HONEYWELL FORGE
Cybersecurity+

BOOST YOUR OT CYBERSECURITY TO HELP PREVENT CYBER ATTACKS & DOWNTIME

PRESENTER

2025

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

INDUSTRY CHALLENGES

OTD BİLİŞİM
GLOBAL VAD

AGENDA

- Industry Challenges
- Honeywell OT Cybersecurity Software Solutions
- Why Choose Honeywell
- User Feedback

WHAT'S NEW FOR 2024

WHAT IS NEW IN CYBER INSIGHTS

1. **Active Polling:** designed to actively poll Windows machines on the network and check for installed or missing security patches, to get a comprehensive picture of current cyber threats.

2. **Tailored Threat Intelligence:** designed to provide curated threat intelligence on reported malicious activities and their relevancy to specific locations, industries and equipment. With the ability to enrich threat data with STIX/TAXII server.

3. **Enhanced Security:** designed to allow single sign-on (SSO) authentication with the following providers: Google, Azure Auth and Auth2.

4. **Integration:** designed to integrate with Service Now CMDB to allow better support.

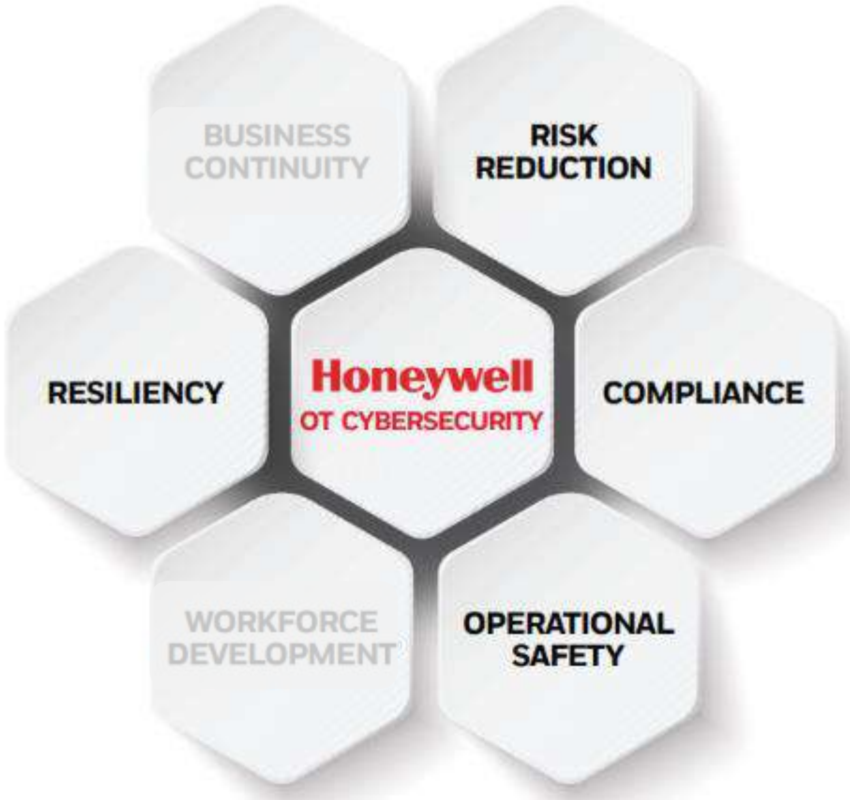
WHAT IS NEW IN CYBER WATCH

1. **Central Governance:** Now designed to continuously monitor your remote sites' adherence to industry standards, including NIS2, OTCC, and SOCI. The full list of standards includes IEC 62443, NERC CIP, NIST, ISO 27001, NIS2, SOCI, OTCC, and organizational policies, as needed.

2. **Topology:** designed to support monitoring of air-gapped networks as well as the Experion DCS fault tolerant ethernet network.

FOCUS ON CYBERSECURITY OUTCOMES THAT MATTER

- The threat of cyber attacks against industrial customers is at an all-time high[1]
- Customers are challenged to get visibility needed to reduce cyber risk of attack
- Honeywell Cyber Insights and Cyber Watch Can help
- Honeywell solutions are designed to help customers achieve critical cybersecurity outcomes that matter



Critical Business Outcomes Enabled by Honeywell Cyber Insights & Cyber Watch

Source-1: https://www.nada.org/nada/nada-headlines/cyber-attacks-shift-gears-growing-threat-automotive-technology, https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability, https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html

OT TARGETED CYBER ATTACKS ON THE RISE

$100M+
potential cost of a cyber-physical attack[1]

75% of OT organizations experienced at least one intrusion in the past year [2]

81% of malware analyzed could cause a disruption to industrial control systems [3]

Ransomware & hacktivism
are a leading cause of most OT targeted attacks [4]

Globally **156** countries have enacted cybercrime legislation[5].

Cyber-physical attacks
are expected to grow, with potential to impact safety of employees[6]

Over **80%**
of CIOs admitted they've had a cyber incident. [7]

[1] Mondelez insurance claim after NotPetya attack, https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit

[2] Fortinet Research, 2023, https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-global-report-finds-75-percent-ot-organizations-experienced-intrusion-last-year#:~:text=Press%20Release-,Fortinet%20Global%20Report%20Finds%2075%25%20of%20OT%20Organizations%20Experienced%20at,Intrusion%20in%20the%20Last%20Year&text=%E2%80%9CFortinet's%202023%20State%20of%20Operational,have%20continued%20opportunity%20for%20improvement.

[3] Industrial Cybersecurity USB Threat Report 2023- Honeywell, https://www.honeywell.com/us/en/press/2023/05/honeywell-releases-cyber-insights-to-better-identify-cybersecurity-threats-and-vulnerabilities

[4] Waterfall 2023, https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-blog/#:~:text=Big%20Impacts%20%26%20Major%20Findings,attackers%20with%20a%20political%20agenda.

[5] Recorded Future Article, Feb 2024, https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/types-of-cybercrime

[6] Honeywell OT Cybersecurity Research 2023

[7] Carbon Black Threat Report, https://www.techrepublic.com/resource-library/whitepapers/the-carbon-black-2016-threat-report/

WHAT IF MALWARE IS ALREADY ON YOUR OT NETWORK?

WOULD YOU KNOW?

- Sophisticated techniques and zero-day exploits evade traditional cybersecurity measures like firewalls and antivirus
- There has been a 140% YoY increase in attacks on industrial organizations[1]
- 270 days is the average dwell time for OT cyber intrusions[2]

EARLY DETECTION IS ONLY POSSIBLE WITH CONTINUOUS MONITORING

[1] SecurityIntelligence, High-impact attacks on critical infrastructure climb 140%June 2023, https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/
[2] Ponemon Institute, 2021, https://www.ponemon.org/

DO YOU KNOW ALL ASSETS CONNECTED TO YOUR OT NETWORK?

ARE YOU SURE THEY ALL BELONG THERE?

- **Most companies are not aware of all the assets they have connected to their OT network, for example:**
  - Neglected maintenance laptops
  - Unmanaged cellular-connected remote access
  - Wireless printers
  - Multiple L2/L3 devices
  - Maintaining harmony between IT and OT
- **Up to 30% assets discovered in Honeywell Cybersecurity Assessments are unknown or unmanaged[1]**

EFFECTIVE CYBERSECURITY PROGRAMS START WITH ASSET MANAGEMENT

[1] Honeywell Cybersecurity Centers of Excellence - 2023

OTD BiLiŞiM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

WHAT IF YOUR CRITICAL SYSTEMS ARE OUT OF CYBERSECURITY COMPLIANCE ?

CAN YOU TRACK THIS?

- **Government regulations and company policies are driving expectations for greater visibility to real-time compliance tracking. Issues include:**
  - Insecure configurations
  - Critical hotfixes missing
  - Antivirus inoperability/outdated
  - Access control inconsistencies
- **$5.87 million in revenue is the average cost due to a single non-compliance event[1]**

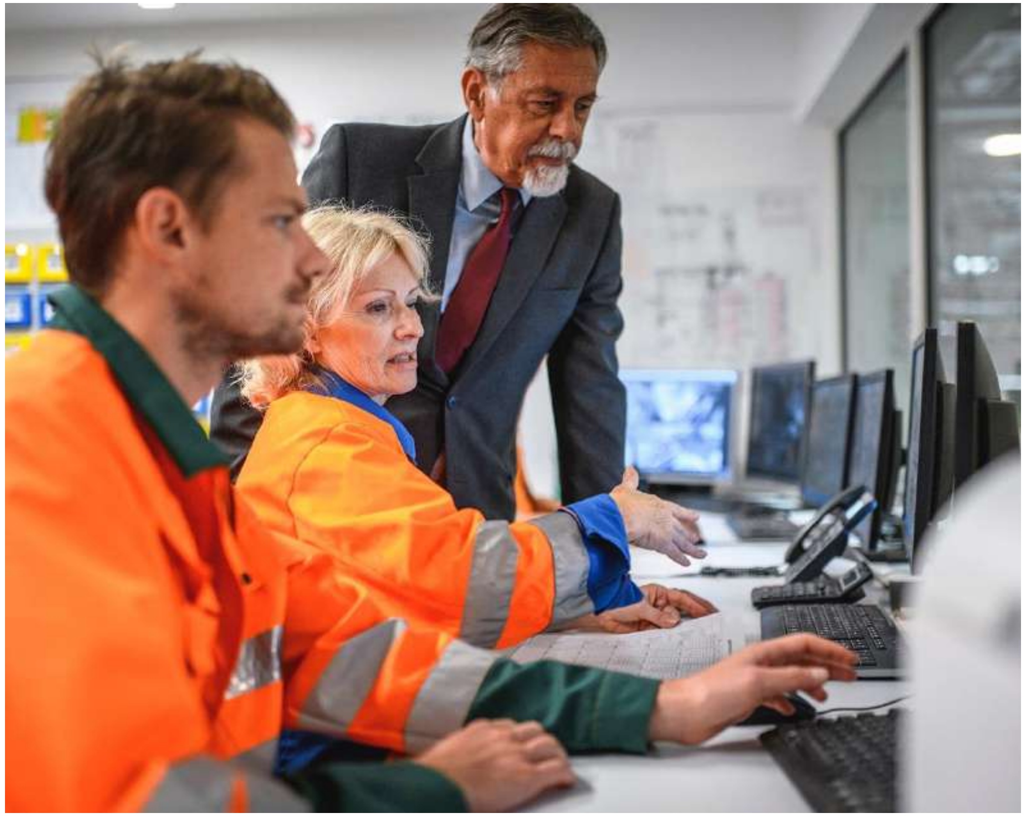
AUDITS ALONE ARE INSUFFICIENT – REAL TIME ASSESSMENTS ARE REQUIRED

[1] Source: Quality Magazine, The Key to Maintaining Safety and Compliance in Manufacturing, March 2024, https://www.qualitymag.com/articles/97858-the-key-to-maintaining-safety-and-compliance-in-manufacturing#:~:text=Organizations%20lose%2C%20on%20average%2C%20%245.87,%2C%20reputation%20damage%2C%20and%20more.

CAN YOU SHOW YOUR CISO THE STRENGTH OF YOUR CYBERSECURITY POSTURE?

DO YOU HAVE A METHOD TO DO SO?

- IT cybersecurity tools don’t work for OT and they often cause breakage
- OT-specific log files in diverse locations, often very different than IT
- Manual and time-consuming reporting to demonstrate cybersecurity
- Only 13% of organizations believe that their OT cybersecurity is “highly mature” versus a comparable 39% for IT[1]



THE RIGHT TECHNOLOGY CAN ENABLE OT TO SHARE CYBER INFORMATION WITH IT

[1] ProofPoint & Fortinet, 2023 State of Operational Technology and Cybersecurity Report; Honeywell extrapolation, chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://d2ka2attjrjsw4.cloudfront.net/files/Partners/Fortinet/Fortinet-2023-report-state-of-OT-Cybersecurity.pdf

ARE YOU PUTTING YOUR SITE’S SAFETY AT RISK?

30%

Of reported OT cyber incidents resulted in physical consequences – with damage up to **$140 M** per incident in 2021[2]

[2] Waterfall 2023, https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-blog#:~:text=Big%20Impacts%20%26%20Major%20Findings,attackers%20with%20a%20political%20agenda.

A NEW FRONTIER FOR OT CYBERSECURITY

CURRENT SITUATION

Time-consuming and infrequent assessments of:

□ cyber risk &
□ security posture

THE OPPORTUNITY

- Know all assets connected to your OT network
- Get near real-time threat & vulnerability detection to enable your security team
- See how sites measure against compliance

HONEYWELL FORGE

Cybersecurity+
Cyber Insights

OTD BİLİŞİM
GLOBAL VAD

CYBER INSIGHTS IS THE FOUNDATION OF A MATURE CYBER POSTURE

Boost your OT cybersecurity to help prevent cyber attacks and reduce downtime

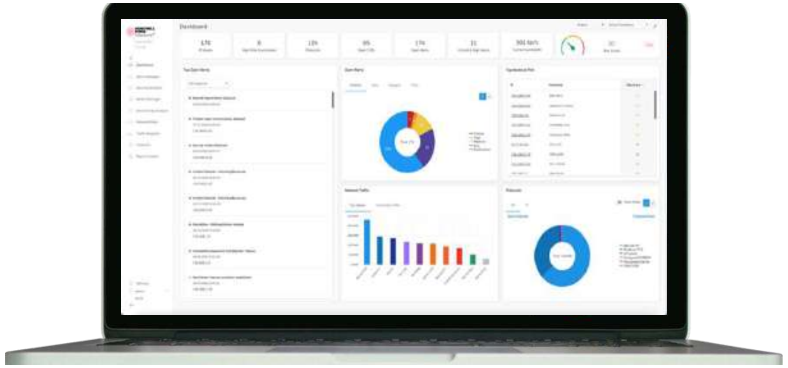
Cyber Insights is designed to:

1 | **Reduce operational risks and help protect safety** through better asset discovery, threat and anomaly detection on all assets in your network using Honeywell-specific security knowledge

2 | **Uncover security weaknesses** with clear insights into vulnerabilities as well as poor cyber hygiene and network configuration issues

3 | **Increase operational efficiencies** through flexible deployment and integration with existing cybersecurity tools/systems

HONEYWELL FORGE
Cybersecurity+
Cyber Insights



GET INSIGHT INTO CYBERSECURITY POSTURE AT YOUR SITE

CYBER INSIGHTS KEY FEATURES

Cyber Insights is designed to do the following:

See what is in the OT network (incl. newly added that can be rogue)

With the help of lifecycle status monitoring, know when the assets need to upgraded or replaced

Get an overall cybersecurity risk score for the site

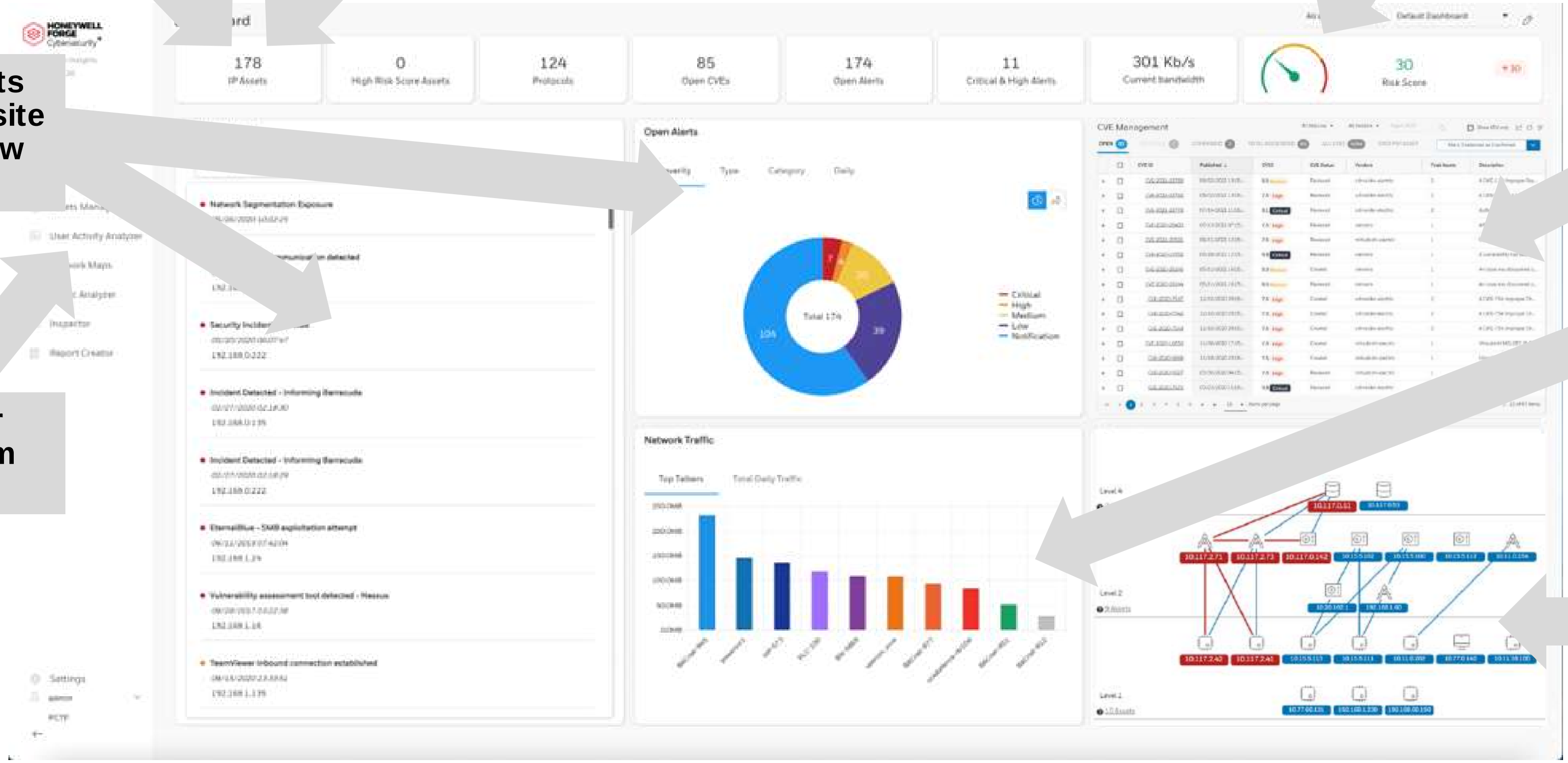
Know what threats are impacting the site right now and how critical they are

Know what vulnerabilities exist at the site and what priority to put on addressing them

Find out who is talking on the network and what language they are using to communicate

Investigate user actions that seem suspicious

Know where the assets are on the network and what they are connected to



KEY FEATURES TO HELP A CUSTOMER SEE THEIR OT CYBER POSTURE

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

RISK REDUCTION

Vulnerability Management

Designed to provide prioritization of known risks using asset risk scores, CVSS and known exploitable vulnerabilities (KEV) as level as the confidence levels between CVE and asset.

Site Risk Profiling

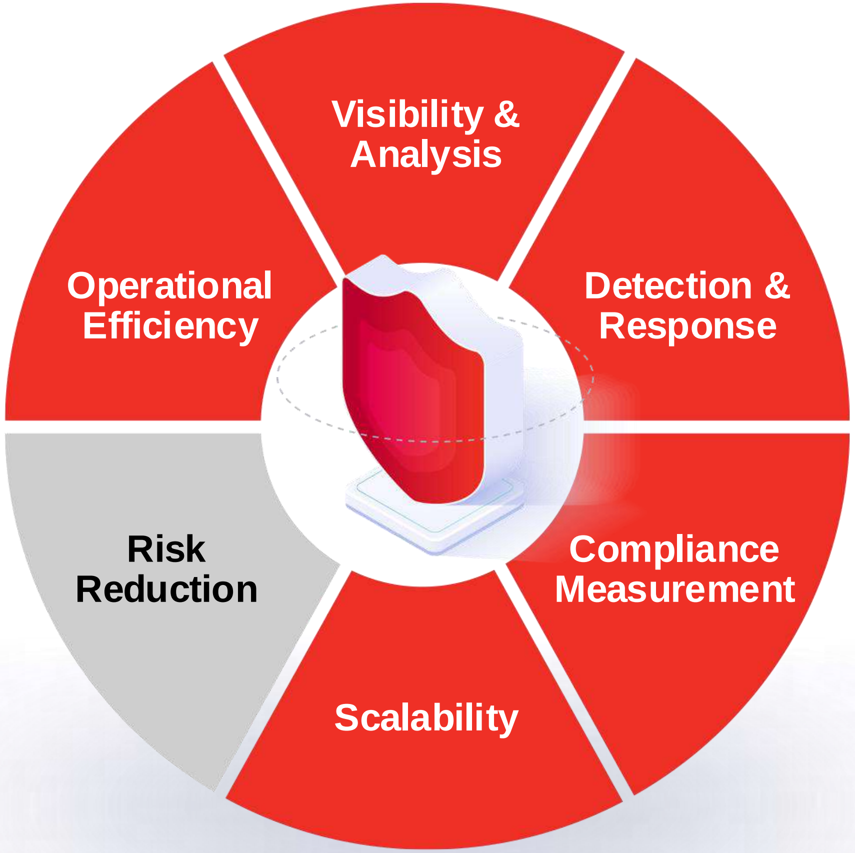
Designed to provide automatic risk profiling at both site and asset level based on their criticality, behavior, risk exposure levels, and prioritization of alerts.

Logical Groups

Capable of providing a connectivity analysis among logical network groups. Useful for analyzing traffic between different network segments, OT sub-segments, OT and IT.

MITRE ATT&CK for ICS

Designed to correlate events to MITRE ATT&CK for ICS model. One-glance updates of the entire organization's threats.



UNDERSTAND & MANAGE OT CYBERSECURITY RISK IN YOUR NETWORK

RISK REDUCTION – CONT.

View & Prioritize Alerts

Advanced current visualization capabilities: prioritized alerts, aggregated alert information, affected asset data, history, forensic data.

Threat Assessment View

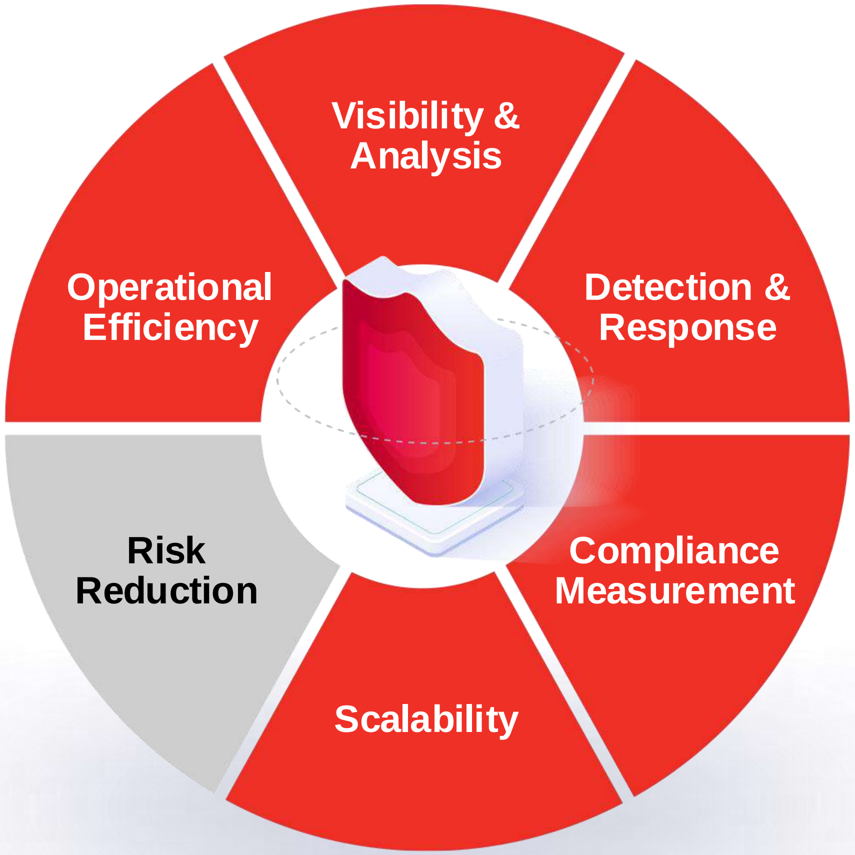
Designed to rate assets based on risk metrics, and quickly determine the most important assets to focus on.

Automated Security Reports

Capable of providing a summary of all alerts including their severity, affected assets list, detailed explanations and remediation recommendations.

Risk Analysis

Designed to perform automatic risk analysis with architectural and security context considered and identify risky connections, risky communication sessions, and possible attack vectors.



PRIORITIZE THREATS TO FOCUS ON THOSE MOST IMPORTANT

OPERATIONAL EFFICIENCY

Operational Visibility

Designed to provide deep visibility into the OT processes, including the ability to monitor industrial commands and their values, and alert on suspicious communication. This helps ensure that the critical OT processes keep running within required norms.

Alert and CVE Management

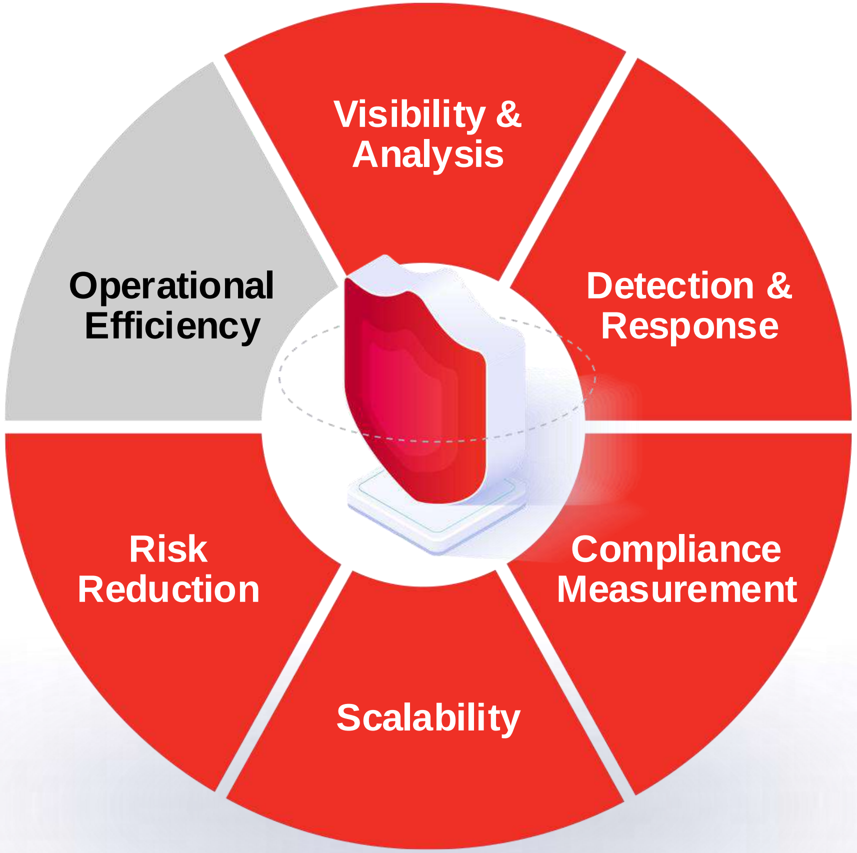
Designed to lower risks and handle security events using alert and CVE management within the solution, or in conjunction with SIEM and SOAR systems.

Sensor-less Deployments

Designed so that there is no need to deploy sensors in every segment. You now have the ability to monitor remote segments in an “agentless” cost effective manner.

Tools to Prioritize Threat Data

Designed to quickly understand and identify the threats that pose the highest risk to safety and operational stability.



INCREASE THE EFFICIENCY OF MANAGING CYBER ACTIVITIES

VISIBILITY & ANALYSIS

Asset Inventory

Designed to provide fully automated asset discovery and inventory – passive and active.

Network Maps

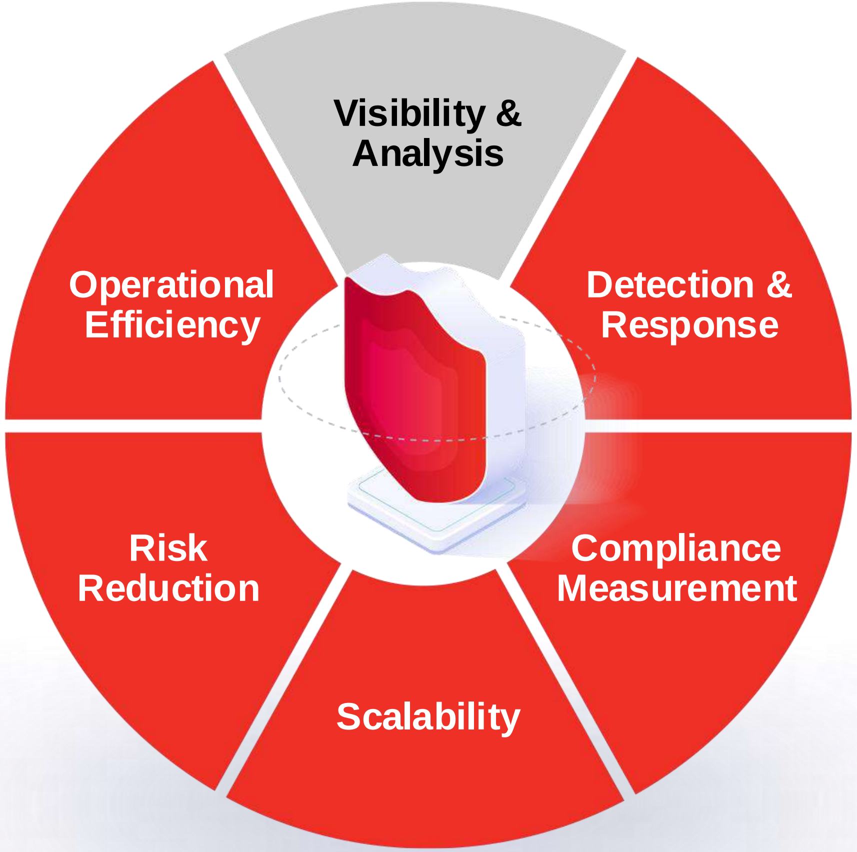
Designed to map the connectivity between each asset including point-to-point mapping, layered mapping and exposure mapping.

Alert Management

Designed to provide notifications on anomalous behavior, malicious actions and/or code, unauthorized network communications, or other unexpected actions.

Vulnerability Management

Designed to provide CVE correlation to relevant assets & prioritize existing vulnerabilities with the product’s network insights.



GAIN MORE VISIBILITY TO YOUR OT NETWORK & POTENTIAL SIGNS OF COMPROMISE

DETECTION & RESPONSE

One Industry-Leading Detection Engine

OT security solutions with high detection rates and low false-positives.

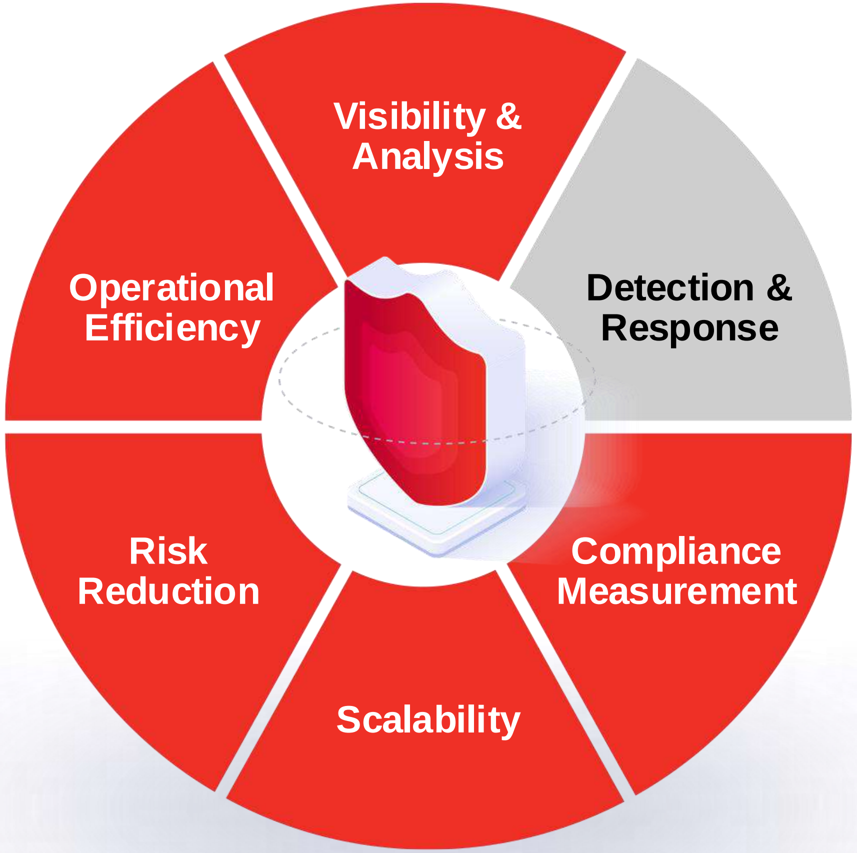
One of the Industry-leading Baselining Technologies

Capable of being fully up and running in days with one of the fewest false-positives rates as compared to current options.

Custom Threat Detection Rules

Custom malware detection rules are designed as part of the signature-based threat detection engine. Provides flexibility to customize rules depending on user needs.

INCREASE CONFIDENCE IN DETECTING CYBER THREATS



ENTERPRISE GRADE & SCALABLE

RBAC

Designed to allow multiple users and departments access to the system, each with its own level of permissions.

Smart Sensors

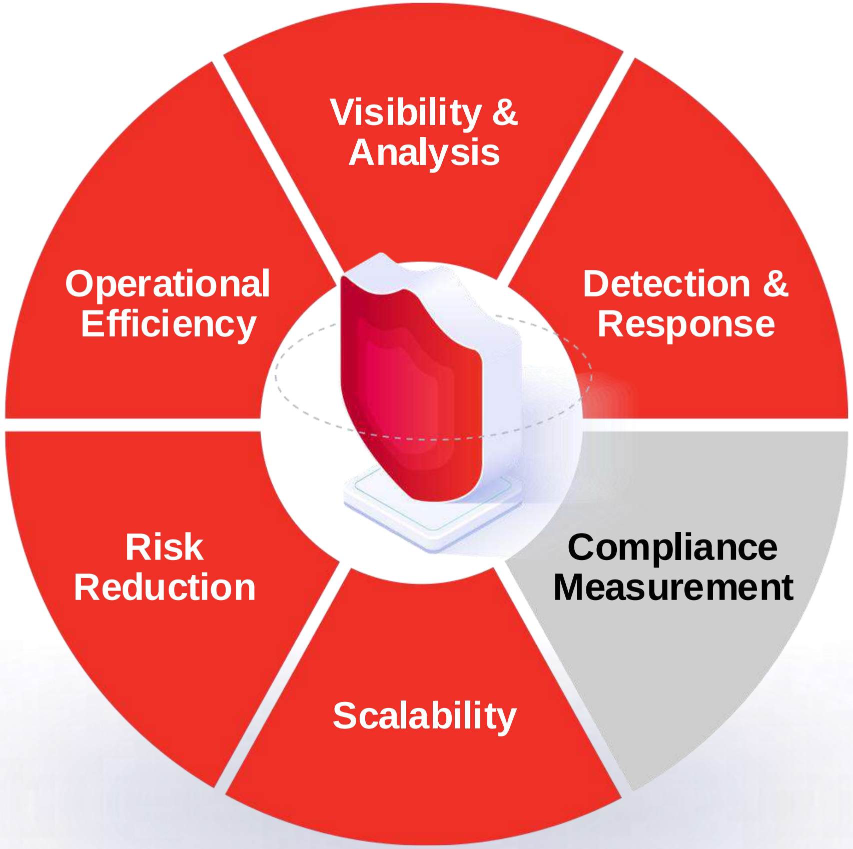
Capable of performing local analysis of the information, optimized for remote low bandwidth and slow connections, that are otherwise difficult to monitor.

Distributed Processing

With sensors processing data locally, rather than forwarding to a central location, capable of providing better scalability and local survivability.

Scale to Additional Sites

Designed to provide multi-site visibility and analysis is available through Cyber Watch.



SCALEABLE SOLUTION

HONEYWELL FORGE

Cybersecurity+ Cyber Watch

OTD BİLİŞİM
GLOBAL VAD

CYBER WATCH IS DESIGNED TO PROVIDE A GLOBAL VIEW OF OT CYBERSECURITY POSTURE

Two Great Ways to Keep Watch…

1) Multi-Site Portal designed to:

- Provide visibility to cyber threats across sites – supports up to hundreds of distributed locations managed centrally via the multi-site portal.
- Deliver a centralized data view - Data from all sites is centrally aggregated, including full asset inventory, traffic and alerts data.

2) Governance Portal designed to:

- Provide governance - enables the IT and audit departments to centrally define and monitor the organization's adherence to company policies.
- Support OT standards & regulations - such as IEC 62443, the NIST framework, and other compliance frameworks for OT.
- Align with internal policies - It also allows for internal policies and best practices across sites.

KEEP WATCH OVER THE CYBER POSTURE OF ALL OPERATING SITES

HONEYWELL FORGE
Cybersecurity+
Cyber Watch

CYBER WATCH LEVERAGES CYBER INSIGHTS

Cyber Watch is designed to aggregate data from multiple sites through Cyber Insights

Cyber Watch – Multi-Site Dashboard

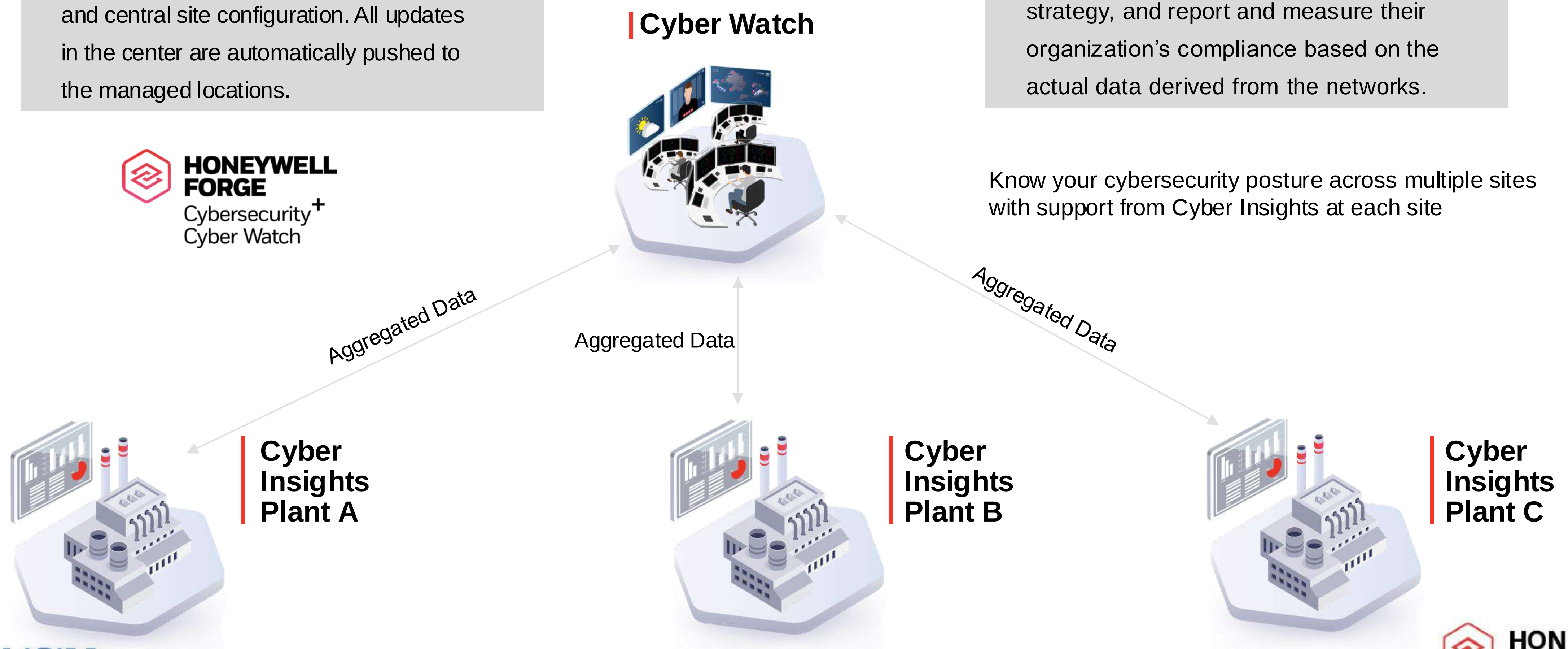
- Includes workflows such as alert handling and central site configuration. All updates in the center are automatically pushed to the managed locations.

Cyber Watch – Governance Dashboard

- Enables CISOs to plan their cybersecurity strategy, and report and measure their organization’s compliance based on the actual data derived from the networks.

HONEYWELL FORGE
Cybersecurity+
Cyber Watch

Know your cybersecurity posture across multiple sites with support from Cyber Insights at each site



Cyber Watch

Aggregated Data

Aggregated Data

Aggregated Data

Cyber Insights Plant A

Cyber Insights Plant B

Cyber Insights Plant C

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

CYBER WATCH COMPLIANCE MEASUREMENT

→ **Central Governance**

Designed to continuously monitor your remote sites' adherence to industry standards (IEC 62443, NERC CIP, NIST, ISO 27001, NIS2, SOCI, OTCC, and others) and organizational policies.

→ **Always Up To Date**

Based on near real-time data extracted from the networks, the system is designed to provide continuous, near real-time visibility to the adherence of regulations and industry frameworks.

→ **Improvement Over Time**

Capable of tracking improvement of organizational compliance over time.

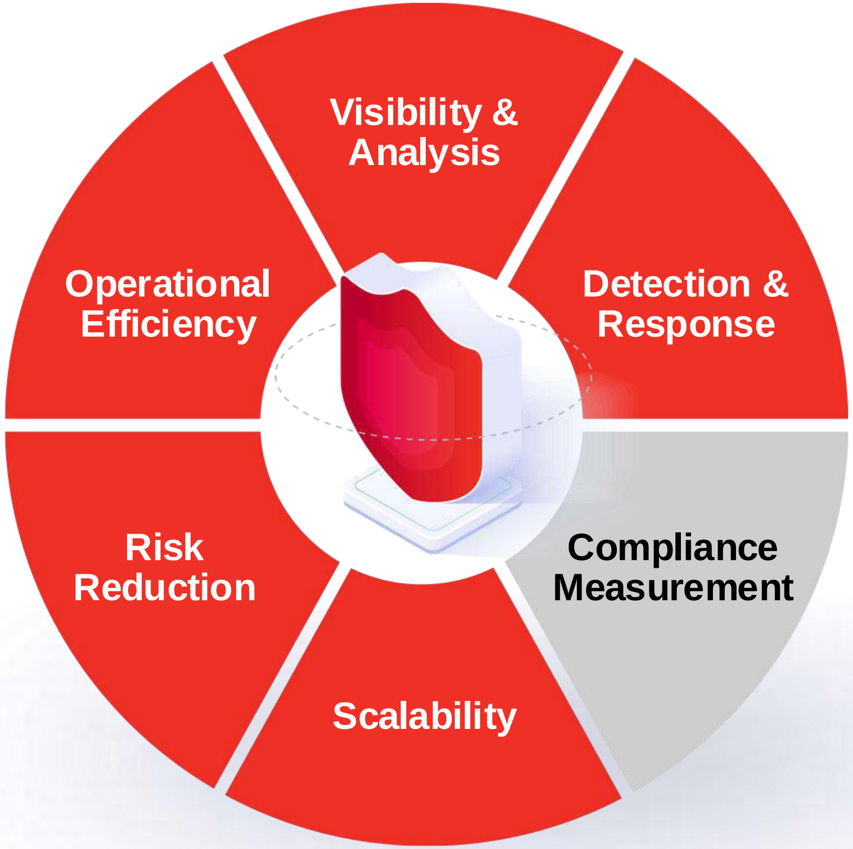
→ **Reporting**

Designed to automatically generate compliance reports to the executive team and the onsite teams for following up on open items.

→ **Reduce Costs**

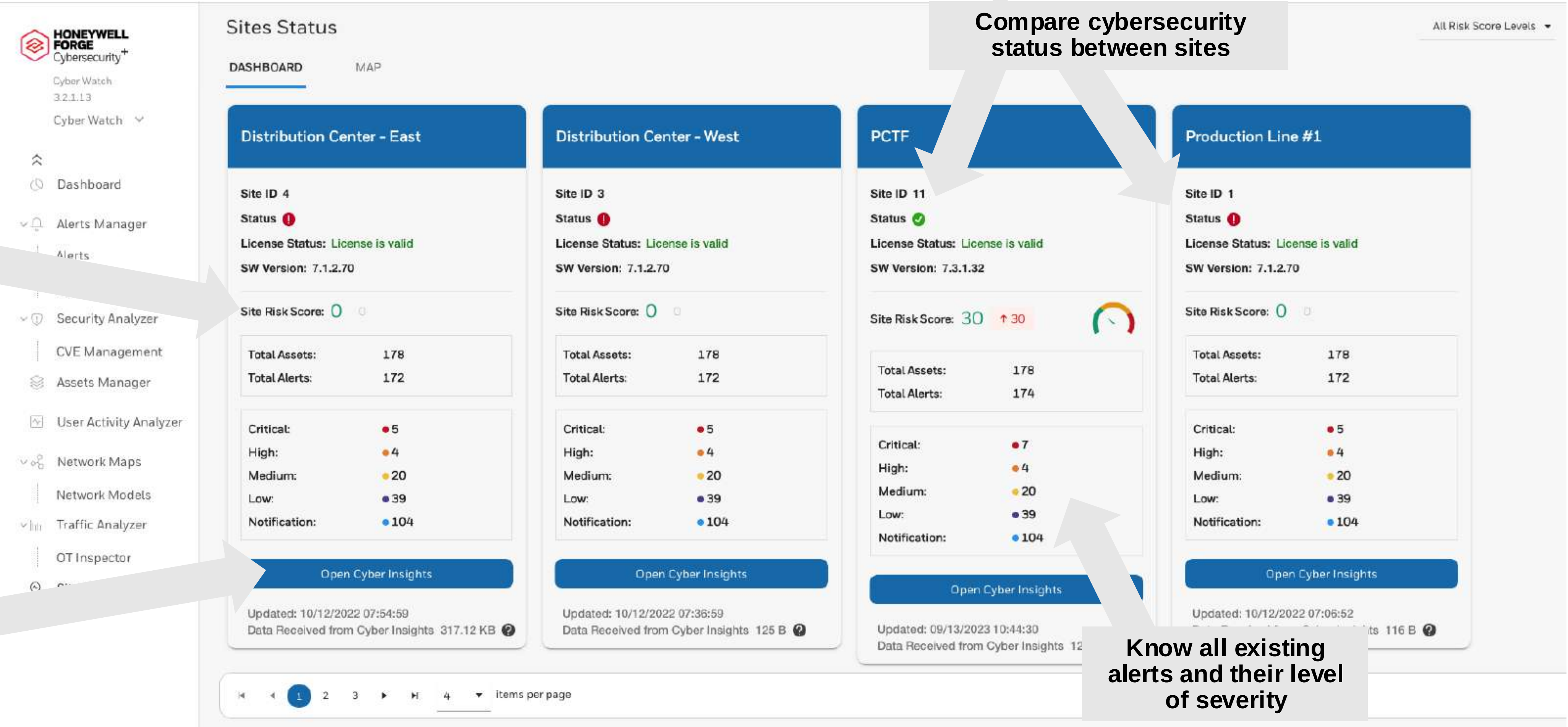
By centrally managing the governance of your organization's remote sites, you may be able to eliminate the need for travel and onsite audits.

KNOW COMPLIANCE STATUS ACROSS ALL SITES



QUICKLY VIEW THE CYBER STATUS OF EACH SITE

Cyber Watch – Multi-Site Dashboard



HONEYWELL FORGE Cybersecurity+

Cyber Watch
3.2.1.13

Cyber Watch

- Dashboard
- Alerts Manager
- Alerts
- Security Analyzer
- CVE Management
- Assets Manager
- User Activity Analyzer
- Network Maps
- Network Models
- Traffic Analyzer
- OT Inspector

Sites Status

DASHBOARD | MAP

All Risk Score Levels

Distribution Center - East

Site ID 4

Status ❗

License Status: License is valid

SW Version: 7.1.2.70

Site Risk Score: 0

Total Assets:	178
Total Alerts:	172
Critical:	● 5
High:	● 4
Medium:	● 20
Low:	● 39
Notification:	● 104

Open Cyber Insights

Updated: 10/12/2022 07:54:59

Data Received from Cyber Insights 317.12 KB ?

Distribution Center - West

Site ID 3

Status ❗

License Status: License is valid

SW Version: 7.1.2.70

Site Risk Score: 0

Total Assets:	178
Total Alerts:	172
Critical:	● 5
High:	● 4
Medium:	● 20
Low:	● 39
Notification:	● 104

Open Cyber Insights

Updated: 10/12/2022 07:36:59

Data Received from Cyber Insights 125 B ?

PCTF

Site ID 11

Status ✓

License Status: License is valid

SW Version: 7.3.1.32

Site Risk Score: 30 ↑ 30

Total Assets:	178
Total Alerts:	174
Critical:	● 7
High:	● 4
Medium:	● 20
Low:	● 39
Notification:	● 104

Open Cyber Insights

Updated: 09/13/2023 10:44:30

Data Received from Cyber Insights 12

Production Line #1

Site ID 1

Status ❗

License Status: License is valid

SW Version: 7.1.2.70

Site Risk Score: 0

Total Assets:	178
Total Alerts:	172
Critical:	● 5
High:	● 4
Medium:	● 20
Low:	● 39
Notification:	● 104

Open Cyber Insights

Updated: 10/12/2022 07:06:52

ts 116 B ?

1 2 3 4 items per page

Compare cybersecurity status between sites

See cybersecurity risk scores for each site and how it has changed over time

Navigate into Cyber Insights to quickly see site specific details

Know all existing alerts and their level of severity

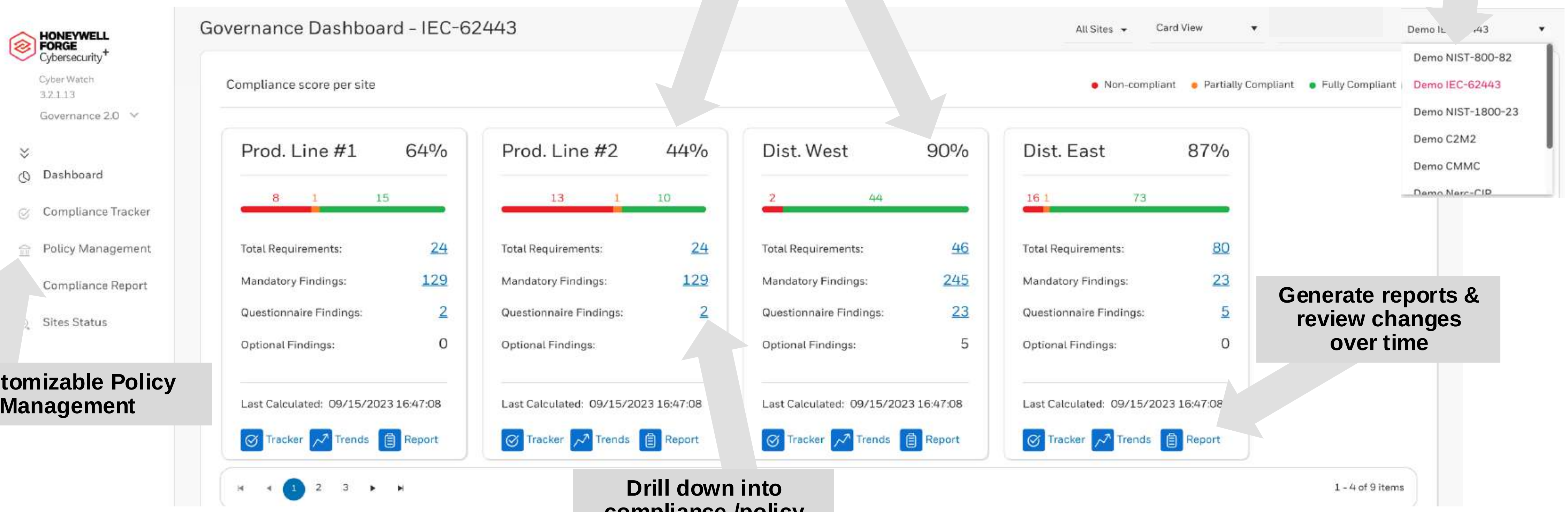
SITE LEVEL ASSET DETECTION & THREAT INTELLIGENCE

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

COMPLY WITH REGULATIONS AND THEN REPORT

Cyber Watch – Governance Dashboard



Governance Dashboard - IEC-62443

Compliance score per site

	Prod. Line #1	Prod. Line #2	Dist. West	Dist. East
	64%	44%	90%	87%
	8 1 15	13 1 10	2 44	16 1 73
Total Requirements:	24	24	46	80
Mandatory Findings:	129	129	245	23
Questionnaire Findings:	2	2	23	5
Optional Findings:	0		5	0
Last Calculated:	09/15/2023 16:47:08	09/15/2023 16:47:08	09/15/2023 16:47:08	09/15/2023 16:47:08

See the compliance scores per site

Track multiple security frameworks and governance policies

Customizable Policy Management

Generate reports & review changes over time

Drill down into compliance /policy details

GET THE INFORMATION NEEDED TO TAKE ACTION AND REPORT

OTD BiLiŞiM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

HONEYWELL FORGE
Cybersecurity+

WHY CHOOSE HONEYWELL

OTD BİLİŞİM
GLOBAL VAD

NORTH AMERICAN CHEMICALS PLANT

IMPACT

Increased visibility to OT assets, reduced false positives on OT cyber alerts, faster installation vs competitive offering previously used

CUSTOMER REQUIREMENT

- Improve asset discovery capabilities, support compliance and governance needs, increase overall effectiveness of OT cyber capabilities and achieve faster time to install.
- CISO had experience with commercial off-the-shelf software from competitive OT provider and was not satisfied with the effectiveness of the product.

SOLUTION

- Installed Honeywell’s Cyber Insights and Cyber Watch at single plant for evaluation then proceeded to implement at additional global sites.

BENEFITS

2X	3X	80%	20%
Cyber Insights detected 2X more devices than competitor in exact same scenario	Cyber Insights was 3X more accurate in identifying Experion control devices	% of features Honeywell technology was equal to or better than competitor product	Increase in assets discovered vs competition

HONEYWELL FORGE Cybersecurity+

“With Cyber Insights, we now have much better visibility into all the assets on the network that manage, monitor and control our industrial infrastructure.”

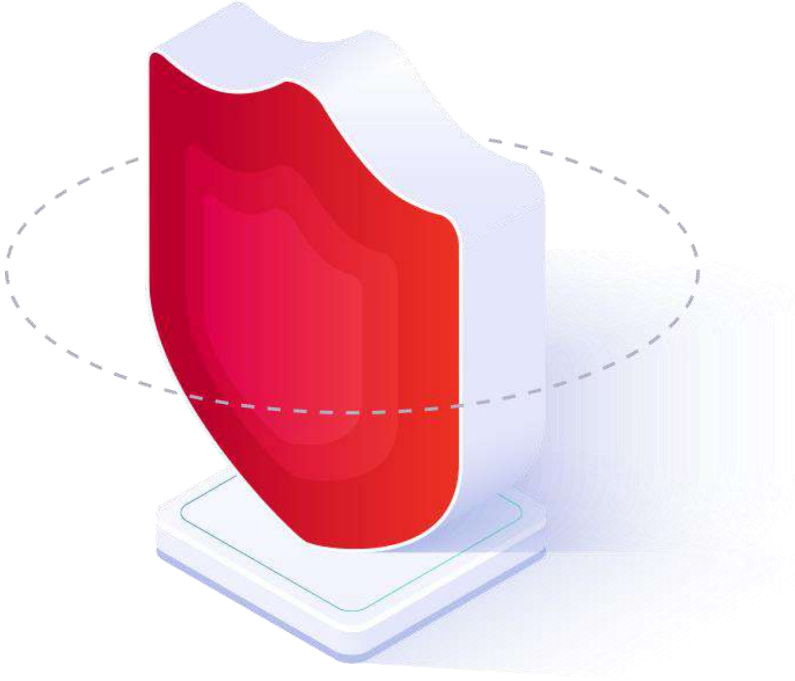
– CISO, Major North American Chemicals Producer

OTD BiLiŞiM GLOBAL VAD

WHY CYBER INSIGHTS & CYBER WATCH?

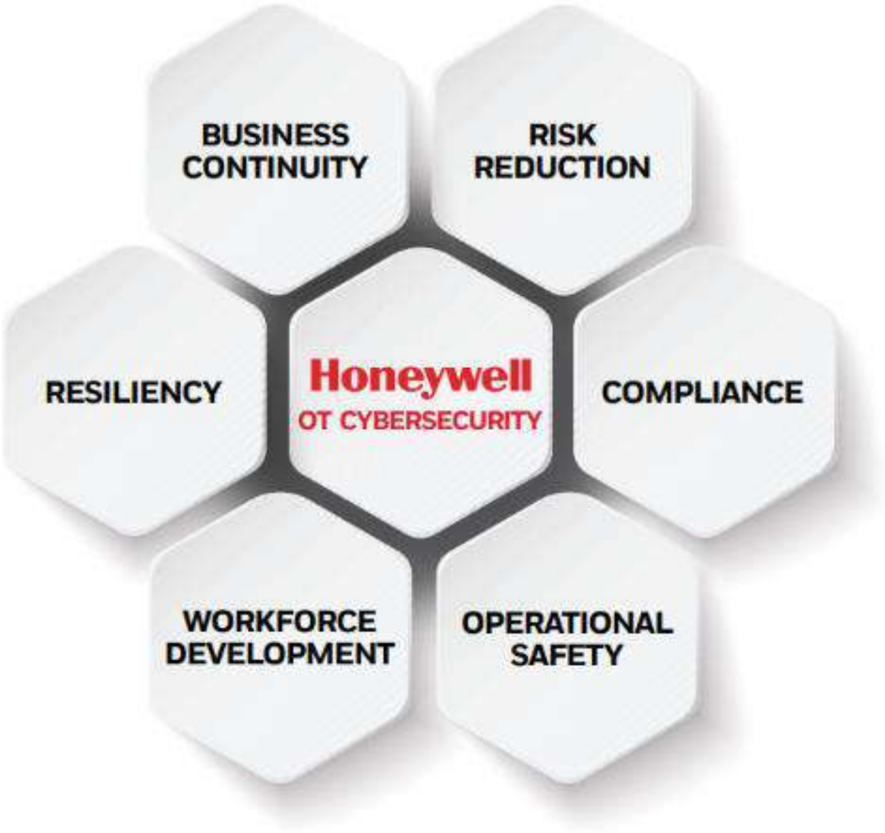
Cyber Insights & Cyber Watch are designed to help:

- ❑ Assure that every system is compliant… all the time
- ❑ Detect cyber threats and vulnerabilities in near real time
- ❑ Validate that all assets on the OT networks belong there
- ❑ Quantify the level of OT cybersecurity risk and prioritize actions to reduce risk
- ❑ Support for Experion users - solutions are certified for Experion control system and they also work in multi-vendor ICS networks beyond Honeywell
- ❑ Improve system security using tested technology that doesn't disrupt the control system



PROTECTING A CONTROL SYSTEM REQUIRES KNOWLEDGE OF DESIGN, OPERATION & SAFETY CHARACTERISTICS

HONEYWELL ADVANTAGE



✓ **Breadth of offerings**
30+ products & services including MSS options

✓ **OT cybersecurity domain experience**
25+ years of experience, 1000's of projects delivered

✓ **Vendor-agnostic**
Solutions for both Honeywell & many non-Honeywell systems

✓ **System integrator**
Able to implement and maintain Honeywell and many non–Honeywell offerings

✓ **Access to OT-specific threat intelligence**
GARD Threat Intelligence

✓ **Global presence**
Currently supporting customers in 100+ countries

✓ **Human resources**
500+ employees focused on OT cybersecurity

✓ **Financial stability**
Fortune 200 company

PART OF A FULL SET OF SOLUTIONS FOR OT CYBERSECURITY

HONEYWELL FORGE Cybersecurity+

Identify Assets that Need Protection

Software-led solutions designed to offer greater visibility to all the assets connected to an OT network.

Key Honeywell Offerings:

- **Cyber Insights**
- **Cyber Watch**
- Professional Services Including Site Assessments

Protect the Assets

Software-led solutions designed to help users better protect assets from the threats of a cyber attack.

Key Honeywell Offerings:

- Managed Security Services
- Secure Media Exchange
- Professional Services
- Centers of Excellence & Innovation - Training

Detect a Cyber Attack

Software-led solutions designed to help users detect an attack underway.

Key Honeywell Offerings:

- **Cyber Insights**
- **Cyber Watch**
- Managed Security Services
- Secure Media Exchange
- Professional Services

Respond to an Attack

Software-led solutions designed to help users respond to an attack.

Key Honeywell Offerings:

- **Cyber Insights**
- **Cyber Watch**
- Secure Media Exchange
- Professional Services for incident response readiness planning

Recover from an Attack

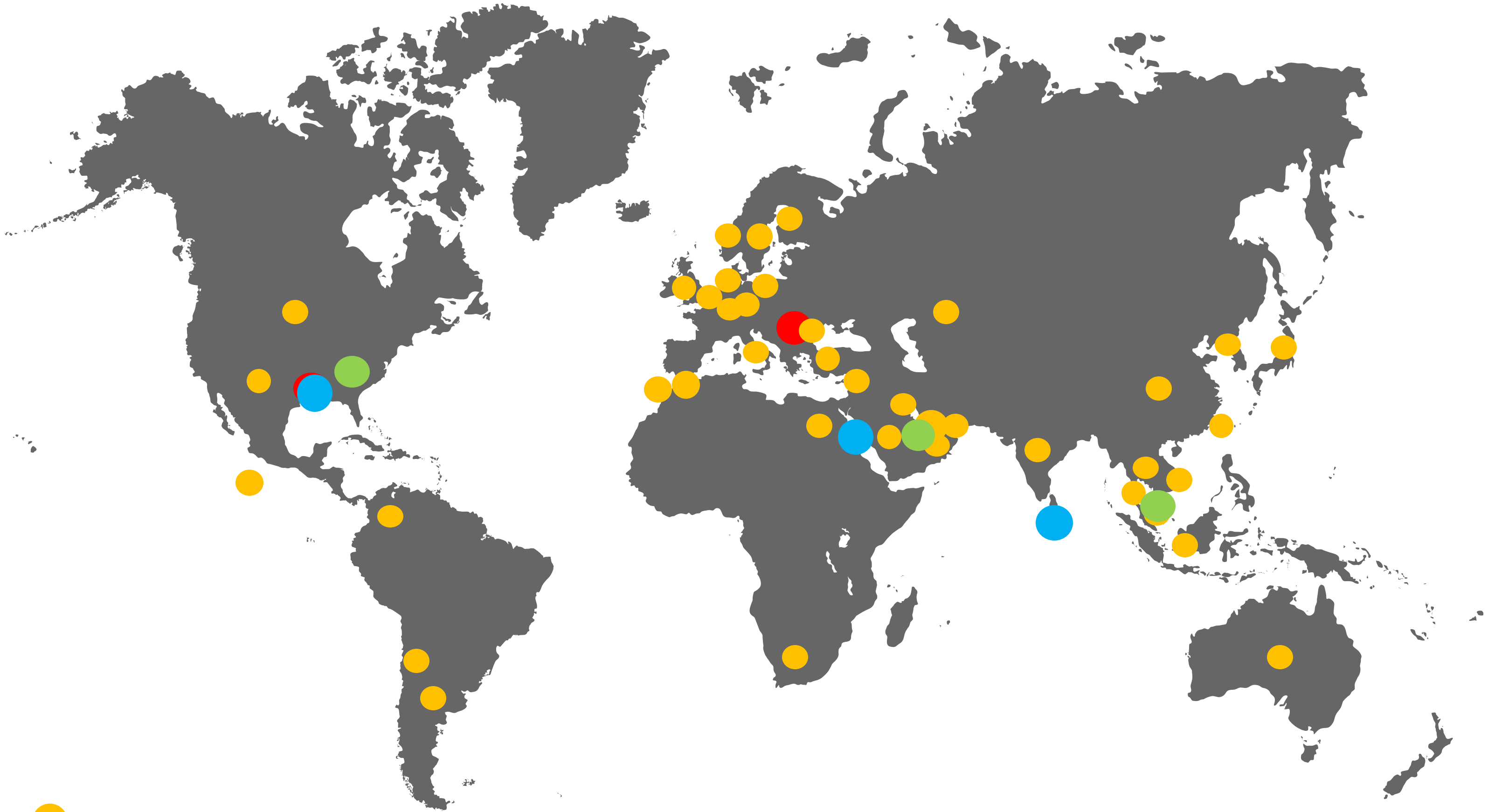
Software-led solutions designed to help users recover from an attack.

Key Honeywell Offerings:

Professional Services

- Recovery planning
- On-site incident response
- Backup & recovery deployment

HONEYWELL OT CYBERSECURITY GLOBAL REACH



🟡 Cybersecurity Consultants (40 countries)

🟢 Cybersecurity Center of Excellence and Innovation

🔴 Center for Managed Security Services

🔵 Cybersecurity Development Center

Regulatory Frameworks & Agencies Covered

ISO 20000 IT Service Management Certified

ISO 27001 Information Security Management Certified

ISA

IEC

ISO

Executive Office of the President of the United States

U.S. Department of Homeland Security

CISA CYBER+INFRASTRUCTURE

Q-CERT

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

NIS2

ANSSI
Agence nationale de la sécurité des systèmes d'information

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

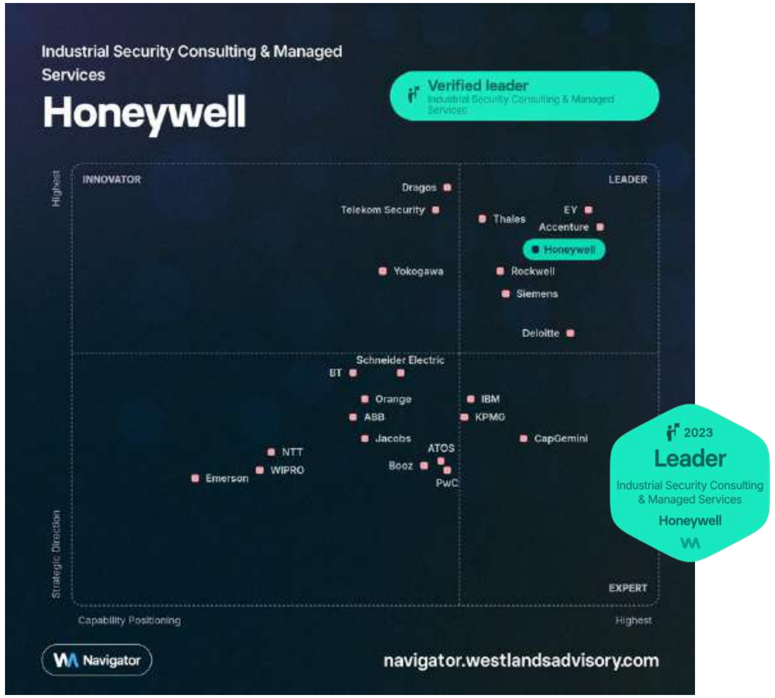
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

ANALYSTS ACKNOWLEDGE HONEYWELL AS A LEADER IN OT CYBERSECURITY

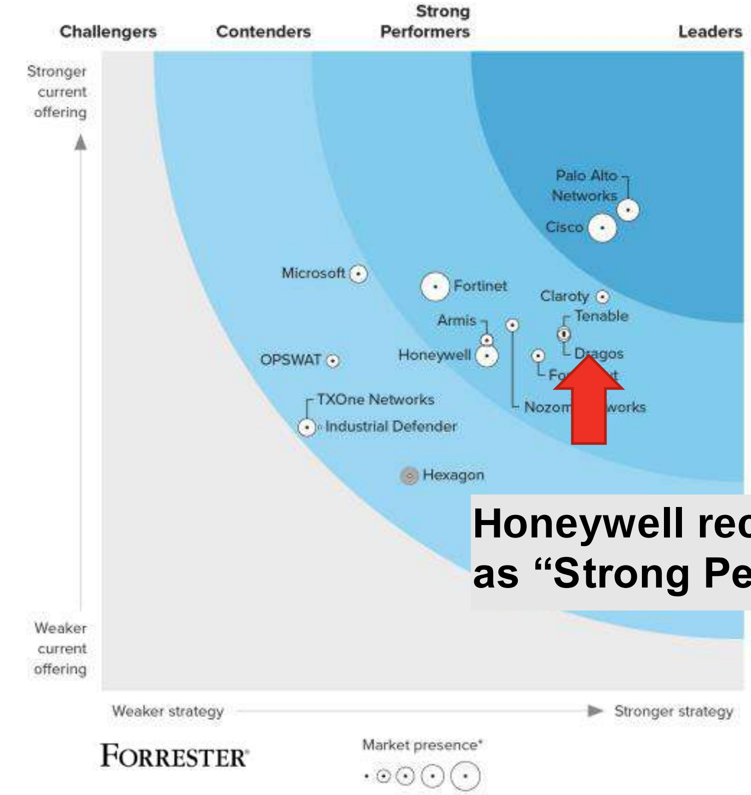
WESTLANDS ADVISORY- NOV 2023:

Honeywell is Leader in Industrial Security Consulting & Managed Services



FORRESTER WAVE ON OT CYBERSECURITY- JUNE 2024:

Honeywell offers OT Asset Management Software and Services, providing an end-to-end OT cybersecurity solution



Honeywell recognized as “Strong Performer”

*A gray bubble or open dot indicates a nonparticipating vendor.

WESTLANDS ADVISORY

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

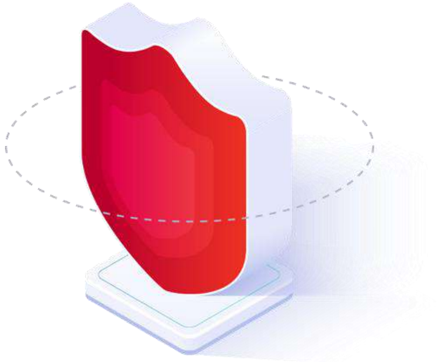
HONEYWELL FORGE
Cybersecurity+

USER FEEDBACK

OTD BİLİŞİM
GLOBAL VAD

[CYBER INSIGHTS] USER FEEDBACK*

Oil & Gas Industry



“[Cyber Insights is designed to watch the network 24 hours a day 7 days a week and that is a giant relief for us... that should mean that there is not anything that goes on the network that we don’t know about by a simple alert on Cyber Insights. I would recommend Cyber Insights to others and I have]”

Process Controls Engineer, Refining and Agricultural Company, North America

“[Cyber Insights really gives us peace of mind. It gives me a tool that helps me to report to my superiors that we are doing what we should be doing in terms of cybersecurity on our network and it just helps you sleep good at night.]”

Process Controls Engineer, Refining and Agricultural Company, North America

“[We were surprised at how valuable it is to have real-time accurate information about our security posture. Cyber Insights extends the power of security engineers, and aligns our entire organization under the same policies and best practices.]”

Supervisor of Infrastructure Systems, Oil & Gas Terminal, Latin America

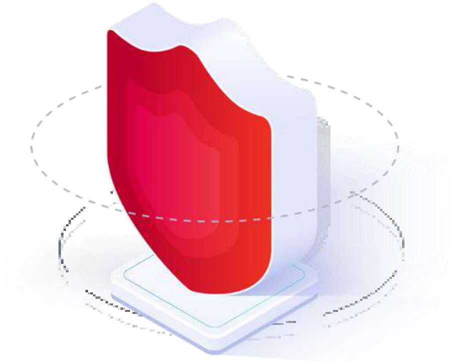
**all customer names withheld to support their cybersecurity*

[CYBER INSIGHTS] USER FEEDBACK*

Pharmaceutical Industry

“[Cyber Insights’ highly accurate asset visibility and inventory tools allowed us to stop using outdated spreadsheets and to complete digitize our network.]”

OT Network Administrator, Pharmaceutical Company, USA



“[Unlike other OT security tools that we are aware of which take 4-6 weeks to display all our OT assets, Cyber Insights had our assets inventory up and ready in only three hours. The quick deployment of Cyber Insights into our environments has been extremely helpful for our efforts to secure our production sites.]”

CISO, Pharmaceutical Company, India

**all customer names withheld to support their cybersecurity*

[CYBER INSIGHTS] USER FEEDBACK*

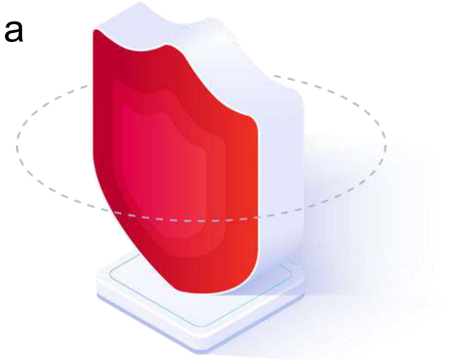
Manufacturing Industry

"[Cyber Insights performance in large-scale networks and detection capabilities are unlike any other platform in the industry that we are aware of.]"

OT Network Engineer, a large EU-based manufacturing facility

"[Cyber Insights helps us provide a more secure environment at our manufacturing plants]"

General Manager, Information Technology, Electronics Manufacturer, Japan



"[Cyber Insights detailed security alerting has allowed my team to quickly detect and mitigate identified malicious activity all across our OT environments]"

VP Operations, Bio Energy Manufacturer, USA

" [Cyber Insights can quickly show visually what's occurring on our network.]"

Security Officer, Major Consumer Products Manufacturer, EU

"[By integrating Cyber Insights into our environment, we were finally able to add OT visibility and monitoring to our ongoing security operations.]"

Security Director, Consumer Products Company, Middle East Region

"Thanks to the visibility we got from Cyber Insights, we were quickly able to see where the ransomware attack was coming from and take the right steps to remediate the exposure points in our production environment. Now, we are tracking the Cyber Insights dashboard as part of our daily work routine.]"

Product & Operational Cybersecurity Officer, Global Manufacturing Company based in the EU

**all customer names withheld to support their cybersecurity*

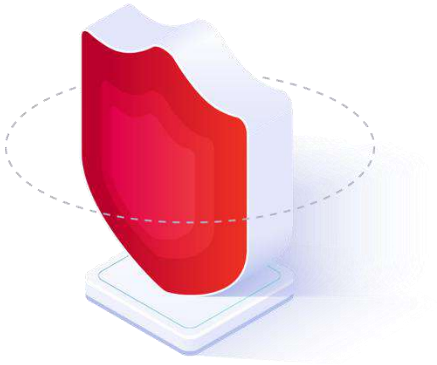
[CYBER INSIGHTS] USER FEEDBACK*

Other Industries

Water

“[If it wasn't for Cyber Insights, we would not have known of those remote access connections, since we thought we had our firewalls set up correctly, but Cyber Insights was able to surface that traffic and then help us to keep the intruders out.]”

Network Administrator, Large Municipal Water / Wastewater Plant in the USA



Power

“[In only ten days of monitoring, Cyber Insights was able to pick up what would take a network professional a couple of months to do.]"

Plant Manager, Electric Power Producer, USA

Distribution

“[Managing OT security risks needs a special solution that is designed for OT environments and Cyber Insights is that special solution.]”

Manager, Distribution Company, Middle East Region

**all customer names withheld to support their cybersecurity*

[CYBER INSIGHTS]
SAMPLE CUSTOMER EXPERIENCE

CUSTOMER INDUSTRY	REGION	MAIN CONTROLLER VENDORS
Chemicals (Honeywell)	Americas	Honeywell control systems
Global Aluminum Manufacturing	Americas, APAC	Siemens, Rockwell
Automotive Components	Europe	Siemens, Fanuc
Pharmaceuticals	APAC	Rockwell, Siemens
Food and Beverage	North America	Rockwell , Moxa, IFM
Global Mining	Africa	Schneider-Electric, Silicom, Siemens
Oil Refining	North America	Rockwell
Consumer Goods Manufacturing	Europe	Siemens, Advantech, WAGO Kontaktechnic
Biofuel Production	South America	Siemens, Schneider, GE, ABB Oy
Electric Power	Europe	Siemens, VAMP
Pharmaceuticals	Middle East	Rockwell, Super-Micro
City Municipalities	North America	Rockwell

COMPREHENSIVE CUSTOMER EXPERIENCE IN MULTIPLE INDUSTRIES AROUND THE WORLD

NEXT STEPS?

1 Understand your OT cybersecurity posture. Do you know all the assets on your network? Are you actively monitoring for potential cyber threats? Honeywell OT cybersecurity consultants can help.

2 Schedule a demonstration of our Cyber Insights & Cyber Watch offerings

3 Learn more about Honeywell's Cyber Insights and Cyber Watch by visiting www.becybersecure.com

CONNECTED
ENTERPRISE

THANK YOU

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL
FORGE
Cybersecurity+

Backup slides

CONTROL SYSTEM TEST ON EXPERION

In March 2024, the Honeywell OT Cybersecurity Product Testing Group performed a series of tests to compare the performance of Honeywell's Cyber Insights solution with a leading competitive alternative. **The following outcomes occurred when testing the competitive offering on the Honeywell Experion control system live test-bed:**

1. **Issues with asset identification accuracy**
2. **False positive alerts generated**
3. **True positive alerts not generated**

None of these outcomes occurred when testing the Honeywell Cyber Insights solution in the exact same test scenario with the Honeywell Experion control system live test-bed.

About the Tests:

The tests were performed by the Honeywell Global Testing Team on a live control system network in a QA environment. This included a full simulation of a control system environment of 500+ nodes (e.g. Honeywell RTUs, PLCs, DCS, SCADA, Safety, PMD and wireless systems),

NOTE: The results of Honeywell's testing as set forth in this report are provided for informational purposes only and are based solely on the results of Honeywell's testing in the specific environment configured by Honeywell for this testing. Results obtained from benchmark testing of this type may be different when conducted in different environments or when such benchmarking is conducted by different parties or with other control systems or data.

CONTROL SYSTEM TEST ON EXPERION - RESULTS

Test Methodology & Findings

Methodology:
Cyber Insights technology was applied on DCS large system test bed in Bangalore & within Honeywell OT Cyber COEs

Findings:

- Technology detected more devices vs competitive product
- Technology had better detection of nodes than competitor
- Technology operated without disruption to the DCS system

Results:

	Cyber Insights	Competitor
Total Devices Detected	329 / 330 **99.6%**	166 / 330 **50.3%**
Accuracy of Experion Control Devices Detected	10 / 15 **66%**	3 / 15 **20%**

Recent Cyber Insights Release

1 **Improved Device Discovery Accuracy**
Implemented product enhancement designed to improve ability to detect DCS specialty control nodes

2 **Implemented DCS Networking Alerts:**
Implemented product enhancement designed to better interpret control system and DCS network redundancy behavior, and reduce false alarm rate

2X Cyber Insights detected 2X more devices than competitor in exact same scenario

3X Cyber Insights was 3X more accurate in identifying Experion control devices

"Cyber Insights technology had better detection & accuracy than Competitor on the Control System."
Honeywell Testing Team

CYBER INSIGHTS OUTPERFORMS THE COMPETITION IN DCS ENVIRONMENTS

CONTROL SYSTEM TEST ON EXPERION – RESULTS CONT.

Significant Number of False Positive Alerts Found Using Competitive Product

Honeywell testing team found significant issues in competing threat detection product regarding the number of cybersecurity false positive alerts generated in control system environment

The Same Scenarios Tested on Cyber Insights & Competitive Product

Traditional day-to-day activities performed on control system environment	False Positive Alerts Generated?	
	Cyber Insights	Competitor
Patch upgrades	No	Yes
Technical maintenance (eg device replacement, migration)	No	Yes
Network management (eg cable removal, switch updates)	No	Yes
Expansion/connection to state of art technology	No	Yes

RESULTS:

1. **Accuracy of reporting** true vs false positives was much higher with Cyber Insights vs competition
2. **Cost to maintain** competitive solution likely significantly higher vs Cyber Insights (more false positives, requires forensic analysis etc to determine true vs false positive)
3. **Difficulty to determine true vs false positive** without deep control system understanding

CYBER INSIGHTS OUTPERFORMED THE COMPETITION IN DETECTING TRUE POSITIVES FROM FALSE POSITIVES ON CONTROL SYSTEM

HONEYWELL SECURITY TEAM REVIEW:

“LEADING TECHNOLOGY SUPPORTING MOST CRITICAL CYBERSECURITY NEEDS”

CISO SECURITY TEAM ANALYSIS:

50 criteria evaluation of Cyber Insights technology vs a market leading competitive product, conducted independently by Honeywell CISO organization at Honeywell sites located in South Carolina and Lotte, Germany.

*NOTE: Honeywell’s corporate security team has **responsibility for the security of 300+ sites worldwide** including many critical infrastructure sites related to specialty chemical production and much more*

“Cyber Insights is equal to or superior to Competitor on most critical functionality and performance dimensions”:

80% % of features Honeywell technology was equal to or better than competitor product

100% % of assets detected on Honeywell Experion (90-95% detection success estimated across other DCS systems)

– Cyber Insights **outshined the Competitor in the most critical areas** for CISOs purchasing decisions, including Asset Discovery, Threat Detection and less False Positives

Honeywell Cyber Insights strengths, based on testing results:

- Better protocol coverage and detection
- Better asset detection and threat detection
- OT/IoT centric solution that does not overlap into IT assets
- Elaborate firewall integration for a quicker response to threats

OTD BiLiŞiM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

TECHNICAL FAQ – PROTOCOL LIST

OT Protocols/Products Support List

The list below details some of protocols that the Cyber Insights is currently designed to support:

ABB CNCP
ABB RNRP
ABB-800 HTTP
ABB Totalflow
BACnet/IP
BACnet L2
Beckhoff ADS/AMS
Bosch Rexroth (Indra)
Bosch Rexroth (SIS)
BSAP
CC-Link
CIP Extensions
COTP L2
CoAP
CSP
DF1
PCCC
EtherNet/IP
Emerson ROC
Emerson DeltaV

EtherCAT
FL-NET
GE SRTP
GE EGD
Honeywell FTE
Honeywell CDA
Honeywell control systems
Honeywell safety systems
HSMS
INCOM (Eaton)
IBP
Keyence VT3
KNX
Kongsberg NetIO
LWE- Lightweight Ethernet
Modbus/TCP
Modbus Unity
Modbus RTU
Modbus RTU Thales
Memobus

Mitsubishi MELSOFT
Mitsubishi MELSEC
Mitsubishi SLMP
NMEA0183
Omron FINS/TCP
Omron FINS/UDP
Omron FINS/ENIP
SECS/GEM
Siemens S7
Siemens S7+
Siemens LOGO!
Profinet DCP
Profinet CM
Profinet AL
PV2
OPC-UA
OPC-DA
Schneider TriStation
SAIA SBUS
RTCM (NTRIP)
HART/IP

Moxa
DNP3
IEC 104 (60870)
IEC 61850
GOOSE
SMV
MMS
ICCP/TASE.2
Synchrophasor
CODESYS
MQTT
Yokogawa Centum DMS
Yokogawa Widefield
Yokogawa HLLS
Yokogawa DMS
Yokogawa Vnet/IP
Wonderware Suitelin

IT Protocols Support List

The list below details some of protocols that the Cyber Insights is currently designed to support:

HTTP
SNMP
SMB
Browser
IP, TCP, UDP, ICMP
CAPWAP
CIFS
FTP
DCE-RPC
VLAN
TFTP
DHCP
ARP
DNS

Kerberos
Telnet
LLDP
CDP
NTLMSSP
LLMNR
MDNS
SSDP
WSDD
RNRP
NTP
VNC
Other

Additional Protocols Support

Our research team is constantly adding support for additional protocols, please contact us if a required protocol is missing from the above lists. With a dedicated research team and our robust dissector engine, we are able to support other protocols, on average within a matter of weeks.

Active Polling - Optional

Cyber Insights is designed to also support active polling (via IT and via native industrial protocols commands). Optionally enabled, this can provide additional details on silent or remote devices.

OTD BiLiŞiM
GLOBAL VAD

HONEYWELL
FORGE
Cybersecurity+

WHY HONEYWELL'S SHIFT TO CYBER INSIGHTS

WE CAN NOT IGNORE THE CLEAR RESULTS AFTER DETAILED, HEAD-T0-HEAD TECHNICAL ANALYSIS

1. **Best vulnerability alarming system for DCS environments**
   – Based on independent tests conducted in Honeywell PCT Testing Lab & Heterogenous Cybersecurity COE testbed, [Cyber Insights] outperformed its competitors with a significantly less false alarms
2. **Best asset detection and controller identification solution for DCS Environments**
   – Based on tests conducted in HON PCT Testing Lab prior to the acquisition [Cyber Insights] detected 2x more devices than its competitors and was 3x more accurate in asset identification.
3. **Control system vendor agnostic and support for 150+ protocols**
   - Experience and capabilities to support non-Honeywell control systems; extensive protocol list provides more accurate asset identification and inventories
4. **Tailored threat intelligence** *- Relevant to your locations, industry and equipment*
5. **Central "enterprise" view** *- All sites including industrial focused governance and compliance automation*
6. **certified for Experion** *- The only Experion certified OT security solution*

PROOF POINTS

Honeywell CISO Team Evaluation:

- Control system test vs market leading competitive product
- Honeywell CISO corporate team evaluation vs Competitor

Cyber Insights vs Competitor:

- Detected 2X more devices
- 3X more accurate
- Zero alert false positives vs competitive product under the exact same test scenario

OTD BiLiŞiM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

CYBER INSIGHTS & CYBER WATCH COMPLEMENT HONEYWELL SERVICE OFFERINGS

Yes	Primary capability
Yes	Secondary capability

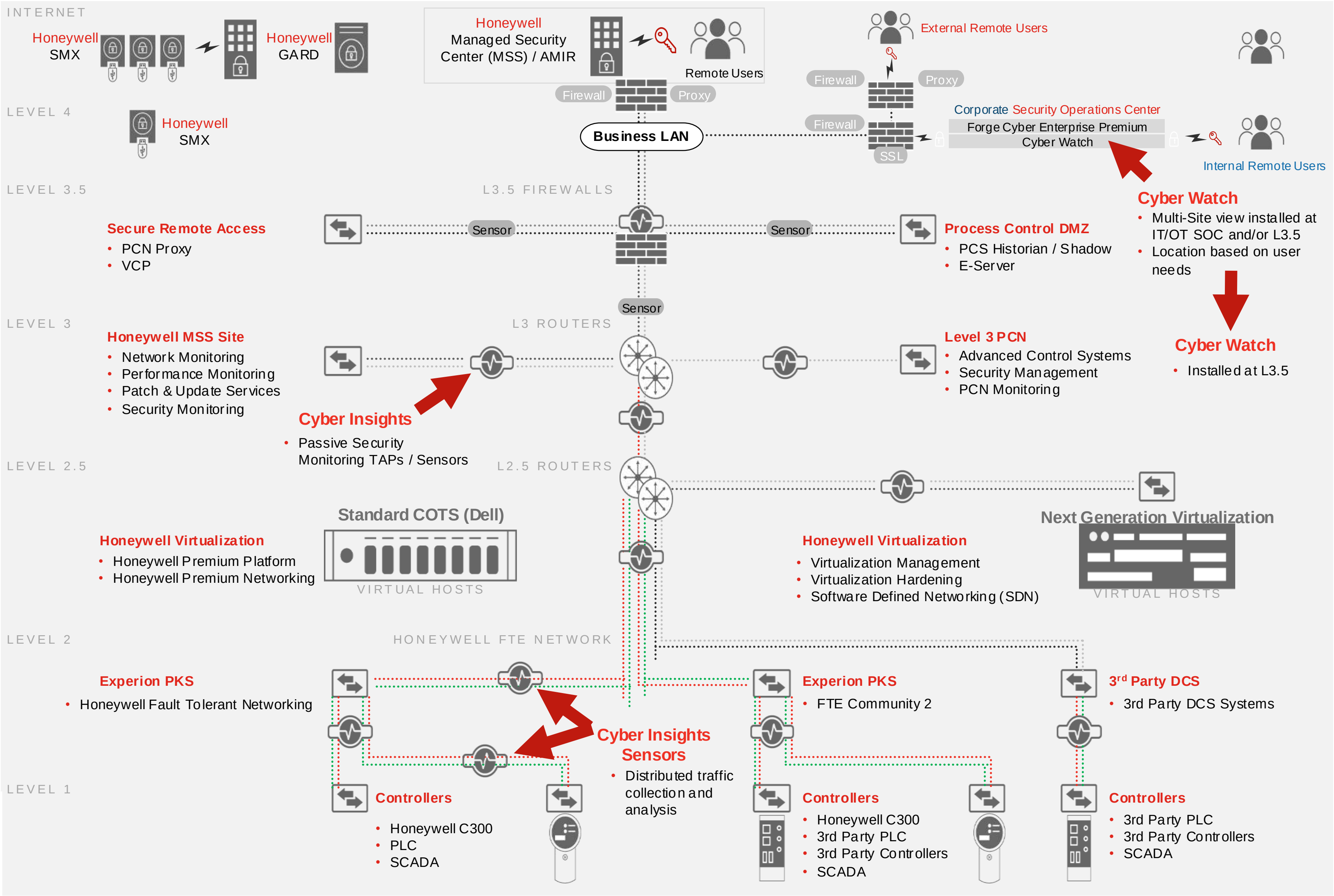
	SOFTWARE		SERVICES	
	Cyber Insights (single site)	**Cyber Watch (multi-site)**	**MSS Advanced Monitoring & Incident Response (AMIR) Services****	**Enabled Services**
Asset Discovery & Inventory	**Yes**	**Yes**	Yes	Yes
Control System Monitoring for Availability				**Yes**
Vulnerability Monitoring	**Yes**	**Yes**		
Compliance Monitoring		**Yes**		
Threat Detection	**Yes**	**Yes**	**Yes**	
Incident Response	Yes	Yes	**Yes**	
Integration with Other Security Tools	**Yes**	**Yes**	Yes	
Non-Honeywell Systems	**Yes**	**Yes**	**Yes**	

**Managed Detection & Response Service

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

HONEYWELL OT CYBERSECURITY SOLUTIONS



Secure Remote Access
- PCN Proxy
- VCP

Process Control DMZ
- PCS Historian / Shadow
- E-Server

Cyber Watch
- Multi-Site view installed at IT/OT SOC and/or L3.5
- Location based on user needs

Honeywell MSS Site
- Network Monitoring
- Performance Monitoring
- Patch & Update Services
- Security Monitoring

Level 3 PCN
- Advanced Control Systems
- Security Management
- PCN Monitoring

Cyber Watch
- Installed at L3.5

Cyber Insights
- Passive Security Monitoring TAPs / Sensors

Honeywell Virtualization
- Honeywell Premium Platform
- Honeywell Premium Networking

Honeywell Virtualization
- Virtualization Management
- Virtualization Hardening
- Software Defined Networking (SDN)

Experion PKS
- Honeywell Fault Tolerant Networking

Experion PKS
- FTE Community 2

3rd Party DCS
- 3rd Party DCS Systems

Cyber Insights Sensors
- Distributed traffic collection and analysis

Controllers
- Honeywell C300
- PLC
- SCADA

Controllers
- Honeywell C300
- 3rd Party PLC
- 3rd Party Controllers
- SCADA

Controllers
- 3rd Party PLC
- 3rd Party Controllers
- SCADA

(L3.5-L5) Cyber Watch

Keep watch over the cybersecurity posture of multiple sites.

(L3) Cyber Insights

Know your OT cybersecurity posture at a single site with industrial grade deep packet inspection and full visibility to assets, network traffic and events

(L2) Optional – Cyber Insights Sensors

Distributed packet analysis, efficient use of network band-width and higher cybersecurity survivability during network outages

HONEYWELL FORGE CYBERSECURITY+

HELP REDUCE CYBER RISK & SUPPORT YOUR DIGITAL TRANSFORMATION ROI

OT CYBERSECURITY SOFTWARE SOLUTIONS

1 Secure Remote Access & File Transfer

2 Asset Discovery & Monitoring

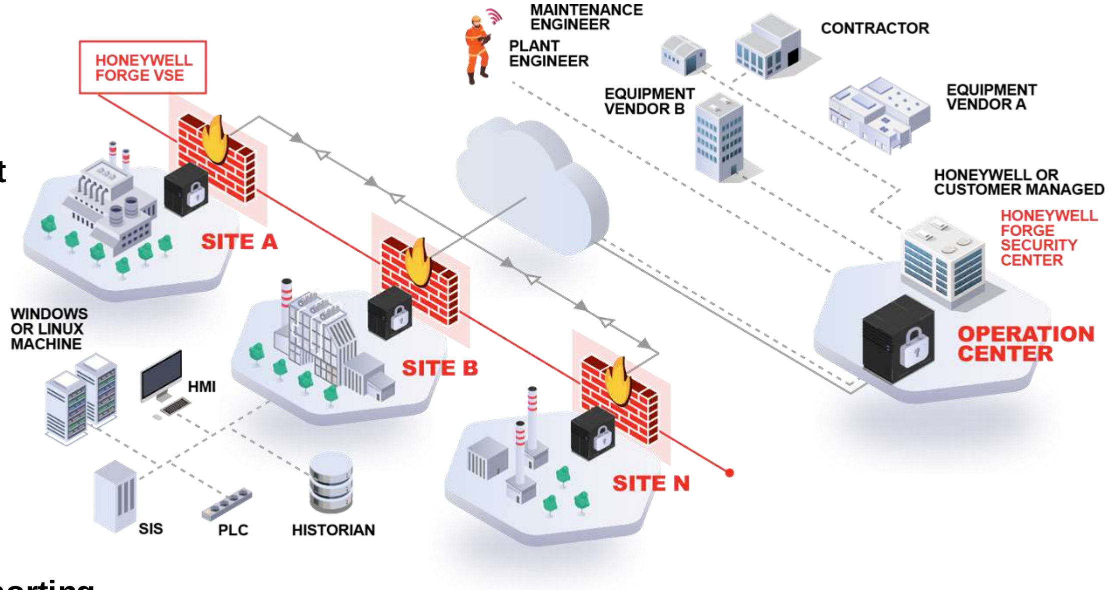
3 File & Network Threat Detection

4 Risk & Compliance Management

5 Patch, AV & Backup Management

6 Centralized Administration & Reporting

HONEYWELL FORGE
Cybersecurity+



OT CYBERSECURITY SERVICES

1 Assessments, Audit, Compliance, Training

2 Advisory, Design, Specification, Remediation

3 OT Network Design & Security

4 OT Endpoint Protection & Detection

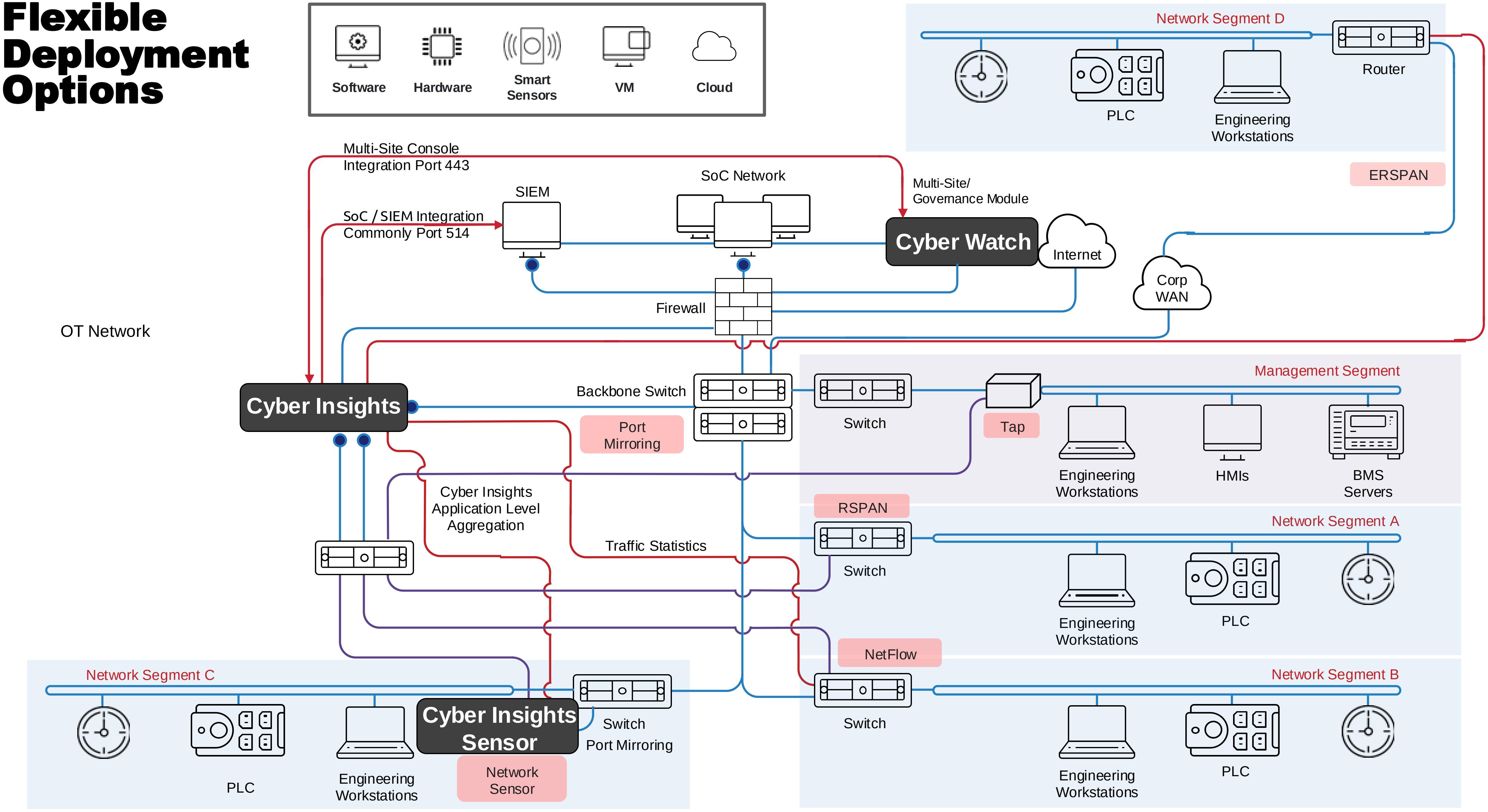
5 Situational Awareness & Intelligence

6 Advanced Monitoring & Incident Response

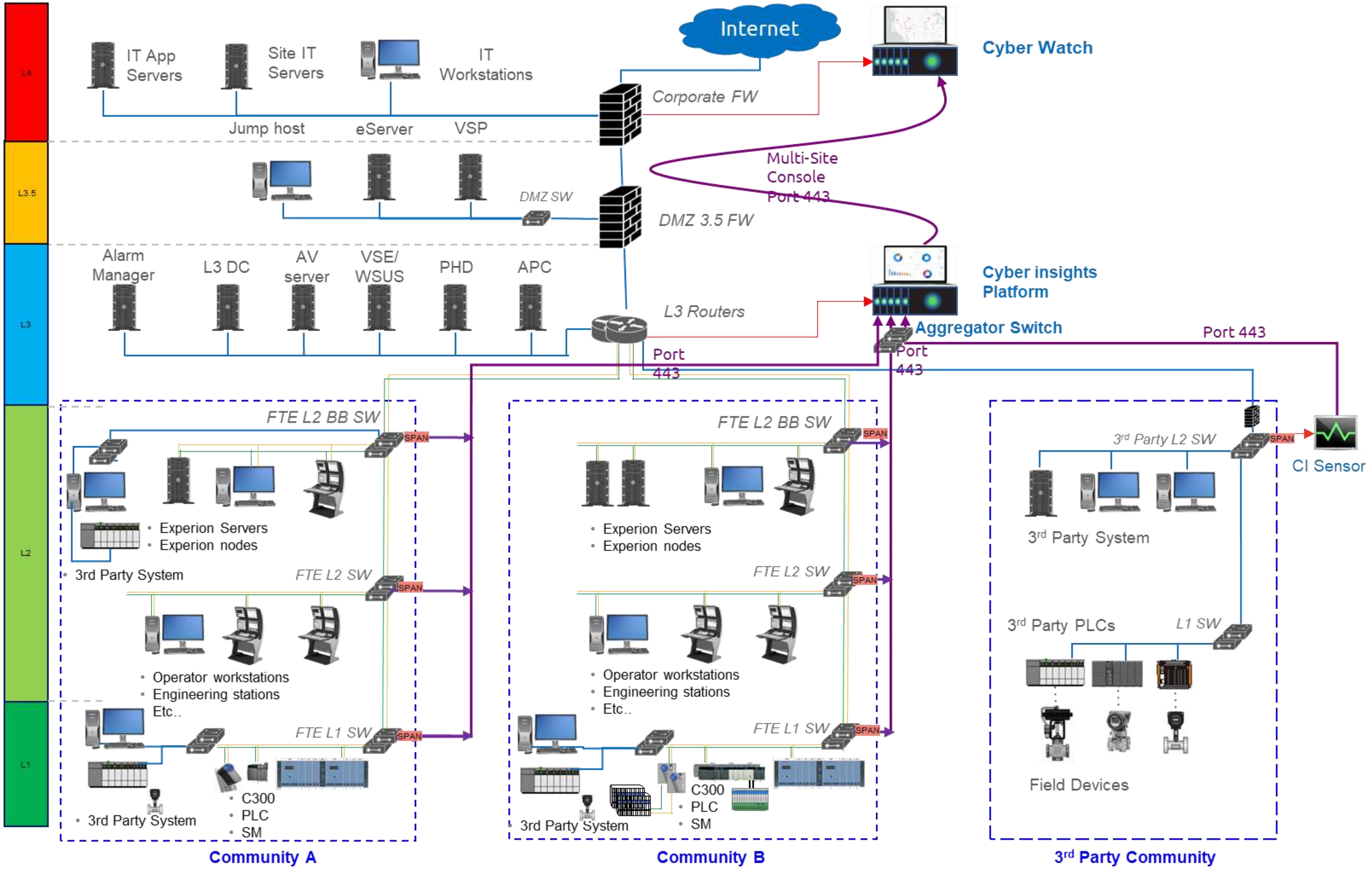
OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

Flexible Deployment Options



ARCHITECTURE



🟩🟨	FTE Network Y/G
🟦	Ethernet
🟪	Traffic statistic
📈	Cyber Insights (Sensor)

Cyber Watch

Keep watch over the OT cybersecurity posture of multiple sites.

Cyber Insights

OT cybersecurity posture at a single site with deep packet inspection and visibility to assets, network traffic and events

Cyber Insights Sensors

Optional. For distributed packet analysis, efficient use of network band-width and higher survivability during network outages

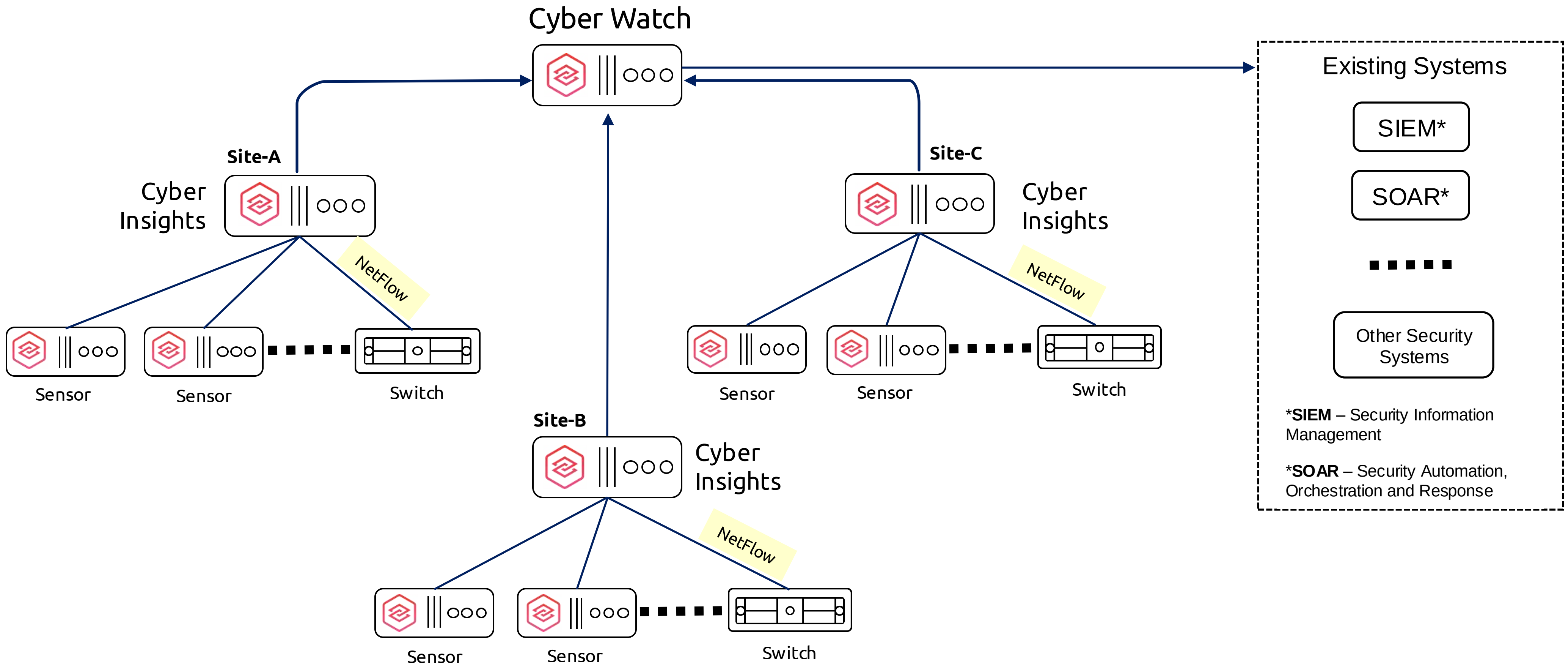
Supported

SPAN (certified on Honeywell IB)
RSPAN
ERSPAN
TAP

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

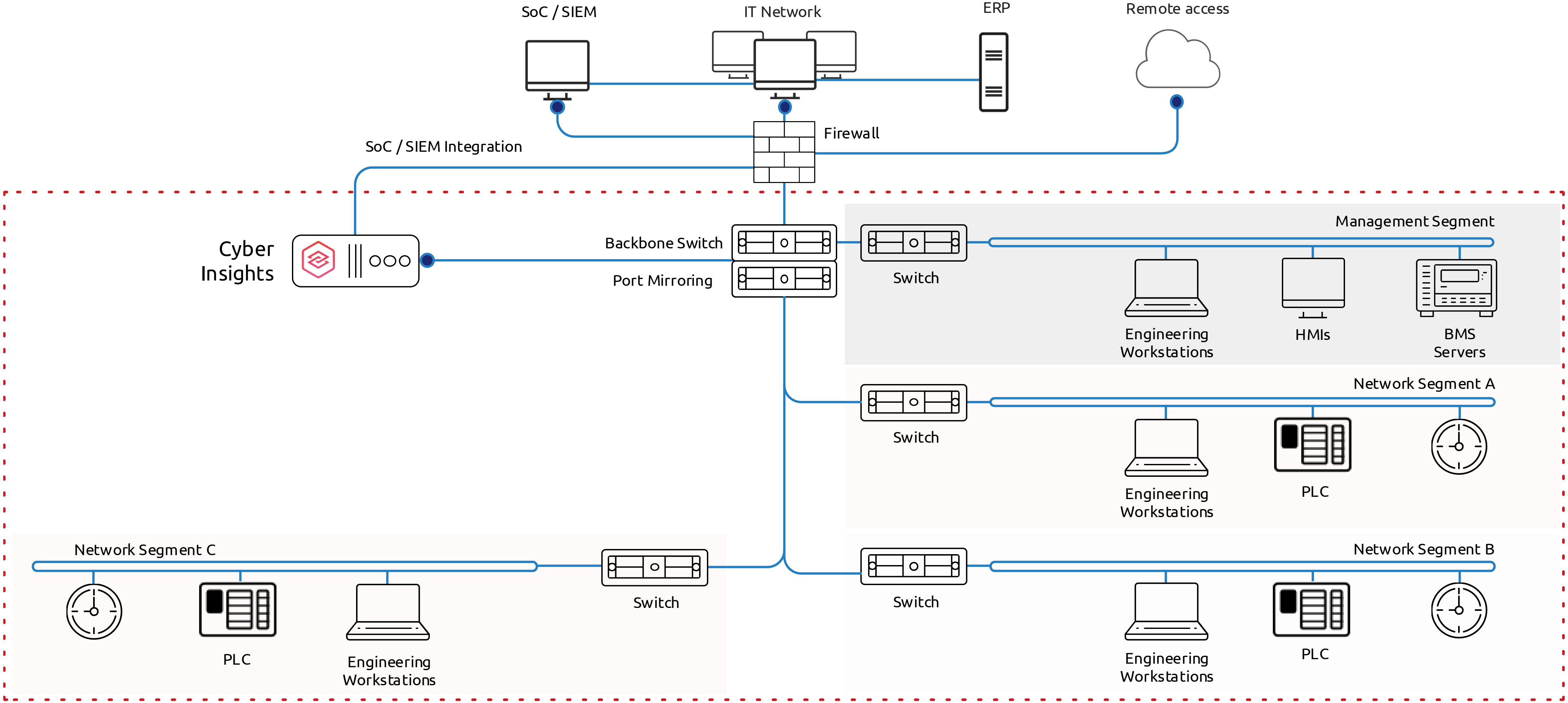
SYSTEM ARCHITECTURE



***SIEM** – Security Information Management

***SOAR** – Security Automation, Orchestration and Response

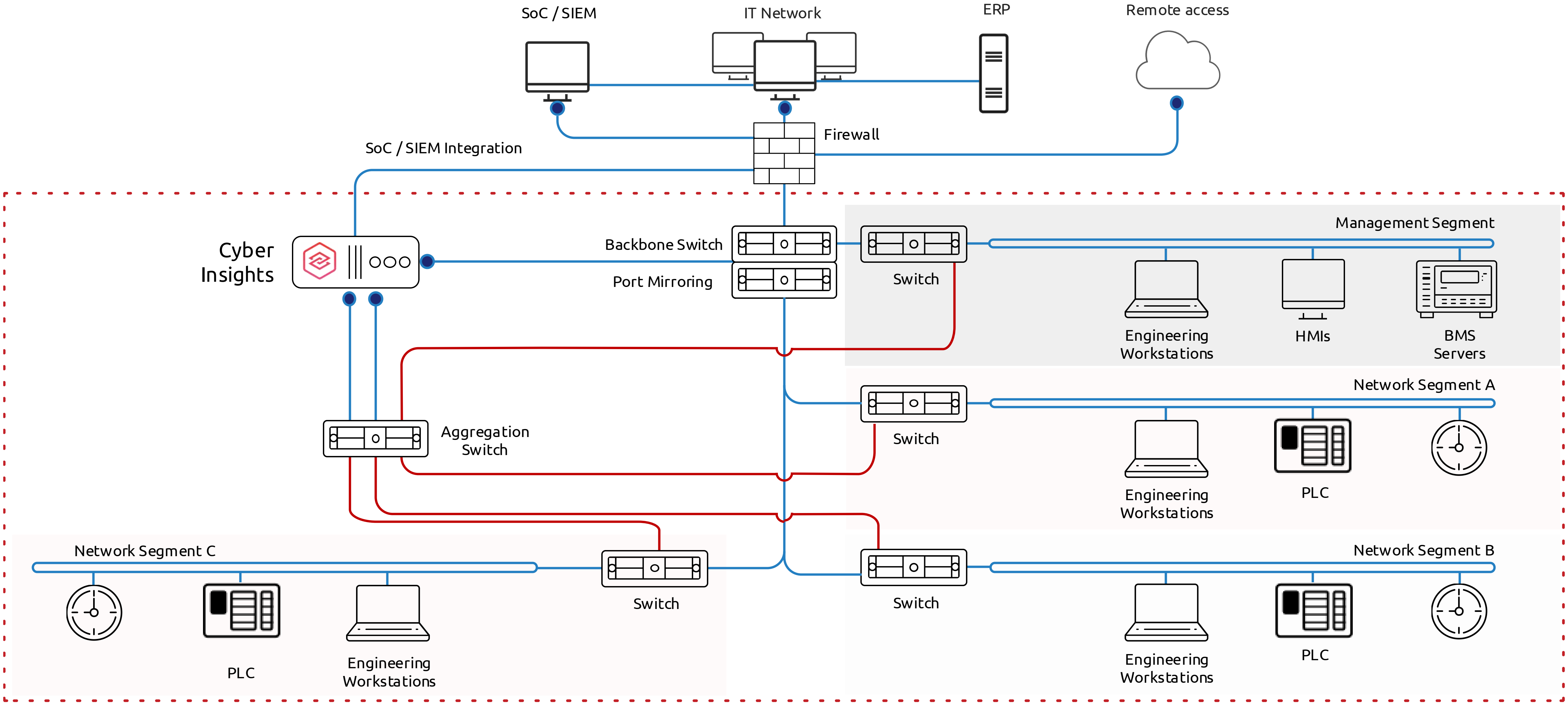
PORT MIRRORING ON A BACKBONE SWITCH



OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

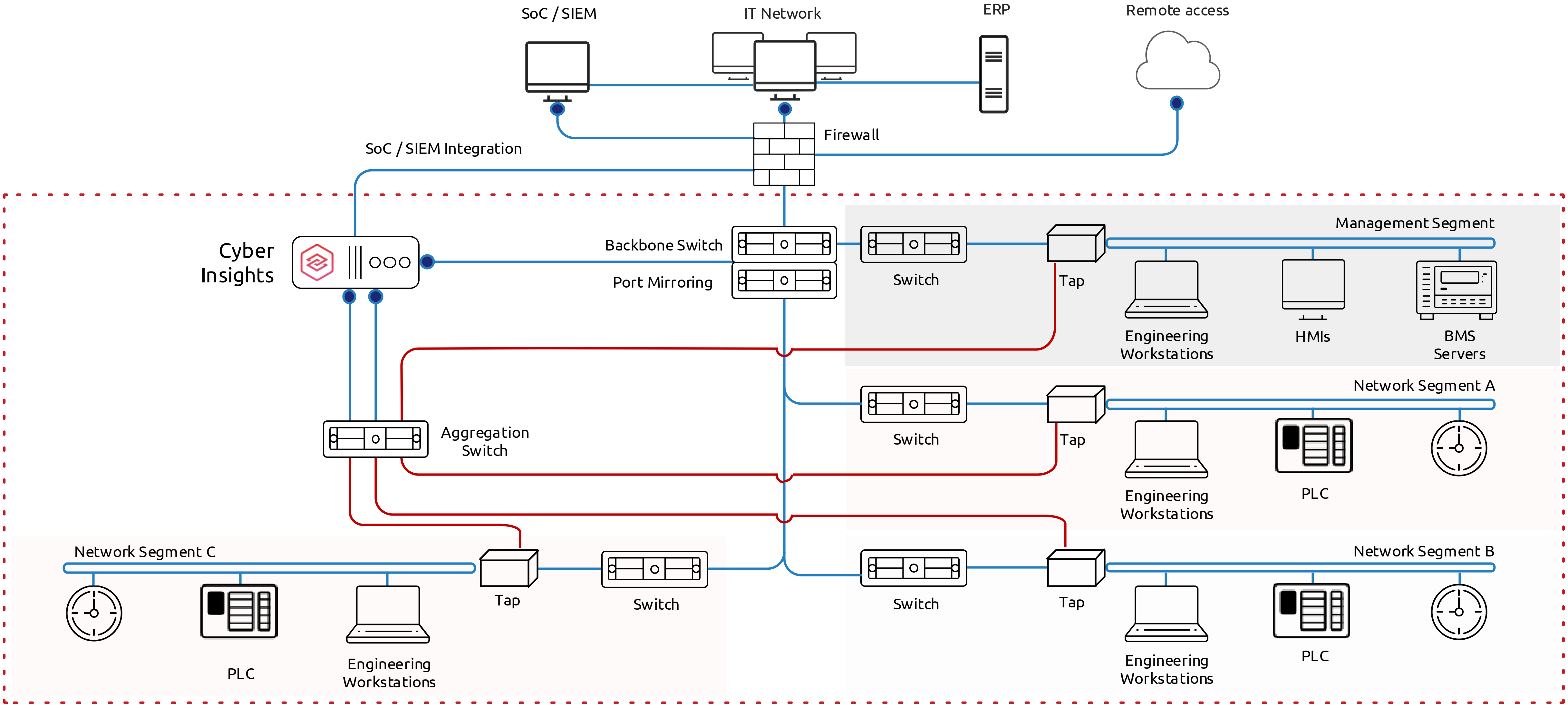
OUT-OF-BAND MONITORING NETWORK



OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

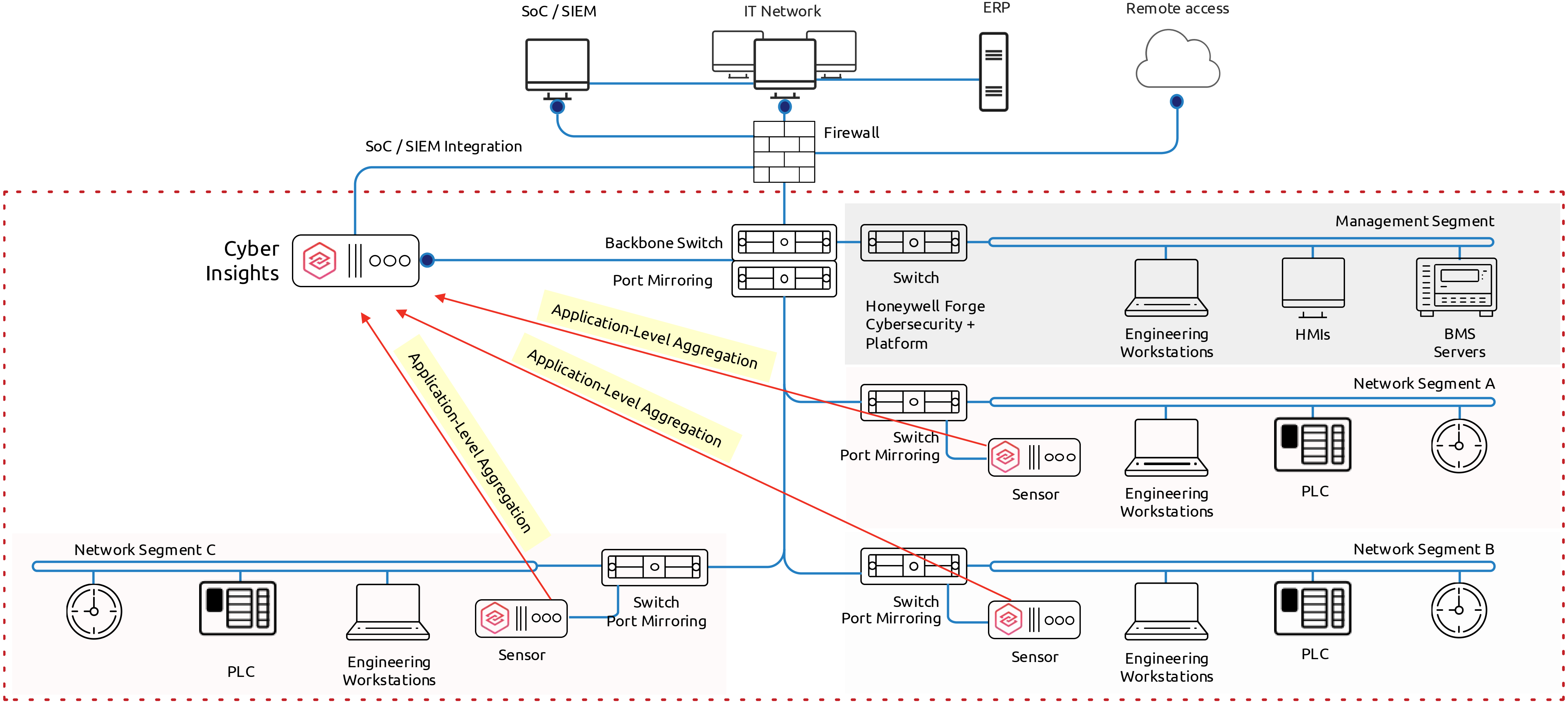
TAP DEVICE AGGREGATION



OTD BiLiŞiM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

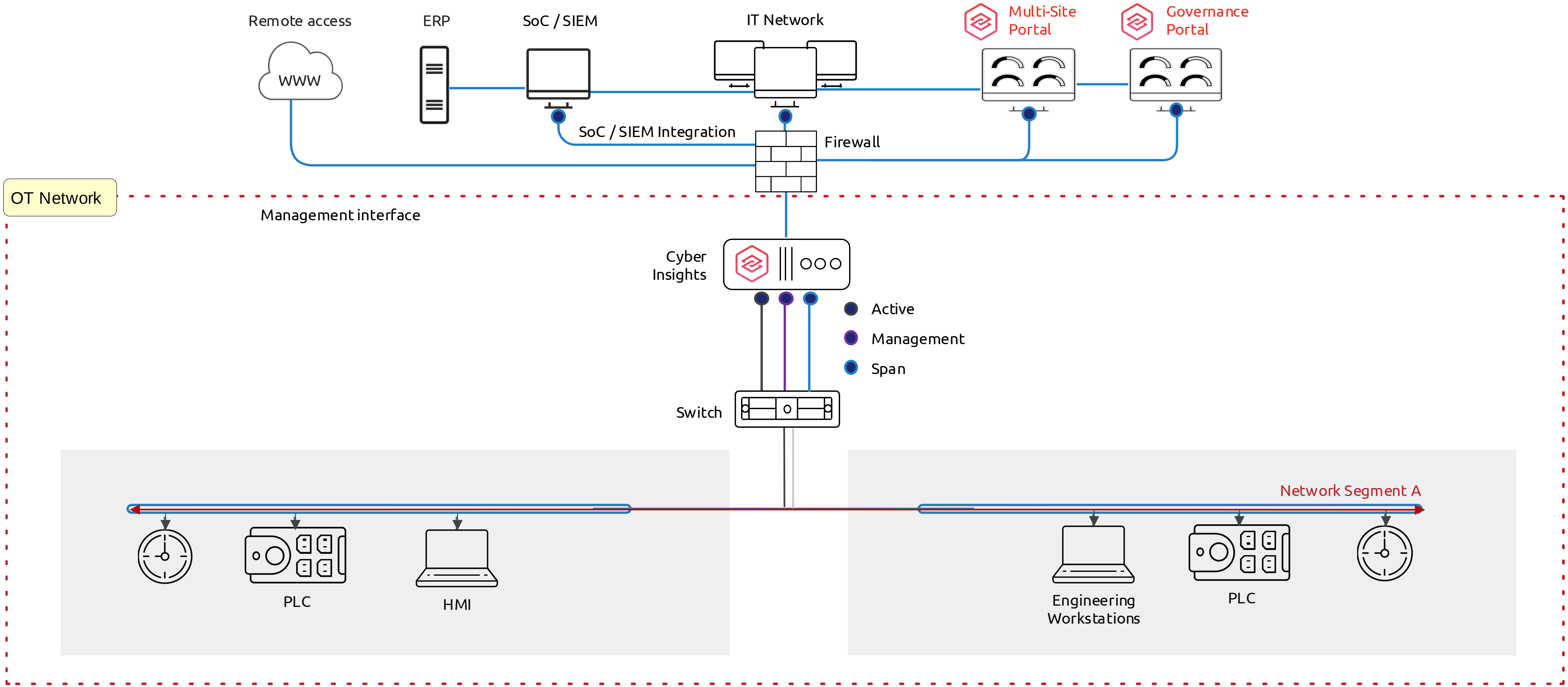
MULTI-SENSOR DEPLOYMENT



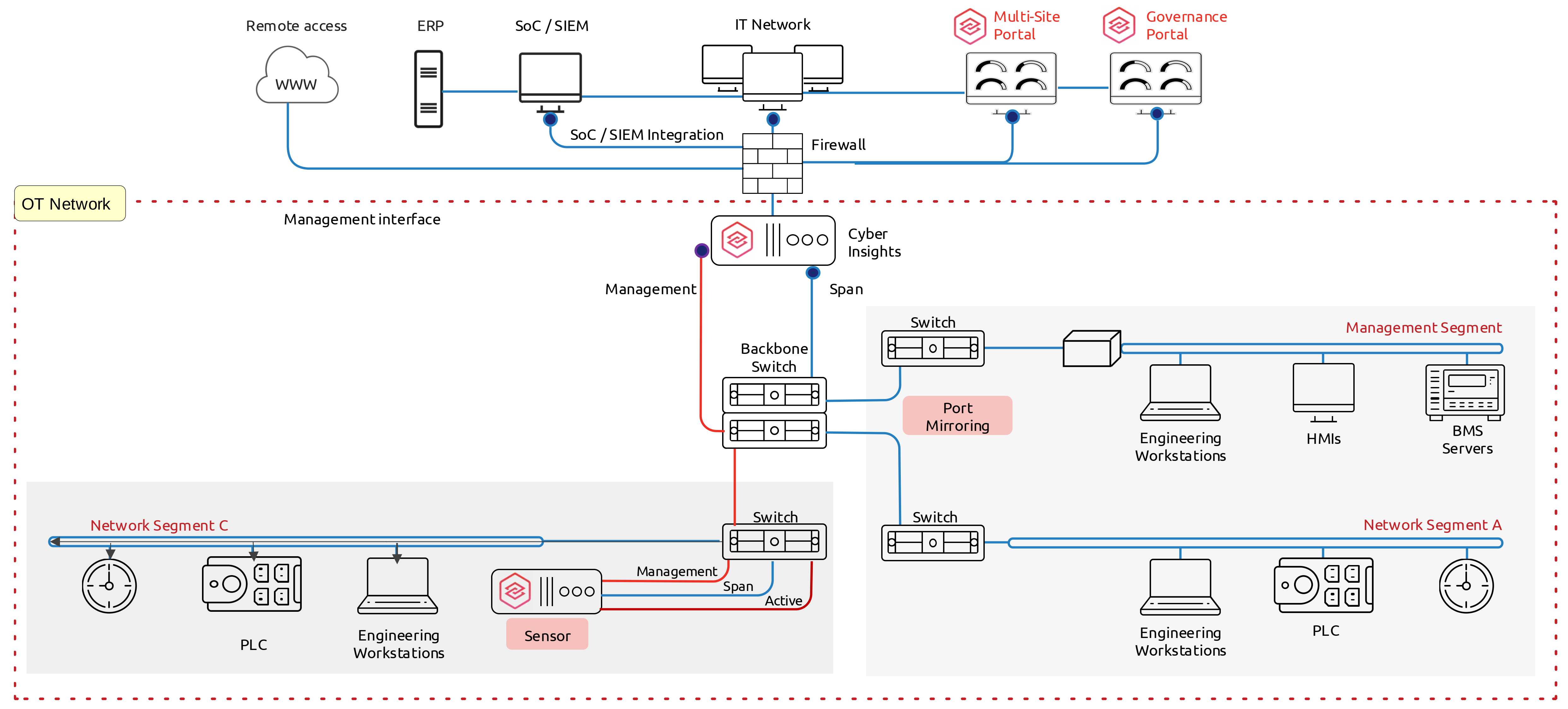
OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+

ACTIVE POLLING INITIATED FROM CYBER INSIGHTS



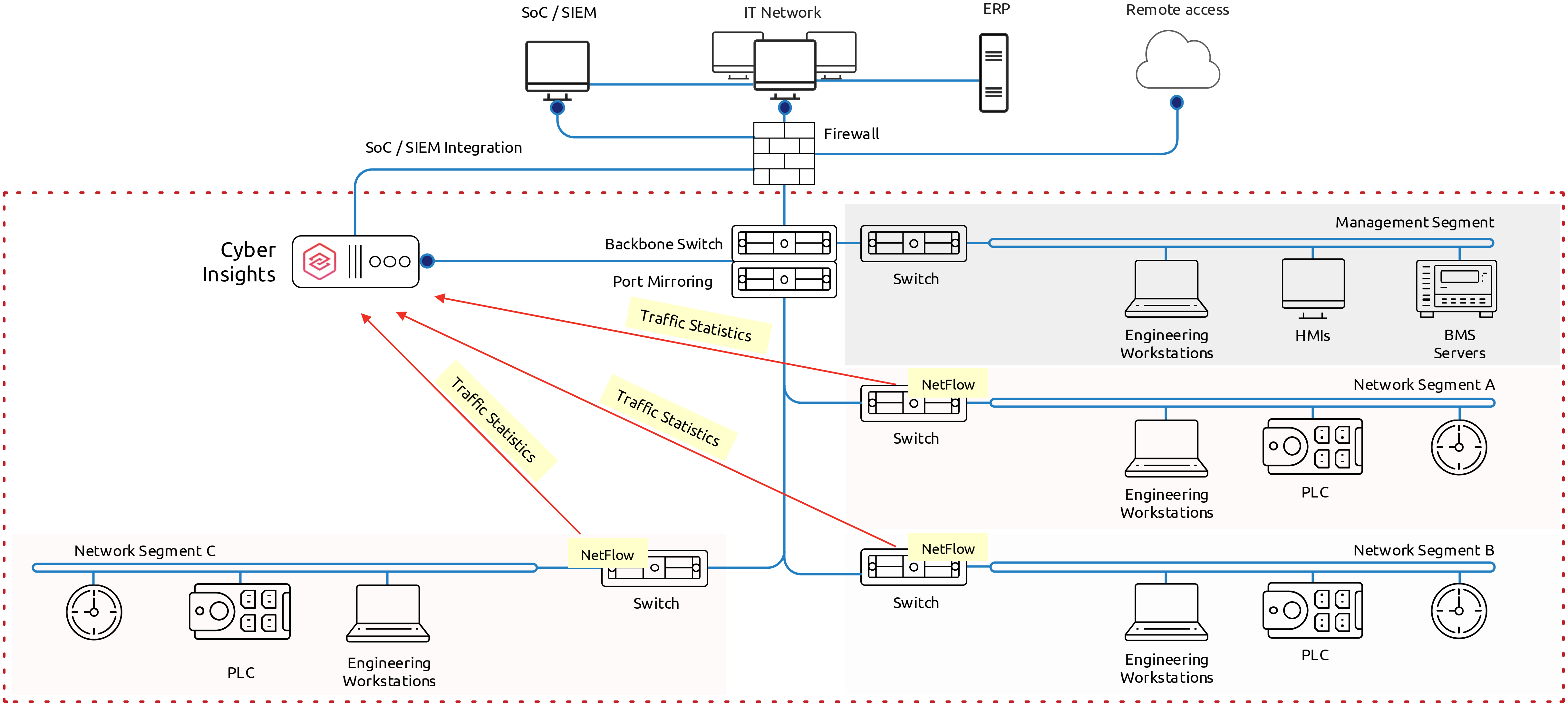
ACTIVE POLLING INITIATED FROM SENSOR



OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

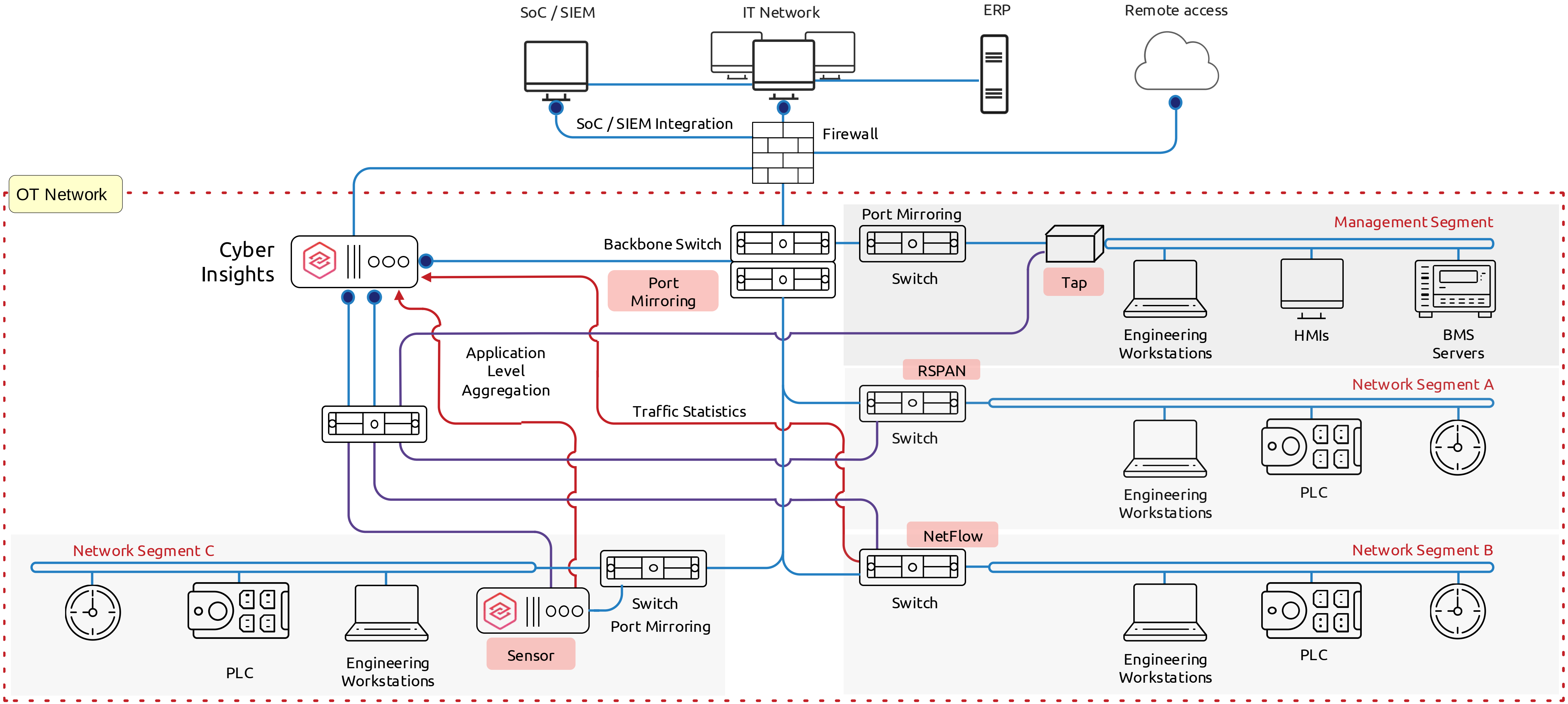
NETFLOW TRAFFIC ANALYSIS



OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

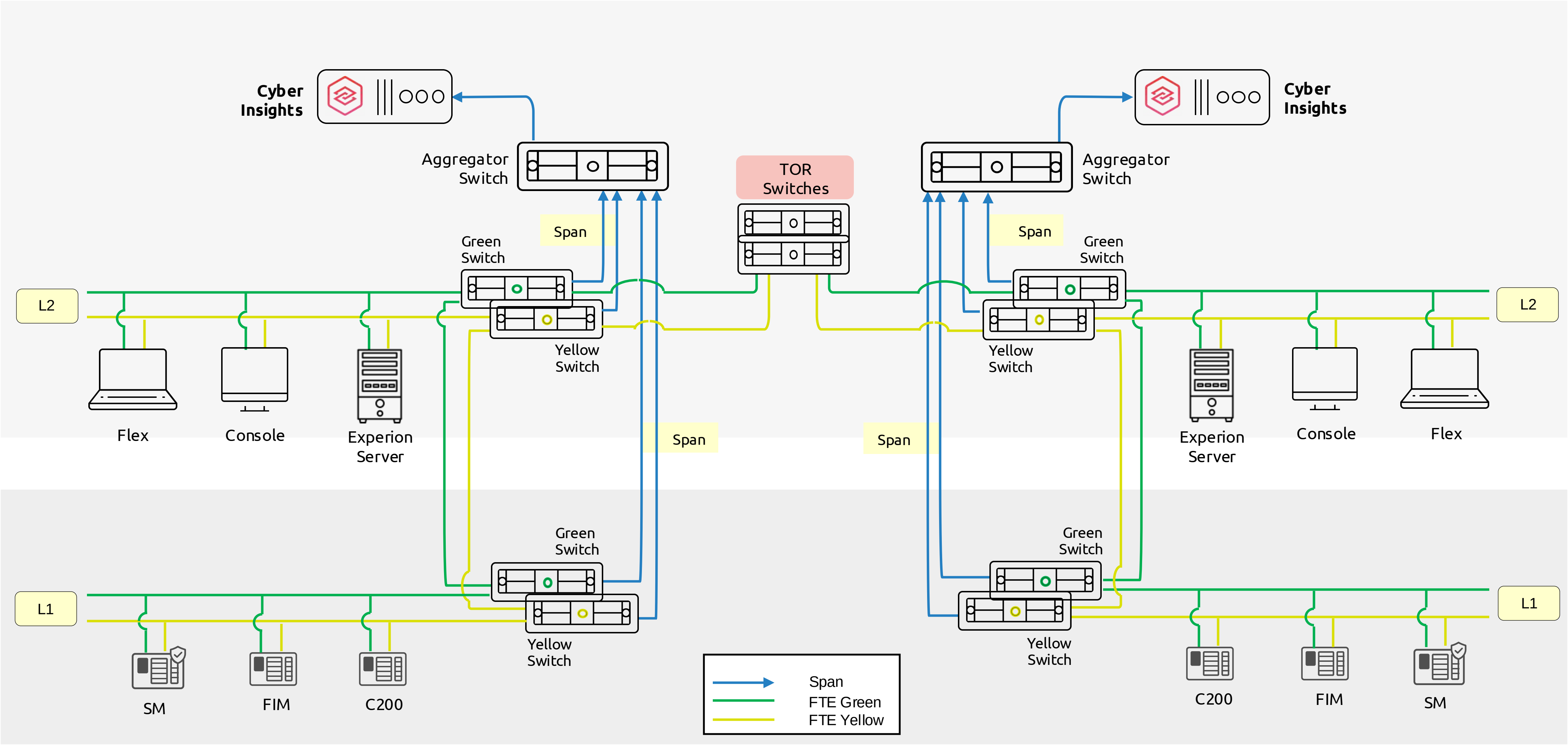
HYBRID DEPLOYMENT MODE



OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

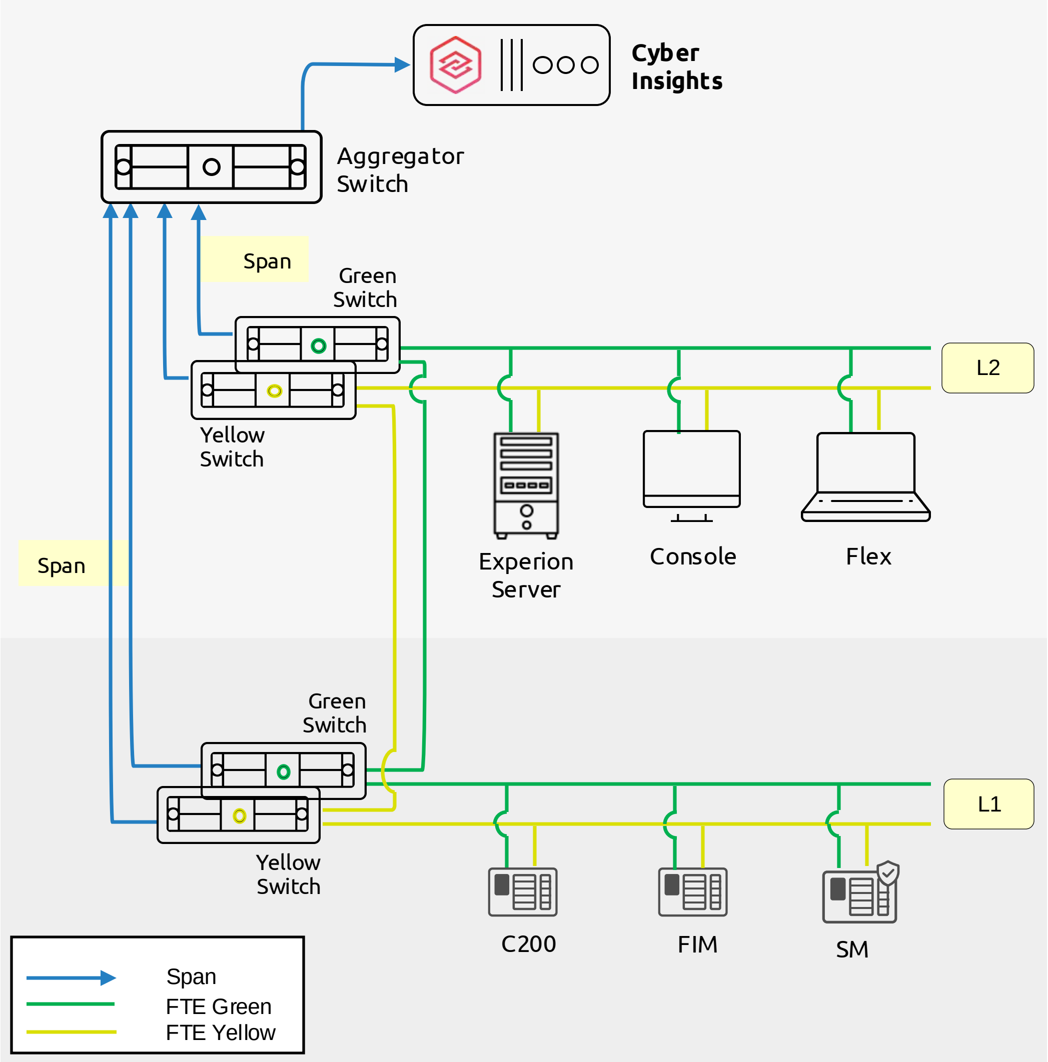
DEPLOYMENT IN EXPERION FTE MULTI-COMMUNITY NETWORK



OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

DEPLOYMENT IN EXPERION FTE SINGLE-COMMUNITY NETWORK


Cyber Insights
Aggregator Switch
Span
Green Switch
Yellow Switch
L2
Experion Server
Console
Flex
Span
Green Switch
Yellow Switch
L1
C200
FIM
SM
Span
FTE Green
FTE Yellow