ICS SHIELD™

OT cyber security management platform for securing connected industrial control system (ICS) environments
Table of Contents

Contents
1. Overview..................................................................................................................................................3
2. The Connected Operation..........................................................................................................................3
3. Securing the Connected Operation...........................................................................................................4
   3.1 Top-down Approach ...............................................................................................................................4
   3.2 Protect the Industrial Assets ..................................................................................................................4
   3.3 Enforce the Security Essentials ............................................................................................................4
4. ICS Shield Highlights....................................................................................................................................5
   4.1 Overview................................................................................................................................................5
   4.2 Essential - Discover and Connect with Secure Remote Access ...............................................................6
   4.3 Enhanced - Protect with Security Patching and Data Transfer .............................................................6
   4.4 Premium - Enhanced Protection with Security Monitoring & Scanning .............................................7
   4.5 Infrastructure & OSS ...........................................................................................................................7
   4.6 Deploying ICS Shield ............................................................................................................................8
   4.7 ICS Shield Infrastructure .......................................................................................................................8
   4.8 ICS Shield – Discover ..........................................................................................................................14
   4.9 ICS Shield – Connect .............................................................................................................................16
   4.10 ICS Shield – Protect ............................................................................................................................18
1. Overview

The purpose of this document is to provide a detailed overview of the Honeywell ICS Shield™, an Operational Technology (OT) security management platform.

The second chapter explains the drivers for a connected operation implemented by modern industrial and critical infrastructure organizations, the risks associated with connected operation and the strategy to minimize these risks.

The third chapter covers steps required in securing a connected operation.

The fourth chapter is an executive summary of ICS Shield product capabilities and benefits.

The fifth chapter provides a detailed overview of ICS Shield product pillars, security essential policies and infrastructure.

2. The Connected Operation

These are exciting times for industrial operations. The Industrial Internet of Things (IIoT), Industrial Internet, Integrated Operation or IT/OT convergence – whatever the name or approach you prefer – promises to revolutionize the use of information in everything from manufacturing plants to generating facilities, pipelines and transmission systems, refineries and more. The connected operation is already enabling more sensors and more connected devices, in more places, and providing more data than has ever been available before.

The benefits of having an integrated and connected operations are too good to ignore. Plant owners and operators can measure everything worth measuring in order to make data driven decisions; to predict operational failures and provide preventive maintenance to improve safety and asset reliability; and to utilize analytics to manage processes more effectively and reduce costs. This all translates to higher levels of safety, improved productivity and better profit margins.

But higher levels of connectivity also increase demands on operational technology (OT) security management. Industrial systems have traditionally benefitted from security through obscurity and isolation. The new emphasis on connectivity provides exposure to the corporate network, and potentially the public internet, which increases the attack surface. Control of the industrial assets no longer requires physical access to the equipment, or even to the plant, as remote access is enabled by network connections. While remote access is intended only for authorized operators and third party suppliers, it can be taken by malicious actors unless safeguards are imposed.

Diagram 1 – Unsecured Connected Operation
Oversight agencies have compiled security standards and regulations designed to guide plant operators in developing a hardened environment: NIST SP 800-82 (Guide to Industrial Control System Security); ISA/IEC 62443 (Industrial Network and System Security); and NERC-CIP (North American Electric Reliability Corporation Critical Infrastructure Protection).

Mitigating the risk of a cyberattack requires a rigorous approach to hardening the security controls around both the IT and the ICS/SCADA platforms. It's a continuous process requiring the collaboration of IT and OT, of the plants and the headquarters.

3. Securing the Connected Operation

3.1 Top-down Approach

Protecting such a complex environment requires a top-down, integrated approach. By “top-down” we mean that security and operations control team should be driving OT security policy, procedures and technology solutions. By “integrated” we mean that the intersection points among IT and OT, remote plants and head office, and third parties such as equipment vendors are all considered when choosing the means to enforce the security policy; i.e., everything works together.

Here are the basic principles of a top-down, integrated approach for ICS protection:

- A central security and operation control team – should set clear plant-wide policies for protecting the industrial assets
- The approach must allow granular policies by plant, asset and by user identity, as not all assets and users can or should be treated in the same manner
- Security policies should be centrally deployed and locally enforced for protecting the network segregation. Enforcement should be automated and monitored for violations. What's more, the central security operations control team must have the ability to tune policies following lessons learned from various activities and events
- If there is a policy breach, the security system should generate an incident alarm, so that a security analyst can investigate the event
- If an incident were to occur, authorized personnel must have the ability to promptly access an asset for incident response
- Backup and restore procedures should allow recovery from an incident
- The head office must be able to generate reports for risk management and compliance.

3.2 Protect the Industrial Assets

The primary focus of OT security should be shielding the field assets. These are the assets that, if compromised, pose the biggest risk to the operation safety, integrity and efficiency. This is different from traditional enterprise IT security that focus on protecting confidentiality, especially of databases storing customer data, source code, etc.

3.3 Enforce the Security Essentials

Organizations should address the security essentials, do the basic things right, again and again across their entire ICS environment. For example, the activities described below simply must be done for every ICS environment:

- Schedule a process to verify that qualified operating system (OS) patches and anti-virus (AV) signatures are installed, and if not, trigger an automatic synchronization with head office systems such as Microsoft Windows Server Update Services (WSUS), McAfee ePolicy Orchestrator (ePO), or Symantec Endpoint Protection Manager (SEPM). Field devices must be monitored to ensure that the new patches are installed successfully and machines reboot properly.
• Schedule the collection of device logs and send them to a centralized Security Information and Event Management (SIEM) system, where activities can be correlated and alerted on if necessary

• Schedule the monitoring of ports, services and applications against the organizational whitelist and blacklist policies

• Manage remote access authorization, privileges and accountability

• Generate compliance reports to assure that company and regulatory requirements are being met, and if they are not, determine what fixes are needed

• Schedule regular scans of IP address ranges and alert on unexpected changes, such as a new device

A top-down, integrated approach can tame the complexity.

By its nature, and considering the scale of the potential consequences, protecting an enterprise SCADA/ICS environment is a complex task. To simplify this complexity and reach an improved security and compliance posture, organizations should embrace a top-down integrated approach for deploying, automating and enforcing policies. Those policies should focus on protecting the industrial assets, and their execution should be automated.

An industrial organization must do the basic things right—those security essentials that if implemented right, systematically across the board bring the highest security ROI. Once the essentials are covered, additional security measures such as Intrusion Prevention System (IPS) can be implemented. After all, before a homeowner buys a sophisticated alarm system, he has to make sure he locks the front door at night.

4. ICS Shield Highlights

4.1 Overview

ICS Shield is a top-down OT security management solution for securing connected ICS/SCADA environments. Empowering organizations to implement integrated operations while minimizing security vulnerabilities, ICS Shield secures remote field assets from a single operations center. This field-proven solution automates the deployment and enforcement of plant-wide security policies while focusing on security fundamentals such as inventory visibility, patching, log collection, incident alarm and response, and compliance reporting. ICS Shield is delivered via 3 software bundles:

![Diagram 2 – ICS Shield Software Bundles](image-url)
4.2 Essential - 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.

4.3 Enhanced - 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.
4.4 Premium - Enhanced 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.)

4.5 Infrastructure & OSS

4.5.1 Security Center & Virtual Security Engine

ICS Shield infrastructure includes a Security Center (SC) located at a company’s headquarters and Virtual Security Engine (VSE) Service Node(s), 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.

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.

4.5.2 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.

4.5.3 Reporting Manager

This module includes a set of reports and report generation capabilities, including built in and self-generated dashboards.
4.5.4 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.

4.6 Deploying ICS Shield
Deploying ICS Shield comprises of installing one Security Center at the Security Operation Center (SOC), one Communication Center at the enterprise Data Center DMZ, and one VSE Service Node per each plant or remote site.

Diagram 3 – Deploying ICS Shield

4.7 ICS Shield Infrastructure
4.7.1 Security Center
The Security Center is installed in a central datacenter. The Security Center is the users’ main portal for top-down OT security management and also 3rd parties access point for remote services and assets monitoring. The Security Center key functions are:

- Distribute plant-wide security policies: ICS Shield includes multiple security essential policies that distributed from the Security Center to the VSE Service Node installed at each plant
- View and respond to vulnerability alerts: 1st and 3rd party users can view alerts, monitor assets, generate compliance report and more according to their privileges
- Funnel and manage remote access: 1st and 3rd party access is initiated by logging into the Security Center and requesting remote access permission. For further details, please read paragraph “Connect”, under section 5.4
- Utilize existing security tools: The Security Center easily integrates with existing security and IT tools such as SIEM server, WSUS server, ePO server, SEPM server, active directory and more.
Accessing the Security Center is performed via ICS Shield advanced authentication mechanism or via the enterprise active directory using LDAP. Using active directory ensures that the same password policy (password strength, periodic resets, etc.) that is used for the enterprise resources is also used for accessing the Security Center.

For customers using ICS Shield authentication, the product is supporting standard practices for password management such as strength and aging.

Once a user is authenticated and access is granted, ICS Shield flexible privileges management capabilities (labeling system) ensure the user will be able to act (view assets, take action) only according to his privileges.

Best Practice for critical network perimeter protection is to use a Terminal Server. The main benefits of using a Terminal Server are:

- Terminal Server dramatically reduce the attack surface (as in malware, viruses) of the connecting desktops inside and outside the organization. Typically, the desktop computers will require an operating system, some antivirus software, and a Terminal Services client
- Terminal Server is able to automatically detect existing vulnerabilities in the machines being used by the Security Centre users, whether internal or external
- Also, by disabling (at the terminal server level) file transfer capabilities from service personnel machines to the Security Center, virus transmission is avoided.

The Security Center maintains operational and audit logs for complete enterprise level transparency and auditing. The Operational log maintains a detailed record of all remote activities conducted by Security Center users. The audit log maintains a detailed record of all user activities relating to the Security Center. These include creating a new user, modifying permissions, developing new scripts, deploying VSE Service Nodes.

The Security Center administrator can set system parameters and other general settings, manage users, VSE Service Nodes and labels, and upload toolkit.

**System parameters:** The Security Center can be tuned and configured per need, for instance configuring the IPs of the remote access servers, default values for the protocols used etc.

**ICS Shield labeling:** "Labeling" is an important capability allowing an organization to easily replicate a matrix business environment into a cyber security practice. Many global organizations manage their business based on Geography and additional dimensions such as by business line. Using ICS shield, enterprises can group its plant in Huston under Americas > North America > USA > Texas > Huston but also “Label” the same plant to Oil & Gas label. Devices supported by Vendor X can be part of Vendor X label, critical devices can be groups under “critical devices” label. Plants & devices can be associated to one or more label.

ICS Shield account: ICS Shield allows defining multiple accounts with different privileges, thus, allowing global organizations to control the degree of ICS cyber security decentralization. Below are ICS Shield account:

- **Security Center Administrator:** Most senior account. The Security Center Administrator is responsible for creating labels, assigning labels manager as well as all the privileges of a label manager
- **Label Manager:** Responsible for managing the label. He is responsible for – add site/plant, add/remove device, assign Security Center operators and additional label managers, as well as all the privileges of an operator
• Security Center Operator: Is given privileges within a label. Such privileges include:
  ▪ Monitoring: View data collected from the plants/devices within the label
  ▪ Enforcing: Distribute, modify and delete a security essential policy for the plants/devices within a label
  ▪ Managing: Managing plants/devices within the label, for example add device, change device status, remove device etc. Managing privilege also allows sending files to a VSE Service Node, perform remote access activity and add new operators to the label

Security Center Operator can be given both monitoring, enforcing and managing privileges or only one or two of these privilege’s.

When an organization is allowing 3rd party users to access the Security Center, the 3rd party user will be a Security Center operator with monitoring and managing rights for a label which include the devices this 3rd party is responsible for monitoring and maintaining.

• VSE Service Node Administrator: Most senior entity within a site or plant. This entity privileges include:
  ▪ Same privileges as a Security Center operator for the devices connected to the VSE Service Node
  ▪ Supervising: Supervise remote access activity, including approve, deny or terminate
  ▪ Create a device manager

• Device Manager: Responsible for managing the devices within a VSE Service Node. Device manager privileges can be part or all (monitor, supervise, create) of the VSE Service Node administrator privileges, within the devices he was granted management right to

Toolkit: The toolkit includes tools helping VSE Service Node Administrator and device manager in their daily work. The toolkit is uploaded to the VSE Service Node by the Security Center Administrator.

4.7.2 The Virtual Security Engine (VSE) Service Node

The VSE Service Node serves as the security policy enforcement agent and is fully controlled by the plant team. Typically, customers install one VSE Service Node per plant, which should be installed where it can connect to the assets. However, this topology is not obligatory, if needed, for instance in cases of networks segregation, multiple VSE Service Nodes can be installed at a single plant.

Since the VSE Service Node should report to the Security Center, it should be installed where it can access the Communication Server. The VSE Service Node connects to assets on the SCADA/ICS network, including workstations, network devices, PLCs, and other proprietary equipment, monitoring and enforcing security policies. The key functions of the VSE Service Node are:

• Plant team security dashboard
• Approve deployed policies per plant: Plant team approve security essential policies scheduled to monitor the plant assets
• Continuous monitoring of field assets: VSE Service Node execute approved policies, delivering continuous visibility across all sites, along with alerts on security vulnerabilities and compliance issues
- Define access privileges to each asset: VSE Service Node enables the provisioning of all user management functionality, enabling permission and access-right control down to the level of individual device

- Manage and control remote access: Plant team can approve and abort remote access session

- Full audit trail: The VSE Service Node maintains comprehensive operational and audit logs, which enable plant administrators to view past events. All devices associated with a remote activity are logged and when applicable, the name of the Security Center user who performed the remote action is logged as well. The following activities are recorded in the audit log: all data and files received and transmitted by the VSE Service Node, along with the associated files, remote such as RDP, VNC, HTTP, SSH, Telnet and so on, every data collection routine that was executed, a separate audit log records for all user interaction performed in the VSE Service Node Administrative console.

![Diagram 4 – VSE Service Node Audit Trail Complies with NERC-CIP & ISA 62443](#)

**4.7.3 Secure Tunnel and Communication Server**

The Communication Server provides a secure, encrypted and authenticated communication over the internet or private communication network between the Security Center and VSE Service Nodes. The Communication Server is installed at the Data Center DMZ.

The Secure Tunnel is an outbound secure, encrypted and authenticated connection starting from the VSE Service Node to the Communication Server and to the Security Center.

The Secure Tunnel is used for two activities:
- Remote access of 1st or 3rd party to a SCADA/ICS
- Data and files transfer

**How does it work?**

Each VSE Service Node utilizes the latest version of standard secure communication protocols to encrypt all communications, namely Transport Layer Security (TLS) v1.0 and higher, with 2048-bit encryption. In addition, the VSE Service Node uses FIPS 140-2 validated cryptographic modules. Data is compressed, encapsulated and encrypted.
A pivot concept at the ICS Shield Secure Tunnel is that communication is initiated outbound only. This single, outbound-only, remote connection provides complete security, equivalent to the security of a "data diode," but with all the additional benefits of bi-directional communication. It enables proper management of connectivity to remote sites from the Security Center and is easier to manage the VPN.

All communication is outbound over port 443. This means that all TCP sessions between the VSE Service Node and Communication Server are initiated by the VSE Service Node. Normally this does not require firewall changes by the enterprise’s IT administrator to enable the VSE Service Node to send information to the Security Center.

Because all communications are outbound, it is not possible for any external party to gain access to the remote site through the firewall. All external connections to the plant/site are funneled through the Secure Center server, which is monitored by the organization’s cyber security experts.

The plant team has the final say in granting remote access to any ICS asset. The SSL tunnel is opened from the VSE Service Node to the Communication Server, figure below.

Transmission of application data only starts after the Secure Tunnel is established. Encrypted information can then flow securely, without the possibility of penetration, between the Communication Server and the VSE Service Node.

During the first three stages in the diagram above, the VSE Service Node and the Communication Server use their certificates to authenticate each other and follow standard public key/private key cryptography protocols to negotiate and transfer the symmetric key for data encryption.

Once the VSE Service Node and the Communication Server have agreed on a symmetric key, all bi-directional dataflow is performed using TLS 2048-bit encryption with the symmetric key, for the highest possible speed and performance.
ICS Shield Trusted Platform Model (TPM).

All equipment in the plant/site is connected only to the VSE Service Node, and not to the external environment. The VSE Service Node is connected to the external environment only through a single outbound-only port in the perimeter firewall. That single outbound port allows only outbound communication to a specific IP address at the corporate data center. Therefore, since there is no inbound port open, it is impossible for any external party to access equipment in the plant through the perimeter firewall. In other words, the outbound-only connection is as secure as a so-called data-diode type connection, at a fraction of the cost, a fraction of the complexity, without additional hardware requirements, and with all the benefits of bi-directional communications, as in the figure.

The only “inbound” firewall port in the entire system is in the firewall of the DMZ of the corporate data center where the Communication Server is located. In order to provide the highest possible security and protection of this important central portion of the infrastructure, Honeywell developed a near strong authentication technology based on a “hardware biometric” factor, which is unique in the remote access industry. This strong authentication technology, called the Trusted Platform Module (TPM) ensures that VSE Service Node software can communicate with the Communication Server, if and only if the VSE Service Node software is running on the hardware on which it was originally installed.

The TPM works as follows:
During the FIPS 140-2 compliant TLS handshake, the VSE Service Node sends its certificate (“something I have”) to the Communication Server, which enables the Communication Server to authenticate the identity of the VSE Service Node, and to validate the identity of the VSE Service Node against the Communication Server’s repository of authorized certificates. However, the VSE Service Node keeps its certificate in an encrypted store that is tied “biometrically” to the hardware on which it was installed, and on which it is running. The encryption key of the certificate store is created from several randomly chosen hardware identification parameters. This TPM-key is created when the VSE Service Node software is first installed on its host server, and used every time the VSE Service Node software needs to access its certificate. Thus, the VSE Service Node certificate, and the VSE Service Node private key can only be accessed using the TPM-key which can only be known if the VSE Service Node is running on the hardware on which it was originally installed. In this way, it is not possible for any machine other than the original host on which the VSE Service Node was installed to connect to the Communication Server, making it virtually impossible for an external party to connect to the Communication Server through the only inbound firewall port in the system.
The protocol described above enables the VSE Service Node and Communication Server to create and sustain a "military grade" secure encrypted tunnel that ensures authentication, confidentiality, data integrity and non-repudiation.

The Secure Tunnel can be operated in two modes, polling and continuous modes:

- **Polling mode:** The VSE Service Node polls the Communication Server every 1 minute for messages. Polling mode is http based and due to its nature is limited and has some latency, for instance Remote Access request sent to the VSE Service Node can be established after a minute or so.

- **Continuous mode:** Is a proprietary Honeywell protocol that has two major advantages in comparison with the polling mode – 1) it is super-fast – messages are pushed to the VSE Service Node 2) it supports unstable network lines, by resuming the connection from the point it stopped. The Continuous mode with combination of a highly efficient VSE Service Node (in utilizing memory and CPU), is the reason why gigs of data can be transferred from VSE Service Node to VSE Service Node.

**4.7.4 Reporting Manager**

![Security Center](image)

**4.7.5 Policy Builder**

We maintain a library of template policies with the ability of the user to add their own policies with a VB like tool.

**4.8 ICS Shield – Discover**

Maintaining an up-to-date assets inventory is critical part of ICS Security. NIST Cyber Security Framework “Identify” function states “Software platforms and applications within the organization are inventoried.” Discover pillar allows maintaining an accurate global asset inventory and track changes from baseline.

ICS Shield is using active and passive methods for creating and updating the assets inventory.

**Active Auto-Discovery**

One of the fundamentals of the cyber security is to know your assets. ICS Shield active Auto-Discovery detects new active hosts in a given IP range, and classifies the hosts by type, operating system and vendor.
Active Auto-Discovery allows the discovery of Windows, Linux, Unix and networking equipment. When a new asset is detected it is added to the VSE Service Node, and an email and/or SMS is sent to the plant admin notifying about the new asset. The plant admin can then take action if needed – it might be an unauthorized action for instance, when an engineer plugged in his laptop to perform maintenance without getting approval.

Once a device/asset is added to the VSE Service Node, list of policies and remote access privileges are automatically applied to it, start querying it, harden it, collecting data and monitor compliance. Policies are associated based on the applicable label of the device. The new asset is also added to the Security Center, with the Security Center operator being notified via email and/or SMS.

1st and 3rd users (Security Center operator), based on their privileges, can perform remote activities such as monitoring, enforcing and managing on the newly added asset. As at the Security Center has a holistic view over the entire assets, the new asset is also added to the compliance reports, widgets and statistics.

ICS Shield Auto-Discovery is using a smart engine that can detect accurately the asset class with minimal load on the ICS network. The engine will approach a device using WMI over port 135, given positive reply it will assume the device is a Windows device, if not, the engine will use SSH over port 22, given positive reply it will assume it is Linux device, etc. This approach is different from other assets discovery tools that are using aggressive methods (IPS, multiple ports and accessing the assets) creating heavy load on the sensitive ICS network.

The Auto-Discovery can be configured by date, IP range and more. VSE Service Node Administrator can always change these parameters.
Configuration Collection
A detailed inventory requires more than an IP address and other basic data obtained by scanning an IP range. ICS Shield supports multiple configuration collection protocols such as WMI for Windows machines and SNMP for Linux machines. Using the assets credentials the VSE Service Node will collect the configuration data of Windows and networking assets. Configuration data include - IPv4 addresses, MAC addresses, OS name and version, Application software name and version, OS patches name and date, HW manufacturer and model, AV agent name and version, AV signatures file version and date, AV service status. This data can be viewed through the Security Center and VSE Service Node. The plant team can also manually add vendor name, custodian and other data point. Additional important data point, requested by ICS security standards, is adding the asset criticality. ICS Shield allows manually adding the device criticality (critical, essential etc.). ICS Shield will notify on changes from base line, primarily on new asset or decommissioned assets. ICS Shield will automatically associate remote access credential to a newly discovered device per the label.

Passive Auto-Discovery
ICS Shield supports optional passive auto-discovery of sensitive assets such as PLCs and RTUs. ICS Shield uses a special sensor that tracks and detects traffic on the network control system. The sensor can analyze the communication between PLCs and HMI s in a non-intrusive way, using port mirroring technology. Each asset is inspected by vendor type and Name\IP, based on a set of known deterministic parameters. In case the system fails to determine the relation between the device to one of the vendors, it will be alerted and reported as an unknown device.

4.9 ICS Shield – Connect
Connect pillar addresses key requirements at every ICS security standard or regulation. “Protect” function at the NIST Cyber Security framework states “Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access” and “Data-in-transit is protected.” Secure remote access facilitates 1st and 3rd party access to an organization’s SCADA/ICS assets. It enables protocols such as RDP and VNC to securely run in OT environment, while ensuring that all sessions are auditable and can be recorded. It includes finer granularity, supporting proprietary protocols, VPN, and file transfer capabilities. The Security Center provides a single, secure and easy to manage access point to funnel all vendors and partners access, avoiding the risks associated with multiple, insecure proprietary tools used by such third parties.

Diagram 7 – Secure Remote Access Flow
ICS Shield AAA secure remote access includes:

- **Access Authentication** – Using ICS Shield or the organization authentication as detailed in Security Center chapter 5.2.1

- **Access Authorization with privileges management** – Using ICS Shield labeling (see chapter 5.3), allows setting access privileges down to the individual device level. Remote sessions are supervised by the plant team (VSE Service Node user). Plant team can set the system to manually approve or reject every remote access, however best practice is to automatically approve remote activities. The solution allows finer granularity of remote access approval or rejection based on time, asset or user requesting the remote access

- **Full audit capabilities** – remote access activities are logged and recorded. Every remote access activity is logged with the user name, time, device and protocol used (RDP, VNC, SSH etc.). The Security Center and VSE Service Node allow viewing every active remote connection, the manager can then terminate the connection by a click of a button

- **RDP sessions recording** are supported when using a jump server (terminal server or similar technology). RDP sessions are recorded at the Security Center as a video and can be viewed for learning and analysis purposes. RDP sessions supervision is also supported. A manager at the Security Center can “shadow” the ongoing RDP session, view it live and if needed terminate it. Telnet and VNC sessions are also recorded at the VSE Service Node and Security Center. The VSE Service Node manager and the Security Center operators can later view the sessions, VNC sessions are saved as a video session, Telnet sessions are saved as plain text

- **Data-in-transit protection using encrypted communication** – remote access using ICS Shield Secure Tunnel detailed in chapter 5.2.3

- **Password vault to efficiently manage devices credentials and better audit connected users** – accessing a device require the user to obtain the device credentials. Sharing credentials with external users may by risky and also add a degree of difficulty to credential management. Shared credential expose the organization to poor, yet common, practices such as yellow sticky note on the 3rd party user desk or screen. Using ICS Shield Password Vault the user doesn’t need to know the credential. ICS Shield will connect authenticated remote users based on their privileges. Naturally, regardless the Password Vault, remote access is audited and recorded.

![Diagram 8 – Remote Access Audit Trail](image)

ICS Shield Secured file transfer and file sharing capabilities:

- **Data and files transfer** enables the center to send files (e.g. qualified patches) and policies to the plant and vice-versa (e.g. log collected from the assets). This mechanism is similar to messaging concept
• File sharing mechanism at VSE Service Nodes allows users to securely upload files from their secured network to plants and have them available for future use. This eliminates the need to connect dangerous portable media drives when technicians need to travel to plants for service.

When a Security Center user wants to send files, request a remote access session or perform other type of remote activity, the Security Center sends a task message to the Communication Server, where it waits for the VSE Service Node to collect it. The VSE Service Node checks its security policy and then allows or rejects the activity accordingly. If the activity is allowed the VSE Service Node initiates the Secure Tunnel and allows the remote session. It is important to note that most remote monitoring activities do not require to open the Secure Tunnel. The 1st or 3rd party user will access only the Security Center and view the data already collected and sent to the Security Center by the VSE Service Node.

4.10 ICS Shield – Protect

4.10.1 Introduction

Industrial organizations require simplified yet effective policy management to standardize plant-wide polices to better secure their dispersed OT networks. ICS Shield automates the policy management process, empowering the creation, deployment and enforcement of plant-wide and granular policies. Leveraging ICS Shield’s policy management, security operations and control teams significantly improve compliance with less OT and IT resources. ICS Shield includes a package of essential security policies allowing every industrial organization to significantly improve security and compliance posture. These essential policies can be fine-tuned per the customer needs and new policies can be created.

4.10.2 Policy Creation & Distribution

ICS Shield Protect pillar includes security essential policies such as – Patching & AV update, Log collection, whitelisting/blacklisting and more. These essential policies allow an industrial organization to comply with significant portion of major standards such as the NIST Cyber Security Framework.

<table>
<thead>
<tr>
<th>Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functions</strong></td>
</tr>
<tr>
<td><strong>Identify</strong></td>
</tr>
<tr>
<td><strong>Protect</strong></td>
</tr>
<tr>
<td><strong>Detect</strong></td>
</tr>
<tr>
<td><strong>Respond</strong></td>
</tr>
<tr>
<td><strong>Recover</strong></td>
</tr>
</tbody>
</table>

*Diagram 9 - Compliance with NIST Cybersecurity Framework*

In addition to the security essential policies, customers can create new policies using the policy builder or ask Honeywell services team to develop a new policy. Policies are distributed from the Security Center to each VSE Service Node and are enforced only after the plant team approves them.
4.10.3 Policy Enforcement & Monitoring

An approved policy will run automatically at each plant by the plant VSE Service Node. This mechanism allows maintaining the network segmentation. An executed policy will result in data or files transferred from the plant VSE Service Node to the Security Center or Vice versa. As an example, log collected from remote assets will be sent by the VSE Service Nodes to the Security Center. In the event of a possible security or operation incident or policy violation, alarm will be sent to the respective VSE Service Node and to the Security Center for analysis and mitigation. As an example, critical assets are using an older patch or a white list service is not running or installed.

Diagram 10 – Incident Alarm

4.10.4 Compliance Reporting

The Security Center will generate a timely report detailing compliance of sites and assets. These reports can be customized using ICS Shield reporting tool, in addition, ICS Shield allows sending data to external reporting tool.

Diagram 11 - Compliance Reporting
4.10.5 Security Essentials - Patch Synchronization

Timely patch synchronization is essential to minimize the window of vulnerability. According to Verizon Data Breach Report 2015, 99.9% of the exploited vulnerabilities were compromised more than a year after the patch was available.

ICS Shield supports automatic synchronization of WSUS updates. The process involves automatic activation by the VSE Service Node of WSUS synchronization on the downstream WSUS.

The delivery of WSUS updates utilizes the Secure Tunnel. This allows the downstream WSUS at the plant to securely connect to the upstream centralized WSUS located at the headquarter and download updates. The Centralized WSUS server will contain list of its qualified patches per vendor.

![Diagram 12 – Patch Synchronization](image)

There are three methods for patch synchronization:

- **Fully Automated** – Update process is started based on a predefined schedule
- **Semi-Automated** – Update process starts on demand. The activation can be initiated from the Security Center or the remote site VSE Service Node
- **Manually** - The Secure Tunnel opens from the downstream WSUS to the upstream WSUS generated by the VSE Service Node manually. Once active, the user will be required to login to the WSUS UI and manually click the “Synchronize now” function. To end the operation gracefully, the user will need to terminate the Secure Tunnel by running a routine at the VSE Service Node.

To ensure successful delivery of new patches the VSE Service Node will connect using Secure Shell (WINRM) to the windows machines at the plant and:

- Check installed patch and list of patches waiting to be installed, taken from the WSUS connected to the Windows machine
- Check the oldest patch that should be installed and is not installed, this shows what is the latest time a patch was updated
- Report compliance per number of days allowed for a patch not updated.
4.10.6 Security Essentials – AV /AM Synchronization

ICS Shield supports automatic delivery of McAfee ePO and Symantec SEPM synchronization. The HQ ePO/SEPM server will replicate its updated components to an HQ ePO/SEPM http repository, the remote site ePO/SEPM will synchronize with the http repository. The delivery of antivirus/antimalware updates utilizes the Secure Tunnel. This allows the AV/AM servers at the remote sites to securely connect to the http repository on the HQ. There are three methods for AV/AM signature synchronization:

- Fully Automated – Update process is started based on a predefined schedule
- Semi-Automated – Update process is started on demand via a diagnosis routine. The activation can be initiated from the SC or the remote site VSE Service Node
- Manually – The Application Tunnel from the remote site ePO to the HQ repository is generated by the VSE Service Node. Once active, the user will be required to login to the ePO UI and manually click the “Pull Now” function. To end the operation gracefully the user will need to terminate the “Application Tunnel” by running a routine at the VSE Service Node.

Remote Activation of Server Tasks

ICS Shield provides the ability to remotely execute ePO/SEPM server tasks and receive reports via email without the need to install an SMTP server at the remote site. Server tasks are configurable actions that run on the ePO/SEPM server on a schedule or on demand. The user can leverage server tasks to help automate repetitive server tasks that need to be performed on the server. McAfee ePO and Symantec SEPM includes preconfigured server tasks and actions out of the box. Remote activation of server tasks allows users to run several tasks at different remote sites and view or receive their results from a centralized location (Headquarter).

Server Tasks include:

- Performing an action using the results of a query
- Emailing and exporting reports automatically on a regular basis
- Purging older events automatically from the McAfee ePO server database
- Deleting inactive machines automatically from your system tree

The server tasks are able to send emails via the HQ SMTP server to the relevant contact person(s).

Automatic Response

ICS Shield provides the ability to configure automatic response to use the SMTP server at the HQ in order to send email notifications. When an automatic response is triggered, the VSE Service Node is invoked to open the Application Tunnel for sending emails, thus allowing the automatic response result to be sent to the relevant personnel. The complete set of event types for which the user can configure an automatic response depends on the software products that are managed by the ePO server.

By default, automatic response can include these actions:

- Create issues
- Execute server tasks
- Run external commands
- Run system commands
- Send email messages
- Send SNMP traps
The user has the ability to specify the event categories that generate a notification message. The user can also configure the frequency to send messages.

Out of the box automatic response include:

- Detection of threats by your anti-virus software product
- Outbreak situations. (E.g., 1000 virus-detected events are received within five minutes)
- High-level compliance of ePolicy orchestrator server events. (E.g., a repository update or a replication task failed)
- Detection of new rogue systems.

4.10.7 Security Essentials - Log Collection

Protect functions at the NIST Cyber Security Framework include a subcategory suggesting "audit/log records are determined, documented, implemented and reviewed in accordance with policy". ICS Shield automates this subcategory. Log collection policy is enforced by the VSE Service Nodes. The VSE Service Node collects log from Windows machines, convert them to a CEF format and send to the Security Center, from which it will be collected for analysis and risk management by the enterprise SIEM server.

Diagram 12 – Log collection
On a predefined interval, the VSE Service Node performs Windows event log collection, as follows:

1. The VSE Service Node collects event log, for all event log types (application, system, and security)
2. The VSE Service Node takes a timestamp of the logs
3. The VSE Service Node reads every event log record, formats it to CEF, and writes it to appropriate file
4. The VSE Service Node transfers log files and blacklists/whitelists alarms at predefined intervals to the Security Center and from there it is imported by the SIEM server (i.e. ArcSight)

4.10.8 Security Essential – Back-up and Restore

Protect functions at the NIST Cyber Security framework include a subcategory recommending “backups of information are conducted, maintained and tested periodically” and “response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place and managed”. ICS Shield automates significant portion of these subcategories.

Back-up and Restore principals are:

- Full and incremental backup of the devices and data files (business data, system data, application data etc.)
- Back-up copies should be stored in an environmentally protected, secure centralized storage
- Restoration tests should be made occasionally to check if the restoration process of the back-up files is successful.
- The back-up and restore operations should be monitored and configured by the system administrator.

These principles match with the requirements of industrial security policies (for example NERC CIP) and implementing them will improve industrial organization compliance posture to ICS cyber security standards. ICS Shield back-up and restore solution addresses the below back-up and restore requirements:

1. Integrate with existing backup software that back-up the devices on the customer’s site
   - The VSE Service Node will monitor the back-up operation and will alert if some of the back-up copies not properly made
   - The VSE Service Nodes can also transfer back-up files from all the plants to a centralized storage (NAS) in the customer’s HQ

2. Preform auto-restoration test of the latest back-up file for the requested devices. Using a virtual machine software, the VSE Service Node will load the back-up file on a virtual machine and will examine the result of the process, if the virtual machine did not load properly an alarm will be generated

3. For each of the devices at the plant, the VSE Service Node will gather information regarding the creation of the back-up files and will ensure that the back-up files are created at the requested time and the file are not corrupted.

The following parameters can be configured as a “back-up policy” for each site/device:

- Back-up frequency: Specify the time interval between the back-up files, the VSE Service Node will manage history of back-up files for each device and with the given time-interval will expect a new backup file to be made
- Grace period: Specify the time period that customer allows a back-up file to be delayed from the last successful back-up operation. If the VSE Service Node detects that the new back-up file does not exist in the requested time interval and the grace period is over an alarm will be raised which can be sent by e-mail/SMS to the site administrator
- Auto restoration frequency: Specify the time interval between the auto restoration tests.
According to the “back-up policy” described above and with the information gathered from the back-up file, the VSE Service Node will calculate compliance, raise alarms if the backup operation is not compliant and generate backup related reports which can be monitored from the VSE Service Node and from the SC in the customer’s HQ.

4.10.9 Security Essential – Whitelists/Blacklists

Whitelist and blacklist policies contain regulations regarding the activities and connectivity of devices and help to maintain a secure behavior of the site network and assets. Such policies are implemented by most of the industrial companies and implementing those policies are suggested by the industrial security policies. The enforcement of the whitelist and blacklist policies and keeping track of the compliance of all the company assets is also an important part of the implementation procedure and Honeywell provides the answer to this need.

The whitelists/blacklists solution will measure the compliance for every site/plant by using a permitted (white) and prohibited (black) lists configuration. Each VSE Service Node will gather the information of all the assets and will compare the results against the whitelists/blacklist in order to calculate the compliance. The devices can be associated to labels and the whitelists/blacklist configuration can be different for each label. The compliance result of all the sites/devices will be also monitored from the SC and compliance reports can be generated for each site. If some of the devices are not compliant, an alarm will be generated and delivered to the administration via email/sms.

The following asset parameters will be monitored and compared against black/white configuration list:

- Services: The VSE Service Node will collect the information of all the services on the device and compare the services information with the authorization (black/white) list

<table>
<thead>
<tr>
<th></th>
<th>White list configuration example</th>
<th>Black list Configuration example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Windows Defender</td>
<td>uTorrent</td>
</tr>
<tr>
<td>Service Installation status</td>
<td>Mandatory</td>
<td>Forbidden</td>
</tr>
<tr>
<td>Service State</td>
<td>Running</td>
<td>Stopped</td>
</tr>
<tr>
<td>Service Startup mode</td>
<td>Manual</td>
<td>Auto</td>
</tr>
</tbody>
</table>

For example, if the VSE Service Node detects a running service on the machine that is configured to be forbidden in authorization list, an alarm will be raised.

- Network Ports: The VSE Service Node will check the state of all the network ports in the given port range and compare the ports status with the authorization list.
Configuration Example:

<table>
<thead>
<tr>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Range</td>
<td>135,8000-9000</td>
</tr>
<tr>
<td>Expected Open Ports</td>
<td>8080,135</td>
</tr>
<tr>
<td>Expected Closed Ports</td>
<td>8000-8079,8081-8900</td>
</tr>
<tr>
<td>Expected Filtered Ports</td>
<td>8900-9000</td>
</tr>
</tbody>
</table>

For example, the VSE Service Node will raise an alarm if some of the network ports did not match the authorization list.

Some of the malware and viruses are using network ports vulnerabilities. Constantly monitoring network ports and calculating compliance may detect such vulnerabilities and prevent from malwares and viruses to breach the customer’s system.

- **Installed Software**: The VSE Service Node will gather the information of all the installed software on the device and compare the result with the authorization list.

Configuration example:

<table>
<thead>
<tr>
<th>White list configuration</th>
<th>Black list configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Name</td>
<td>ESET NOD32 Antivirus</td>
</tr>
<tr>
<td>Software Status</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

For example, if the VSE Service Node detect that one of the software that forbidden has been installed on the device or mandatory software has been deleted an alarm will be raised.
For More Information

To learn more about how Honeywell’s ICS Shield visit 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