Honeywell

CONNECTED LIFE SAFETY SERVICES (CLSS)

LIVRE BLANC SUR LA CONFIDENTILITE, L'HEBERGEMENT ET LA SECURITE

Janvier 2024

VERSION 2.3

A PROPOS DE CE DOCUMENT

Ce document est principalement conçu pour Connected Life Safety Services (CLSS), les intégrateurs de systèmes et les techniciens soucieux de comprendre la stratégie de sécurité d'Honeywell pour la solution CLSS. Il approfondit également le cadre de sécurité, les processus et les mesures de protection, guidant la façon de configurer en toute sécurité les communicateurs CLSS sur site.

Avertissement :

Le contenu de ce document est fourni à titre d'information uniquement. Le contenu et le produit décrits sont sujets à changement sans préavis. Honeywell ne fait aucune déclaration ou garantie concernant ce document. En aucun cas Honeywell ne sera responsable des omissions ou erreurs techniques ou éditoriales dans ce document, ni des dommages directs ou accessoires, découlant de ou liés à l'utilisation de ce document. Aucune partie de ce document ne peut être reproduite sous quelque forme que ce soit sans l'autorisation écrite préalable d'Honeywell.

Confidentialité :

Honeywell reconnaît l'importance de la confidentialité pour notre entreprise et la confiance de nos clients. Nous nous engageons à traiter de manière responsable toutes les données des clients. Notre politique de confidentialité explique notre approche de la confidentialité et la manière dont les personnes peuvent exercer leurs droits : https://www.honeywell.com/us/en/privacy-statement

En tant qu'organisation axée sur la conquête de la confiance de nos clients et la gestion de leurs actifs d'information avec soin, Honeywell s'efforce de développer une solide culture de conformité et des garanties de sécurité robustes. Nos conditions d'utilisation intègrent des conditions de traitement des données, qui sont publiées à l'adresse suivante : https://trust.honeywellforge.ai/content/dam/forge/en/documents/legalterms-and-conditions-/10_HCE_Data_Processing_Terms_v1.0.pdf

Conditions d’utilisation:

Les conditions d'utilisation des services de sécurité connectés Honeywell (CLSS) sont publiées à l'adresse suivante : https://fire.honeywell.com/#/CLSSPortalTermsAndCondition

Cybersécurité :

Chez Honeywell, la cybersécurité est une priorité pour tous nos produits, logiciels et services. Nous utilisons une approche de bout en bout et un ensemble de pratiques de sécurité pour protéger les clients contre les menaces cyber. Nous comprenons la gravité de ces menaces et notre équipe d'experts met en œuvre des mesures continues pour évaluer, détecter et atténuer les risques. Nous mettons constamment à jour nos produits et nos conseils de sécurité avec les meilleures pratiques. Notre approche holistique et disciplinée se traduit par des produits et des services cyber-résiliants afin de maintenir un système de sécurité des vies sécurisé.

INTRODUCTION AU CLSS

Connected Life Safety Services (CLSS) est une plateforme de bout en bout qui exploite la puissance de la technologie connectée au cloud, plaçant la connectivité au cœur de la sécurité des vies. Elle permet aux intégrateurs de systèmes et aux gestionnaires d'installations de fournir un service de sécurité incendie amélioré, tout en maximisant les gains de performance offerts par les systèmes de détection et d'alarme incendie de confiance d'Honeywell.

LA PLATEFORME CLOUD CLSS

La plateforme cloud Connected Life Safety Services (CLSS) contient divers micro-services pour prendre en charge les fonctionnalités de la passerelle CLSS, de CLSS Pathway, de l'application mobile et de l'application Web. Elle est sécurisée, évolutive, construite selon des normes sur la plateforme de gestion d'entreprise Honeywell Forge. Le déploiement basé sur le cloud est géré selon le cadre de conformité unifié d'Honeywell, aligné sur les principaux cadres de sécurité informatique, notamment NIST SP 800-171 et ISO 27001. Toutes les communications internes entre les différents services cloud utilisent HTTPS pour l'intégrité et la confidentialité au sein du cloud.

MESURES DE SECURITE DE L'INFRASTRUCTURE CLOUD

- **CONNEXION ET CONTRÔLE D'ACCÈS :**

  - Une authentification forte basée sur les identifiants et les mots de passe est utilisée pour les applications mobiles et Web.
  - Des mécanismes de contrôle d'accès basés sur les rôles sont employés pour faire respecter les privilèges d'accès pour les différents ensembles de données.
  - Des mesures d'authentification et d'autorisation robustes sont mises en œuvre au niveau de l'application pour contrôler étroitement l'accès à toutes les données de l'application.

- **PARE-FEU :**

  - La sécurité périmétrique est assurée par un pare-feu grâce à l'IPS/IDS et l'inspection des paquets.
  - Un pare-feu d'applications Web, communément appelé, Web Application Firewall (WAF) est activé pour les applications CLSS. Les WAF offrent une protection contre les cyberattaques telles que les injections SQL, le cross-site Scripting, les téléchargements de programmes malveillants, les attaques par déni de service à l'application,etc.
  - Le durcissement de la sécurité de tous les serveurs est segmenté via des réseaux virtuels et des serveurs virtuels.
  - Toutes les machines virtuelles cloud CLSS sont protégées par un anti-logiciel malveillant.

- **LA SECURITE AU NIVEAU DU TRANSPORT :**

  - Au niveau du transport, toutes les données sont chiffrées. Toutes les connexions sont établies avec TLS, qui applique TLS1.2 comme minimum.
  ▪ TLS entre les applications clientes et la passerelle d'application Microsoft Azure CLSS
  ▪ TLS entre les services d'application principaux et Microsoft Azure IoT et Microsoft Entra ID
  ▪ TLS entre les services d'application principaux et les applications tierces (SendGrid, APIGee).

- **CHIFFREMENT :**

  - Les données sensibles comme les jetons de sécurité et les clés cryptographiques sont gérées via le coffre-fort de clés Azure (Azure key vault). Le coffre-fort de clés Azure fournit des modules de sécurité matériels validés -Hardware Security Modules- (HSM) FIPS 140-2 niveau 2 pour stocker les données sensibles.
  - Toutes les données sont chiffrées au repos sur Microsoft SQL DB et Azure Cosmos DB à l'aide du chiffrement AES-256.
  - Les données des disques gérés par Microsoft Azure sont chiffrées à l'aide du chiffrement AES-256 et sont conformes à la norme FIPS 140-2.
  - Les mots de passe sont gérés dans Microsoft Entra ID. Les mots de passe sont hachés à l'aide de la fonction Password-Based Key Derivation Function 2 (PBKDF2), en utilisant HMACSHA256 à 1 000 itérations. Pour plus d'informations, veuillez consulter le site Web.
  - L'accès au niveau de l'administrateur système est limité à l'équipe des opérations numériques autorisée d'Honeywell. Des sauvegardes régulières sont effectuées pour restaurer le système à son état normal en cas de perte accidentelle. Au repos, toutes les données sont chiffrées à l'aide de SSE (Solid State Encryption).

- **AUTRES MESURES DE SECURITE :**

  - Processus standard d'application périodique des correctifs de sécurité avec des provisions pour des traitements prioritaires en fonction des risques.
  - La plateforme cloud CLSS est construite sur la plateforme Honeywell Forge et hébergée sur le cloud Microsoft Azure. La plateforme Honeywell Forge est auditée selon SOC2 Type 1. Le cloud Microsoft Azure est certifié SOC1 Type2, SOC2 Type2, ISO27001. Pour une liste complète, veuillez consulter le site Web.

DONNEES PERSONNELLES

Toutes les informations d'identification personnelle - Personally Identifiable Information - (PII) sont protégées par le chiffrement lors du stockage. La protection des données personnelles est conforme aux exigences réglementaires du RGPD et aux normes de confidentialité d'Honeywell. Honeywell restreint la collecte et le traitement des données personnelles au minimum requis pour atteindre des objectifs commerciaux valables.

LES COMMUNICATEURS CLSS

Les communicateurs CLSS servent de pont entre le Système de Sécurité Incendie (SSI) et la plateforme cloud CLSS.

LA PASSERELLE CLSS

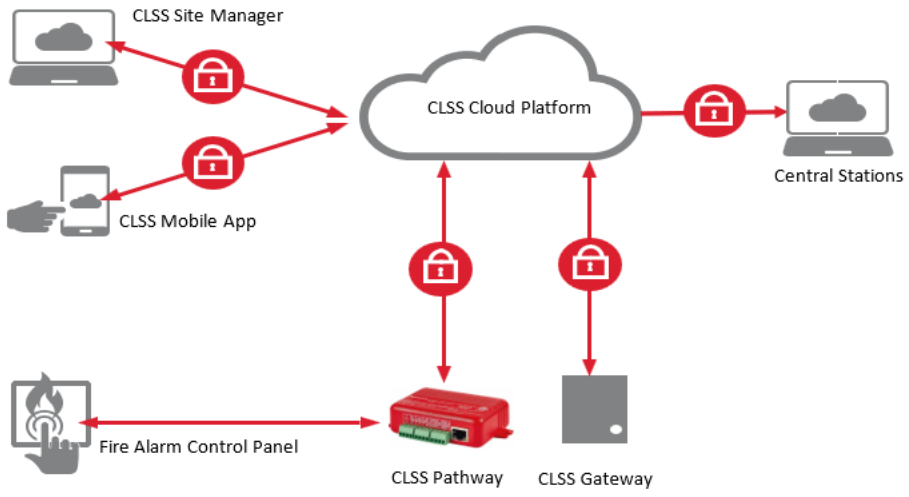
La passerelle CLSS offre un moyen de connecter de manière sécurisée le SSI sur site au cloud et fournit un chemin unique du site au cloud, s'assurant que tous les services et applications cloud CLSS utilisent la même méthode auditée et surveillée pour recevoir les événements et envoyer des commandes au SSI sur site via la passerelle CLSS.

TRANSMISSION DES DONNEES DU SYSTEME SUR SITE AU CLOUD

Pour atteindre les cas d'utilisation des fonctionnalités de l'application mobile CLSS et de l'application Web (Tests de conformité et Tableau de bord des sites), les données suivantes provenant de la passerelle CLSS sur site sont transmises au cloud :

- Inventaire des appareils reçu du panneau incendie.
- Événements, alarmes et défauts reçus du panneau incendie.
- Événements, alarmes et défauts générés par la passerelle CLSS.
- Journaux d'audit de la passerelle CLSS avec horodatage.

L'inventaire des appareils contient tous les appareils (détecteurs, modules, etc.) y compris le Système de Détection Incendie (SDI) et le Centralisateur de Mise en Sécurité Incendie (CMSI) du SSI.



SECURISATION DE LA TRANSMISSION DES DONNEES

Pour gérer la surface d'attaque du système d'un point de vue sécurité, le connecteur cloud de la passerelle CLSS n'effectue que des appels sortants, et aucune communication entrante n'est acceptée. Les connexions sortantes effectuées se limitent à HTTPS pour initier la communication, puis à AMQP sur HTTPS pour la messagerie avec le

chiffrement TLS1.2 et versions ultérieures.

L'authentification basée sur les certificats est utilisée entre la passerelle CLSS sur site et la plateforme cloud CLSS.

L'INFRASTRUCTURE REQUISE POUR LA TRANSMISSION DES DONNEES

La passerelle CLSS sur site établit une connexion sécurisée avec le cloud. La passerelle CLSS utilise une sécurité de communication robuste, utilisant le chiffrement HTTPS/TLS, pour des fonctions telles que la surveillance à distance, la transmission d'alarmes à une centrale (États-Unis uniquement), la maintenance digitalisée et Horizon Connected Cloud. La communication entrante de la passerelle CLSS vers les applications sur site, comme LAN Connected Horizon, est sécurisée à l'aide du chiffrement TLS.

Port entrant (In) : Un port entrant est un port qu'un autre ordinateur utilise pour se connecter à la passerelle CLSS afin d'accéder aux fonctionnalités de la passerelle ; c'est-à-dire qu'une application sur la passerelle CLSS sera activement à l'écoute sur ce port pour les connexions des clients.

Port sortant (Out) : La passerelle CLSS utilise des ports sortants pour se connecter à Internet/la plateforme cloud CLSS ; c'est-à-dire que les services dans le cloud seront à l'écoute sur ces ports en attendant une connexion de la passerelle CLSS.

Par défaut, bloquez toutes les connexions entrantes et sortantes et autorisez uniquement les ports et points de terminaison (End-Point) répertoriés dans les 2 tableaux ci-dessous lors de l'utilisation de l'interface Ethernet ou Wi-Fi :

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

Voici la liste des points de terminaison permettant de communiquer avec la plateforme cloud CLSS :

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.honeywell.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

La passerelle CLSS offre également une connectivité cloud via le réseau cellulaire. Les données envoyées par la passerelle CLSS sont chiffrées de bout en bout. De plus, CLSS utilise un APN (Access Point Name) privé dédié plus fiable avec des opérateurs sélectionnés, offrant une plus grande disponibilité ainsi qu'une sécurité renforcée.

DEMARAGE SECURISE ET MISE A JOUR SECURISEE DU MICROLOGICIEL

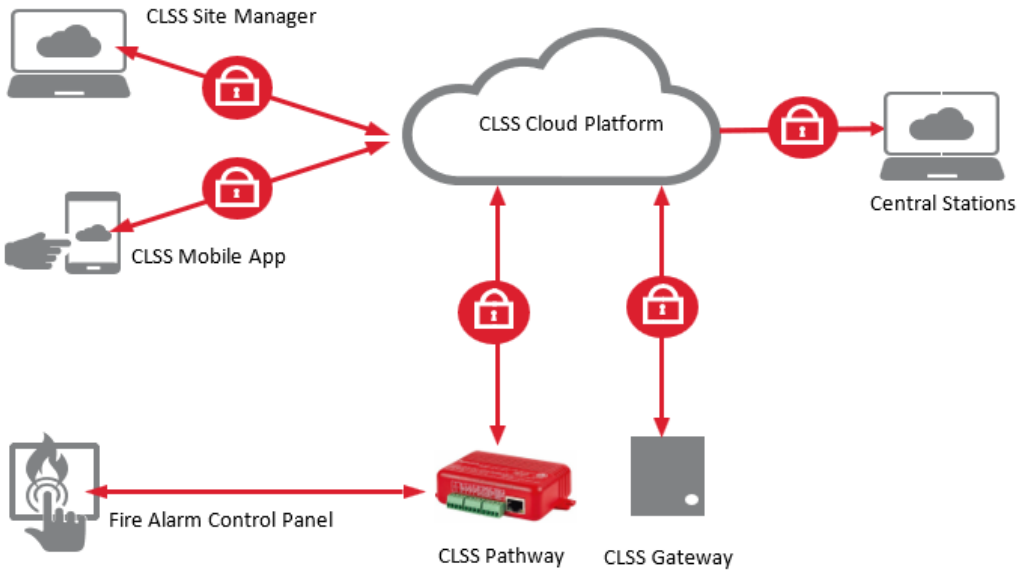
Honeywell utilise le démarrage sécurisé pour établir un environnement protégé pour les mises à jour du micrologiciel de la passerelle CLSS. Le démarrage sécurisé implique le processus de validation de la signature numérique du micrologiciel avant d'autoriser son exécution. Cela se fait en s'assurant que la signature du micrologiciel est valide et intacte avant son exécution. Dans le cadre des mises à jour sécurisées du micrologiciel, ce processus s'étend à la validation du nouveau micrologiciel avant qu'il ne remplace la version actuellement opérationnelle. La signature du micrologiciel implique la génération d'une signature numérique pour le micrologiciel pendant sa phase de développement. Cette signature garantit l'intégrité du micrologiciel et s'assure que toute modification non autorisée serait détectable.

Honeywell publie périodiquement des correctifs de sécurité et des packages de mise à jour pour le micrologiciel de la passerelle CLSS. Les packages publiés sont chiffrés et signés numériquement par Honeywell pour assurer la confidentialité, l'intégrité et l'authenticité (c'est-à-dire que le package provient d'Honeywell) du package publié. La passerelle CLSS vérifie la signature pendant les processus de démarrage sécurisé et de mise à jour du micrologiciel.

Les détails sensibles tels que la(les) clé(s) de périphérique privée(s) sont gérés via des puces de sécurité conformément aux pratiques et recommandations de sécurité généralement acceptées dans l'industrie.

CLSS PATHWAY

Le CLSS Pathway est un communicateur cellulaire à double voie, fonctionnant sur une alimentation CC de 24 volts provenant d'une centrale à laquelle il est également câblé via contacts secs. Il prend en charge à la fois deux opérateurs locaux différents. Il transmet les données d'une centrale (par exemple une centrale d'alarme incendie) via la plateforme CLSS Cloud à un Télésurveilleur.



TRANSMISSION DE DONNEES DU SYSTEME SUR SITE VERS LE CLOUD

Pour réaliser la transmission d'alarme, les données suivantes du CLSS Pathway sur site sont transmises aux Télésuveilleurs via la Plateforme CLSS Cloud :

- Événements, alarmes et problèmes reçus du panneau incendie.
- Signaux de supervision de ligne (Heartbeat) et test périodique (lorsque configuré) du CLSS Pathway.

SECURISATION DE LA TRANSMISSION DE DONNEES

Pour gérer la surface du système d'un point de vue sécurité, le CLSS Pathway n'effectue que des appels sortants, et aucune communication entrante n'est acceptée. Les connexions sortantes sont limitées au TCP pour initier la communication avec un chiffrement de données AES 128. De plus, l'UDP est utilisé pour les connexions sortantes, permettant la transmission de battements de cœur périodiques avec une clé de session propriétaire.

LES BESOINS EN INFRASTRUCTURES POUR LA TRANSMISSION DE DONNEES

Le CLSS Pathway établit une connexion sécurisée avec le cloud. Le CLSS Pathway emploie une sécurité de communication forte, utilisant le chiffrement AES 128, pour des fonctions telles que la Surveillance à Distance, la Transmission d'Alarme aux Pompiers (États-Unis uniquement), et le Cloud Connected Horizon.

Port Sortant (Out) : Le CLSS Pathway utilise des ports sortants pour se connecter à Internet/plateforme CLSS Cloud ; c'est-à-dire que les services dans le cloud seront à l'écoute sur ces ports en attendant une connexion du CLSS Pathway. Les exigences de port sortant sont essentielles spécifiquement pour le CLSS Pathway lors de l'utilisation de connexions IP.
Par défaut, autorisez uniquement les ports listés dans le tableau ci-dessous lors de l'utilisation de l'interface Ethernet du CLSS Pathway :

NUMERO DE PORT	TYPE	ENTREE (IN)/ SORTIE (OUT)	OBJECTIF/ REMARQUES
9000	TCP	Out	Pour transmettre les alarmes du CLSS Pathway vers la plateforme CLSS Cloud.
9000	UDP	Out	Pour envoyer les signaux “Heartbeat” du CLSS Pathway vers la plateforme CLSS Cloud.

LE SITE CLSS (LA PLATEFORME WEB CLSS)

La plateforme web CLSS est une application web utilisée par les mainteneurs / Intégrateurs de Systèmes et les techniciens pour effectuer des activités administratives et de gestion en back-office. Il fournit une vue consolidée des systèmes de leurs clients. Il permet aux mainteneurs d'intégrer les bâtiments de leurs clients, leurs utilisateurs et techniciens, ainsi que de configurer les privilèges d'accès pour leurs techniciens.
Communication entre la plateforme web CLSS et le cloud : Toutes les communications issues de l'application web du navigateur vers la plateforme cloud CLSS se font via HTTPS avec un tunnel chiffré TLS 1.2.

L'APPLICATION MOBILE CLSS

L'application mobile CLSS est utilisée par les techniciens pour configurer la Passerelle CLSS, le CLSS Pathway pendant l'installation et pour effectuer des tests de fonctionnement réguliers des appareils connectés et non connectés. L'application est également utilisée pour générer des rapports de conformité (rapport de maintenance).

Communication entre mobile et cloud : Toutes les communications issues du téléphone mobile vers la plateforme cloud CLSS se font via HTTPS avec un tunnel chiffré TLS 1.2.

Communication entre mobile et Passerelle CLSS : L'application mobile est utilisée via une connexion Bluetooth (BLE) sécurisée avec la Passerelle CLSS pour la configuration de la passerelle. La connexion BLE ne fonctionne que lorsque l'utilisateur est à proximité de la Passerelle CLSS. Les clés de sécurité nécessaires pour s'associer à la Passerelle CLSS ne sont accessibles qu'aux techniciens autorisés via la plateforme cloud.

Données stockées et échangées via l'application mobile CLSS : L'application mobile échange des détails avec la plateforme CLSS Cloud pour la configuration de la passerelle, pour les cas d'utilisation de la gestion des inspections. Les données ne sont pas conservées de manière permanente dans l'appareil mobile. Elles sont uniquement pour un usage temporaire et les détails sont effacés de la base de données de mémoire de l'application lorsque les données sont synchronisées avec le cloud.

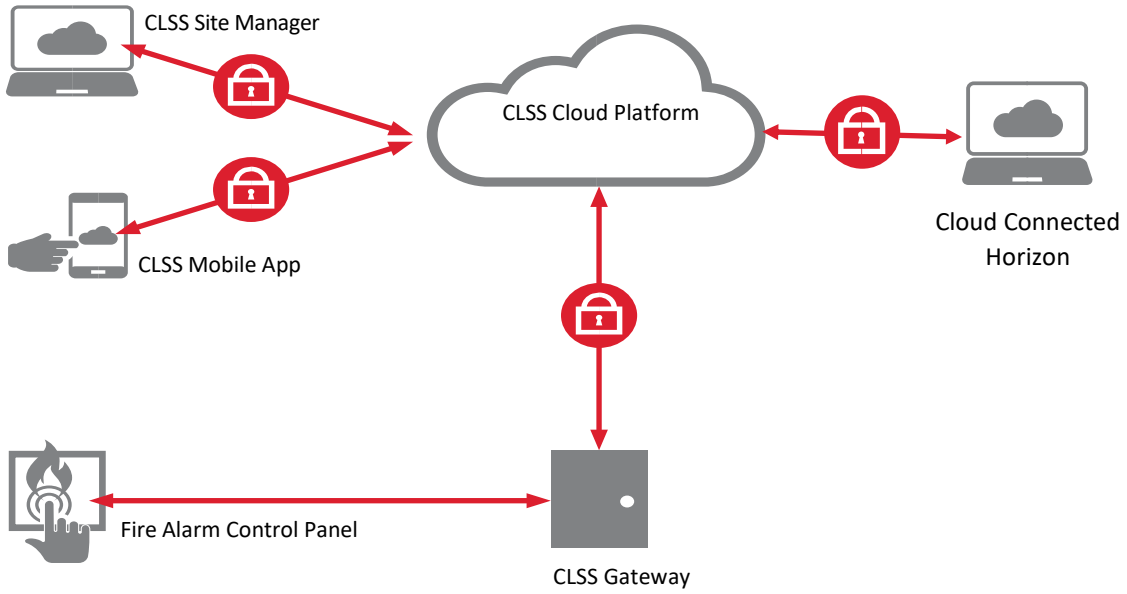
CLSS HORIZON

Horizon est une suite de produits qui permet aux utilisateurs de surveiller les Systèmes de Sécurité Incendie et d'annoncer les événements (signaux de changement d'état) qu'il reçoit du système d'incendie. Il existe deux variantes : CLSS LCH (LAN Connected Horizon) est une solution de surveillance locale qui communique via la passerelle CLSS, et CLSS CCH (Cloud Connected Horizon) est une solution de surveillance à distance qui communique via le cloud CLSS.

Cloud Connected Horizon :

1. Cloud Connected Horizon établit une communication par canal chiffré HTTPS avec TLS 1.2 avec la plateforme cloud CLSS en utilisant l'authentification basée sur OAuth2 et l'autorisation basée sur les rôles.

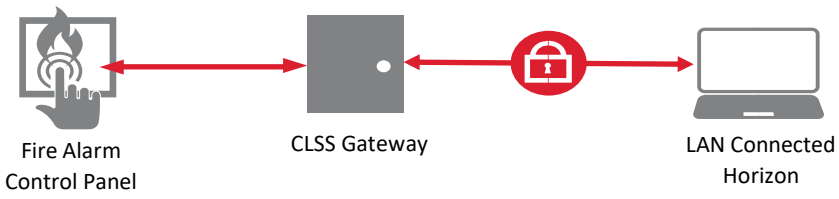
2. Les données personnelles sont protégées conformément à la réglementation RGPD et aux normes de confidentialité d'Honeywell.



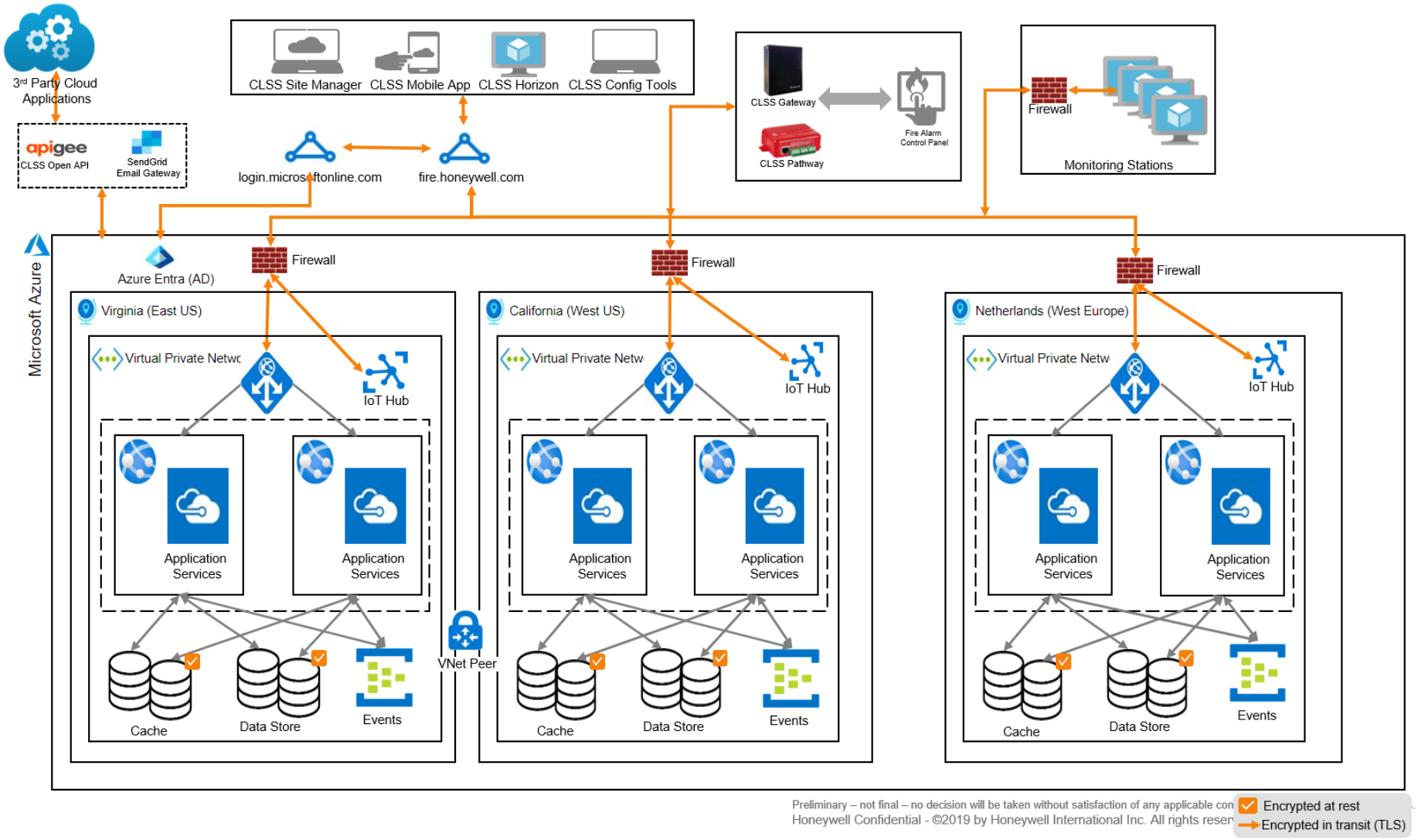
LAN Connected Horizon:

1. LAN Connected Horizon établit une communication par canal chiffré TCP avec TLS 1.2 avec la passerelle CLSS en utilisant une authentification basée sur les certificats.

2. La connexion à LCH est gérée par une authentification forte basée sur les mots de passe avec masquage du mot de passe.



L'ARCHITECTURE CLSS LE DIAGRAME DE RESEAU



APPROCHE DE LA CYBERSECURITE DANS LE DEVELOPPEMENT DE PRODUITS

Tous les logiciels doivent intégrer les meilleures pratiques en matière de cybersécurité et de confidentialité pour minimiser les problèmes de cybersécurité. C'est pourquoi nous croyons qu'il faut inclure la sécurité et la confidentialité dès le début du processus de développement de produits. Les produits de Honeywell Building Automation subissent des examens et des tests de sécurité rigoureux avant d'être approuvés pour la mise sur le marché, quel que soit leur lieu de fabrication. Nos produits sont évalués par rapport à nos normes de cybersécurité et doivent être approuvés par notre directeur technique dans le cadre de notre processus standard d'introduction de nouveaux produits.

Honeywell suit le modèle de maturité de la sécurité intégrée - Building Security in Maturity Model (BSIMM) - et s'assure que les normes et exigences du cycle de développement sécurisé sont respectées pour les produits.

La plateforme CLSS intègre les considérations de sécurité dans tous les aspects du développement, du déploiement et de la gestion des risques. Le système a été développé à l'aide du cycle de développement de logiciels sécurisé - Secure Software Development Lifecycle (SSDLC) - d'Honeywell, qui intègre les considérations de sécurité à toutes les étapes, des exigences aux tests, au déploiement et aux opérations continues.

Le développement du système couvre tous les aspects, de la dérivation des exigences à partir des normes ANSI/ISA 62443 et des meilleures pratiques, à l'architecture et à la conception sécurisées via l'analyse des risques architecturaux, la modélisation des menaces, les lignes directrices de codage sécurisé et l'analyse statique et dynamique du code, ainsi que les tests de sécurité utilisant des approches manuelles et automatisées.

L'ensemble de la plateforme CLSS est développé par Honeywell et le code source est géré conformément aux politiques de gestion du code source d'Honeywell. Des revues de code sont effectuées pour détecter les failles de sécurité dans le code source. Les bibliothèques open source utilisées dans le produit ont fait l'objet d'une autorisation de sécurité selon les pratiques standard d'Honeywell.

L'analyse statique du code et les outils d'analyse binaire sont intégrés dans le pipeline CI/CD (Continuous Integration/Continuous Delivery) et exécutés lors de chaque génération de build. Les risques de sécurité sont enregistrés dans les outils JIRA avec une notation CVSS et corrigés selon un calendrier établi en fonction de la gravité.

TESTS D'INTRUSION ET EVENEMENT DE TEST D'INITIALISATION

Avant tout lancement majeur et l'introduction d'une nouvelle version des services cloud dans l'environnement de production, des tests d'intrusion approfondis sont exécutés. Une équipe spécialisée dans les tests d'intrusion effectue des évaluations de sécurité suivant des cadres reconnus comme OWASP Top 10 pour détecter les vulnérabilités. De plus, l'infrastructure du produit est évaluée conformément aux directives décrites dans la norme NIST 800-115. Chaque problème identifié est documenté et résolu pour assurer une atténuation efficace.

SUPPORT HONEYWELL ET PROCESS DEVOPS

L'ensemble du système de production est géré par une équipe d'assistance 24h/24 et 7j/7 qui surveille l'infrastructure ainsi que les applications. Il existe des politiques internes détaillées qui couvrent la manière dont nous détectons, enquêtons et répondons aux incidents de sécurité et de confidentialité.

Honeywell utilise divers outils de diagnostic d'applications pour différentes parties du système afin de surveiller les paramètres de santé du système. Nous suivons la santé du système (utilisation du CPU, utilisation de la mémoire, opérations d'Entrée/Sortie - I/O - sur disque) et tout écart déclencherait une alerte.

COMMENT SIGNALER UNE VULNÉRABILITÉ DE SÉCURITÉ ?

Honeywell dispose d'une équipe d'intervention en cas d'incident de sécurité des produits - Product Security Incident Response Team (PSIRT) - pour surveiller et gérer les incidents et minimiser les risques des clients liés aux vulnérabilités de sécurité en fournissant des informations, des conseils et des correctifs en temps opportun.

Cliquez ici pour en savoir plus sur le processus PSIRT d'Honeywell. Pour signaler une éventuelle vulnérabilité de sécurité sur un produit Honeywell, veuillez suivre les instructions ici.

Pour plus d'informations

www.honeywell.com

Honeywell International Inc.

715 Peachtree St NE,

Atlanta, GA 30308, United States

877.841.2840

CLSS – Livre blanc cybersécurité | Rev 03 | 01/2024 www.honeywell.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell