Honeywell

CONNECTED LIFE SAFETY SERVICES (CLSS)

PRIVACY, HOSTING AND SECURITY WHITE PAPER

January-2024

VERSION 2.3

ABOUT THIS DOCUMENT

This document is mainly designed for Honeywell Connected Life Safety Services (CLSS) ESDs, system integrators, and technicians keen on comprehending Honeywell's security strategy for the CLSS solution. It further delves into the security framework, processes, and protective measures, guiding how to set up the CLSS communicators securely on-site.

Disclaimer:

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

Privacy:

Honeywell recognizes the importance of privacy to our business and customer trust. We are committed to handling all customer data responsibly. Our privacy policy explains our approach to privacy and how individuals may exercise their rights: https://www.honeywell.com/us/en/privacy-statement

As an organization focused on earning our customers' trust and handling their information assets with care, Honeywell strives to develop a strong compliance culture and robust security safeguards. Our terms of use incorporate Data Processing Terms, which are published at: https://trust.honeywellforge.ai/content/dam/forge/en/documents/legal-terms-and-conditions-/10_HCE_Data_Processing_Terms_v1.0.pdf

Terms of use:

Honeywell Connected Life Safety Services (CLSS) terms of use are published at: https://fire.honeywell.com/#/CLSSPortalTermsAndCondition

Cyber Security:

At Honeywell, cybersecurity is a priority for all our products, software, and services. We utilize an end-to-end lifecycle approach and set of security practices to protect customers from cyber threats. We understand the seriousness of such threats and our team of experts implement continuous measures to assess, detect and mitigate risk. We continuously update our products and security guidance with best practices. Our holistic, disciplined approach results in cyber resilient products and services to maintain a secure life safety system.

INTRODUCTION TO CLSS

Connected Life Safety Services (CLSS) is an end-to-end platform that leverages the power of cloud-connected technology, placing connectivity at the heart of life safety. It enables systems integrators and facilities managers to deliver an enhanced fire safety service, while maximizing the performance efficiencies offered by Honeywell's trusted Fire detection and alarm systems.

CLSS CLOUD PLATFORM

Connected Life Safety Services (CLSS) Cloud platform contains various micro services to support functionalities of CLSS Gateway, CLSS Pathway, mobile app, and web app. It is secure, scalable, standards built on the Honeywell Forge enterprise management platform.

The cloud-based deployment is managed as per Honeywell's unified compliance framework that is aligned to major IT security frameworks including NIST SP 800-171 and ISO 27001.

All internal communications between various cloud services use HTTPS for integrity and confidentiality within the cloud.

CLOUD INFRASTRUCTURE SECURITY MEASURES

- **LOGIN AND ACCESS CONTROL:**
  - Strong login and password-based authentication is used for mobile and web apps.
  - Role-based access control mechanisms are employed to enforce access privileges for distinct datasets.
  - Robust authentication and authorization measures are implemented at the application level to tightly control access to all application data.

- **FIREWALL:**
  - Firewall in perimeter security is ensured through IPS/ IDS and packet inspection.
  - WAF (Web Application Firewall) is enabled for CLSS applications. WAFs provide protection against cyber-attacks like SQL injections, cross-site Scripting, malware uploads, application DDoS etc.
  - Security hardening of all servers is segmented via virtual networks and virtual servers.
  - All CLSS cloud virtual machines are protected with Anti-malware.

- **TRANSPORT LEVEL SECURITY:**
  - At the transport layer, all data is encrypted. All connections are made with TLS, which enforces TLS 1.2 as a minimum.
    - TLS between client applications and Microsoft Azure Application CLSS Gateway
    - TLS between core application services and Microsoft Azure IoT and Microsoft Entra ID
    - TLS between core application services and 3rd party applications (SendGrid, APIGee).

- **ENCRYPTION:**
  - Sensitive data like security tokens and cryptographic keys are managed through **Azure key vault**. Azure key vault provides FIPS 140-2 Level 2 validated hardware security modules (HSM) to store the sensitive data.
  - All data is encrypted at rest on Microsoft SQL DB and Azure Cosmos DB using AES-256 encryption.

- Data in Microsoft Azure managed disks is encrypted using AES-256 encryption and is FIPS 140-2 compliant.
- Passwords are managed in Microsoft Entra ID. Passwords are hashed using Password Key Derivation Function 2 (PBKDF2), using HMACSHA256@ 1000 iterations. For detailed information please visit **here.**
- System admin level access is restricted to the authorized Honeywell Digital operations team. Regular backups are taken to restore system to normal state in case of accidental loss. At rest, all the data is encrypted using SSE (Solid state encryption).

- **OTHER SECURITY MEASURES:**
  - Standard process to apply Security patches periodically with provisions for risk based expedites.
  - CLSS Cloud Platform is built on Honeywell Forge platform and hosted on the Microsoft Azure Cloud. Honeywell Forge platform is audited under SOC2 Type 1. Microsoft Azure Cloud is certified with SOC1 Type2, SOC2 Type2, ISO27001. For a complete list please visit **here.**

PERSONAL DATA

All personally identifiable information (PII) is safeguarded through encryption while stored. The safeguarding of personal data aligns with both GDPR regulatory requirements and Honeywell's privacy benchmarks. Honeywell restricts the gathering and handling of personal data to the least extent required for fulfilling valid business objectives.

CLSS COMMUNICATORS

CLSS Communicators serve as a bridge between the fire alarm control panel and CLSS Cloud platform.

CLSS GATEWAY

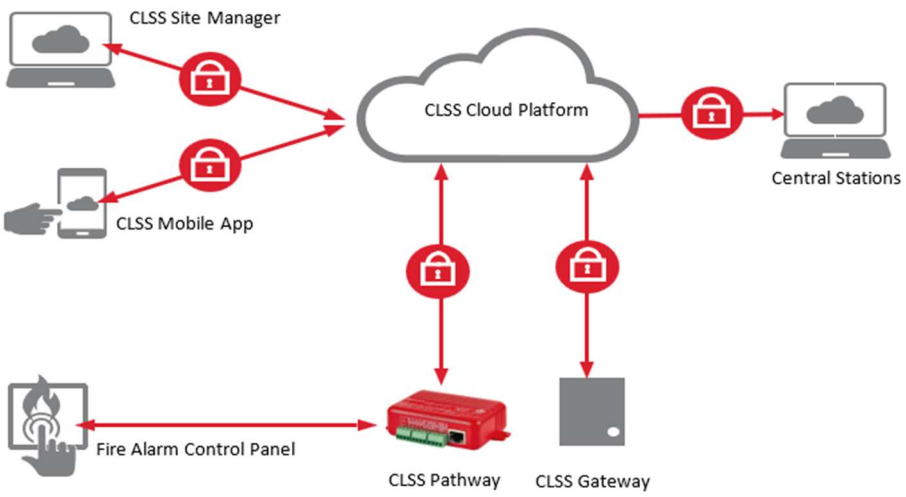
CLSS Gateway provides a way to securely connect on-premises fire alarm control panel to the cloud and provides single path from site to cloud ensures all CLSS cloud services and applications use the same audited and monitored method to receive events and send commands to on-premises fire alarm control via CLSS Gateway.

DATA TRANSMISSION FROM ON-SITE SYSTEM TO CLOUD

For achieving CLSS Mobile app and Web app (Inspection manager and Site manager) functionality use cases, the following data from the on-site CLSS Gateway is transmitted to cloud:

- Device inventory received from the fire panel *(only on fire panels that support this functionality)*
- Events, alarms, and troubles received from the fire panel.
- CLSS Gateway generated events, alarms, and trouble.
- CLSS Gateway Audit logs with timestamp.

The Device inventory contains all the devices (e.g., detectors, modules) including fire panel connected to the fire alarm system network.



SECURING THE DATA TRANSMISSION

To manage the surface area of the system from a security perspective the CLSS Gateway Cloud Connector only makes outbound calls, and no inbound communication is accepted. The outbound connections made are limited to HTTPS for initiating communication and then AMQP over HTTPS for messaging with TLS1.2 and above encryption. AMQP is an OASIS standard messaging protocol designed for reliable and robust messaging which is well suited to scenarios where confirmation of commands and data transfer is required.

Certificate based authentication is used between on-premises CLSS Gateway and CLSS Cloud platform.

INFRASTRUCTURE NEEDS FOR DATA TRANSMISSION

The on-premises CLSS Gateway forms a secure connection with the cloud. The CLSS Gateway employs strong communication security, utilizing HTTPS/TLS encryption, for functions such as Remote Monitoring, Alarm Transmission to Central Station (US-Only), Digitized Maintenance and Cloud Connected Horizon. Inbound communication from the CLSS Gateway to on-premises applications, like LAN Connected Horizon, is safeguarded using TLS encryption.

Inbound (In) Port: An inbound port is a port another computer uses to connect to the CLSS Gateway to access the gateway functionality; that is, an application on the CLSS Gateway will be actively listening on this port for client connections.

Outbound (Out) Port: The CLSS Gateway uses outbound ports to connect to Internet/CLSS Cloud platform; that is, the services in the cloud will be listening on these ports waiting for a connection from the CLSS Gateway.

By Default, block all inbound and outbound connections and allow only the ports and endpoints listed in the below 2 tables only while using ethernet or Wi-Fi interface:

PORT NUMBER	TYPE	IN / OUT	PURPOSE / REMARKS
443	TCP	Out	Https Communication to CLSS Cloud platform
53	UDP	Out	DNS client to server lookup
2020	TCP	Out	Alarm Transmission

The following are the list of endpoints to communicate to CLSS Cloud platform:

REGION	ALL END-POINTS
Global	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europe	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://t02aprodcloudapp.sentience.honeywel.com
US	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://t01aprodcloudapp.sentience.honeywell.com
US Alarm Transmission	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com https://honrtprodeast.firesignals.us https://honrtprodwest.firesignals.us

CLSS Gateway also offers cloud connectivity over Cellular network. The data sent by the CLSS Gateway is end-to-end encrypted. Also, CLSS uses a more reliable dedicated private APN (Access Point Name) with select operators which provides higher availability along with enhanced security.

SECURE BOOT AND SECURE FIRMWARE UPGRADE

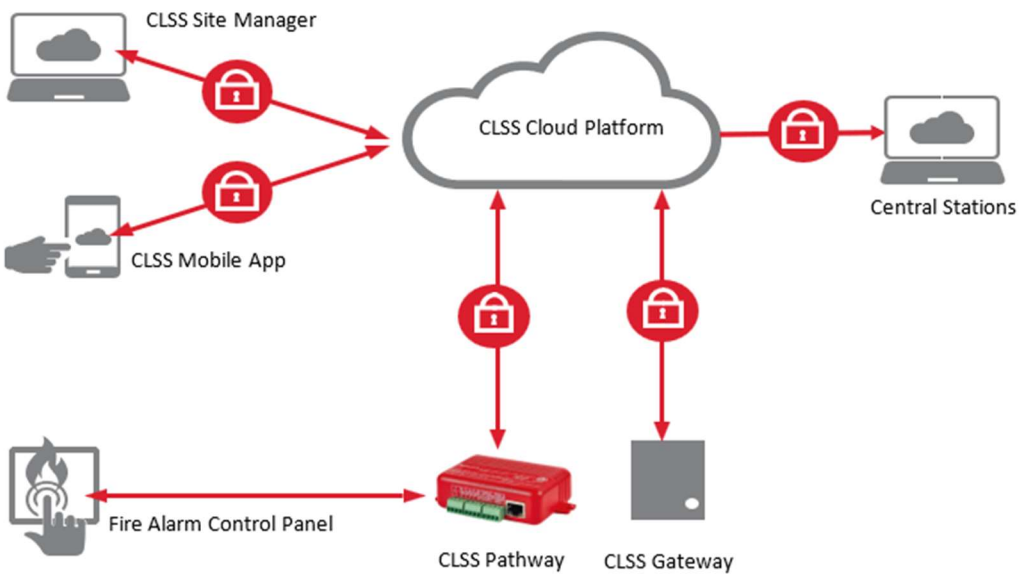
Honeywell utilizes Secure Boot to establish a protected environment for CLSS Gateway firmware updates. Secure Boot involves the process of validating the digital signature of firmware before permitting its execution. This is achieved by ensuring that the firmware's signature is valid and unaltered before it is executed. In the context of secure firmware upgrades, this process extends to validating new firmware before it replaces the currently operational version. Firmware signing involves generating a digital signature for the firmware during its development phase. This signature guarantees the integrity of the firmware and ensures that any unauthorized modifications would be detectable.

Honeywell periodically releases security hotfixes and upgrade packages to the CLS Gateway's firmware. The released packages are encrypted and digitally signed by Honeywell to ensure the confidentiality, integrity, and authenticity (i.e., package originated from Honeywell) of the released package. The CLSS Gateway verifies the signature during secure boot and firmware upgrade processes.

Sensitive details such as private device key(s) are managed via security chips as per commonly accepted security industry practices and recommendations.

CLSS PATHWAY

The CLSS Pathway is a dual-path cellular communicator, which runs on a 24-volt DC power from its panel. It supports both AT&T and Verizon LTE. It transmits data from its fire alarm control panel via CLSS Cloud platform to the central monitoring station.



DATA TRANSMISSION FROM ON-SITE SYSTEM TO CLOUD

For achieving Alarm Transmission, the following data from the on-site CLSS Pathway is transmitted to Central Stations through CLSS Cloud Platform:

- Events, alarms, and troubles received from the fire panel.
- Line Supervision signals (Heartbeat) and Periodic test (when configured) from CLSS Pathway.

SECURING THE DATA TRANSMISSION

To manage the surface area of the system from a security perspective the CLSS Pathway only makes outbound calls, and no inbound communication is accepted. The outbound connections made are limited to TCP for initiating communication with AES 128 data encryption. Additionally, UDP is utilized for outbound connections, enabling the transmission of periodical heartbeats with a proprietary session key.

INFRASTRUCTURE NEEDS FOR DATA TRANSMISSION

The CLSS Pathway establishes a secure connection with the cloud. The CLSS Pathway employs strong communication security, utilizing AES 128 encryption, for functions such as Remote Monitoring, Alarm Transmission (US-Only), and Cloud Connected Horizon.

Outbound (Out) Port: The CLSS Pathway uses outbound ports to connect to Internet/CLSS Cloud platform; that is, the services in the cloud will be listening on these ports waiting for a connection

from the CLSS Pathway. Outbound port requirements are essential specifically for the CLSS Pathway when utilizing IP connections.

By Default, allow the ports listed in the below table only while using ethernet interface in CLSS Pathway:

PORT NUMBER	TYPE	IN / OUT	PURPOSE / REMARKS
9000	TCP	Out	For transmitting alarms from CLSS Pathway to CLSS Cloud platform.
9000	UDP	Out	For sending Heartbeat signals from CLSS Pathway to CLSS Cloud platform.

CLSS SITE MANAGER (WEB APP)

CLSS Site manager is a web application that is used by ESD / System Integrators and technicians to perform back-office administrative and management activities. It provides a consolidated view of their customers' systems. It allows ESDs to onboard their customers' buildings, their users, and technicians as well as, configure access privileges for their technicians.

Communication between CLSS Site Manager and cloud: All communication arising out of the web app from browser to CLSS cloud platform are over HTTPS with TLS 1.2 encrypted tunnel.

CLSS MOBILE APP

CLSS Mobile App is used by technicians to configure CLSS Gateway, CLSS Pathway during installation time and to perform regular walk test functionality of both connected and non-connected devices. The app is also used to generate compliance reports.

Communication between mobile and cloud: All communication arising out of the mobile phone to CLSS cloud platform are over HTTPS with TLS 1.2 encrypted tunnel.

Communication between mobile and CLSS Gateway: Mobile app being used over Secure BLE Link Connection with CLSS Gateway for gateway configuration. The BLE connection works only when the user is near the CLSS Gateway. The security keys required to pair up with CLSS Gateway are accessible only for authorized technicians through cloud platform.

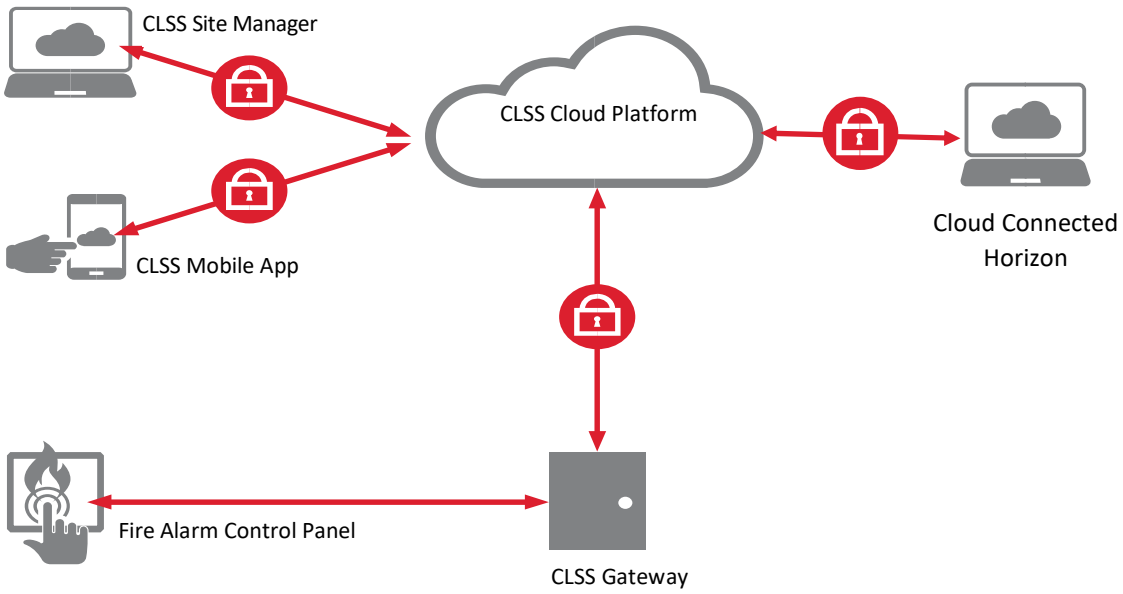
Data stored and exchanged through CLSS Mobile App: The mobile app exchanges details with the CLSS Cloud platform for gateway configuration, for inspection management use cases. The data is not maintained in the mobile device permanently. It is only for temporary use and details are erased from app memory database when data is synced with cloud.

CLSS HORIZON

Horizon is a suite of products that allows users to monitor life safety systems and annunciates events (status change signals) that it receives from the fire system. It has two variants, CLSS LCH (LAN Connected Horizon) is on-prem monitoring solution & communicates through CLSS Gateway and CLSS CCH (Cloud Connected Horizon) is remote monitoring solution & communicates through CLSS Cloud.

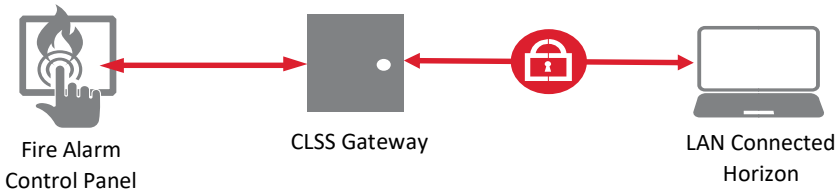
Cloud Connected Horizon:

1. Cloud Connected Horizon establishes HTTPS with TLS 1.2 encrypted channel communication with CLSS Cloud Platform using OAuth2 based Authentication and Role-Based Authorization.
2. Personal data is protected as per GDPR regulatory compliance and Honeywell's privacy standards.

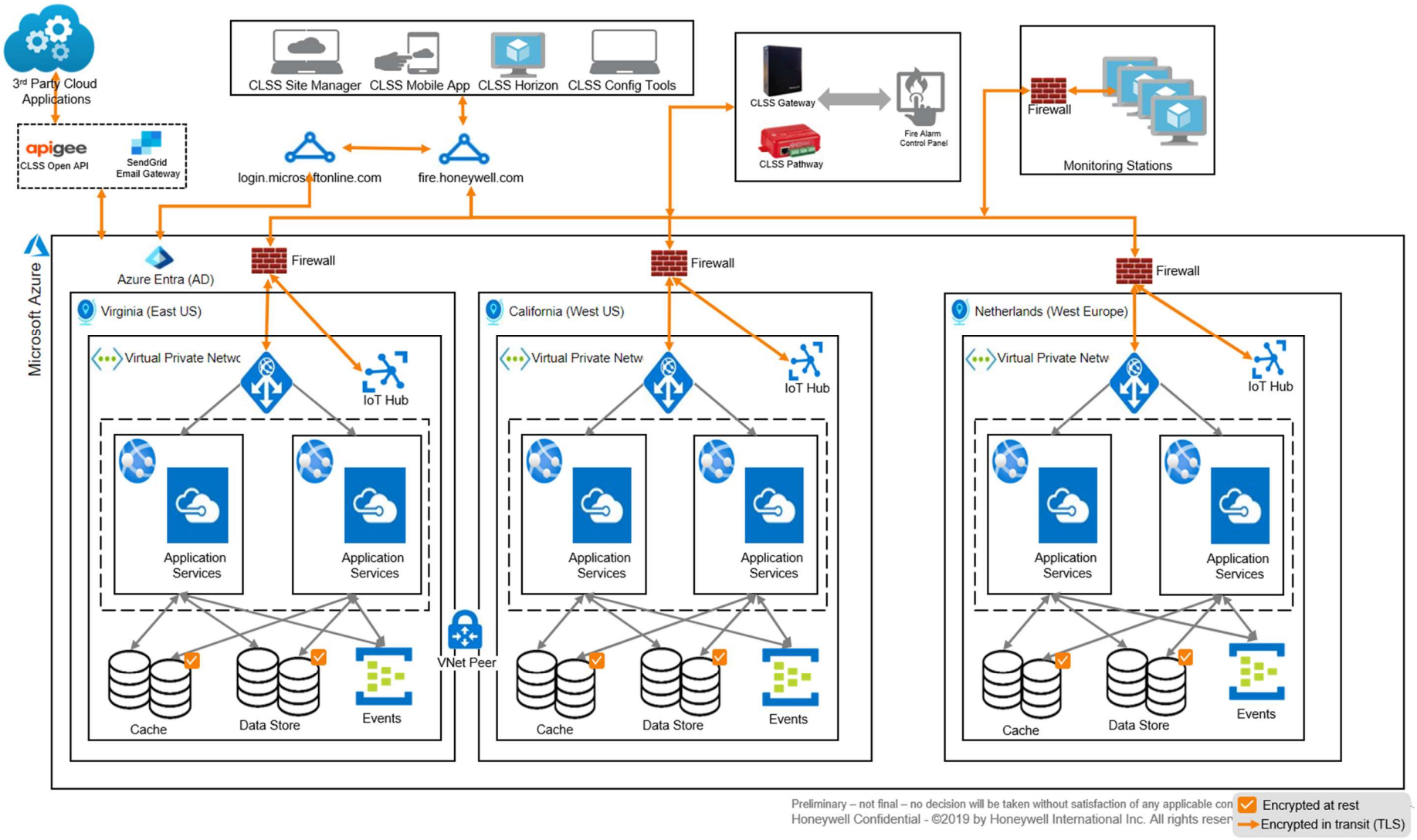


LAN Connected Horizon:

1. LAN Connected Horizon establishes TCP over a TLS 1.2 encrypted channel communication with CLSS Gateway using Certificate based Authentication.
2. LCH login is managed by strong password-based authentication with password masking.



CLSS ARCHITECTURE AND NETWORK DIAGRAM



APPROACH TO CYBER SECURITY IN PRODUCT DEVELOPMENT

All software should incorporate cybersecurity and privacy best practices to minimize cybersecurity issues from occurring. That's why we believe in including security and privacy when the product development process begins. Honeywell Building Technologies' products undergo stringent security reviews and testing before approved for release, no matter where they are manufactured. Our products are assessed against our cyber standards and require approval by our chief technical officer as a part of our standard new product introduction process.

Honeywell follows the Building Security in Maturity Model (BSIMM) framework and ensures Secure Development Life Cycle standards and requirements for products.

The CLSS platform integrates security considerations in all aspects of development, deployment, and risk management. The system was developed using Honeywell's Secure Software Development Lifecycle (SSDLC) which integrates security considerations in all stages from requirements to testing deployment and ongoing operations.

System development covers all aspects from deriving requirements from standards ANSI/ISA 62443 and best practices, secure architecture and design via architectural risk analysis, threat modeling, secure coding guidelines and static and dynamic code analysis, and security testing using manual and automated approaches.

The entire CLSS platform is developed by Honeywell and source code is managed per Honeywell source code management policies. Code reviews are done to detect security loopholes in the source code. Open-source libraries used in the product have gone through security clearance as per Honeywell standard practice.

Static code analysis and binary scanning tools are integrated with the CI/CD (Continuous Integration/ Continuous Delivery) pipeline and executed when each build is generated. The security risks are recorded in JIRA tools with CVSS scoring and remediated per agreed plans to a mandated schedule based on severity.

PENETRATION TESTING AND TEST INITIATION EVENTS

Before any major releases and the introduction of a new version of cloud services to the production environment, thorough penetration testing is executed. A specialized penetration testing team performs security evaluations following recognized frameworks such as OWASP Top 10 to detect vulnerabilities. Additionally, the product infrastructure is assessed in accordance with the guidelines outlined in NIST 800-115. Every identified issue is documented and resolved to ensure effective mitigation.

HONEYWELL SUPPORT AND DEVOPS PROCESS

The entire production system is managed by a 24/7 support team which monitors the infrastructure as well as applications. There are detailed internal policies which cover how we detect, investigate, and respond to security and privacy incidents.

Honeywell use various application diagnostics tools for different parts of the system to monitor health parameters of the system. We keep track of system health (e.g., CPU usage, memory usage, disk IO operations) and any deviation would trigger an alert.

HOW TO REPORT A SECURITY VULNERABILITY?

Honeywell has Product Security Incident Response Team (PSIRT) to monitor and manage incidents and to minimize customers' risk associated with security vulnerabilities by providing timely information, guidance, and remediation of vulnerabilities in our products.

Click **here** to learn more about the Honeywell PSIRT process. To report a potential security vulnerability against any Honeywell product, please follow the instructions **here**.

For more information

www.honeywell.com

Honeywell International Inc.

715 Peachtree St NE,

Atlanta, GA 30308, United States

877.841.2840

THE FUTURE IS WHAT WE MAKE IT

Honeywell