ПРОГРАММЫ

Технические характеристики

на Forge Cybersecurity Suite

SCALABLE SOLUTIONS
FOR OT CYBERSECURITY

As industrials digitally transform by connecting their operational technology (OT) assets and enable remote capabilities, cybersecurity becomes fundamental for protecting business continuity. From safely operating a complex ecosystem of plant control systems to avoiding non-compliance fines, industrials need a simple, centralized way to administer cybersecurity across the enterprise.

Honeywell Forge Cybersecurity Suite is a unified software solution that simplifies, strengthens, and scales industrial cybersecurity for businesses with a complex OT environment. From a single site to a global footprint, Cybersecurity Suite:

**Strengthens
Business Continuity**

**Increases visibility to
vulnerabilities and threats**

**Enables proactive action
to mitigate risks**

**Improves   cybersecurity
management efficiency**

STREAMLINED AND VENDOR-AGNOSTIC

Simplify

Unifies the most commonly needed OT security capabilities in a single solution.

Strengthen

Combines cybersecurity essentials with advanced asset security management.

Scale

Uses a cloud-capable, vendor-agnostic approach so it seamlessly integrates and grows with the business.

BENEFITS

- Increase staff productivity by 35% with access to experts[1]

- Reduce cyber operations cost by $1.2M/ year by consolidating platforms[1]

- Improve issue time-to-resolve by 90%[1]

- Improve compliance and reduce regulatory fines by potential millions[2]

ENABLING SECURE REMOTE ACCESS FOR INDUSTRIALS

Remote operations are no longer on the wish list for industrials – they are critical for business continuity in an era when supply chains and labor can be easily disrupted. While connecting OT assets brings great benefit it also exposes them to cyber threats that can harm critical assets or even the workforce.

Honeywell Forge Cybersecurity Suite offers a remote access solution to enable employees, vendors, and systems remote access to OT assets in the field, all controlled from a single security and operations center. Cybersecurity Suite uses a single outbound connection approach to:

- Simplify the manageability and visibility of complex OT environments

- Provide granular access control to assets based on privileges

- Automate deployment and enforcement of system-wide security policies

- Streamline patching and log collection

Compliance

Cybersecurity Suite complies with:

- IST Cybersecurity Framework
- IST SP 800-82 guidelines
- International standards
  - o NERC CIP
  - o ENISA
  - o PERA
  - o ISO 27001
  - o ISA/IEC-62443
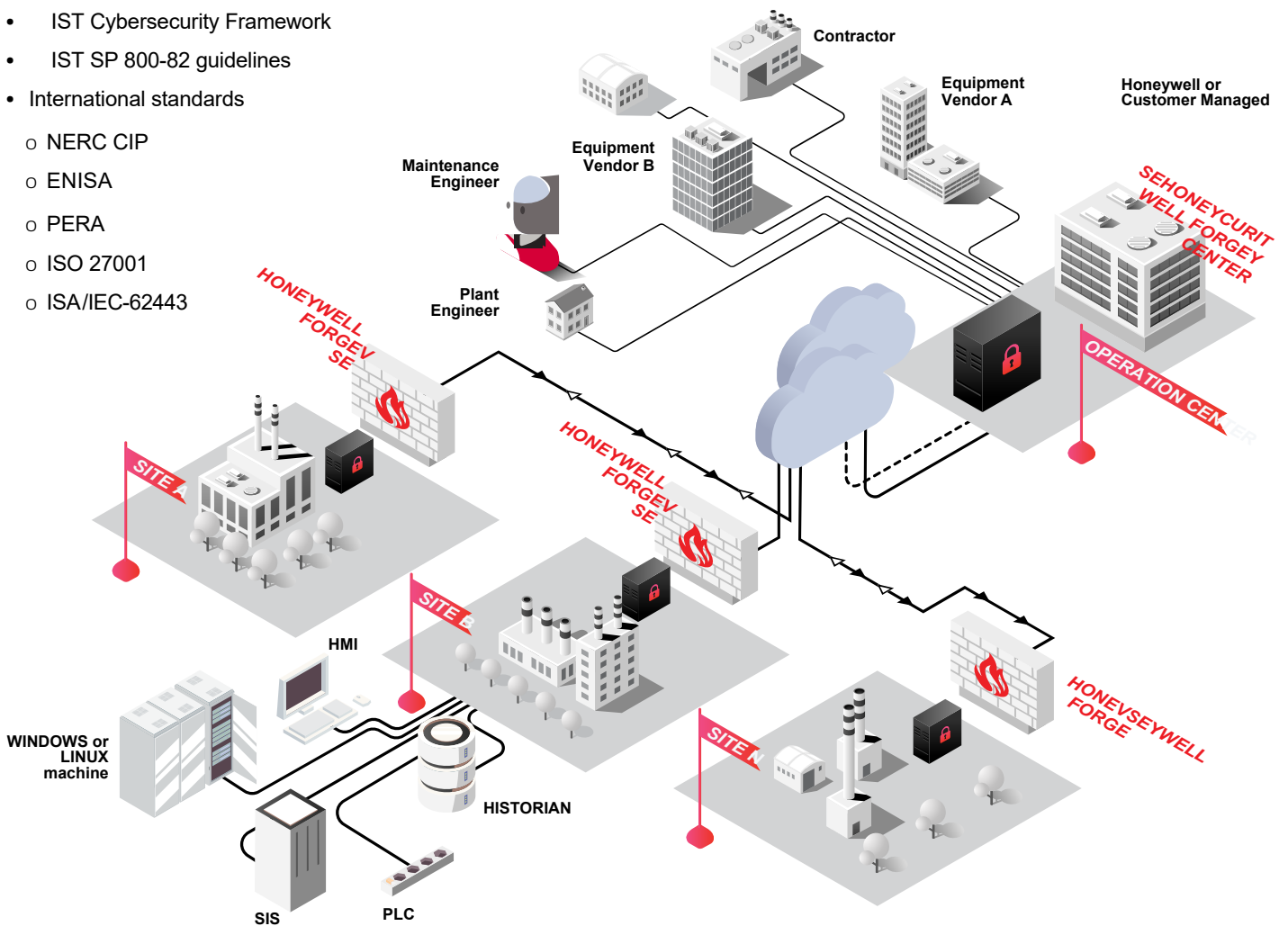
SOLUTIONS
TO FIT YOUR NEEDS

Honeywell Forge Cybersecurity Suite is available in three offerings:

01

Enterprise Core
Includes key cybersecurity management features:

Secure Remote Access:
Advanced granular controls designed for industrials

Secure Content Transfer: With built-in, file-based threat detection

Enterprise Security:
Centralized management with one or more site-level virtual security engines (VSEs)

02

Enterprise Premium
Core features, plus:

Asset Discovery and Inventory:
Automatically find and catalog assets

Asset Monitoring and Alerting:
Detects and warns of threats to individual assets

Software Patch and Antivirus (AV) Management:
Ensures assets have the latest approved security updates

Risk and Compliance Monitoring:
Real-time monitoring to ensure operations are running as designed

03

Site
Features for single sites:

Asset Discovery and Inventory:
Passive and active methods built for industrial operations

Risk Monitoring:
Continuous monitoring and scoring of cybersecurity risks to help with faster response times

BEST FOR
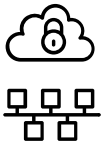
Multi-site environments needing secure remote access solutions
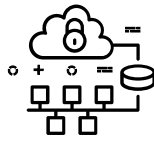
Multi-site environments with advanced OT cybersecurity operations requirements

Best for single site OT environments

INDUSTRIES

Honeywell Forge Cybersecurity Suite is designed with Honeywell's deep understanding of the unique needs of industrials, specifically:

- **Oil & Gas**
- **Metals, Minerals & Minerals**
- **Utilities & Power**
- **Food & Beverage**
- **Manufacturing**
- **Pharma & Biotech**

DELIVER VISIBILITY, RELIABILITY, AND COMPLIANCE

| Feature and Benefit Comparisons

FEATURE

Risk Monitoring	Secure Remote Access	Secure Content Transfer	Asset Discovery and Inventory	Software Patch and AV Management	Risk and Compliance Management
●	● ●	● ●	● ●	●	●

DESCRIPTION

Risk Monitoring	Secure Remote Access	Secure Content Transfer	Asset Discovery and Inventory	Software Patch and AV Management	Risk and Compliance Management
At-a-glance visibility into an intuitive asset risk score, with drill- down capabilities to fully view information on risk factors.	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.	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

Risk Monitoring	Secure Remote Access	Secure Content Transfer	Asset Discovery and Inventory	Software Patch and AV Management	Risk and Compliance Management
• Gain visibility into process control network security status • Speed and simplify OT cybersecurity reporting • Focus cyber operations resource efforts on assets that are most at risk • Proactively manage OT networks • Automate data collection of key cybersecurity indicators • Automate notifications specific to customer environment and organization	• 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 acton 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	• 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 actionsto 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 • Proactively manage OT networks • Automate data collection of key cybersecurity indicators • Automate notifications specific to customer environment and organization

# SUPPORT BACKED BY HONEYWELL'S GLOBAL REACH AND EXPERTISE

Cybersecurity Centers of Excellence (COE)

Visit these state-of-the-art facilities and specialized technical personnel to help you simulate, validate and accelerate industrial cybersecurity initiatives
in a safe and secure environment.

Cybersecurity Managed Services

Need help to reduce time-to-operations and increase cybersecurity compliance? Honeywell offers global managed security and consulting services. Access skilled design and implementation resources, ongoing critical industrial cybersecurity management, and monitoring.

- ● Managed Security Service Center
- ● Cybersecurity Customer Innovation Center
- ● Cybersecurity Development Center

Our COE footprint continues to expand together with customer needs.
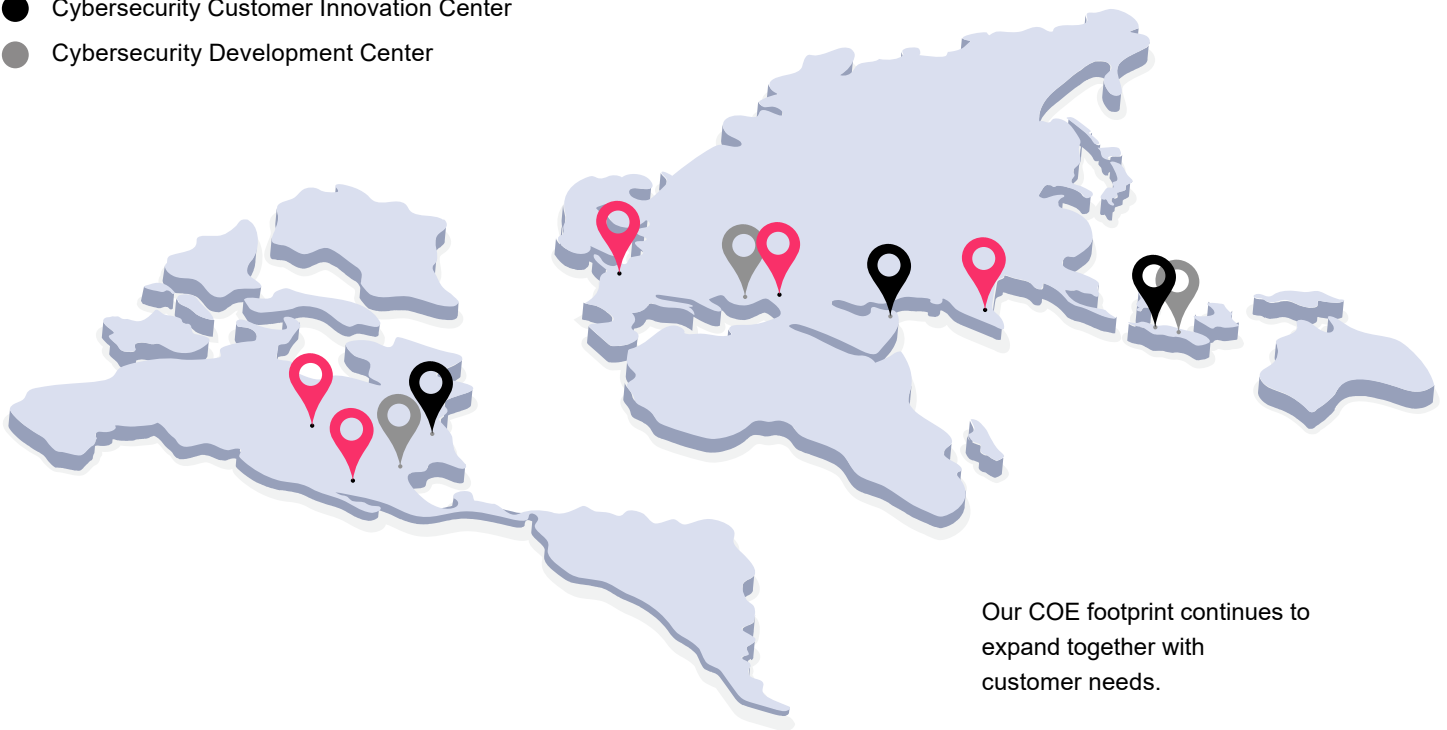
По вопросам продаж и поддержки обращайтесь:

Алматы (7273)495-231
Ангарск (3955)60-70-56
Архангельск (8182)63-90-72
Астрахань (8512)99-46-04
Барнаул (3852)73-04-60
Белгород (4722)40-23-64
Благовещенск (4162)22-76-07
Брянск (4832)59-03-52
Владивосток (423)249-28-31
Владикавказ (8672)28-90-48
Владимир (4922)49-43-18
Волгоград (844)278-03-48
Вологда (8172)26-41-59
Воронеж (473)204-51-73
Екатеринбург (343)384-55-89
Иваново (4932)77-34-06
Ижевск (3412)26-03-58
Иркутск (395)279-98-46
Казань (843)206-01-48

Калининград (4012)72-03-81
Калуга (4842)92-23-67
Кемерово (3842)65-04-62
Киров (8332)68-02-04
Коломна (4966)23-41-49
Кострома (4942)77-07-48
Краснодар (861)203-40-90
Красноярск (391)204-63-61
Курган (3522)50-90-47
Курск (4712)77-13-04
Липецк (4742)52-20-81
Магнитогорск (3519)55-03-13
Москва (495)268-04-70
Мурманск (8152)59-64-93
Набережные Челны (8552)20-53-41
Нижний Новгород (831)429-08-12
Новокузнецк (3843)20-46-81
Новосибирск (383)227-86-73
Ноябрьск(3496)41-32-12

Омск (3812)21-46-40
Орел (4862)44-53-42
Оренбург (3532)37-68-04
Пенза (8412)22-31-16
Пермь (342)205-81-47
Петрозаводск (8142)55-98-37
Псков (8112)59-10-37
Ростов-на-Дону (863)308-18-15
Рязань (4912)46-61-64
Самара (846)206-03-16
Санкт-Петербург (812)309-46-40
Саранск (8342)22-96-24
Саратов (845)249-38-78
Севастополь (8692)22-31-93
Симферополь (3652)67-13-56
Смоленск (4812)29-41-54
Сочи (862)225-72-31
Ставрополь (8652)20-65-13
Сургут (3462)77-98-35

Сыктывкар (8212)25-95-17
Тамбов (4752)50-40-97
Тверь (4822)63-31-35
Тольятти (8482)63-91-07
Томск (3822)98-41-53
Тула (4872)33-79-87
Тюмень (3452)66-21-18
Улан-Удэ (3012)59-97-51
Ульяновск (8422)24-23-59
Уфа (347)229-48-12
Хабаровск (4212)92-98-04
Чебоксары (8352)28-53-07
Челябинск (351)202-03-61
Череповец (8202)49-02-64
Чита (3022)38-34-83
Якутск (4112)23-90-97
Ярославль (4852)69-52-93

Россия +7(495)268-04-70   **К**азахстан +7(7172)727-132   **К**иргизия +996(312)96-26-47

сайт: www.honeywell.nt-rt.ru || эл. почта: hwn@nt-rt.ru