Cyber Security Sales Reference

Industrial Control Systems are rapidly advancing and Invensys products are becoming more complex, requiring additional levels of experience and technology knowledge. To help facilitate this trend, we have outlined a number of cyber security solutions that Invensys global cyber security team supports and delivers. In addition to these solutions, we have other numerous workshops and services that focus on both regulatory and non-regulatory standards. For more information, please visit our website or view our monthly newsletter archive to read feature articles from our consultants about relevant cyber security topics. Invensys' approach to cyber security is to focus on the Process Control Level, providing cyber security for the critical infrastructure and providing secure data acquisition across the facility.

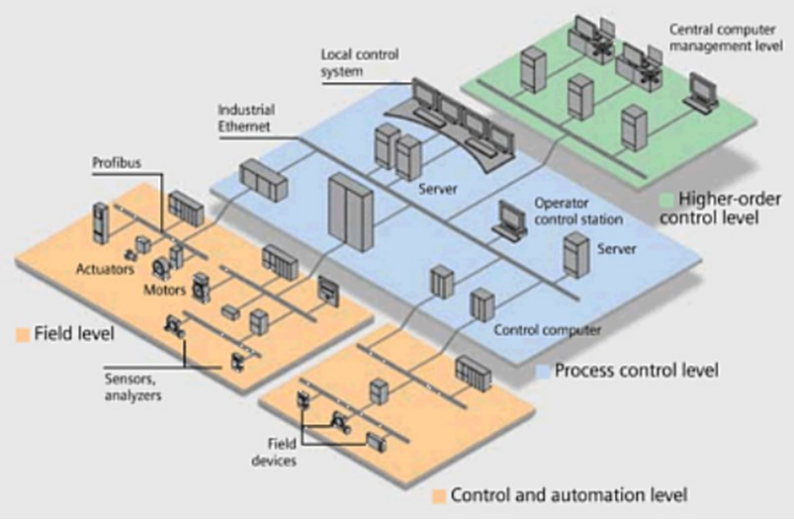
Cyber security is more than just a point solution such as anti-virus software or firewalls. For this reason, the Invensys global cyber security team offers a comprehensive list of cyber security solutions to help address any internal needs, regulatory requirements, or program mandates. All of these elements are synergistic, providing not only a broad scope of security but also the defense-in-depth necessary for true cyber security compliance.

The Invensys global cyber security team is uniquely qualified to design, deliver, and deploy cyber security solutions in an Industrial Automation setting. In addition to an array of training and certifications, our consultants have backgrounds in process and network engineering as well as experience with both non-regulatory and regulatory requirements such as NIST, NERC, and NEI.

Next time you are talking with a customer who is interested in cyber security, you can refer to this guide to answer any questions about cyber security solutions and regulations.

Cyber Security Buzz Words

- ⇒ Firewalls
- ⇒ Switching
- ⇒ Hardening
- ⇒ Active Directory (AD)
- ⇒ Remote Access Server
- ⇒ Technology Assessment
- ⇒ Asset Identification
- ⇒ Patch Management
- ⇒ Network Performance Management
- ⇒ ePO
- ⇒ Whitelisting
- ⇒ Security Information and Event Monitoring (SIEM)
- ⇒ Device Control
- ⇒ Host Intrusion Prevention (HIPS)



FIREWALLS

When is it necessary?

Firewall Configuration and Installation should be provided in any proposal where the customer has either requested a firewall and/or multiple firewalls are already in the network. In many cases, firewalls are deployed indiscriminately at various access points and without a focus on the configuration rules sets and policies. The Firewall Configuration and Installation solution reviews the network architecture, helps the client with proper firewall deployment, and ensures the appropriate configuration rule sets and policies are in place.

Key Words

Key words to look for in a proposal that indicate a firewall should be recommended:
firewalls, access control, isolation

Without Firewall Configuration and Installation rule sets, customers have no visibility into dropped traffic or attacked traffic.

What is it?

Firewalls are typically viewed as "isolation" devices that provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. However, firewalls are much more than this when implemented as part of a comprehensive cyber security plan. Data communication is important across any facility; few areas of any facility work in total isolation, and isolating them for security purposes is not an option. Firewalls are a critical tool in providing secure data acquisition and information flow across a plant's networks. This service implements a zoned firewall network approach. The firewall zones will allow the client to create independent security zones that limit inbound and outbound access to their assets.

What does it include?

Typically, a Firewall Installation and Configuration can include:

- Firewall installation, configuration, and commissioning
- Intrusion Detection/Prevention rule installation on CISP-installed firewalls
- Anti-virus installation and rule-set implementation on CISP-installed firewalls
- Documentation for zone network firewall
- Rule-sets as implemented
- Port scans verifying implemented rules are performing correctly
- Documented findings

At a Glance

- ⇒ **Firewalls provide protection against outside threats by shielding your network.**
- ⇒ **Controls for restricting access to the PCN Cyber Assets from the remote networks.**
  - ⇒ **Port restrictions for source and destination**
  - ⇒ **IP restrictions for source and destination**
- ⇒ **Intrusion detection and protection.**
- ⇒ **Anti-virus detection and protection.**

SWITCHING

When is it necessary?

A Secondary network is essential in providing a central infrastructure to host cyber security solutions and should be proposed with solutions such as

- Backups
- Anti-Virus Management
- Patch Management
- Event/Logging Management
- Network Monitoring Services
- Network Performance Management
- Security Information and Event Monitoring (SIEM)
- Active Directory Control
- Secure Zone – Remote access relay server
- Plus support of future requirements

Key Words

Key words to look for in a proposal that indicate that a Secondary Network switch should be recommended: **centralize control, Network Management, AD, and any of the above solutions**

Without a Secondary Network switch, the ability to provide a centralized architecture that will support cyber security solutions is not practical. This is due to the nature of interfacing servers directly to the Process Control Network (PCN) backbone network.

What is it?

Virtually every facility's PCN runs across an Ethernet type network, whether it is referred to as the PCN or some other name. This network is the primary backbone of the facility, carrying important process control information across the facility's control system. Any interruption to data flow in this network can have major consequences in both safety and operation. A Secondary Network or Plant Information Network (PIN) is a critical first step in securing the control network as part of a larger overall cyber security compliance program. The secondary network is comprised of adding a switch, effectively creating a secondary network that will not compromise the resiliency or data flow of the PCN. The importance of this secondary network is that it provides a centralized location for a number of cyber security elements: switch for traffic management, patch management, centralized network control, and authentication control for the Active Directory servers, to name a few. This centralized concept also eliminates the need to touch every server or workstation in the network.

What does it include?

This service typically includes a secondary switch architecture plan, which will identify current PCN elements to be part of the secondary switch architecture. The required network hardware and services (domain controllers, switching, and firewalls) should also be identified.

Additionally, a secondary network switch for the PCN can be installed and the secondary network interface configured with an IP address, Netmask, and Gateway. A network design, network bill of materials, and installed secondary network plan can be included with this service.

At a Glance

- ⇒ **Creates centralized access to the greater network, enabling additional centralized cyber security services.**
- ⇒ **Does not interfere with the primary PCN.**
- ⇒ **Easy to expand as the network grows and is capable of supporting copper or fiber network inputs.**

HARDENING

When is it necessary?

One the most basic cyber security best practices and the most overlooked of services is hardening. The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by removing all non-essential software programs and utilities from the computer. While these programs may offer useful features to the user, if they provide "back-door" access to the system, they must be removed during system hardening.

Key Words

Key words to look for in a proposal that indicate hardening should be recommended: **server hardening, base lining, server security**

Without Hardening, servers are at a greater risk for attack. Hardening reduces the attackable profile of the system.

What is it?

Every operating system has vulnerabilities and the purpose of a hardening effort is to identify applications, services, and ports needed to perform the assigned role for a particular cyber asset. System hardening is a systematic process of securely configuring cyber assets to protect against unauthorized access while also taking steps to make the cyber asset more reliable. Generally, by reducing exposed vulnerabilities, the risk of potential security incidents decreases, enabling the cyber asset to become more secure and more reliable. Hardening also ensures a common base line for assets. Once a new server is configured in the field it needs to be hardened. Hardening helps set a baseline of what the normal network configuration is, making it easier to run network scans to look for changes.

What does it include?

Hardening typically includes:

- Scanning systems to identify open ports, patch levels for the operating system, and running services as well as to update anti-virus definitions
- Performing and documenting scans, demonstrating systems are virus-free and virus patterns are updated (not available on Sun OS)
- Hardening of system bios
- Implementing operating system best practices for removal of unneeded software

At a Glance

⇒ **Hardening plan per cyber asset**
⇒ **Cyber asset vulnerability report created from scans**
⇒ **Cyber asset open ports and running services**
⇒ **Base-line established, improving network monitoring performance**

ACTIVE DIRECTORY

When is it necessary?

Many Industrial Control Systems use Microsoft Active Directory as a key component of PCN management and security with the adoption of Microsoft as the standard for server and workstation operating systems. Active Directory controls the core security of the Microsoft Windows network environment. The directory service is responsible for authenticating user and computer accounts within the Active Directory infrastructure. In addition, the directory service provides a mechanism for centralized, delegated administration of resources within the forest. An Active Directory workshop goes beyond the initial vendor-specific Active Directory installation, taking full advantage of the active directory server.

Key Words

Key words to look for in a proposal that indicate an Active Directory Workshop should be recommended: **I/A 8.X release, I/A server, user access control, AD server, off-MESH, user change management control**

Without an Active Directory Workshop, clients are left with the task of dealing with the complexity of setting up and deploying their Active Directory.

What is it?

The Active Directory Workshop assists ICS customers in the decision-making process by providing a clear and concise path for designing the Active Directory infrastructure for their ICS and then creating a deployment plan for ICS installation services. The Active Directory Workshop is based on best practices and real-world ICS experience and offers considerations and alternatives to meet a particular client's site requirements. The Invensys Cyber Security team has developed the Active Directory Workshop to assist ICS clients in deploying vendor-specific Active Directory services.

What does it include?

The Active Directory Workshop with Installation can include the following:

- Installing and commissioning active directory domain controllers that control the security roles and operating system access controls
- On-site visit and workshop with necessary personnel that will provide an implementation plan, a matrix of users, and a checklist for verification
- Active Directory data collection worksheet with architecture plan
- Installed Active Directory verification plan

At a Glance

⇒ **Provides central location for access to user information for a given network.**

⇒ **Provides central user account information, providing authentication, authorization, password management, and updates that enforce security policies.**

REMOTE ACCESS SERVER

When is it necessary?

In today's current industrial facilities, communicating remotely between different facilities or from corporate offices to the plant is not uncommon. Typical remote access would be between remote servers communicating between a firewall. A "Secure Zone" provides remote access control with mutual security along with secure data acquisition as well as a more robust solution and platform to build on. This solution should be proposed to customers who are looking to secure or isolate their Process Control Network (PCN) from the corporate network. In many cases, customers believe that a simple firewall is sufficient when, in fact, the corporate network is protecting itself from the PCN.

Key Words

Key words to look for in a proposal that indicate a Secure Zone should be recommended: **network segregation, DMZ, data access, remote access**

Without a Secure Zone, there is no buffer before the network traffic can traverse into the DCS network.

What is it?

Remote Access means no direct access paths from the corporate network to Data Acquisition, Compliance/History, and DCS Zones cyber assets. This service protects the Data Acquisition, Compliance/History, and DCS secure zones from exposure to the corporate network by deploying a Remote Relay Access Server.

What does it include?

This service should include installing Microsoft Server 2008 and configuring Microsoft Active Directory to support remote user access. The operating system installation and configuration process typically includes basic hardening (i.e. changing the administrator account, disabling unneeded services, and applying security templates) and applying network settings on Primary Network Interface Card (NIC) for System Management.

At a Glance

- ⇒ **Service includes installing and configuring Microsoft Server 2008 and Hyper-V.**
  - ⇒ **A VMWare ESX technology deployment option is also available.**
- ⇒ **The installation and configuration process for Microsoft Server 2008 will include setting up network settings on Primary NIC for System Management, bringing the server to current patch levels for the operating system, installing anti-virus software on the Hyper-V host, and setting up exclusions needed for Hyper-V server hosting.**
- ⇒ **Hyper-V installation process will include changing the server hardware bios settings to support Hyper-V, installing the Hyper-V server role, setting up virtual switches as identified from gathered information, and Hyper-V hardening.**

TECHNOLOGY ASSESSMENT

When is it necessary?
A Technology Assessment is an ideal first step that should be proposed in cases where customers are unsure or unaware of what cyber security solutions are available or even applicable to them.

Key Words
Key words to look for in a proposal that indicate a Technology Assessment should be recommended: **roadmap, regulatory requirements, cyber security program, security integration**

Without a proper cyber security Technology Assessment, many customers tend to either overestimate or underestimate what needs to be done and the order in which it needs to be done, losing focus on the real cyber requirement.

What is it?
The Technology Assessment workshop will help the client develop a roadmap for the secure network support of current and future business and industrial control system requirements. It includes a one-week site visit and workshop with all necessary parties. Consultants will establish the current architecture, define the desired security posture, design the required architecture to achieve the desired security posture, and outline a migration path in conjunction with the client's constraints.

What does it include?
A technology assessment typically includes a report and presentation about the current security state of the client's environment and recommended security mitigations as well as a list of findings and recommendations to improve areas such as policies and procedures, network security, and best practices.

At a Glance

- ⇒ **Provides a cyber security roadmap with management-level presentation.**
- ⇒ **Contains the current security state of the network and recommended security mitigations.**
- ⇒ **Includes findings and recommendation to improve areas such as policies and procedures, network security, and best practices.**

ASSET IDENTIFICATION

When is it necessary?

Asset Identification is an ideal first step that should be proposed to customers who are embarking on a cyber security program and trying to define what network elements (assets) should be secured.

Key Words

Key words to look for in a proposal that indicate an Asset Identification should be recommended: **critical infrastructure, regulatory requirements, cyber security program, security integration, asset management, asset identification**

Without performing Asset Identification, customers run the risk of overestimating what network elements should be identified as critical and tend to overestimate the scope of work and the amount of resources required.

What is it?

One of the first steps to planning or implementing a cyber secure network is identifying what elements are critical to operation and need to be secured. Skipping this step can lead to securing numerous network elements that are not critical, resulting in an expansive and costly scope of work. Asset identification is a process of using a defined description of what a critical asset is and then working through a facility to identify and log those elements that fall under that definition. NERC CIP's definition of critical assets, which is commonly used in power generation facilities but has been adopted across other industries, breaks down assets into two areas:

Critical Asset: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the facility.

Critical Cyber Assets (CCAs): Programmable electronic devices and communication networks including hardware, software, and data that are essential to the reliable operation of critical assets.

What does it include?

After completing the onsite critical asset survey, the data collected can be used to

- Identify cyber assets associated with a critical asset
- Compile a list of cyber assets
- Create an initial cyber asset data report in Microsoft Excel with description, category, building, room/cabinet, unit, and expanded description
- Create a final cyber asset data report in Microsoft Excel with details on each cyber asset

PATCH MANAGEMENT

When is it necessary?

The Patch Management solution should be provided in nearly all network proposals. Patch Management, as the name implies, is a solution that helps centralize the control of all software patches and updates for a secure push out to the larger network while reducing the need to update individual workstations. The Patch Management solution ensures that the customer has the most current patches available and can deploy them to the network at any time convenient to them based on their requirements.

Key Words

Key words to look for in a proposal that indicate Patch Management should be recommended: **software updates, software patching, centralized management**

Without Patch Management, clients are left without a centralized approach to applying both current vendor-authorized patches as well as customer-approved third-party patches.

What is it?

Updating anti-virus software, firmware, and software patches across a facility's Process Control Network (PCN) is critical to ensuring that the network is operating at current levels. Missing and outdated patches are one of the main reasons for network security breaches. Without a patch management system, operators must run from machine to machine, or worse, rely upon users to patch their own systems. A centralized patch management server, hosted from a Secondary Network, allows patches to be deployed from a single point across the covered network. Patch management systems enable you to maintain full control of your systems' patching activities. You can deploy security patches to test machines, and then push them out to the rest of the machines. You can also run reports to ensure that you have 100% compliance across all servers and workstations. You can use your patch management system to provide reports to management and auditors so that management knows what is going on and auditors' requests are easy to meet.

What does it include?

Patch management typically includes:

- Creating and updating custom patch scanning profiles
- Performing training sessions on reporting capabilities for patching and reporting patch results as well as running missing patch reports and remediation reports
- Documenting the patch management solution

At a Glance

⇒ **Patch management provides a centralized location for patches.**

⇒ **Patch management enables administrators to manage PCN and Microsoft patches and service packs for all languages supported by Microsoft.**

⇒ **Patch management allows custom patch scanning profiles and scheduling of patches at times that best suit the user.**

NETWORK PERFORMANCE MANAGEMENT

When is it necessary?
Network performance management should be provided as part of a larger cyber security roll out or for networks that already have in place security elements and desire a solution to monitor the network.

Key Words
Key words to look for in a proposal that indicate Network Performance Monitoring (NPM) should be recommended: **network management, performance management, network monitoring**

Network performance management is a very important part of monitoring the overall status of the network and the state of the cyber security elements. Without network performance management, the operators are blind to the status of the network and any changes in the state of the network security.

What is it?
NPM is far more strategic than its name implies. It involves watching for problems 24/7, but it's also about optimizing data and access in a complex and changing environment. Network performance management tools offer monitoring and management options that can extend the reach of a single operator and improves the effectiveness of monitoring and troubleshooting performance problems on the Plant Information Network (PIN) or PCN. One of the top concerns regarding PCNs and/or Industrial Control Systems is the lack of visibility into the PCN or PIN to effectively troubleshoot and resolve performance problems. Only through greater visibility and shared knowledge can ICS administrators prevent outage issues. Network performance monitoring and management enables operators to quickly detect, diagnose, and resolve network performance problems and outages.

What does it include?
A typical NPM service should provide the client with a set of requirements and configuration changes needed to support NPM, such as:

- New configurations for monitoring PCN and/or PIN switches
- Updated PCN/PIN workstation configurations
- Custom reports for client-deemed critical devices monitored by the NPM, obtained by working with client-designated staff to identify commonly used or recommended reports such as
    - PCN/PIN Switch Availability
    - PCN/PIN Switch Performance

    - PCN/PIN Station Availability
    - PCN/PIN Workstation High Disk and CPU Utilization
- Alerting rules as identified during the Network Review phase (consultants will configure NPM to relay SMTP alerts to client-designated email accounts via SMTP relay server; this feature requires the client to supply a SMTP relay for email forwarding to client-designated email accounts)

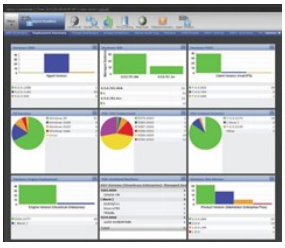
At a Glance

⇒ **Network performance monitoring is a centralized solution, monitoring the entire network from a single location.**

⇒ **Network performance monitoring simplifies detection, diagnosis, and resolution of network issues before outages occur.**

⇒ **Network performance monitoring tracks response time, availability, and uptime of routers, switches, and other SNMP-enabled devices.**

⇒ **Network performance monitoring displays performance statistics in real time via dynamic, drillable network maps.**



ePOLICY ORCHESTRATOR (ePO)

When is it necessary?

Centralized control points is one of the challenges facing Industrial Control System (ICS) administrators. Central control simplifies the process and the steps needed to deploy and manage software and updates. McAfee ePO provides powerful workflow capabilities to increase ICS administrators' effectiveness, allowing ICS administrators to quickly define and deploy security as well as respond to security events and issues.

Key Words

Key words to look for in a proposal that indicate ePO should be recommended: **malicious software, prevention, HID, HIP, A/V, McAfee**

Without a ePO, there is no central control for a number of security elements, such as anti-virus, whitelisting, and HIPS.

What is it?

With ePO, DCS administrators can unify security management across end-points, networks, and data. Clients can use ePO to manage a centralized anti-virus program for profile updates.

- Necessary ePO policies for controlling USB drives (HIPS), host firewall policies, rogue system detection setup, and policy implementation
- Procedure/mechanism for ePolicy server to receive AV DAT updates from a centralized proxy server (if available)
- Determine alerting requirements and set up ePO Alerting

What does it include?

This service typically includes installation and configuration of ePO software. Limited rule sets may be applied depending on the SAT requirements for testing. CISP should also meet with the client to determine items such as:

- User access requirements (i.e. defining ePO administrators)
- Hardware restrictions
- Reporting needs
- Alerting needs
- Custom Network Access Controls

At a Glance

⇒ **End-to-end visibility —Drillable, drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks for immediate insight and faster response times.**

⇒ **Simplified security operations — Streamline workflows for proven efficiencies. An open, extensible architecture — Leverage your existing network infrastructure.**

⇒ **ePO software connects management of both McAfee and third-party security solutions.**

WHITELISTING

When is it necessary?
Whitelisting is a technique that allows content or software to be able to run and deny or restrict anything else. Applications like whitelisting should be proposed when customers are looking to control access to what applications can run on workstations or servers or when customers are deploying remote access systems and need to lock down what applications operators have access to.

Key Words

Key words to look for in a proposal that indicate Whitelisting should be recommended: **application control, end point protection, blacklisting, whitelisting, file integrity control**

Without whitelisting, controlling access to specific lists of applications on servers and workstations is difficult. In many cases, the programs are just deleted from the systems only to be reinstalled at a later time.

What is it?
Unlike blacklisting, a list of known threats to check against, whitelisting is a user-defined database of known clean applications that are approved to run in a given environment. If an unknown application or program (.exe file) that is not on the whitelist tries to run, it would be prohibited from opening. Blacklisting is based on an ever-expanding list of threats that must be added to the database. Conversely, a whitelisting database is relatively small since it is based on known good programs, so the CPU cycle times to run whitelisting are less than that for blacklisting.

What does it include?
A typical Whitelisting service should include:

- Installation and configuring of the whitelisting software
- Creation of the whitelisting database
- Report outlining the whitelisting process

At a Glance

⇒ **Whitelisting is designed to protect against unauthorized and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.**
⇒ **While primarily implemented to prevent the execution and spread of malicious software (malware), it can also prevent the installation or use of unauthorized software.**
⇒ **Application whitelisting comprises the following technical steps:**
  ⇒ **Identifying specific executables and software libraries that should be permitted to execute on a given system**
  ⇒ **Preventing any other executables and software libraries from functioning on that system**
  ⇒ **Preventing users from being able to change which files can be executed**

SECURITY INFORMATION AND EVENT MONITORING

When is it necessary?

Security Information and Event Monitoring (SIEM) should always be proposed to customers looking to gain real-time visibility into all activity on their network. Real time situational awareness and the speed to and scale required to identify critical threats, respond appropriately, and ensure continuous compliance monitoring is key to defending against network threats.

Key Words

Key words to look for in a proposal that indicate a SIEM should be recommended:
intrusion prevention, security monitoring, threat monitoring

Without SIEM, the operators may rely on much less robust anti-virus and malware software to try and protect against intrusions and to help mitigate Denial-of-Service (DoS).

What is it?

SIEM solutions are a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event management). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. The objective: To help companies respond to attacks faster and organize mountains of log data. Increasingly, SIEM solutions are being used to log security data and generate reports for compliance purposes. SIEM product capabilities include gathering, analyzing, and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database, and application logs; and external threat data. A key focus is to monitor and manage user and service privileges, directory services, and other system configuration changes as well as provide log auditing and review and incident response.

What does it include?

A typical SIEM service can include these elements:

- Installing the SIEM hardware/software for collecting security events from Industrial Control System cyber assets
- SIEM tuning
- Verification of the following:
    - The security monitoring controls issue block or alert actions for detected cyber security incidents.
    - The SIEM detects and alerts for attempts at or actual unauthorized accesses, where technically feasible.

At a Glance

⇒ **SIEM is ideal for compliance and reporting.**
⇒ **SIEM technology gives a view of internal and external threats.**
⇒ **SIEM solutions improve operational efficiencies and cut administrative costs.**
⇒ **SIEM technology is flexible and can be made into a managed service.**

DEVICE CONTROL

When is it necessary?

Removable media such as USB drives are almost as ubiquitous in the plant as they are in the office. This causes a number a security concerns since control is typically lacking over what comes in on the USB drive and what may leave on it. Device control is the ability to manage and control not only what devices can be used but also who has access to them.

Key Words

Key words to look for in a proposal that indicate Device Control should be recommended: **malicious software, prevention, USB drives, data control**

Without Device control, there is no way to ensure that only approved devices are be used by approved personal.

What is it?

Device Control helps control and block confidential data copied to removable storage devices. Device parameters such as product ID, vendor ID, serial number, device class, and device name can be specified and categorized. Furthermore, different policies such as block or encrypt can be enforced based on the content loaded onto the devices.

- Support for plug-and-play devices and removable storage devices
- Removable storage devices can be blocked or made read-only
- Content-aware protection for removable storage devices
- File access protection for files that reside on removable storage devices
- Non-system hard disks rule blocks and monitors read-only files and provides notifications of user actions on fixed disk drives

What does it include?

Device Control is typically integrated with ePO. For this configuration, ePO software should be installed and configured. Limited rule sets may be applied depending on the SAT requirements for testing. User access requirements (i.e. defining ePO administrators), hardware restrictions, user restriction needs, and custom network access controls can also be determined.

At a Glance

⇒ **Supported by ePO, providing controlled access to USB drives, MP3 players, CDs and DVDs**

⇒ **Comprehensive Device Management — Control how users copy data to removable devices as well as from Bluetooth and IR devices, imaging equipment, COM and LPT ports**

⇒ **Granular Controls — Deploy and update Device Control agents via ePO software**

⇒ **Centralized management to define and deploy which devices can and can't be used as well as user restrictions**

Host Intrusion Protection Service (HIPS)

When is it necessary?

With security breaches on the rise, many clients are looking for ways to extend their capabilities beyond just anti-virus software. Clients want to actively monitor their networks for potential threats. Host Intrusion Protection Service (HIPS) is an intrusion detection system that monitors and analyzes the internals of a computing system as well as (in some cases) the network packets on its network interfaces.

Key Words

Key words to look for in a proposal that indicate a HIPS solution should be recommended: **network protection, intrusion prevention, network protection, HIDS (Host Intrusion Detection Services) or NIDS (Network Intrusion Detection Services)**

Without a HIPS, there is no ability to actively monitor and analyze the network for possible threats, internal or external.

What is it?

Host Intrusion Prevention Service (HIPS) is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks. It protects against unauthorized viewing, copying, modifying, and deleting of information and the compromising of system and network resources and applications that store and deliver information.

- Defends servers and applications from attacks and prevents data loss
- Filters HTTP requests to prevent directory traversal
- Uses predefined shielding policies and rules to prevent attacks and loss of data
- Examines database queries to prevent attacks, such as SQL injection
- Uses predefined shielding policies and rules to ensure normal behavior and prevent tampering of data

What does it include?

The HIPS software can be fully integrated with ePO. For the HIPS configuration, ePO software should be installed and configured. Limited rule sets may be applied depending on the SAT requirements for testing. The following items can also be determined:

- User access requirements (i.e. defining ePO administrators)
- Hardware restrictions
- Network access criteria
- Alerting needs

At a Glance

⇒ **HIPS features: Intrusion prevention, Firewall, Application blocking**
⇒ **HIPS principal mechanisms: Signature-based IPS and Spot and block new vulnerabilities**
⇒ **HIPS categories: Known threat, Signature threat, unsolicited outbound traffic**

INDUSTRY REGULATIONS

Cyber security standards, regulatory requirements, and best practices have evolved over the past few years, moving beyond security for the IT environment and focusing more on critical infrastructure and cyber security for Industrial Control Systems. Virtually every government is working on cyber security infrastructure regulations and standards. Most of these rely heavily on the work that has already been done by organizations such as NERC, NIST, and NEI. These standards organizations help companies develop effective cyber security strategies. While these organizations have different approaches, they all have a common element—to establish a "Best Practice" approach to cyber security.

Cyber security standards today are very prescriptive, outlining what guidelines or steps need to be done to be compliant while lacking specific detail on technical solutions. They leave customers with the need for cyber security solutions that are flexible enough for their unique network requirements and will assist them in becoming compliant. Invensys' cyber security team addresses those very needs with a comprehensive approach to cyber security and cyber security solutions.

NERC CIP

North American Electric Reliability Corporation Critical Infrastructure Protection

NERC maintains comprehensive reliability standards that define requirements for planning and operating the bulk electric system (BES). Among these are ten Critical Infrastructure Protection (CIP) Cyber Security Standards, which specify a minimum set of controls and processes for power generation and transmission companies to follow to ensure the cyber security of the North American power grid. Penalties and fines are applied to companies that are in violation.

NERC-CIP v5

Industry: Power Generation

CIP-002	BES Cyber System Categorization
CIP-003	Security Management Controls
CIP-004	Personnel and Training
CIP-005	Electronic Security Perimeter(s)
CIP-006	Physical Security of BES Cyber Systems
CIP-007	System Security Monitoring
CIP-008	Incident Reporting and Response Planning
CIP-009	Recovery Plans for BES Systems
CIP-010	Configuration Change Management and Vulnerability Assessments
CIP-011	Information Protection

NIST

National Institute of Standards and Technology

Industry: All industries

In February 2013, President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity. The order calls for the development of a voluntary, risk-based Cybersecurity Framework—a set of existing standards, guidelines, and practices to help organizations manage cyber risks. The result is the NIST Cybersecurity Framework that allows organizations—regardless of size, degree of cyber risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. The NIST Framework referenced over 320 National and International Standards, Guidelines, Directives, Best Practices and Regulations including input from: ANSI, ISA, NERC, API, ISO, IEC, NEI, NIST, NFPA, OIG, OLF, OPC, SANS, TIA.

The three main elements described in the document are Core, Tiers and Profiles.

Framework Core: The core presents five functions—identify, protect, detect, respond, and recover—that taken together allow any organization to understand and shape its cybersecurity program.

Tiers: The tiers describe the degree to which an organization's cybersecurity risk management meets goals set out in the framework and "range from informal, reactive responses to agile and risk-informed."

Profiles: The profiles help organizations progress from a current level of cybersecurity sophistication to a target improved state that meets business needs.

AWWA

American Water Works Association

Industry: Water, Wastewater

In response to Executive Order 13636, the AWWA has created ANSI/AWWA G430: Security Practices for Operations and Management. The AWWA Cybersecurity Guidance and Tool represent a voluntary, sector-specific approach that supports the NIST Cybersecurity Framework. The Cybersecurity Guidance and Tool are living documents, and it is expected that further revisions and enhancements will be implemented based on input from users.

List of recommended cyber security practices:

- Governance and Risk Management
- Business Continuity and Disaster Recovery
- Server and Workstation Hardening
- Access Control
- Application Security
- Encryption
- Telecommunications, Network Security, and Architecture
- Physical Security of PCS Equipment
- Service Level Agreements
- Operations Security (OPSEC)
- Education
- Personnel Security

CFATS

Chemical Facility Anti-Terrorism Standards

Industry: Chemical and industries that use identified chemicals

The U.S. Department of Homeland Security (DHS) has released an interim final rule that defines comprehensive federal security regulations for high-risk chemical facilities. The CFATS rule establishes risk-based performance standards for the security chemical facilities. It requires covered chemical facilities to prepare Security Vulnerability Assessments, which identify facility security vulnerabilities, and to develop and implement Site Security Plans, which include measures that satisfy the identified risk-based performance standards (RBPS).

List of CFATS Risk Base Performance Standards

RBPS 1	Restrict Area Perimeter
RBPS 2	Secure Site Access
RBPS 3	Screen and Control Access
RBPS 4	Deter, Detect, Delay
RBPS 5	Shipping, Receipt, and Storage
RBPS 6	Theft or Diversion
RBPS 7	Sabotage
RBPS 8	Cyber

For additional information, visit us at http://iom.invensys.com/CyberSecurity
Don't forget to visit our blog at invensyscybersecurity.blogspot.com

Schneider Electric • 1820 Preston Park Blvd, Suite 1900, Plano, TX 75093 • Tel: 1 (613) 591-1943 • Fax: 1 (613) 591-1022 • www.schneider-electric.com

Schneider Electric, the Schneider Electric logo, ArchestrA, Avantis, Eurotherm, Foxboro, IMServ, InFusion, SimSci-Esscor, Skelta, Triconex, and Wonderware are trademarks of Schneider Electric, its subsidiaries or affiliates. All other brands and product names may be the trademarks or service marks of their representative owners.

© 2014 Schneider Electric. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Schneider Electric.

Rev. 201401