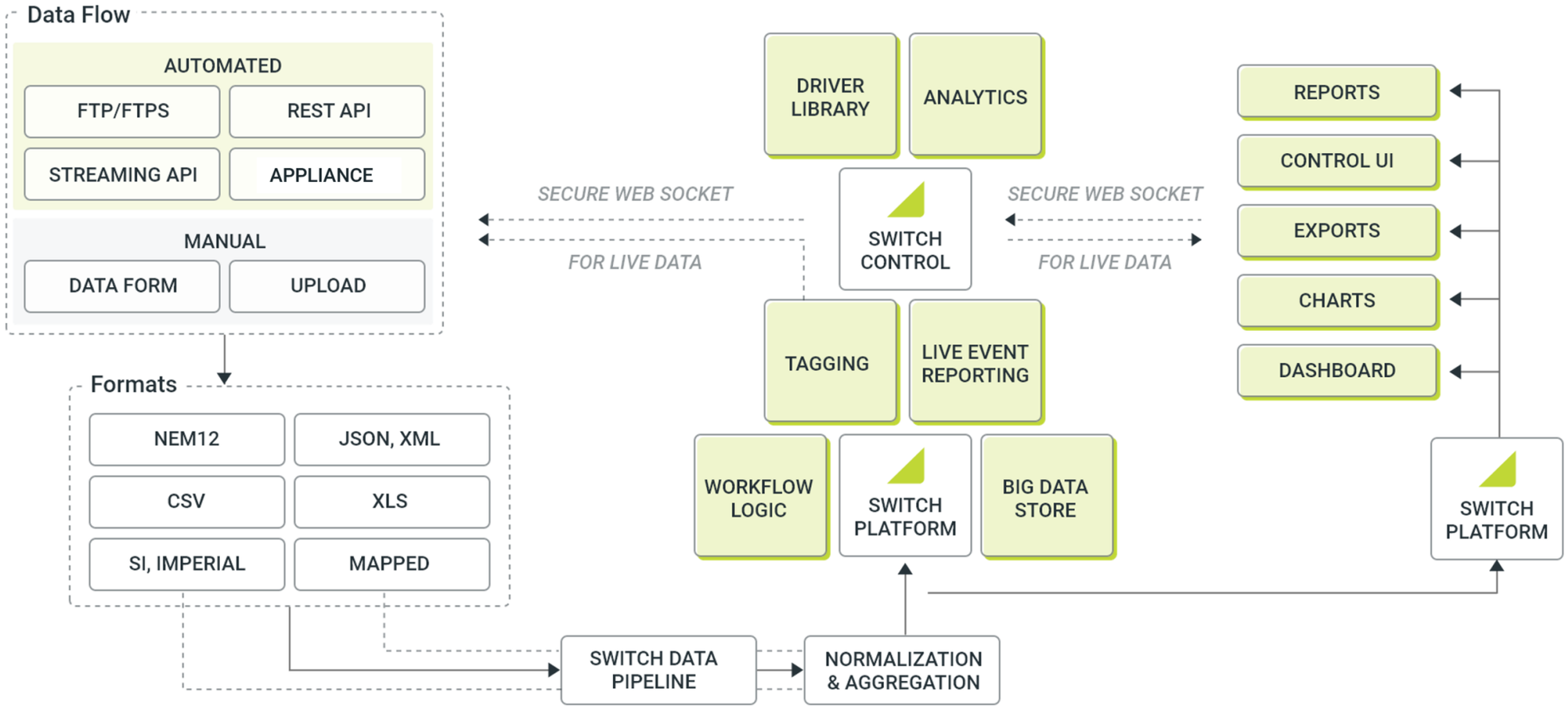


Typical ‘smart buildings’ program architecture



Data flows within the Switch cloud

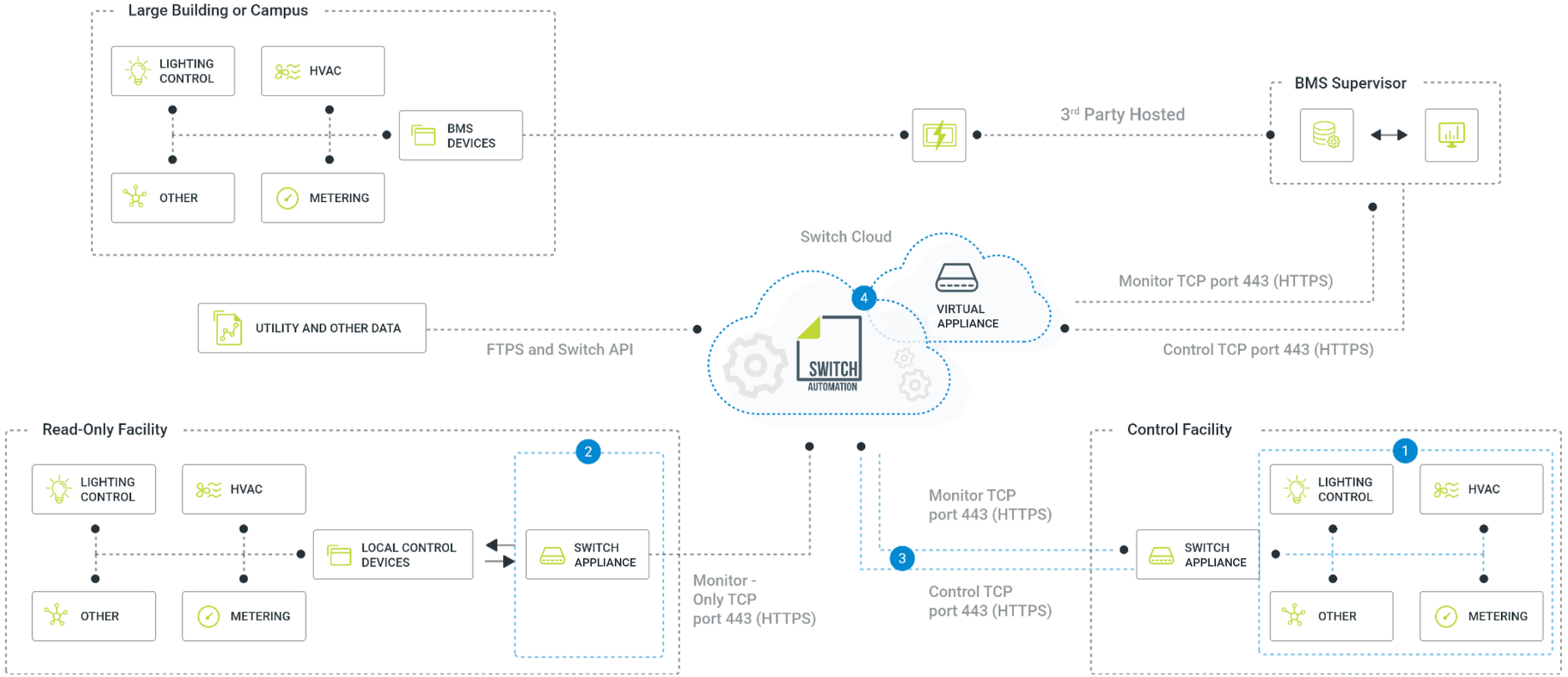
Once imported, data is stored in Switch's Azure cloud and accessed by users via browser



Security Features

4 areas of focus for security

1. BMS/BAS/ "edge device" LAN
2. Switch applliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure



BMS / BAS / ‘Edge Device’ LAN

Field control, metering devices and local area networks, which typically don’t need internet to function locally

Switch does not provide this hardware—we’re agnostic

Switch appliance communicates with devices and can provide a single source of external internet connectivity

Most OEM hardware is standardizing on BACnet IP and Modbus TCP protocols (Switch supports other protocols / hardware as well)

Dell Edge 3003 embedded device

1. BMS/BAS/ "edge device" LAN
2. Switch appliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure

Details

- Intel CPU E3815 1.46GHz (512KB L2 cache)
- Ubuntu Core 16
- 2GB DDR3L - 1067MHz (Soldered)
- 8GB eMMC (No WWAN) or 32GB (WWAN Base)

Security

Secure Boot

- During bootup, firmware verifies OS is trusted and not tampered

Trusted Apps

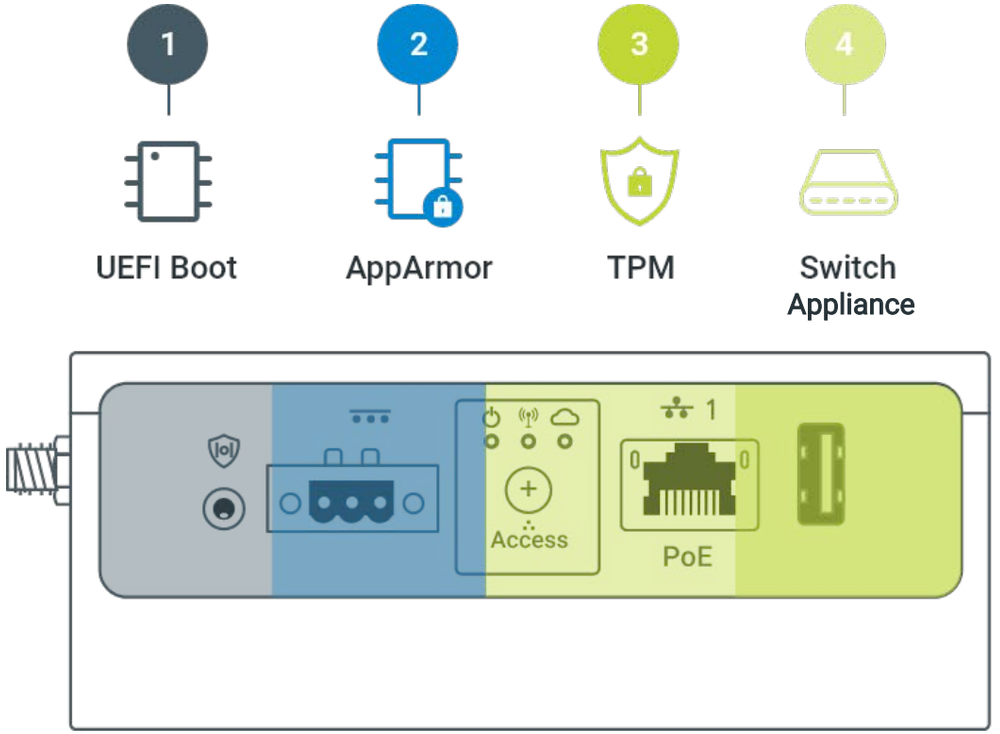
- Verifies only white-listed apps are able to run
- Verifies apps have access only to allowed appliance resources

Delivery

- Updates to OS + Applications (Switch appliance services)
- Switch manages these updates per terms of SLA

Switch appliance

1. BMS/BAS/ "edge device" LAN
2. Switch appliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure



1. **UEFI (Unified Extensible Firmware Interface):** is a standard on securing firmware on devices. Ensures that software loaded for boot up is not tampered. Enables Secure Boot and replaces the old unsecure BIOS.

2. **Device Guard:** Kernel level feature which confines apps to limited / controlled set of resources.

3. **TPM (Trusted Platform Module):** is an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.

4. **Switch Appliance Services:** Software packages are temper resistant and digitally signed for integrity.

Switch appliance

Technical Specifications

Firewall

- All Incoming Ports Blocked
- Outbound Connections via 443

Communications

- Supports Https for Project Meta Data
- Supports Secure Web Socket for Real Time Control
- Supports Proxy Servers

Management & Support

- Headless Mode Only
- Remote Access to OS via SSH
- Remote Monitoring & Management via Microsoft Intune

Online Mode

- Real-time Control Via Authorized Devices

Offline Mode

- Local Control via Authorized Local Devices
- Logic Continues to Run
- Schedules Continue To Run

Appliance to cloud communication

Switch can operate under many network configuration scenarios:

- Cellular (4G, Cradlepoint, etc.)
- Physically segmented corporate network
- Logically segmented corporate network
- Virtual Private Networks

Switch appliance communicates with the Switch cloud via outbound port 443 (https) to whitelisted Azure URLs (see next slide)

Appliance to cloud communications utilize secure web sockets (wss)

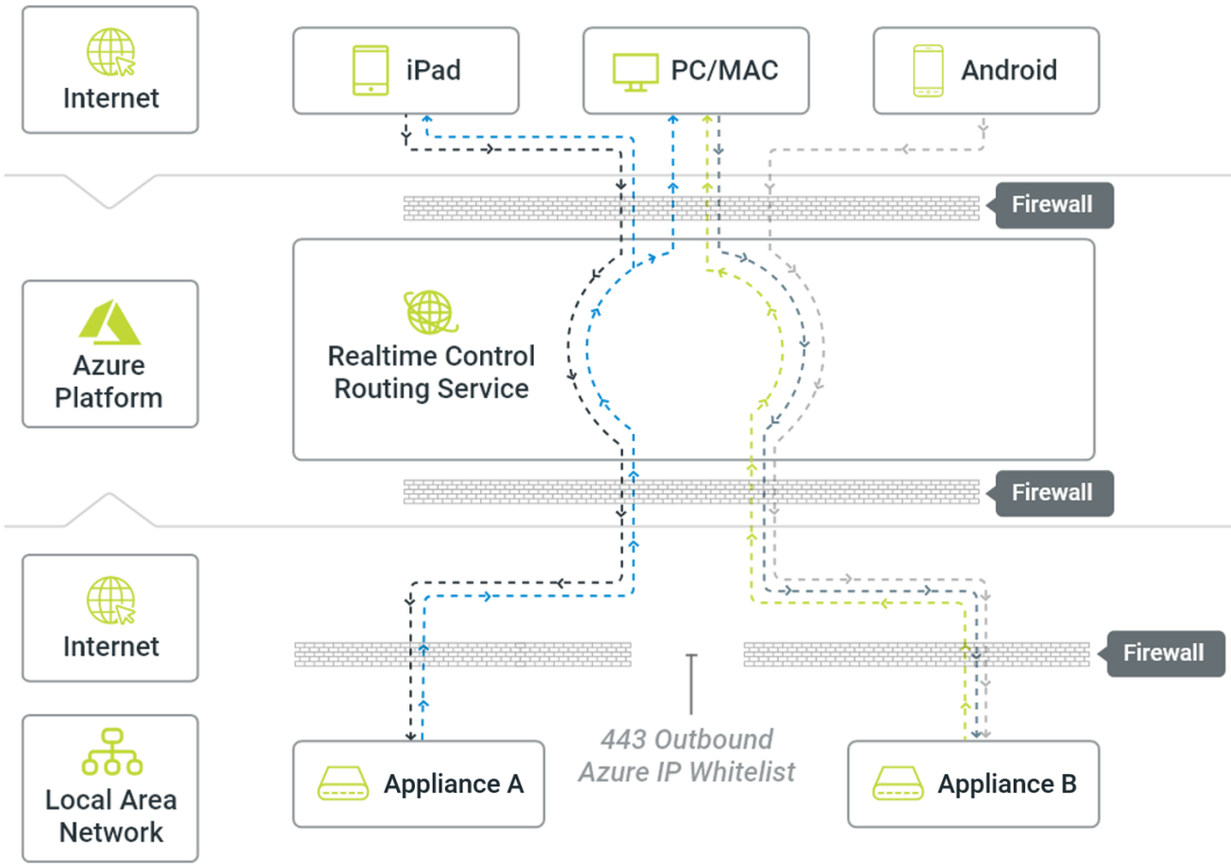
Switch ports and URL requirements

For a Switch appliance to communicate with the Switch Platform, the following URLs need to be opened for outbound traffic from the firewall (inbound ports not required):

URL	Port Number
Hub.switchautomation.com	443
Us.switchautomation.com	443
Switchdal.switchautomation.com	443
Switchdal-us.switchautomation.com	443
Platformapi-us.switchautomation.com	443
Platformapi-ea.switchautomation.com	443
Switchdal-us.switchautomation.com	443
Command.switchautomation.com	443
Command-us.switchautomation.com	443
Realtime.switchautomation.com	
Realtime.ably.io	
Switchdocker.azurecr.io	443
Relay.switchautomation.com	443

Appliance to cloud communication

Realtime control routing services

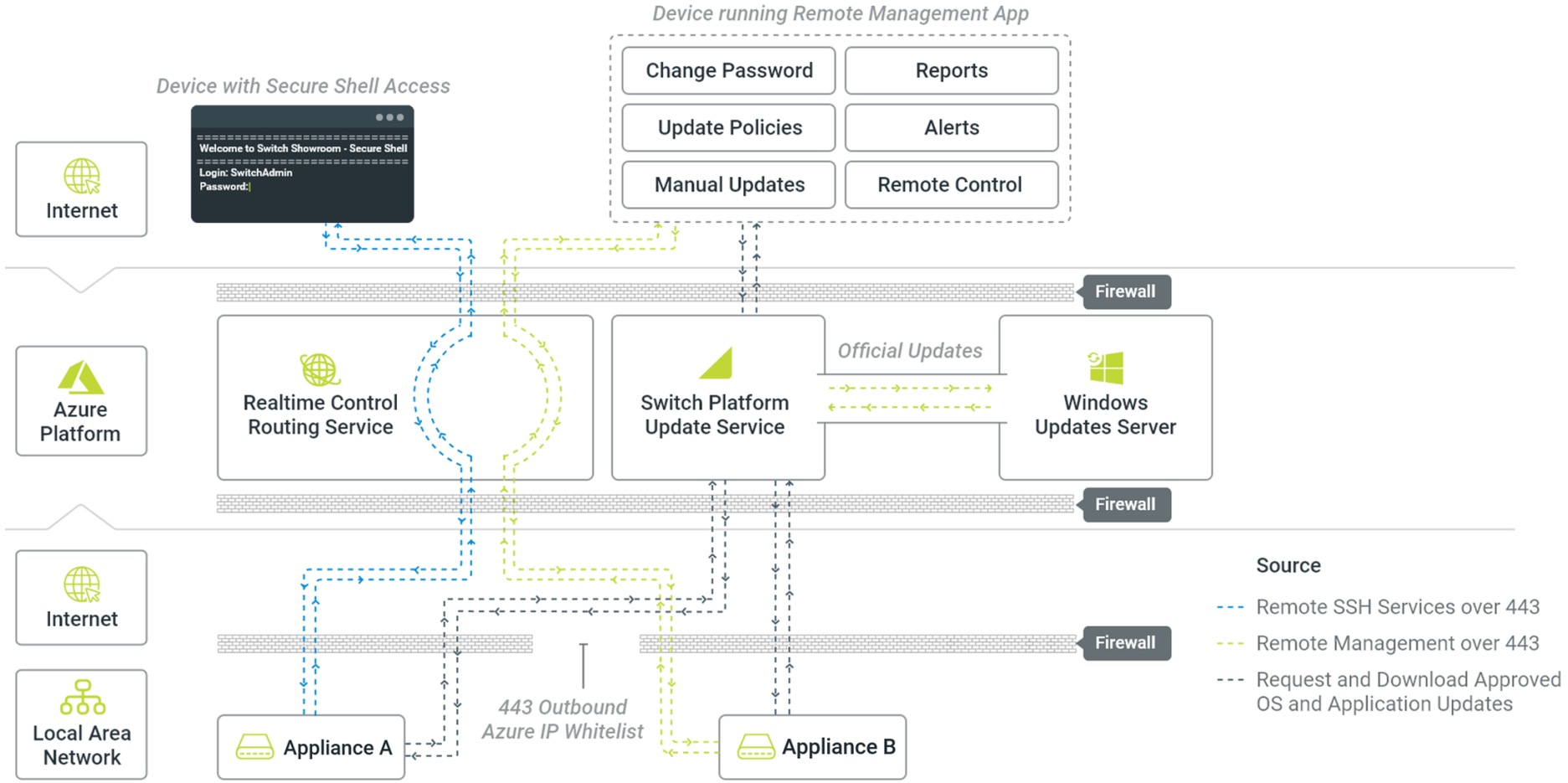


Source	Destination	Command
Appliance A	iPad	Device Status Update
Appliance B	PC/Mac	Device Status Update
PC/Mac	PC/Mac	Device Control
Android	Appliance B	Command
iPad	Appliance B	Device Control
	Appliance A	Command

Appliance update

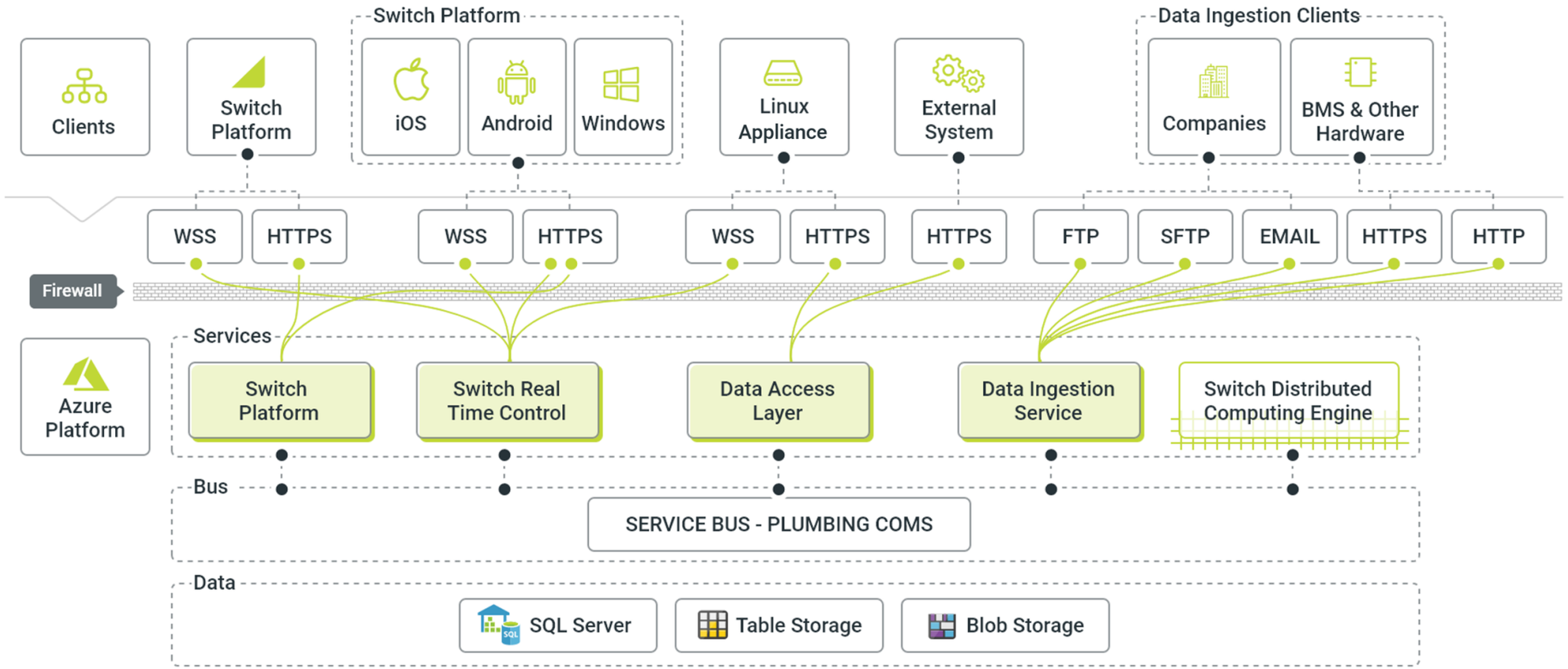
1. BMS/BAS/ "edge device" LAN
2. Switch appliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure

Switch Platform update service



Switch cloud on Microsoft Azure

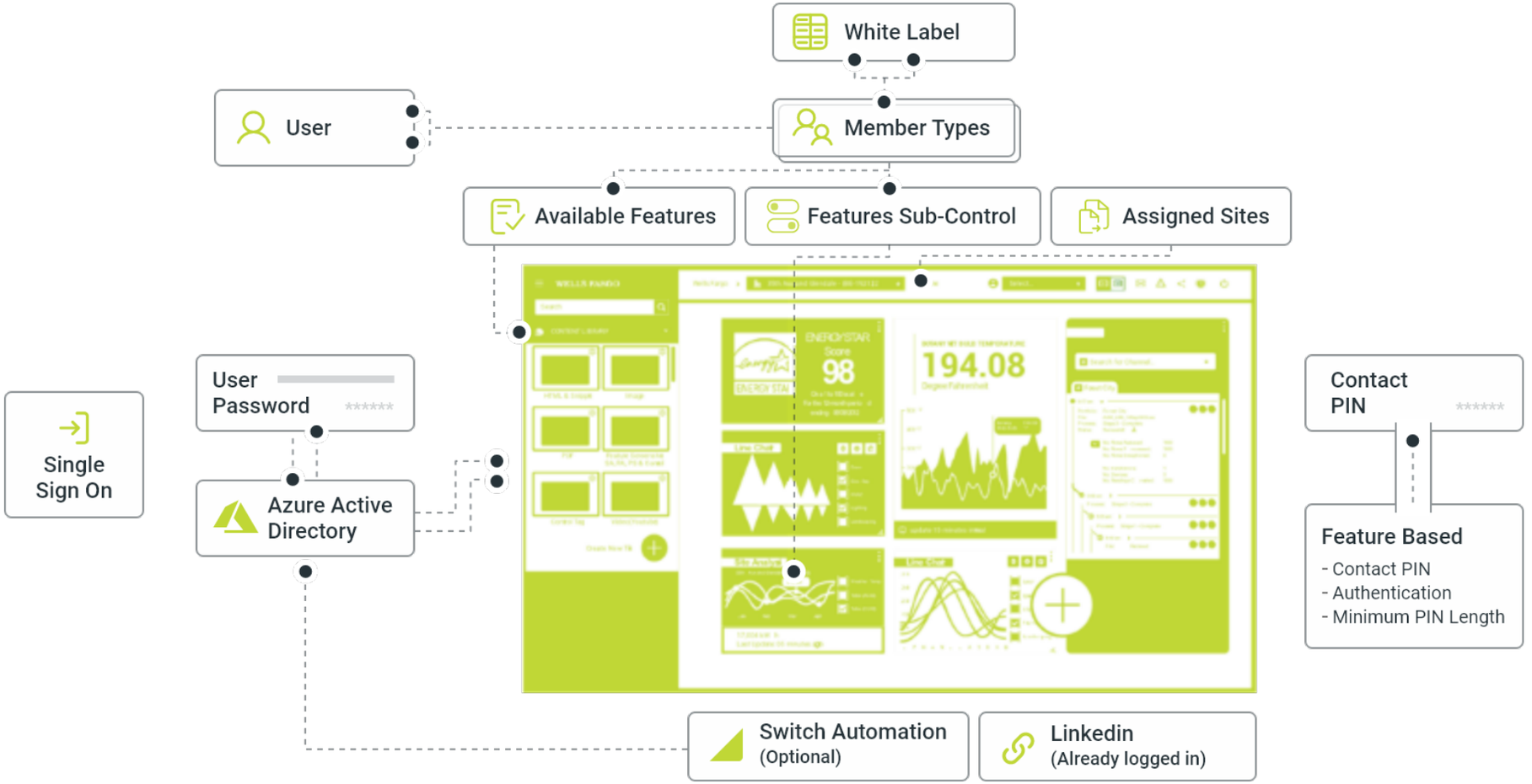
1. BMS/BAS/ "edge device" LAN
2. Switch appliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure



Switch cloud on Microsoft Azure

1. BMS/BAS/ "edge device" LAN
2. Switch appliance
3. Appliance to cloud communication
4. Switch cloud on Microsoft Azure

Platform security features



Appendix

Glossary

- API – Application Programming Interface. In this context, an API allows for streamlined integration of the Switch platform with otherwise distinct applications and databases for purposes of data transfer. https://en.wikipedia.org/wiki/Application_programming_interface
- REST – Representational State Transfer. The software architectural style of the World Wide Web. A set of properties and constraints that serve as a protocol of sorts to facilitate communication between systems. Switch's API is RESTful. https://en.wikipedia.org/wiki/Representational_state_transfer
- FTP – File Transfer Protocol. A standard network protocol used to transfer files from one host to another over the internet. Switch can receive data via FTP in common file formats, such as csv files, and automatically post that data to the platform. https://en.wikipedia.org/wiki/File_Transfer_Protocol
- FTPS – An extension to FTP that adds support for the Transport Security Layer (TLS) and Secure Socket Layer (SSL) encryption. https://en.wikipedia.org/wiki/FTPS
- OEM – Original Equipment Manufacturer. In this context, the OEM for a BMS solution is the original manufacturer of the hardware, often re-sold by a licensed vendor or corporate sales team assigned to a specific geography.
- URL – Uniform Resource Locator. URL is the technical term for a "web address" that one would type into a browser in order to navigate to a web page or other content on the internet. https://en.wikipedia.org/wiki/Uniform_Resource_Locator
- HTTP – Hypertext Transfer Protocol. The foundational protocol for data communication on the World Wide Web. In most network configurations, HTTP traffic communicates on port 80. https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
- HTTPS – HTTP Secure. A secure version of HTTP encrypted by Transport Layer Security (TLS) or Secure Sockets Layer (SSL). HTTPS provides authentication of the website and associated web server and provides bidirectional encryption of communications between a client and server. User access to the Switch Platform is via HTTPS, and all appliance communications with the cloud utilize HTTPS. In most network configurations, HTTPS traffic communicates on port 443. https://en.wikipedia.org/wiki/HTTPS
- WSS – Web Socket Secure (or, alternately, Secure Web Sockets). WebSocket is a protocol providing full duplex communication over a single HTTPS connection (port 443). The Switch appliance communicates with with the Azure cloud via WSS, enabling real time control and feedback, as well as camera feeds and live alerting. WSS communications are encrypted and utilize a secure key to initiate the "handshake" between client and server. https://en.wikipedia.org/wiki/WebSocket

Switch 3003 appliance hardware

But can also serve as a SCADA system or scalable BAS solution.

VISIT US

www.switchautomation.com

EMAIL US

contact@switchautomation.com

FIND US ON TWITTER

@SwitchHQ