Honeywell OT Cybersecurity

MANAGED SECURITY SERVICES
SECURE REMOTE ACCESS

SERVICE INFORMATION NOTE

Remote Connectivity for Today’s Threat Environment

With the increased adoption of remote work and cloud components, companies must do more to support their operational technology (OT) cybersecurity. Best-in-class organizations are doing more to protect their networks with increased visibility and secure access control to their ICS network. These companies are taking the steps needed to help ensure that connections are properly authenticated, and transmissions are securely encoded.

Honeywell’s Managed Security Services (MSS) offer industrial-grade Secure Remote Access to help secure business operations, manage remote access and reduce cybersecurity risk. Honeywell's latest technology applies principles of least privilege to deliver what is designed to be a Zero Trust solution for OT networks. With decades of experience in cybersecurity for industrial control systems, Honeywell professionals deploy Secure Remote Access solutions designed to maintain the optimum performance, integrity and security of network assets.

Zero Trust & Remote Privileged Access Management

Centralized remote access and cybersecurity support are crucial for business continuity and mitigating the cyber risks of managing global OT infrastructure. Honeywell's Secure Remote Access is designed to introduce Zero Trust security privilege controls and remote privileged access management (RPAM) to the OT environment. The solution layers on top of the existing environment in a way that can easily accommodate a wide range of protocols common to OT settings. By centralizing visibility and control, Honeywell's Secure Remote Access can help customers reduce operational costs and enforce compliance.

Key Features of Honeywell's Secure Remote Access Solution

Access Controls

- **Multi-factor authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

Connectivity Controls

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- **Terminate Connection** once work is complete

Oversight Controls

- Full **Audit Trail &** complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery for Business Continuity**

Overview of the Honeywell Secure Remote Access Solution

The core building blocks of the Honeywell Secure Remote Access platform are the 1) SRA Controller 2) Global Service Edge and 3) Local Service Edge. The following is a description of each element:

1. **Secure Remote Access (SRA) Controller** - The SRA Controller is designed to terminate the Transport Layer Security (TLS) 1.3 connections and enforce the access policies configured by the Honeywell SRA administrator. As a 'reverse-proxy,' all decryption and enforcement occur behind organizational firewalls. It is designed to provide the following:
    - Encrypted (TLS 1.3) outbound channel to the Edges
    - Identity access control - MFA
    - Policy enforcement
    - ZTNA model
    - Asset list with multiple supported RA protocols (RDP/VNC/SSH)
    - Session recording, approval, supervision, and termination
    - Session File Transfer brokering
    - Certificates are specific for each deployment (public & private keys)

2. **Global Service Edge -** The Global Service Edge is a cloud-based broker that routes users' requests based on a Server Name Indication (SNI) header to the relevant SRA Controller. The Global Service Edge also routes traffic from the users to the SRA Controller. The Global Service Edge is designed to never decrypt any traffic – the Secure Remote Access solution upholds the principles of Zero Trust. It is also designed to:
    - Route traffic from the users to the SRA controllers
    - Not store or decrypt data
    - Serve as intermediate connections between end-users and the controllers

3. **Local Service Edge –** The Local Service Edge is an on-premises broker that routes users' requests based on an SNI header to the relevant SRA. In all deployment models, the Local Service Edge is designed to route traffic from the users to the SRAs. The Local Service Edge can operate without any external connections, which makes Honeywell Secure Remote Access an ideal secure access solution for OT environments that are air-gapped or disconnected from the Internet. The Local Service Edge is designed to:

   - Connect to the Global Service Edge network with outbound connectivity (TLS1.3)
   - Not store or decrypt data
   - Serve as an intermediate connection between end-users and the controllers
   - Allow local LAN users to stay local when connecting to the controller

Honeywell Remote Access Solution – Application Access, Not a VPN Network Tool

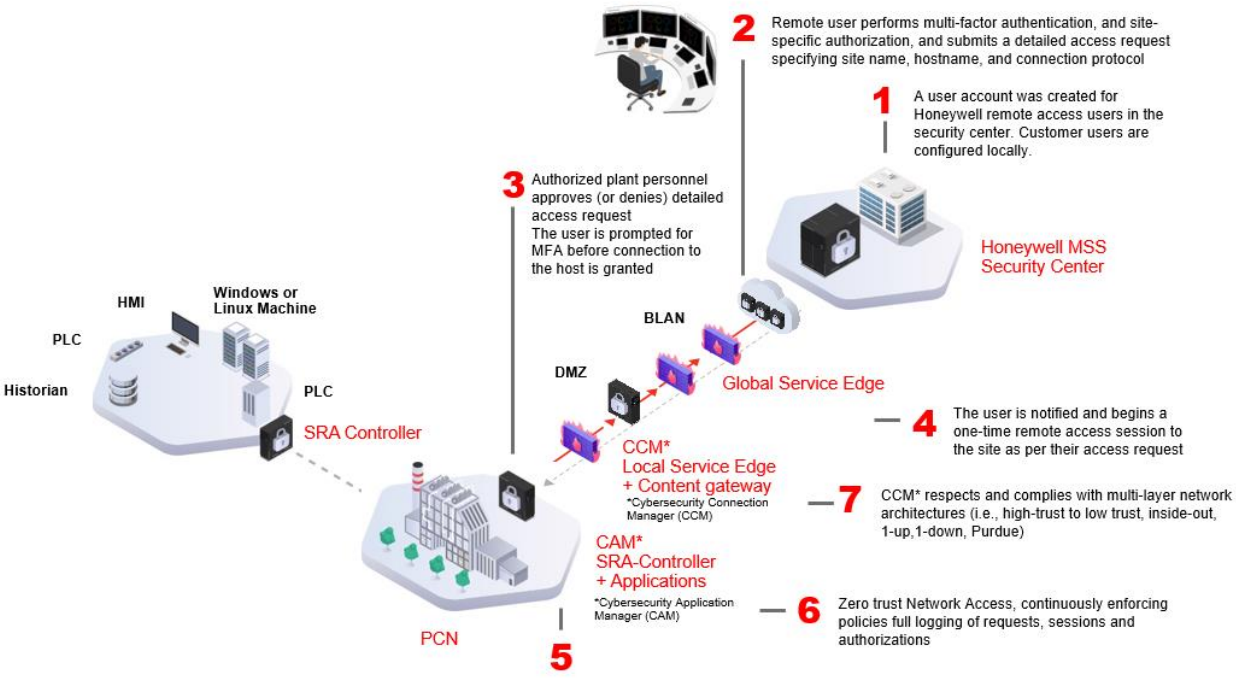
Application Manager - SRAs are designed to communicate outbound, whether they connect users' sessions coming from the Edges (on port 443) or whether they communicate with the published applications they serve (on their specific port).

Connection Manager - Identity providers (IdPs) are designed to confirm the user seeking access is who or what they claim to be across multiple platforms, applications, and networks. Honeywell Secure Remote can integrate with existing IdPs or using Honeywell Secure Remote Access's local (native) IdP that is included as part of the SRA setup. The SRA connects directly to the IdP (not through the Edges).

Zero Trust Security Built for OT

Modernization, improved security, and cloud-enabled efficiencies are possible for OT environments — without a drastic, unrealistic rip-and-replace. Industrial enterprises need tools designed to support OT priorities and address the real-world scenarios involved in OT security. By shifting to an identity-based access model and bringing zero-trust improved security to the OT environment, organizations can implement modern security practices that are designed to avoid hindering the speed or safety of critical processes and operations.

Honeywell Secure Remote Access Workflow



Benefits of Honeywell's Secure Remote Access Solution

Maintain Business Continuity

- Enable remote workforce
- Manage assets more safely and securely from off-site
- Keep staff safe or isolated
- Augment site skills

Improve Incident Response

- Both operational and cyber events
- Access cybersecurity professionals on-call
- Respond faster, reduce impact
- Eliminate travel time and travel cost

Industrial-Grade

- Designed for high security OT/ICS environments
- Customer-controlled authorization per session, per user, per protocol
- Site-controlled password vault
- Support staff & 3rd-party access

Increase Safety & Security

- Secure-by-default (no access)
- Reverse tunnel (no direct attack surface)
- Single use, just-in-time, channel
- Real-time supervision, recording, playback

Rely on a Trusted Partner

- Powered by Honeywell Cybersecurity, trusted by Honeywell, customers, OEM partners for 1000s of sites
- Numerous audits of 3rd-party providers of centers and software
- ISO/ISA/IEC-certified software development organization

Support Continuous Operations & Help Reduce Cyber Risk

With increased adoption of remote work and cloud components, best-in-class organizations are doing more to protect their networks with increased visibility and secure access control to their ICS network. Honeywell Secure Remote

Access is designed to secure business operations, manage remote access and reduce risk. As a Managed Security Service offering, Honeywell provides the technology and services to help keep your plants secure with the latest innovations including the principles of Zero Trust and remote privileged access management (RPAM). Rely on Honeywell professionals to deploy Secure Remote Access solutions to help support continuous operations and reduce cyber risk.

Why Honeywell?

Honeywell has more than 100 years of experience in the industrial sector and more than 20 years of experience in industrial cybersecurity and thousands of projects delivered world-wide. We provide cybersecurity solutions that protect industrial assets' availability, safety and reliability worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting and integrated security solutions. We combine industry-leading cybersecurity experience with decades of process control knowledge to provide the premier industry solutions for an operational technology environment.

For More Information:

To learn more about Honeywell OT Cybersecurity, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 3030

www.HoneywellForge.ai

March 2024

Honeywell