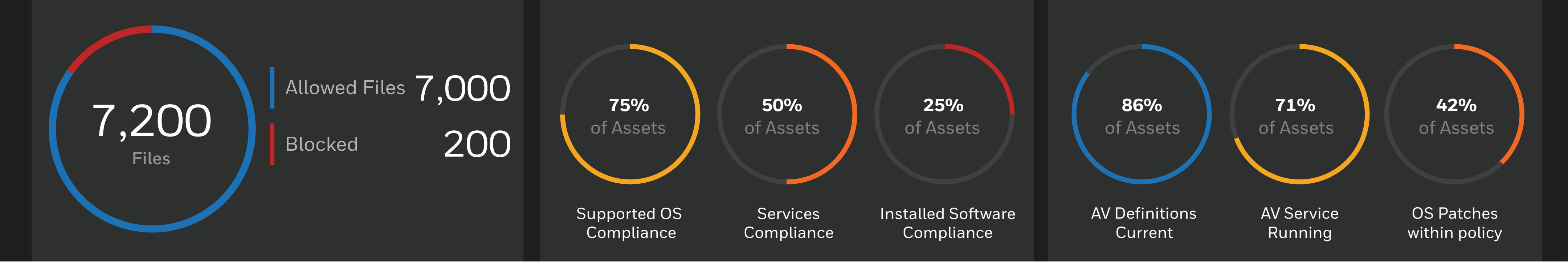
HONEYWELL FORGE CYBERSECURITY PLATFORM

Simplify, Strengthen and Scale Industrial Cybersecurity Across Your Enterprise

Honeywell



THE NEED FOR AN ENTERPRISE APPROACH TO CYBERSECURITY

As businesses move to digitally connect their operations, having a site-specific strategy on cybersecurity is no longer safe or practical.

Organizations leading digital transformation are developing enterprise-wide cybersecurity solutions that drive greater consistency and protection across operational technology environments.

Solutions should meet industry standards and regulatory compliance requirements while remaining easy to use by teams stretched with increased responsibilities.

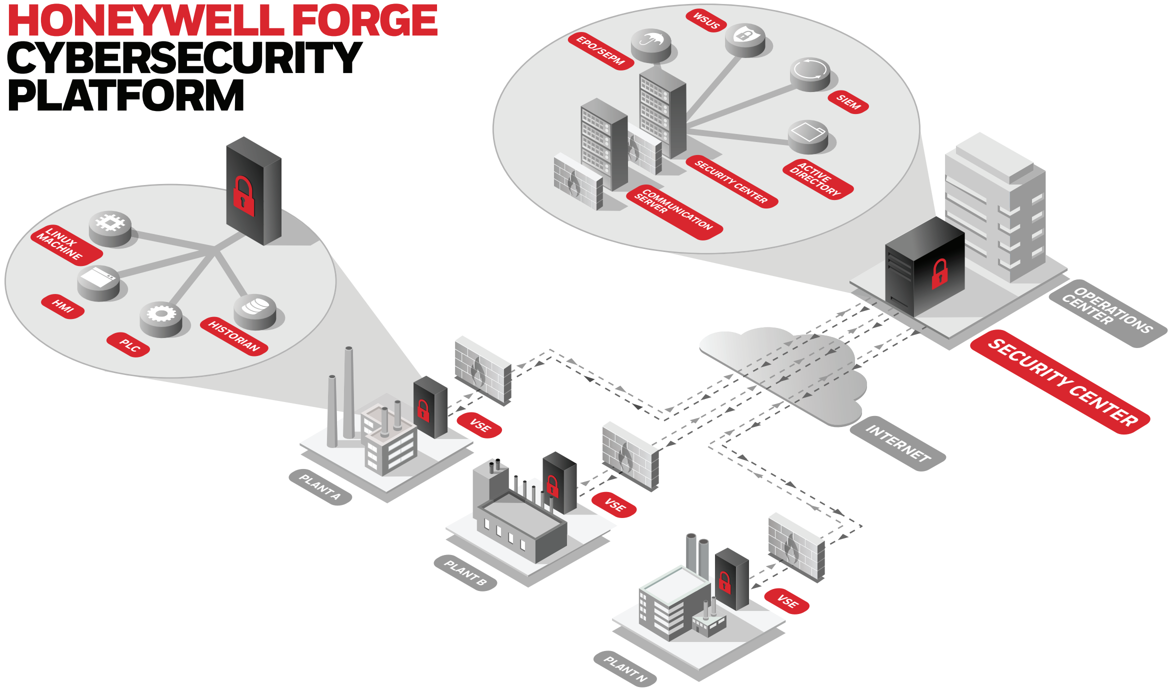
A UNIFIED PLATFORM TO SAFELY MANAGE GROWTH AMIDST HIGH CYBERSECURITY RISK

Introducing Honeywell Forge Cybersecurity Platform, a robust software solution that simplifies, strengthens and scales industrial cybersecurity operations for any asset-intensive business facing evolving threats.

Honeywell Forge for Cybersecurity improves cybersecurity performance—at a single site or across multiple sites—by increasing visibility into vulnerabilities and threats, enabling proactive action to mitigate risks and improving cybersecurity management efficiency.

As cyberattack costs can run into millions of dollars, the software delivers a simple yet scalable threat management option for companies in any stage of cybersecurity maturity. From inventorying assets on a network; to moving and using operations data; to strengthening endpoint and network security; to improving cybersecurity compliance and more, the new platform delivers a grow-as-you-go software solution to better address cybersecurity pain points in operational technology (OT) and industrial internet of things (IIoT) environments.

HONEYWELL FORGE CYBERSECURITY PLATFORM



HIGH-LEVEL BENEFITS

- **Simplifies** cybersecurity for industrial operators by unifying the most commonly needed OT security capabilities in one software platform.
- **Strengthens** the cybersecurity of industrial assets across an enterprise with a field-proven platform that combines the essentials of cybersecurity operations with advanced asset security management.
- **Scales** cybersecurity investments with grow-as-you-go software that continually delivers more security and operations management capabilities, all from one global strategic provider.

HIGH-LEVEL FEATURES

- **Software solution** that improves OT cybersecurity performance across an enterprise.
- **Single platform** for multi-site OT cybersecurity operations.
- **Vendor-neutral solutions** that help strengthen cyber defenses, regardless of control system.

SECURE REMOTE ACCESS FOR SAFE CONNECTIVITY

Honeywell Forge Cybersecurity Platform helps secure remote field assets from a single security and operations center. This field-proven technology automates the deployment and enforcement of system-wide security policies while focusing on cybersecurity essentials such as inventory visibility, patching, log collection, remote access and compliance.

Complying with the NIST Cybersecurity Framework, the NIST SP 800-82 guidelines and leading international standards (including NERC CIP, ENISA, PERA, ISO 27001 and ISA/IEC-62443), Honeywell Forge Cybersecurity Platform improves the cybersecurity compliance posture across industrial organizations.

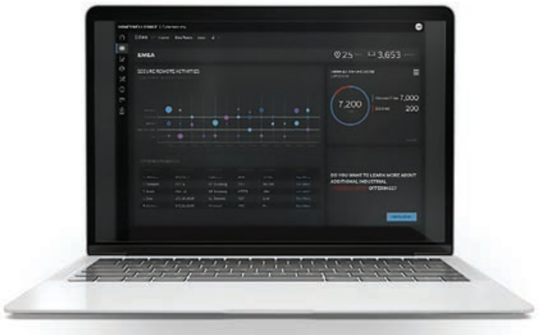
Deployed at thousands of sites worldwide in diverse sectors ranging from oil and gas, utility, chemical, mining and manufacturing, Honeywell Forge delivers unrivaled visibility, reliability and compliance for plant operations.

Oil & Gas | Metals, Minerals & Mining | Chemicals

Utilities & Power | Pulp and Paper | Water & Wastewater | CPG

Food & Beverage | Drinking Water | Pharma & BioTech | Manufacturing

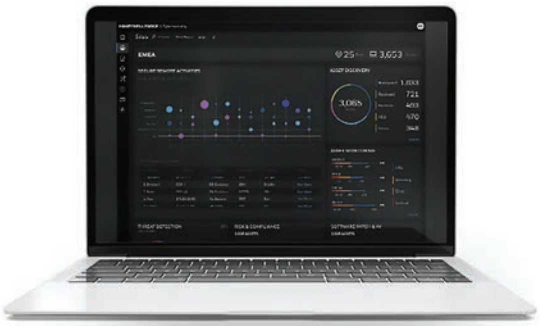
THREE DIFFERENT OFFERINGS TO SUIT GROWING NEEDS



ENTERPRISE CORE

For companies with multi-site secure connectivity needs, Enterprise Core delivers key cybersecurity operations management features including:

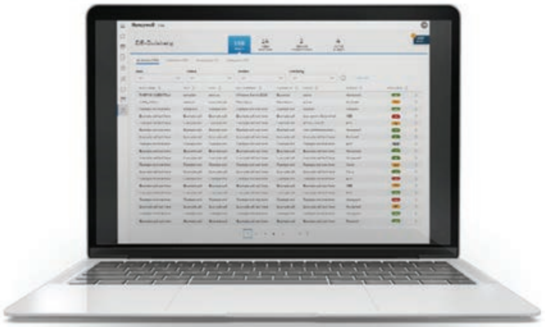
- Secure Remote Access with advanced granular controls engineered for industrial environments.
- Secure Content Transfer with built-in file-based threat detection.
- The platform Security Center server components.
- One or more site-level Virtual Security Engines (VSEs)



ENTERPRISE PREMIUM

For companies seeking to take full advantage of Honeywell's latest cybersecurity innovations, Enterprise Premium can be applied in addition to Enterprise Core, providing asset security management capabilities across multiple sites. Modules in the Enterprise Premium offering include:

- Asset Discovery and Inventory
- Asset Monitoring and Alerting
- Software Patch and Antivirus (AV) Management
- Risk and Compliance Management



SITE OFFERING

For companies exploring select platform capabilities at a single-site level, the Site Offering features include:

- Asset Discovery and Inventory
- Asset Monitoring and Alerting
- Risk and Compliance Monitoring

UNRIVALED VISIBILITY, RELIABILITY AND COMPLIANCE

HONEYWELL FORGE CYBERSECURITY PLATFORM OVERVIEW

● ENTERPRISE CORE
🔴 ENTERPRISE PREMIUM
○ SITE OFFERING

FEATURE	RISK AND COMPLIANCE MONITORING	SECURE REMOTE ACCESS	SECURE CONTENT TRANSFER	ASSET DISCOVERY AND INVENTORY	MONITORING AND ALERTING	SOFTWARE PATCH AND AV MANAGEMENT	RISK AND COMPLIANCE MANAGEMENT
	○	● 🔴	●	○ 🔴	○ 🔴	🔴	🔴
DESCRIPTION	At-a-glance visibility into an intuitive asset risk score, with drill-down capabilities to fully view information on risk factors and compliance with predetermined security policies.	Increase cybersecurity by connecting to IT or OT assets for service delivery, troubleshooting or remote operations.	Increase cybersecurity by moving and using OT-centric data for file delivery, analytics and more; built-in threat detection inspects files transferred between sites for potentially malicious material.	Provides a comprehensive list of assets on the network using active or passive discovery.	Monitor assets for potential cybersecurity issues and alert operators with notifications for items that require resolution.	Patch OT assets and manage antivirus per organizational standards.	Provides an enterprise-level view into site compliance and risk levels with drill-down capabilities to fully gain information on risk factors, compliance with predetermined security policies and remediation advice.
BENEFIT	• Gain visibility into process control network security status • Speed and simplify OT cyber security reporting • Focus cyber operations resource efforts on assets that are most at risk or out of compliance with security policies	• Simplify access to cross-vendor assets • Centralize control over all remote access sessions enterprise wide • Standardize remote access procedures • Supervise and audit sessions • Control via role-based and device-specific access permissions and privileges • Lower cost and complexity for managing third-party resources and maintenance personnel	• Reduce data leaks— securely distribute files within/in/out of OT • Analyze and act on insights— transfer logs and performance data to SIEM at a corporate SOC • Improve recovery time sending large files to/from file backup and restore	• Accurately identify assets, including specific configuration details • Automate the maintenance of asset inventory with device information to expedite future risk determination	• Proactively manage OT networks • Automate data collection of key cybersecurity indicators • Automate notifications specific to customer environment and organization	• Reduce vulnerabilities—centrally manage software updates • Comply with internal standards—patch Windows systems (using Microsoft WSUS) • Control update timing, approach and configuration to protect uptime • Update Experion® PKS, HMIs and historians • Coordinate AV patching across OT network environments	• Gain visibility into site cybersecurity status • Easily identify related actions to improve ICS security posture • Speed and simplify cybersecurity reporting • Focus cyber operations resource efforts on site assets that are most at risk or out of compliance with security policies

CYBERSECURITY AS-A-SERVICE

For companies seeking complete support and management of Honeywell Forge Cybersecurity Platform by cybersecurity experts, Honeywell provides multiple service options, including Managed Security Services and Consulting Services. These global capabilities deliver skilled design and implementation for the software platform as well as ongoing critical industrial cybersecurity management and monitoring to reduce time-to-operations and increase cybersecurity compliance.

HIGH-LEVEL CUSTOMER CHALLENGES

- **Elevated Cybersecurity Risk**
  Cybersecurity risk is high for certain industrial operators amidst increasing network connectivity, digital transformation initiatives and evolving operational landscapes.

- **Costly Threat Impact**
  The impact of cybersecurity risks on manufacturing operations has become more publicly visible to executive leaders and government regulators, placing great pressure on industrial companies to ramp up defenses.

- **Changing Security Ownership**
  IT leadership is increasingly hands-on in defining requirements for and choosing plant cybersecurity solutions, yet OT retains critical needs.

- **Provider Density**
  Market-disrupting vendors are making it harder for industrial companies to protect what matters most, adding too many products which increases workload on already stretched staff who are not all cybersecurity experts.

PLANT-LEVEL CHALLENGES

- **Invisible Risk**
  Little/no OT asset visibility, monitoring and alerting.

- **Safety Implications**
  Need to protect assets, operations and people.

- **OT Complexity**
  Stretched teams and difficult to acquire new talent.

- **Increasing Company and Regulatory Compliance**
  Heavy fines for cybersecurity noncompliance.

INDUSTRY-PROVEN TECHNOLOGY

CUSTOMER CASE STUDIES*

Pulp & paper producer leverages Honeywell Forge for Cybersecurity solution to help protect 140+ sites

A large industrial manufacturer relies on Honeywell Forge for Cybersecurity technology to help secure over 140 sites around the world. Cybersecurity operations are simplified with the use of Honeywell Forge secure remote access and content transfer capabilities.

Global food & beverage producer relies on Honeywell Forge for Cybersecurity solution to help protect 100+ sites worldwide

One of the world's leading producers of confectionary relies on Honeywell Forge for Cybersecurity technology to help secure over 100 industrial facilities in multiple countries with secure remote access, remote monitoring and more.

**Company names withheld for security reasons*

USE CASES & BENEFITS

Consolidate Secure Remote Access
From many to one: reduction of unmanaged network connections

Securely Transfer Content and Data
Enable connected OT and digital transformation

Automate Asset Discovery and Inventory
$200K+ per year in labor reduction per site[1]

Mitigate Cybersecurity Risk; Continuously Monitor
$75M+ in attack damage mitigation[2]

Avoid Regulatory Noncompliance
$10M+ penalty potential with policy enforcement[3]

Improve Cybersecurity Performance
35%+ efficiency gains through automation[3]

Sources

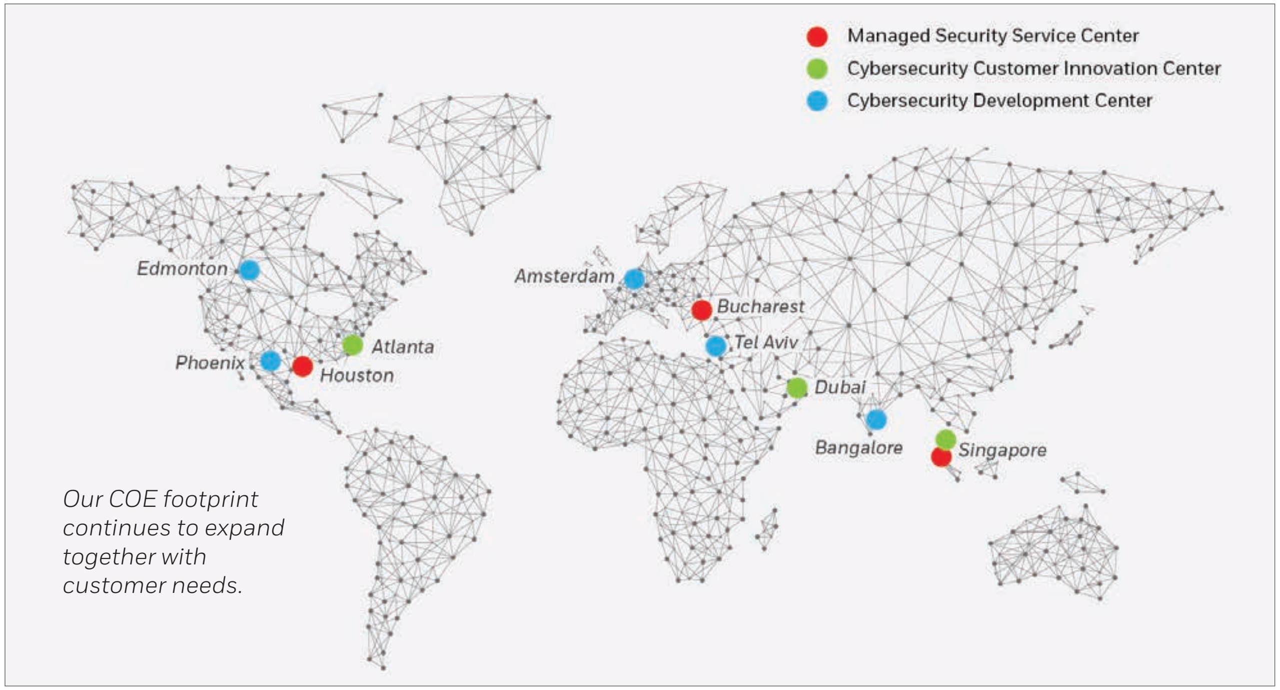
[1] Based on Honeywell project experience in 2019.
[2] CPOmagazine.com. August 2, 2019.
[3] SecurityWeek.com. February 4, 2019.

TOUR OUR GLOBAL CYBERSECURITY CENTERS OF EXCELLENCE

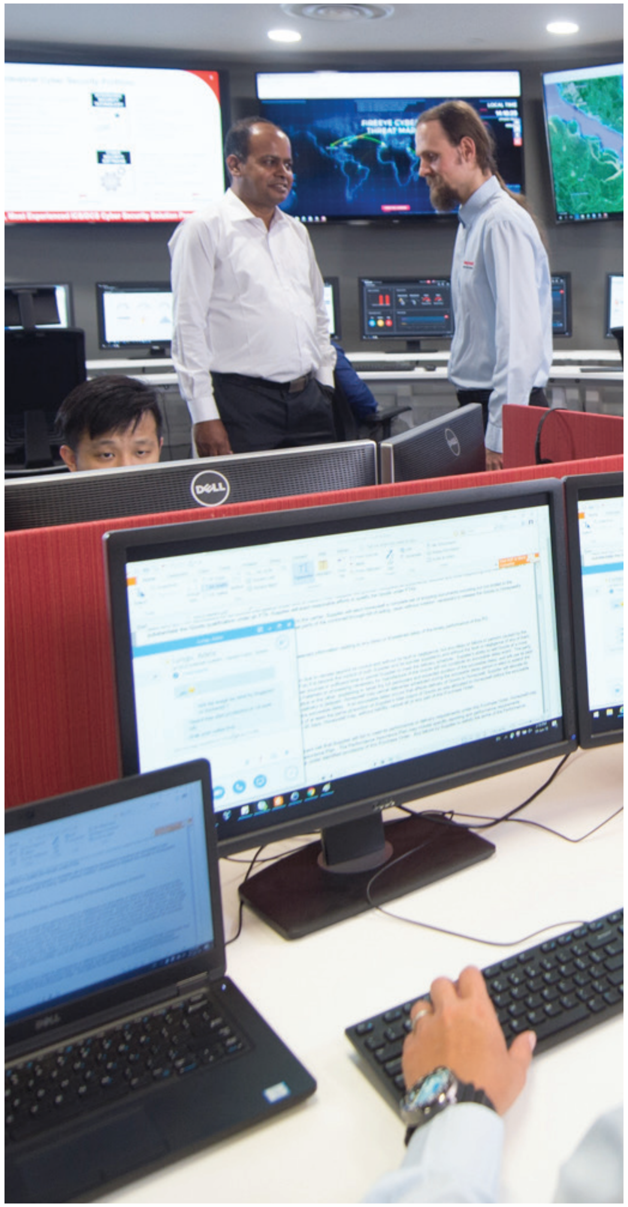
Honeywell's Cybersecurity Centers of Excellence (COEs) provide state-of-the-art facilities and specialized technical personnel to help customers simulate, validate and accelerate industrial cybersecurity initiatives—all in an exciting setting with world-class demonstration capabilities. By leveraging Honeywell's COE resources, customers can ultimately save time, budget and costly security mistakes as they improve their organization's industrial cybersecurity maturity.

COEs help educate operators, engineers and executive leadership, sharing the latest best practices to help protect process control networks from current and emerging industrial cybersecurity threats. At our COEs worldwide, customers can experience simulated control system cyberattacks, safely test industrial solutions and try out both existing and experimental new security solutions.

Honeywell COEs are currently available in Atlanta, Georgia (USA), Dubai (UAE), and Singapore and are open to any customer or interested party around the world.


● Managed Security Service Center
● Cybersecurity Customer Innovation Center
● Cybersecurity Development Center
Edmonton
Phoenix
Houston
Atlanta
Amsterdam
Bucharest
Tel Aviv
Dubai
Bangalore
Singapore

Our COE footprint continues to expand together with customer needs.



THE HONEYWELL ADVANTAGE

INDUSTRIAL EXPERIENCE, AWARD-WINNING TECHNOLOGY AND CYBERSECURITY EXPERTS

With 100+ years of domain experience, Honeywell is a leader in industrial manufacturing and technology innovation. We have used that expertise over the past 15+ years to become a leader in industrial cybersecurity solutions that help protect the world's most critical infrastructure.

Our broad portfolio includes OT cybersecurity software products and services that allow customers flexibility in determining the best level of engagement, from Managed Security Services to cybersecurity consulting to industry-proven software. At Honeywell, we leverage our award-winning technology and industry-leading expertise with certified cybersecurity experts you can trust.

Founding member

> *Honeywell Forge for Cybersecurity is a big step forward in the company's overall cybersecurity strategy, moving from separate product offerings to a unified suite of applications, services and products that can address a range of end user cybersecurity requirements from asset discovery and monitoring and secure remote access to fully managed services. Honeywell Forge also represents a common approach to OT level cybersecurity that recognizes the impact of IoT on manufacturing, including the monitoring of virtual machines, firewalls, and other assets in industrial environments.*
>
> *— Larry O'Brien, Vice President of Research, ARC Advisory Group*

For More Information
To learn more, visit:
www.becybersecure.com or
contact your Honeywell
Account Manager, Distributor
or System Integrator.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, GA 30308
www.honeywell.com

BR-19-43-ENG
Sept 2019

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell