OPERATIONAL INTELLIGENCE CYBER SECURITY

Brochure

Honeywell

CYBER SECURITY INFORMATION

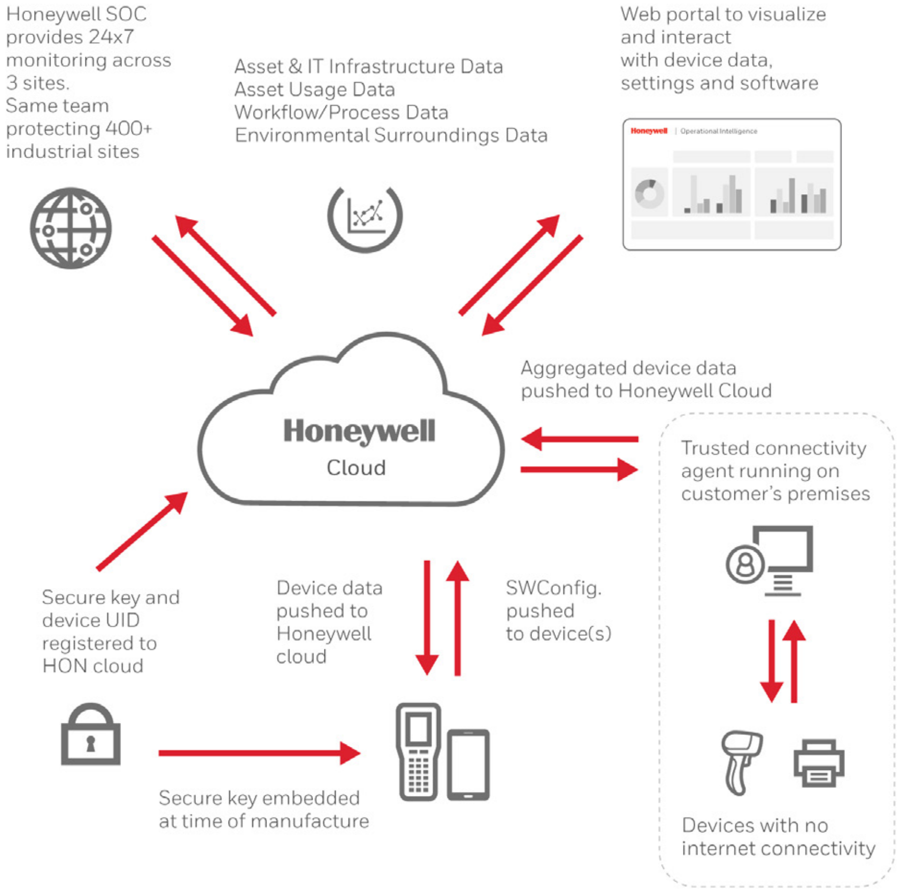
Honeywell's Operational Intelligence is backed by the Honeywell Product Cybersecurity platform. Our security platform is based on knowledge that in today's connected world, threat creators are working around the clock to identify vulnerabilities and ultimately harm your business. When you choose Honeywell, you'll know our products and solutions are secure by design, informed by intelligence and defended with vigilance so you can operate our solutions with confidence that both your data and operations are secure.

SECURE BY DESIGN

Honeywell's Secure System Design Lifecycle (SSDL) drives the development of our products and solutions. The Honeywell SSDL gathers critical information from numerous sources, including current cybersecurity standards like the ISA 62443. This information is used to create security requirements that products must meet from their inception. Our security efforts also include detailed architectural analysis, code review and security testing, with each iteration building on affording you the benefit of current security fixes and patches.

Honeywell Operational Intelligence cloud provider, Microsoft Azure, adheres to standards from organizations such as the Cloud Security Alliance and the European Network and Information Security Agency to ensure confidentiality, integrity and availability of your data on our platform.

Source: https://docs.microsoft.com/en-us/compliance/regulatory/offering-enisa


Honeywell SOC provides 24x7 monitoring across 3 sites. Same team protecting 400+ industrial sites
Asset & IT Infrastructure Data
Asset Usage Data
Workflow/Process Data
Environmental Surroundings Data
Web portal to visualize and interact with device data, settings and software
Honeywell
Cloud
Aggregated device data pushed to Honeywell Cloud
Trusted connectivity agent running on customer's premises
Secure key and device UID registered to HON cloud
Device data pushed to Honeywell cloud
SWConfig. pushed to device(s)
Secure key embedded at time of manufacture
Devices with no internet connectivity

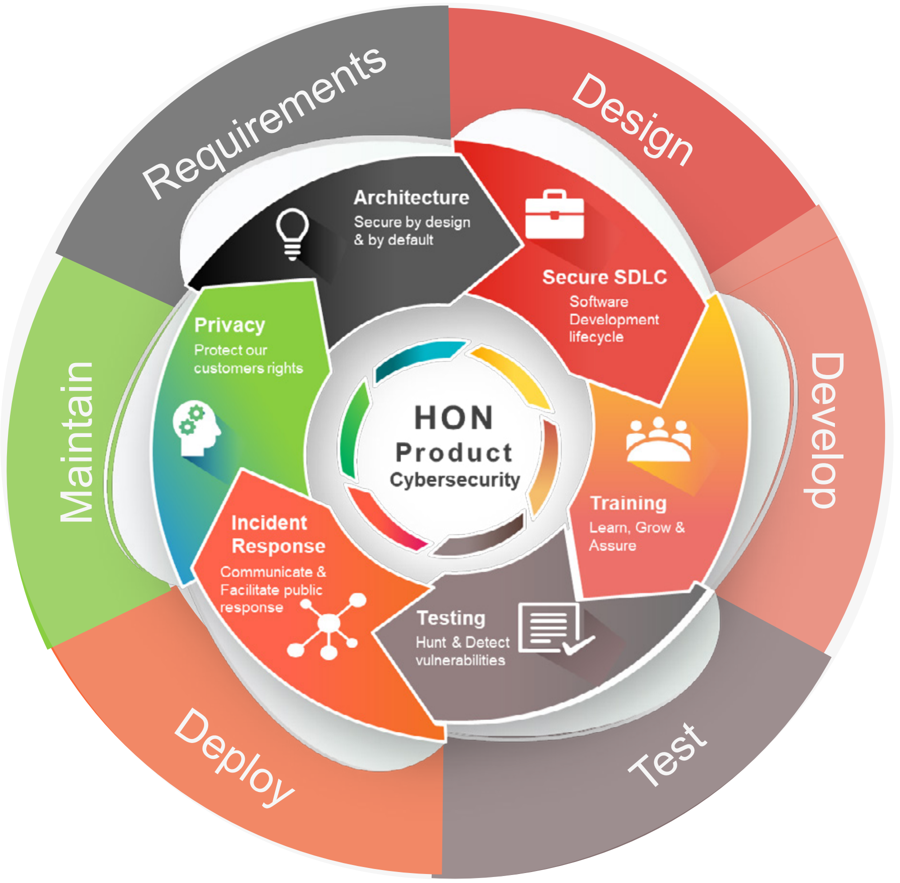
Honeywell has worked to ensure that we have minimized the attack surface area, established secure defaults from the very start, and have worked hard on defending with depth our cloud infrastructure. Honeywell treats the security of Honeywell Operational Intelligence as a foundational feature that is built into every other functionality of our offering. Continuously working and evolving our DevSecOps pipeline, while aligning our cybersecurity program to the Building Security in Maturity Model (BSIMM v12) framework is an organizational endeavor Honeywell takes seriously.

Honeywell Operational intelligence is hosted on the Microsoft Azure platform. Security controls around business continuity and disaster recovery have been built into the platform from its inception. As the platform is easily scalable, resilient and portable, our infrastructure providers ensure that they meet the latest advancements in cyber security protections for customer data.

Microsoft Azure Trust center - https://azure.microsoft.com/en-us/overview/trusted-cloud/

Honeywell has been working to ensure a cohesive DevSecOps strategy throughout our software development lifecycle and` Honeywell Operational Intelligence inherits controls that have made Honeywell a trusted partner for governmental organizations and customers in the national security and critical infrastructure domains.

Role based access controls and workflows have been well defined and architected to ensure auditing around actions taken by users throughout the entire platform. Tenant level and permissions are controlled at the customer level with permissions for each feature layer.


Requirements
Design
Develop
Test
Deploy
Maintain
Architecture
Secure by design & by default
Secure SDLC
Software Development lifecycle
Training
Learn, Grow & Assure
Testing
Hunt & Detect vulnerabilities
Incident Response
Communicate & Facilitate public response
Privacy
Protect our customers rights
HON Product Cybersecurity

We took a holistic approach to securing the solution as a cloud platform and have gone through our Secure Software Development Lifecycle to ensure security requirements, threat modeling, penetration testing have all been baked in from the very beginning. Our privacy impact assessment process has been closely aligned with regulatory requirements such as GDPR or CCPA to ensure compliance and best practices for securely storing data. Honeywell has taken care to ensure no sensitive or Personally Identifiable Information is stored on our cloud infrastructure.

SECURE BY DESIGN

- Commitment to Honeywell's

  Secure System Design Lifecycle (SSDL)
- Adherence to standards like ISA 62443
- Solution architectural analysis, code review and security testing

OUR MISSION & VISION

- **Build better products through secure by design & by default software development practices.**
- Ensure Honeywell products protect our customer's privacy consistent with our policies and regulations
- **Manage cyber issues effectively** and with transparency.

HOW:

- **Design in Security** – Incorporate best practices from ISA 62443, NIST, ISO 27001.
- **Never stop training:** Always vigilant and keeping our cyber teams and Developers trained on the latest risks and mitigations
- **Testing** - Our software goes through robust security testing during development, and at the product & program level.
- **Maintain** via patches & enhancements – regularly deploying updates as new protections and controls become available.

INFORMED BY INTELLIGENCE

Honeywell's large footprint in multiple industries gives us a broad view of emerging cybersecurity threats in their earliest stages. This allows us to identify issues, develop countermeasures and deploy them to our customers earlier than the competition. Also, Honeywell's size and strength allows us to leverage the broad investment in security across our enterprise.

Honeywell is involved in 70 industry sectors often involving critical infrastructure and national security. Honeywell Operational intelligence has inherited the body of knowledge and work being done in cybersecurity that Honeywell has at its disposal from more than 300 dedicated cybersecurity professionals that work across our company.

Honeywell Operational Intelligence has been put through its paces. A group of dedicated white-hat penetration testers (OSCE/OSCP certified), completely independent from the engineering team continuously tests our solution to ensure we have the strictest standard for defense.

- Analysts work 24/7 to identify and report risks
- Expedited delivery of patches for specific threats
- Updates issued on a consistent basis

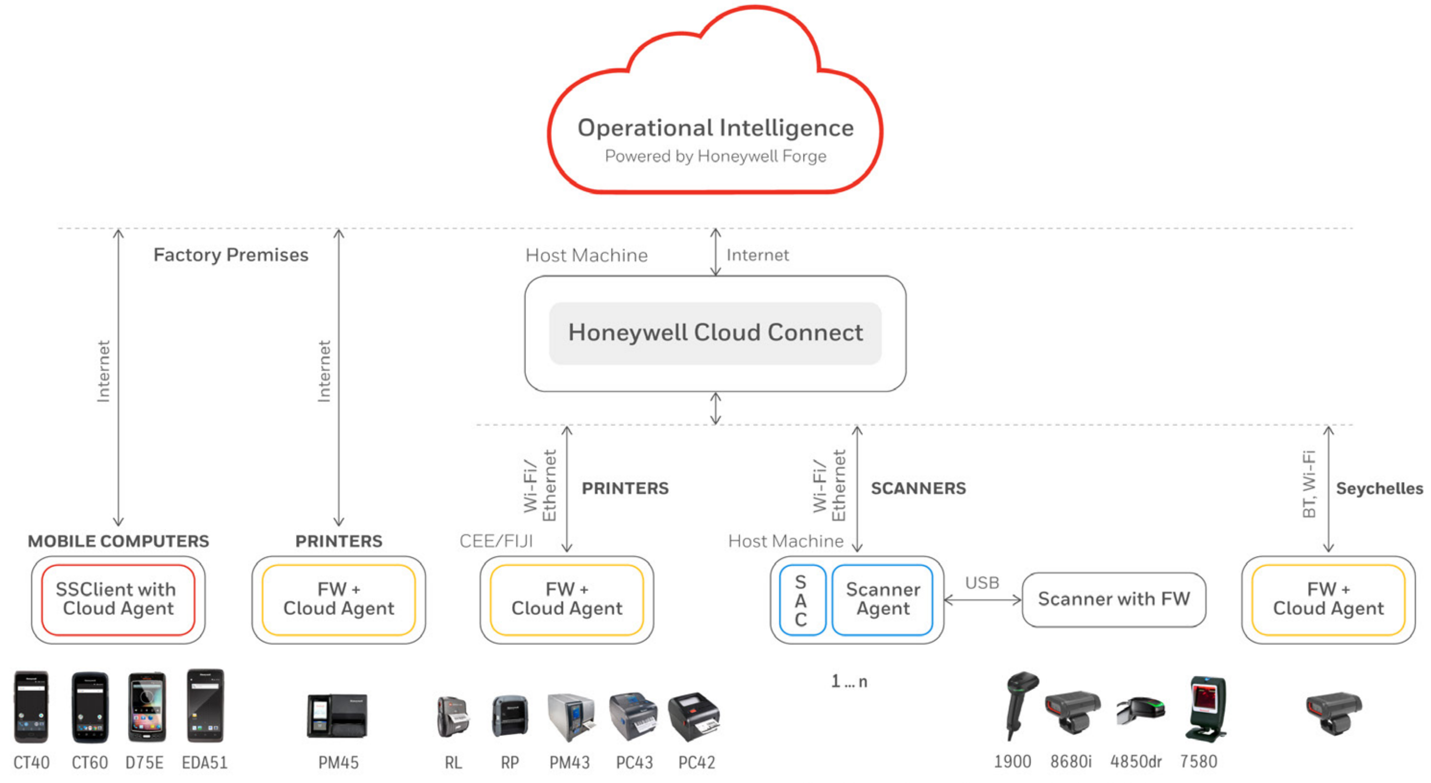
DEFENDED WITH VIGILANCE

To maintain the highest level of vigilance, Honeywell employs a team of analysts working diligently to identify and report potential security risks. To stay ahead, you'll receive security patches on a consistent basis, based on updates from Honeywell and our partners. With this continual monitoring of systems' security, you can be confident Honeywell is in-the-know and stands ready to partner with you in the protection of your critical resources and data.

Honeywell Operational Intelligence is constantly being monitored by our team of professionals using up-to-the-minute centralized logging and alerting methodologies to ensure that you have constant access to your critical data. Additionally our offering relies strictly on encrypted protocols to transmit data, and Transparent Data Encryption to store data that is encrypted. These two methodologies enable Multi-Tenancy and segmentation of your data.

- Continuous testing of our solution
- 300 dedicated security professionals
- Security partnerships with Intel, Qualcomm and Google

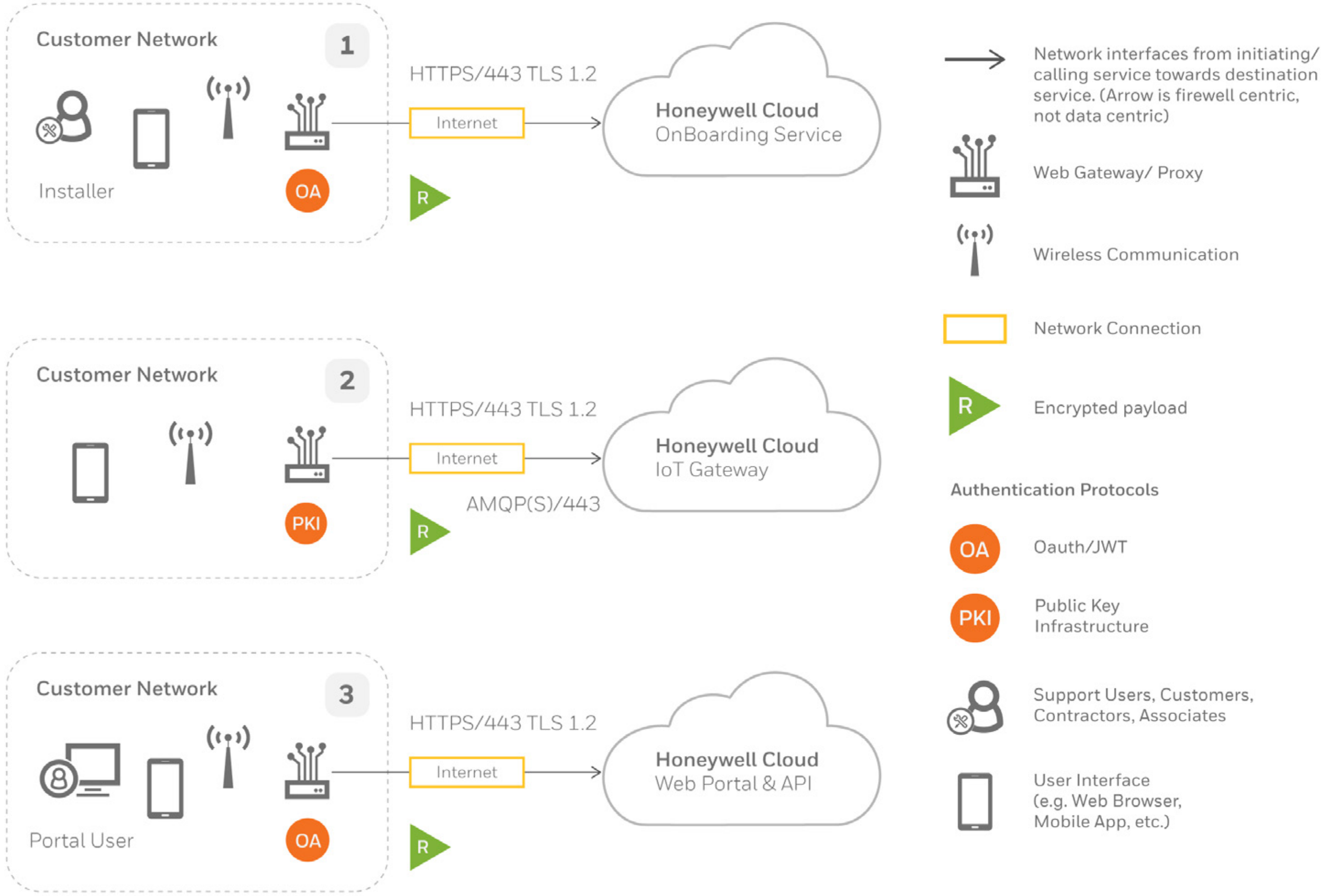
NETWORK CONNECTIVITY



Note: One machine can be associated only with 1 Scanner only

MOBILE COMPUTERS

Mobile computer devices are on-boarded to Honeywell Operational Intelligence's cloud platform and establish direct connectivity via internet.



1. Device Onboarding- User on-boarding device to Honeywell Operational Intelligence pushes configuration to device via scanning barcode or as file. Device agent executes onboarding workflow, with OAuth2.0 token available in Configuration.

2. Telemetry and Event upload: On-boarded device to Honeywell Operational Intelligence upload telemetry data (Reboot count, Scan counts etc.) on configured interval. The data points / elements to be uploaded are based on configuration. Events like battery low, power connected etc. are also uploaded based on configuration. Device agents establish secured AMQP connectivity and trust with Honeywell Cloud IoT gateway on PKI based authentication.

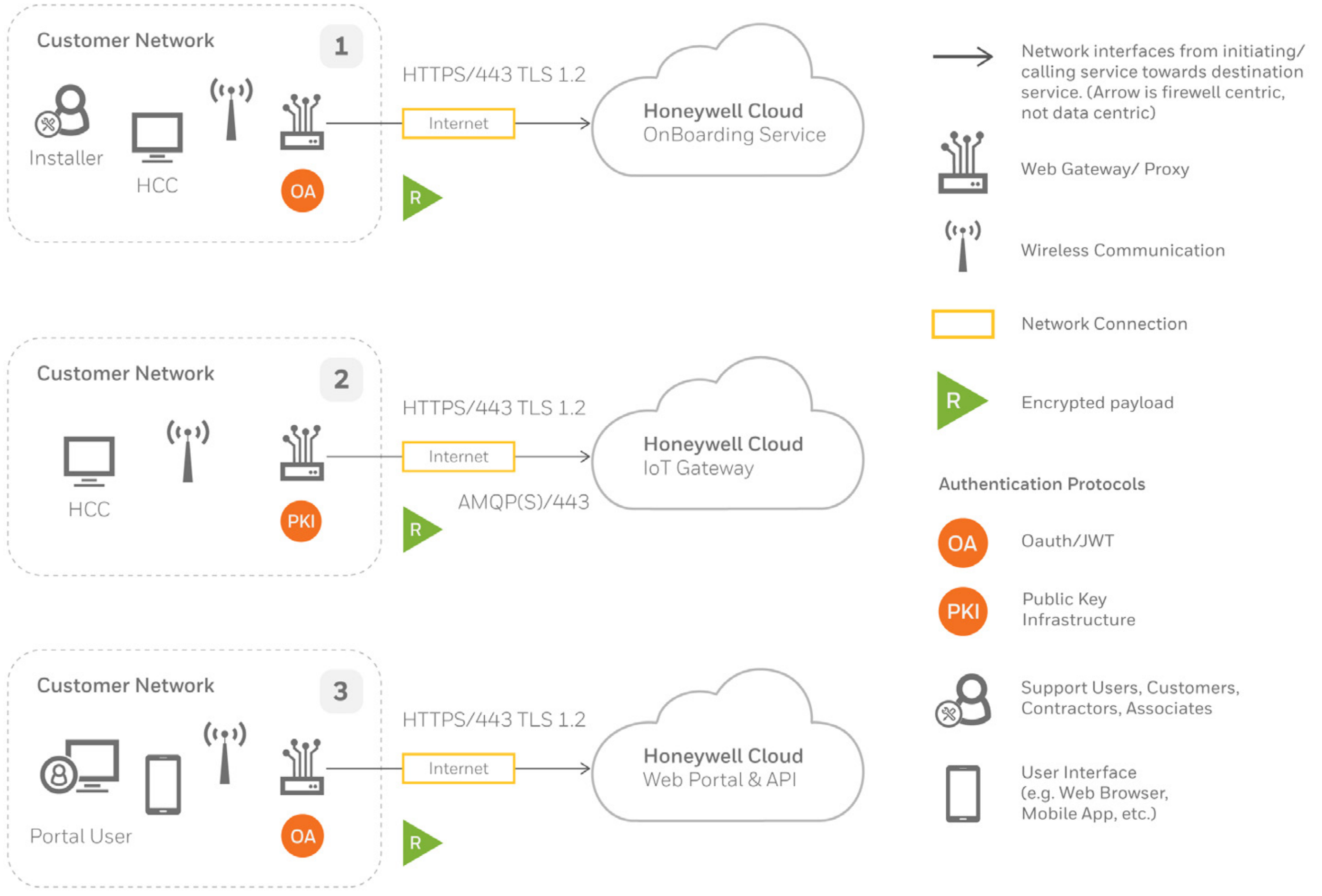
3. Commands and Notifications: Devices connected, receives commands and notifications like SW Download, Remote control et.c via the secured pre-established channel with IoT gateway.

4. File Download: Device agent downloads SW/Configuration files from Honeywell Cloud storage over secured HTTP after SAS token-based authentication.

5. Honeywell Operational Intelligence Portal (Web/Mobile UI): End users like Administrator, store manager, employees logs in to Web/ mobile portal UI after OAuth 2.0 based authentication. User gets authorized based on permissions granted by customer's administrator for application workflows, with a role level access control. All resources and data from server is accessed via secured HTTP protocol.

PRINTERS AND BARCODE SCANNERS

Printers or barcode scanners are on-boarded to Honeywell Operational Intelligence's cloud platform and establish connectivity via edge/ field gateway i.e. Honeywell Cloud Connect (HCC).



1. HCC Onboarding- User log-in to HCC user interface and perform registration workflow.

2. Telemetry and Event upload: On-boarded device to Honeywell Operational Intelligence upload telemetry data (Reboot count, Scan counts etc.) on configured interval. The data points / elements to be uploaded are based on FW configuration. Events like battery low, power connected etc. are also uploaded based on configuration. HCC establish secured AMQP connectivity and trust with Honeywell Cloud IoT gateway on PKI based authentication.

3. Commands and Notifications: HCC receives commands and notifications like SW Download etc. via the secured pre-established channel with IoT gateway for one or multiple devices enrolled.

4.File Download: HCC downloads SW/Configuration files from Honeywell Cloud storage over secured HTTP after SAS token-based authentication.

5. Honeywell Operational Intelligence Portal (Web/Mobile UI): End users like Administrator, store manager, employees logs in to Web/ mobile portal UI after OAuth 2.0 based authentication. User gets authorized based on permissions granted by Customer administrator for application workflows, with a role level access control. All resources and data from server is accessed via secured HTTP protocol.

DATA COLLECTION, PRIVACY AND USE

When enabled, the product collects geolocation data, which the customer may be able to associate with individuals. The customer as controller of the information in the product should therefore make its assessment of the product as required by the GDPR and other privacy legislation. The collected data and the data processing results are always under our customer's control and ownership.

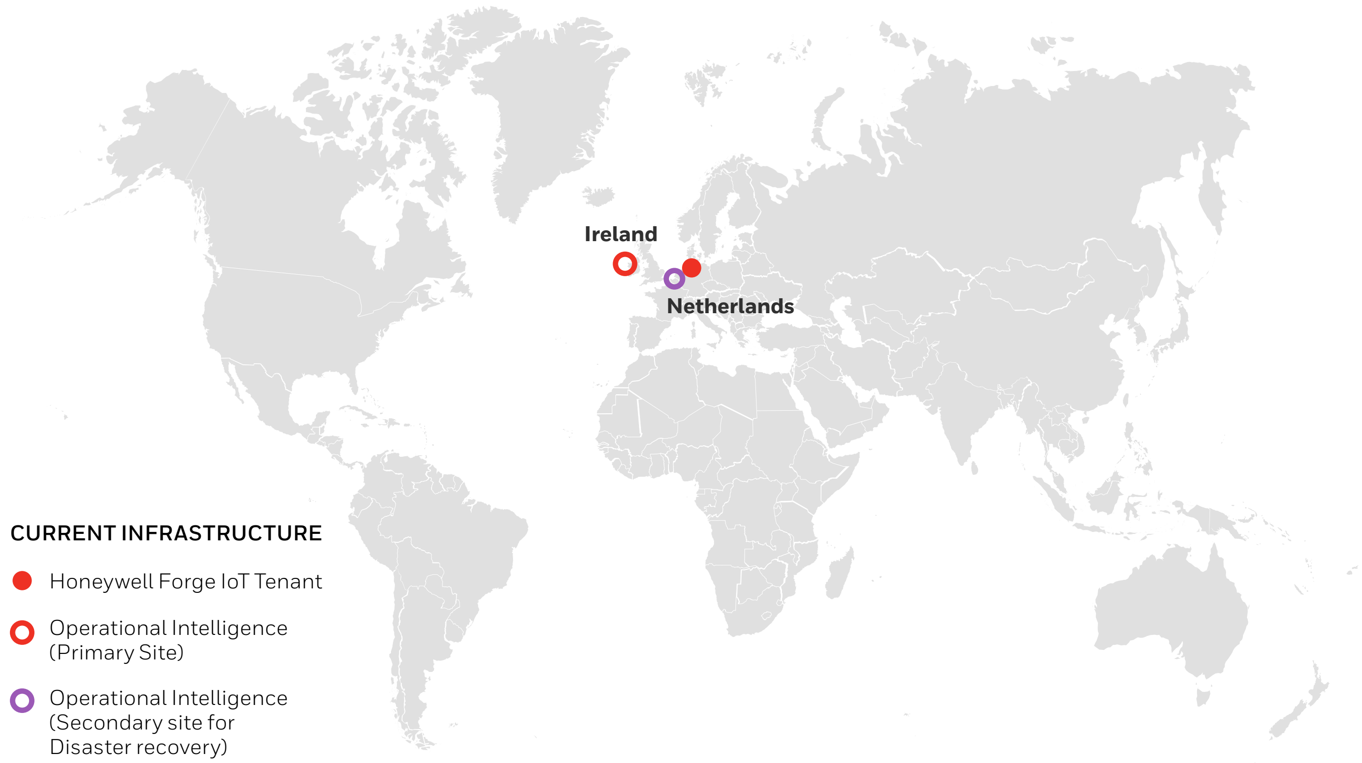
Honeywell Operational Intelligence insights, including dashboards and reports, are delivered via our web portal, which is secured using defense-in-depth methodology. Honeywell Operational intelligence platform processes Name and business email address of web portal users for the purposes of authentication and authorization.

CLOUD PROVIDER

Honeywell Operational Intelligence leverages the world's leading cloud infrastructures, such as Microsoft Azure, that provides best-in-class physical and cyber security services. Honeywell continuously endeavors to not only comply with the best cybersecurity practices recommended by incorporating cybersecurity measures in the very design of the solution and keeping those measures current with changes in the cybersecurity landscape throughout the offering lifecycle.

The entire Operational intelligence platform including customer-owned data is hosted within Microsoft North Europe and West Europe data centers.

Operational Intelligence- enabled devices communicate with the back-end platform using only encrypted protocols with industry-leading ciphers for encryption. The secured channel ensures that data is protected and cannot be accessed by unauthorized entities as it travels between devices and the platform. All stored data is encrypted at rest leveraging keys securely located in a vault solution separate from encrypted data.


Ireland
Netherlands
CURRENT INFRASTRUCTURE
● Honeywell Forge IoT Tenant
○ Operational Intelligence (Primary Site)
○ Operational Intelligence (Secondary site for Disaster recovery)

For more information

sps.honeywell.com

Honeywell Safety and
Productivity Solutions
855 S Mint Street,
Charlotte, NC 28202
800-582-4263
www.honeywell.com

Google, Qualcomm Microsoft and Azure are trademarks
or registered trademarks of their respective owners.

Operational Intelligence Cyber Security
Brochure | Rev A | 05/22

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell