ICS SHIELD™
Top-down security for multi-vendor OT assets
OT SECURITY NEED

Industrial organizations are increasingly integrating their OT and IT infrastructures. The huge benefits of such “connected operations” include improved productivity and safety that come with data-driven decisions, as well as enhanced capabilities to automate the monitoring and maintenance of remote assets. Yet as the ICS environment becomes ever more connected, its attack surface increases in tandem. Despite large investments in multiple security tools and engineering resources, industrial operators are struggling to protect their highly complex multi-site, multi-vendor SCADA networks. What’s needed is a centralized solution that simplifies and delivers ICS security.
ICS SHIELD
SYSTEM ARCHITECTURE

Top-down OT security management for securing connected industrial control system (ICS)/SCADA environments

ICS/SCADA Complexity
- Multiple sites
- Multiple vendors requiring access to assets
- Multiple protocols on ICS network
- Multiple businesses
- Mix of legacy and proprietary equipment

IT/OT Misalignment
- ICS security ownership is not clear
- OT/IT mindsets are very different
- Transition from plant-by-plant to plant-wide security practices

Skilled Resources Shortfall and Budget Limitation
- Cannot place experts at every site
- Manual processes don’t scale and only provide limited security
- Multiple security solutions partially utilized

High-level Challenges of IT-OT Integration

- Secure Tunnel / connection
- File & Data Transfer
- Remote access
- Continuous Monitoring
- Asset Discovery
ICS Shield™ is Honeywell’s top-down OT cyber security management solution for securing connected ICS/SCADA environments. Empowering organizations to implement connected operations while minimizing cyber security vulnerabilities, ICS Shield secures remote field assets from a single security and operations center. This field-proven solution automates the deployment and enforcement of plant-wide security policies while focusing on security essentials such as inventory visibility, patching, log collection, remote access, and compliance reporting. Complying with the NIST Cyber security Framework, the NIST SP 800-82 guidelines, and leading international standards (including NERC CIP, ENISA, PERA, ISO 27001 and ISA/IEC-62443), ICS Shield improves the security compliance posture of industrial organizations. Deployed at thousands of sites worldwide in the oil and gas, utility, chemical, mining and manufacturing sectors, ICS Shield delivers unrivaled visibility, reliability and compliance for industrial plant operations.

ICS Shield is an award-winning technology – Best IT Solution for Critical Infrastructure. IT World Awards, 2017 Gold
“Industrial companies need a comprehensive, cost-effective solution for cyber security management and compliance. While there is an abundance of point solutions for each piece of the puzzle, there are very few solutions like Honeywell’s that offer a comprehensive, unified solution for ICS/SCADA cyber security. This solution provides support from asset discovery to policy enforcement and monitoring, all the way to real-time protection. The solution provides industrial companies with multiple sites a fully integrated platform to easily manage and secure their operational technology.”

Sid Snitkin, VP and GM, Enterprise Advisory Services, ARC Advisory Group
**DISCOVER**

**Discovery Automation**
The first step in protecting an OT environment is identifying precisely what’s on the network. ICS Shield helps you achieve an accurate inventory of your ICS assets including hardware, software and service configurations. Automating this discovery process, ICS Shield enables end-to-end visibility of OT assets, empowering your organization to effectively enforce its security procedures. ICS Shield enables leading asset discovery technologies for optimized results.

**Main discovery automation capabilities:**
- Asset auto-discovery: Scheduling discovery of ICS assets for an up-to-date inventory
- Configuration collection: Collecting detailed data about each asset
- Asset classification: Classifying assets by their level of criticality
- Change management: Monitoring changes in asset inventory and configuration
- Asset visualization: Providing a clear view of all field assets by business and geography.

**CONNECT**

**Secure Remote Access**
In order to maintain high levels of security, uptime and safety of distributed devices, secure remote access to field assets is required by first- and third-party personnel and machines. Providing extremely granular and robust AAA remote access, ICS Shield ensures secure remote access and monitoring, protected file distribution to devices, and safe data transfer from plants to HQ for analysis and risk management.

**Main secure remote access capabilities:**
- AAA remote access: Including centralized authentication, granular authorization, and session accounting and control
- Password vault: Authenticating remote users without sharing device credentials
- Secure file distribution & data transfer: Securely distributing files to devices and sending data from devices to central security and operations center.
PROTECT

Security Policy Management
Industrial organizations require simplified yet effective security policy management to better secure their dispersed OT networks. ICS Shield unifies and automates the policy management process, empowering the creation, deployment and enforcement of plant-wide and granular security policies. Leveraging ICS Shield’s security policy management, operations and control teams significantly improve OT cyber security and compliance.

Main security policies:
• Patching and anti-malware updating: Decreasing window of vulnerability between patch qualification and update
• Log collection: Empowering improved risk management
• Whitelists/blacklists: Hardening OT devices and reducing attack surface
• Securely move backup files to an offsite location improving incident recovery capabilities
• Custom policy creation: Enabling refining of organization’s cyber security
• Compliance reporting: Allowing compliance monitoring and the communication of identified vulnerabilities.

“Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.”

SCALE

Robust Infrastructure
ICS Shield infrastructure is designed for multi-site, multi-vendor deployment, with all sites connected to the security and operations center via Honeywell’s Secure Tunnel. This distributed architecture guarantees data security and integrity. Policies and files are easily distributed through the Secure Tunnel from the Security Center (SC) located at the enterprise data center to the Virtual Security Engine (VSE) installed at each plant. Data collected from the ICS assets by the VSE is sent to the SC for reporting, analysis and risk management purposes.

Main infrastructure components:
• Secure Tunnel: Powering secure communications using TLS encryption, with every session initiated outbound only using a single port and firewall rule.
• Security Center (SC): Serving as organizational security team’s main portal for top-down OT cyber security management and monitoring via an intuitive dashboard, while communicating with VSEs at plants and multiple IT security tools
• Virtual Security Engine (VSE): Enforcing policies and supporting a wide range of protocols for connecting to multiple assets
• Policy Manager: Powering the creation, deployment and enforcement of plant-wide granular policies and custom policies
• Reporting Tool: Generating customized and pre-defined compliance reports.
HOW HONEYWELL CAN HELP

Recent years have seen a major increase in cyber security incidents related to industrial control systems. As new threats emerge and the industrial cyber security landscape evolves, you need an experienced and trusted partner to help protect the availability, reliability and safety of your plant automation system, as well as safeguard people and processes involved in all facets of your operation.

- Tailored solutions to efficiently secure industrial controls, without impacting processes
- Global/regional industrial cyber security service hubs close to our customers
- Extensive coverage of industrial control networks
- Ability to support our customers from security assessments to cyber security program development
- Track record of completing over 1,000 global industrial cyber security engagements
- Mature solutions with 300+ managed industrial cyber security sites