ICS Shield™
Product Information Note

Top-down cyber security for multi-vendor OT assets. Achieve end-to-end visibility of all field assets, ensure the reliability of your ICS network and improve OT compliance.

ICS Shield™ is Honeywell’s top-down OT security management platform for securing connected Industrial Control Systems (ICS)/SCADA environments. Empowering organizations to implement connected operations while minimizing security vulnerabilities, ICS Shield secures remote field assets from a single security and operations center. This field-proven technology 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. ICS Shield can assist in 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). ICS Shield improves the security compliance posture of industrial organizations. Deployed at thousands of sites worldwide in the oil & gas, utility, chemical, mining and manufacturing sectors, ICS Shield delivers unrivaled visibility, reliability and compliance for industrial plant operations.

FEATURES & BENEFITS

Visibility
- Asset discovery
- Configuration collection
- Asset classification
- Change management
- Asset visualization

Reliability
- Authentication, Authorization and Accounting (AAA) remote access
- Secure file distribution
- Secure data transfer

Protection
- Patching & anti-malware updating
- Log collection
- Ports & services whitelists/blacklists
- File backup/restore
- Custom policy creation
- Compliance reporting

Assist in Compliance
- NIST Cybersecurity Framework
- NIST SP 800-82
- NERC CIP
- ENISA
- PERA
- ISO 27001
- ISA/IEC-62443

Simplify Security
- Password vault
- Centralized platform ensures uniformity across plants
- Remote access makes patching/updates easy, no need to send employees to locations to patch
1) Essential Bundle – Discover and Connect with Secure Remote Access

The first step in protecting an OT environment is identifying precisely what’s on the network. With the Essential software bundle, ICS Shield helps you achieve an accurate inventory of your ICS assets including hardware, software and service configurations. To maintain high levels of security, up-time and safety of distributed devices, secure remote access to field assets is required by first-and third-party personnel and machines.

Main capabilities:

- **Secure remote access** - allows remote users to connect to devices in the site via RDP and VNC protocols. Site administrators can set security policies to govern remote access (can allow/deny/require manual approval for all connections, or set policy for individual users).

- **Encrypted two-factor authentication** - provides an additional layer of security for all users connecting to a Security Center. In addition to requiring a username and password, users must provide further proof of their identity. This is often something like an RSA token that generates a second numeric password which changes several times every minute. When logging in, users must provide their username and password along with this secondary password.

- **Password vault** - allows administrators of a site to store remote access passwords in a local “vault”. Approved remote access users can connect with these credentials without the site administrator needing to share the passwords. This eliminates the need to share plaintext passwords with users, and simplifies changing system passwords to meet security policies (remote users don’t need to worry about the password changes).

- **Complete auditing** (reporting & video playback) - creates a complete recording of all remote access sessions which can be played back at any time from the Security Center. Details about authorized remote access sessions can also be included in reports.

- **Initial active asset discovery** (optional) - an administrator provides appropriate credentials to the active asset discovery, which then searches the network for PC and network devices, and tries to gather information about them using those credentials. As part of the Essential bundle, this is a one-time discovery to populate the device database initially, but not find devices that are added/removed/changed in the future.

2) Enhanced Bundle – Protect with Security Patching and Data Transfer

Building on all the features included in Essential, the ICS Shield Enhanced bundle adds robust capabilities around file and data transfer, system patching and log collection that equip plant engineers with a set of tools to greatly improve the efficiency of industrial operations security.

Main capabilities:

- **Secure file distribution and data transfer** - the VSE Service Node is capable of sending and receiving files according to its security policy. These files can be transferred to/from the Security Center (SC to VSE file transfer) or to/from another VSE instance (VSE to VSE file transfer). This capability is the backbone of several other services (such as patch delivery and offsite backups).

- **Patching** – supports the following update capability: downstream WSUS servers, Symantec Endpoint Protection Server, McAfee ePO Server, Windows Update Agent (on VSE hosts only) and McAfee AV (VSE hosts only).

- **Log collection** - collects local log files, formats them for use by a SIEM, and uses VSE to VSE file transfer to send the files to a corporate SIEM. The current implementation supports ArcSight as the enterprise SIEM.

3) Premium – Elevate Protection with Security Monitoring & Scanning

For the most comprehensive set of operational security capabilities, the Premium software bundle extends everything
from Essential and Enhanced, and provides additional asset discovery options, vulnerability scanning and compliance checking to support stricter requirements around risk intelligence and regulatory compliance.

Main capabilities:

- **Continuous active asset auto discovery** - the same discovery as described in Essential except scheduled to run periodically on an ongoing basis. This allows any changes in the system (devices added/removed/modified) to be detected throughout the life of the system. These changes can also be updated in the device configurations in the VSE Service Node.

- **Passive asset discovery** (optional) - the devices themselves are not directly scanned (as is done for active detection methods), but rather their presence and identity is inferred based on the network traffic in the system. Passive detection systems require the traffic to be fed into the appliance, which may require the use of network taps or mirror/span ports to capture the traffic.

- **Vulnerability scanning** - uses a dedicated vulnerability scanning server, sets of appropriate credentials, and a feed of known vulnerabilities and tests used to detect them (called Network Vulnerability Tests, or NVTs). A report is then generated with the known vulnerabilities on each monitored end device, along with the severity and classification of each vulnerability.

- **Compliance checking** - validates the configuration of monitored devices against established/expected system policies. Compliance checking is an important part of all relevant security standards (ISA/IEC 62443, NERC-CIP, etc.)

**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 ICS Shield’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 Service Node installed at each plant. Data collected from the ICS assets by the VSE Service Node is sent to the SC for reporting, analysis and risk management purposes.

**Main infrastructure components:**

Security Center & Virtual Security Engine Service Node:
ICS Shield infrastructure includes the Security Center (SC) located at a company’s headquarters and VSE Service Nodes, installed in each site. The Security Center enables OT security personnel to centrally define their security policies, distribute and deploy them to the VSE Service Nodes at the remote sites, together with rules for monitoring and reporting.

The VSE Service Nodes connect to the assets on the SCADA/ICS network, including workstations, network devices, PLCs, and other proprietary equipment, monitoring and enforcing its security. Once the system is configured with security policies, it runs automatically, delivering continuous visibility across all sites, along with alerts on security vulnerabilities and compliance issues.

ICS Shield provides vendor agnostic, multi-site capabilities

- PAGE 3 -
The SC and the VSE Service Node are connected via ICS Shield secure tunnel. A single, outbound-only, remote connection providing complete security, equivalent to the security of a “data diode,” but with all the additional benefits of bi-directional communication.

**Secure Tunnel:**
The secure tunnel uses a single firewall rule for the highest security and the easiest management. All communication is outbound over port 443 only. This means that all TCP sessions between the VSE Service Node and SC are initiated by the VSE Service Node.

**Reporting Manager:**
This module includes a set of reports and report generation capabilities, including built in and self-generated dashboards.

**Policy Builder:**
The policy builder allows developing new policies for improved OT security, operation and compliance measurement. The policy builder includes a wizard for specifying what data to collect, how to collect it, when to collect it, how to analyze it and which workflow should be triggered.

**Enhance ICS Shield with Managed Security Services**
Honeywell’s Managed Security Services (MSS) deliver 24/7 expertise to monitor and manage ICS environments at one site or across multiple sites. The result is reduced operational downtime and lower cyber risk.

Honeywell can provide hosting and/or management for ICS Managed Security Service Center. Get the most out of ICS Shield when pairing it with MSS:

- Increased cyber resilience - improves operating system security, robustness and stability to reduce the risk of downtime
- Expedited risk mitigation - remote service from experts expands resources to ensure ongoing security work is accurately completed
- Improved recovery time – on-call expertise delivers technical guidance as new ICS vulnerabilities are uncovered
- Better safety record - fewer service people on site reduces safety incidents and maintenance costs.

**Honeywell’s Enterprise ICS Cyber Security Solution**
At Honeywell, we are committed to providing cyber security solutions, technology and services that help the process and critical infrastructure sectors defend the availability, reliability and safety of their operations. Honeywell’s portfolio of end-to-end solutions enables industrial facilities to improve their cyber security posture and provide ongoing threat management. They are enabled by advanced technology, and include the training of people and application of the operational process controls necessary to ensure effectiveness. Our industrial cyber security solutions leverage Honeywell’s long history in plant safety and proven know-how in process control environments. Having delivered hundreds of industrial cyber security projects globally, Honeywell’s team of certified experts provide consultation and solutions across verticals such as Oil & Gas; Chemicals; Refining and Petrochemicals; Energy and Power; and Minerals, Mining and Metals.

---

**For More Information**
To learn more about Honeywell’s Industrial Cyber Security visit our website [www.becybersecure.com](http://www.becybersecure.com) or contact your Honeywell Account Manager

**Honeywell Process Solutions**
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Industrial Park, Pudong New Area, Shanghai 201203

[www.honeywellprocess.com](http://www.honeywellprocess.com)