Schneider Electric

Cyber Security Services
by Schneider Electric

Cyber Security Sales Reference

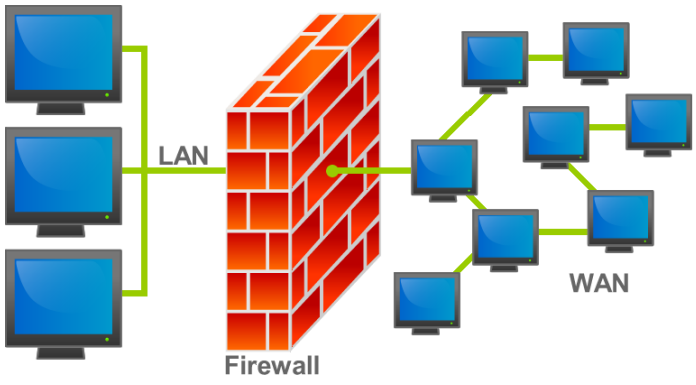
Schneider-Electric's Cyber Security Services Team provides detailed and customizable solutions for the items listed in this document. These solutions and offerings address cyber security elements such as firewalls and anti-virus that you may find in a Industrial Control System (ICS), Process Control Network (PCN) or Building Automation Management Systems (BAMS) and can help customers who are interested in adding these elements to their networks. This document will assist you and your customers with any questions relating to the following cyber security elements.

Table of Contents

FIREWALLS

Firewall	A computer system or network that is designed to block unauthorized access while permitting outward communication.
Packet Filtering	Packet filters act by inspecting the "packets," which are transferred between computers on the Internet. If a packet matches the packet filter's set of filtering rules, the packet filter will drop (silently discard) the packet or reject it (discard it and send "error responses" to the source).
Layer 2	Firewalls deployed in Layer 2 mode provide the most transparent method for integrating with existing routing and IP designs as well as existing services
Stateful	Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 – Transport Layer of the OSI model. This is achieved by retaining packets until enough information is available to make a judgment about its state.
Application Layer	These switches provide the same basic functionality as unmanaged switches, but they can be configured with some advanced functionality to further optimize a network.

Firewalls are one the most commonly deployed hardware point solutions for cyber security. However, there are many types of firewalls all specific uses and applications. Traditional **firewalls** inspect network traffic by comparing the source and destination addresses against a rule set and determining whether to forward the traffic or discard it. However, modern firewalls will examine packets of data for well-known signatures that specify the type of application that created it and the specific data protocols used.



Packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT). Packet filtering is part of a firewall program for protecting a local network from unwanted intrusion.

Modern network attack techniques are quite sophisticated at fooling traditional firewalls by forging the parts of the data packet that are examined to compare against rules. New firewall technologies that mitigate these risks include Layer 2 (often called “transparent”) Firewalls and Stateful Firewalls that utilize Deep Packet Inspection (DPI).

Layer 2 firewalls are designed to inspect traffic in a way that makes them extremely difficult to bypass or fool in regards to forged addressing. Because they function at the Data Link layer of the

OSI Reference Model, not at the Network layer, they are able to process data without establishing a presence at the Network layer. This makes them nearly undetectable, with the added benefit that their stealth protects them from most intrusion attempts.

Layer 2 firewalls, when deployed in mission-critical production environments, can be configured to "fail open" or function as a simple piece of wire in the event of its total failure. This ensures that the important data traffic can continue to flow even if the firewall fails completely.

Stateful firewalls are designed to keep track of all stages of communication between hosts from set -up through data transfer to tear-down. Before stateful firewalls existed, a firewall did not keep track of "conversations between hosts" and had no way to know if a packet it received was part of an existing approved conversation or was a rogue packet containing headers of a conversation in progress, but malicious or faulty data.

Deep Packet Inspection is a technique through which the stateful firewall scans the actual payload of a data packet, rather than just the labels on different areas of the packet, to ensure that it actually contains the type of data that it indicates. Another name for a stateful firewall is application-layer firewall. Application-layer firewalls contain additional intelligence in their scanning engines, which allows them to compare the data inside a packet against common data patterns of a given type.

For example, a forged packet that appears to contain a "GET" request to a Web server in HTTP format may in fact contain a malicious command or corrupted string of text. A traditional firewall would pass the packet through based on source, destination, headers, and labels being correct. A stateful firewall utilizing DPI would inspect the actual text and discard the packet because the contents are not a legitimate request.

Because different segments of the network have different security requirements and types of traffic, it is often useful to divide the network into logical zones. For example, the most sensitive and critical part of the network, the DCS Network, can be incorporated as a "DCS Zone." The PCN, with its management, trending, and monitoring systems, could be called a "Data Acquisition Zone." There could be a "Remote Access Zone" encompassing Citrix servers, Terminal Server systems, dial-up access servers, and VPN concentrators.

By segmenting the network logically according to types of traffic and level of trust, firewall rules can be built and assigned to specific physical interfaces on the firewall, to logical address blocks, and to specific VLANs. This allows the ICS group the highest level of control over which traffic origins and profiles are allowed access to their critical assets

An **Application firewall** is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall which is - without additional software - unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

- A network-based application layer firewall is a computer networking firewall operating at the application layer of a protocol stack,[1] and is also known as a proxy-based or reverse-proxy firewall.

- A host-based application firewall can monitor any application input, output, and/or system service calls made from, to, or by an application. This is done by examining information passed through system calls instead of or in addition to a network stack. A host-based application firewall can only provide protection to the applications running on the same host.

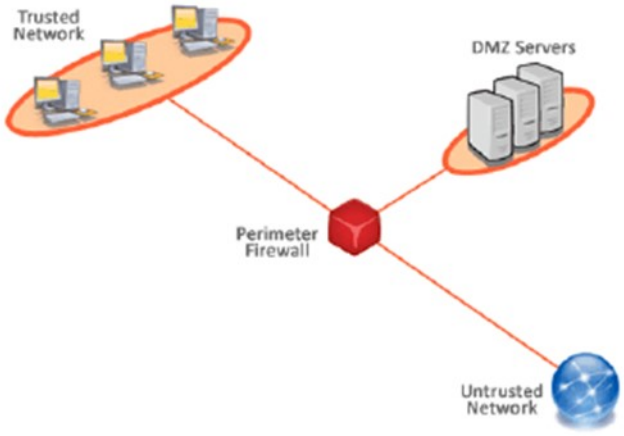
DMZ

DMZ	A DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
Single Firewall - DMZ	Single firewall DMZ, comprises of a firewall with three network interface cards (NICs) installed in it. The first connected to the external network (Internet), the second connected to the computers placed inside the trusted local network, and the third NIC is used to form a DMZ
Dual Firewall - DMZ	Dual firewall model whereby a distinctly separate network is configured to act as a layered security zone between the perimeter firewall and a second DMZ/LAN firewall located ahead of the trusted network – more security.

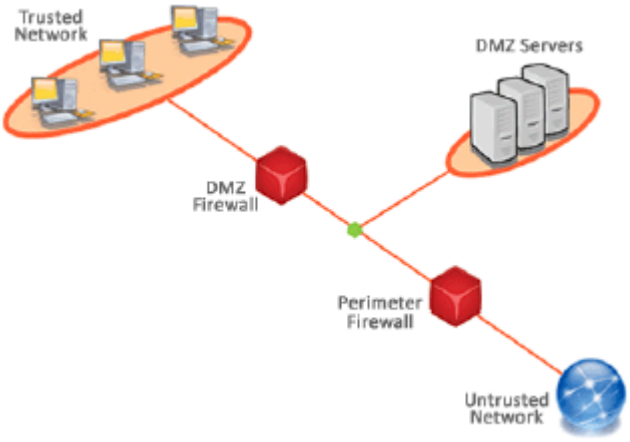
In computer security, a **DMZ** or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network—usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone," an area between nation states in which military operation is not permitted.

There are two basic DMZ architectures:

A **Single Firewall** with at least 3 network interfaces can be used to create a network architecture containing a DMZ. The external network is formed from the ISP to the firewall on the first network interface, the internal network is formed from the second network interface, and the DMZ is formed from the third network interface. The firewall becomes a single point of failure for the network and must be able to handle all of the traffic going to the DMZ as well as the internal network. The zones are usually marked with colors; for example, purple for LAN, green for DMZ, and red for Internet (often with another color for wireless zones).



A **Dual Firewall** is a more secure approach compared to the two firewalls to create a DMZ. The first firewall (also called the "front-end" or "perimeter" firewall) must be configured to allow traffic destined to the DMZ only. The second firewall (also called "back-end" or "internal" firewall) only allows traffic from the DMZ to the internal network. This setup is considered more secure since two devices would need to be compromised. There is even more protection if the two firewalls are provided by two different vendors, because it makes it less likely that both devices suffer from the same security vulnerabilities. For example, accidental misconfiguration is less likely to occur the same way across the configuration interfaces of two different vendors, and a security hole found to exist in one vendor's system is less likely to occur in the other one.



SWITCHING

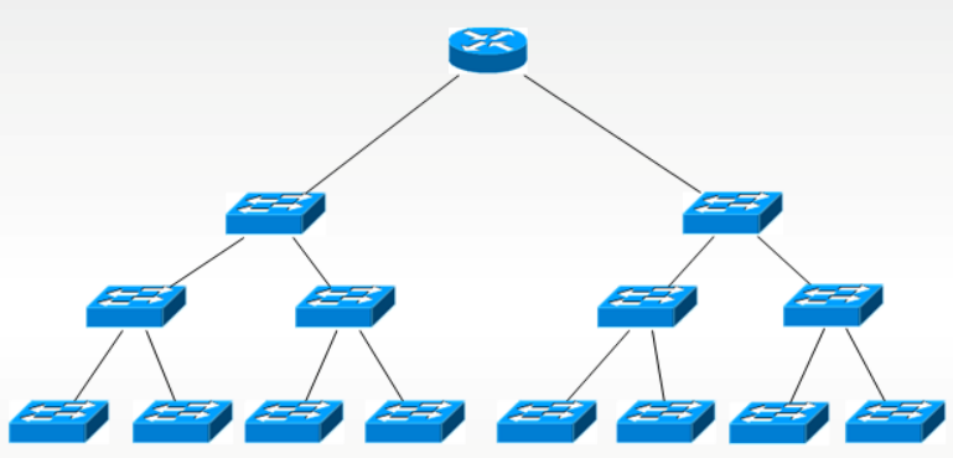
Aggregator – Switch	A network can be established by connecting hosts through the following three devices:
Hubs	Any network communication that comes in one port is broadcast out of every port. This increases the traffic on a network. These devices are not configurable.
Unmanaged Switches	These devices learn what hosts are attached to each port and examine data packets so that data is sent only to the port that it is intended to go. These devices are not configurable.
Managed Switches	These switches provide the same basic functionality as unmanaged switches, but they can be configured with some advanced functionality to further optimize a network.

Switches are a commonly used aggregation device in networks. There are numerous types of switches all developed for different network needs. Typical switches are sized by how many ports, typically Ethernet, that they support; 8-port, 12-port, 24-port and 48-port.

Hubs are the predecessor to today's configurable switches providing basic network connectivity at the Layer 2. An ICS network should always contain managed switches. ICS networks should leverage available features from managed switches to provide increased protection.

Unmanaged switches limit the diagnosis of network problems and the available technical controls that can optimize an ICS.

Managed switches include core features such as Port Mirroring and Link Aggregation. Port Mirroring is a technique where a port on a switch can be configured to see all traffic that is passing through the switch. An IDS/IPS system (explained below) can be attached to this port to examine traffic on the network for anomalies. Link Aggregation is a technique where multiple switch ports can act as a single port, in effect multiplying the bandwidth that would have been available for that connection and/or provide a redundant connection for possible fail over needs.



Another managed switch feature that could enhance security is Port Security, which allows administrators to specify exactly which devices are allowed to connect to the switch. Broadcast Control and Rate Limiting can also protect traffic volume-sensitive PCN systems from Denial-of-Service due to excessive network traffic.

While managed switches do provide a more robust network feature set, they should be configured with strong passwords and encrypted management (SSL, SSH) when possible to protect against hijacking.

SERVERS

Server	A computer or computer program that manages access to a centralized resource or service in a network.
Active Directory Server	An Active Directory domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.
Client Servers	Servers are computer programs running to serve the requests of other programs, the clients.
SQL Servers	Any database server that implements the Structured Query Language. Microsoft SQL Server, a relational database server from Microsoft.
Web Server	A Web Server is a program that uses the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP). Every computer on the Internet that contains a Web site must have a Web server program. It is sometimes referred to as IIS (Internet Information Server) Server.

Servers are the true workhorse of any control network. Servers provide the flexibility to provide data storage all they up through hosting Virtual Machines. The differences are only in the OS running, the number of hard drives needed, processing power and memory needs.

Servers operate within a client-server architecture. Servers are computer programs running to serve the requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. The clients typically connect to the server through the network but may run on the same computer.

Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet.

A **Client Server** network is the most efficient way to provide:

- Databases and management of applications
- Communications and Document management.
- Network management.
- Centralized file storage.

The client/server model is basically an implementation of distributed or cooperative processing. At the heart of the model is the concept of splitting application functions between a client and a server processor. The division of labor between the different processors enables the application designer to place an application function on the processor that is most appropriate for that function. This lets the software designer optimize the use of processors—providing the greatest possible return on investment for the hardware.

Client/server application design also lets the application provider mask the actual location of application function. The user often does not know where a specific operation is executing. The entire function may execute in either the PC or server, or the function may be split between them. This masking of application function locations enables system implementers to upgrade portions of a system over time with a minimum disruption of application operations, while protecting the investment in existing hardware and software.

A **SQL Server** is a relational database management system developed by Microsoft. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users.

A SQL Server is offered in several editions with different feature set and pricing options to meet a variety of user needs, including the following:

- Enterprise: Designed for large enterprises with complex data requirements, data warehousing, and Web-enabled databases. Has all the features of SQL Server, and its license pricing is the most expensive.
- Standard: Targeted toward small and medium organizations. Also supports e-commerce and data warehousing.
- Workgroup: For small organizations. No size or user limits and may be used as the backend database for small Web servers or branch offices.
- Express: Free for distribution. Has the fewest number of features and limits database size and users. May be used as a replacement for an Access database.

A **Web Server** is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a Web server program. Two leading Web servers are Apache, the most widely-installed Web server, and Microsoft's Internet Information Server (IIS). Other Web servers include Novell's Web Server for users of its NetWare operating system and IBM's family of Lotus Domino servers, primarily for IBM's OS/390 and AS/400 customers.

Web servers often come as part of a larger package of Internet- and intranet-related programs for serving e-mail, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages. Considerations in choosing a Web server include how well it works with the operating system and other servers; its ability to handle server-side programming and security characteristics; and publishing, search engine, and site building tools that may come with it.

NETWORK INTERFACE CARD (NIC)

NIC	A Network Interface Card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network.
1000Base-T	Gig-E is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second.
SX - Fiber	1000BASE-SX is a fiber optic gigabit Ethernet standard for operation over multi-mode fiber using a 770 to 860 nanometer wavelength.
FX - Fiber	100BASE-FX is a version of Fast Ethernet over optical fiber. It uses a 1300 nm near-infrared (NIR) light wavelength.

Every computer on a network, both clients and servers, requires a Network Interface Card (or NIC) in order to access the network. A NIC is usually a separate adapter card that slides into one of the server's motherboard expansion slots. Selection of a NIC has to do with several factors; wiring media such as copper of fiber, speed supported on network and distance to traverse – segment length.

A **NIC** is a Physical layer and Data Link layer device. Because a NIC establishes a network node, it must have a physical network address, also known as a MAC address. The MAC address is burned into the NIC at the factory, so it cannot be changed. Every NIC ever manufactured has a unique MAC address.

Ethernet Standards		
Standard	**Speed**	**Segment Length**
10Base5	10Mbps	50m / 164ft
10Base2	10Mbps	185m / 606ft
10Base-T	10Mbps	100m / 328ft
100Base-T	100Mbps	100m / 328ft
100Base-TX	100Mbps	100m / 328ft
1000Base-T	1Gbps	100m/ 328ft
100Base-FX (Fiber)	100Mbps	2 km
1000Base-SX (Fiber)	1Gbps	550m (multi-mode)

ACTIVE DIRECTORY

Active Directory	Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and service.
AD Domain Controller	An Active Directory domain controller (server). Runs Microsoft Windows OS, authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.
AD Services	Active Directory services include Group Policies, DNS and the domain namespace, Domains, Forests, Trees, and Sites.

The **Active Directory** is the core security repository for your network. It contains users/groups and what functions they are allowed to perform. This centralizes management of your servers and workstations to simplify day-to-day management of the network while also meeting regulatory needs for centralized management.

As part of your ICS, Active Directory can be utilized. In Active Directory, a specialized Microsoft Windows server called a **Domain Controller** is installed. A Domain Controller contains the Active Directory. It is recommended that customers install a minimum of two Domain Controllers for proper failover needs.

Active Directory Services like Group Policies are applied to users or computers and limit what changes can be made on a workstation. These policies are enforced on the network to help ensure security. There is some "perceived stigma" in the control industry of operations being impeded by required logons and other restrictions. This is due to the experience people have had with IT implementations of Active Directory, which tend to be very restrictive. However, the features of Microsoft Active Directory are extremely customizable to be only as restrictive as is needed by industry regulations and the customer.

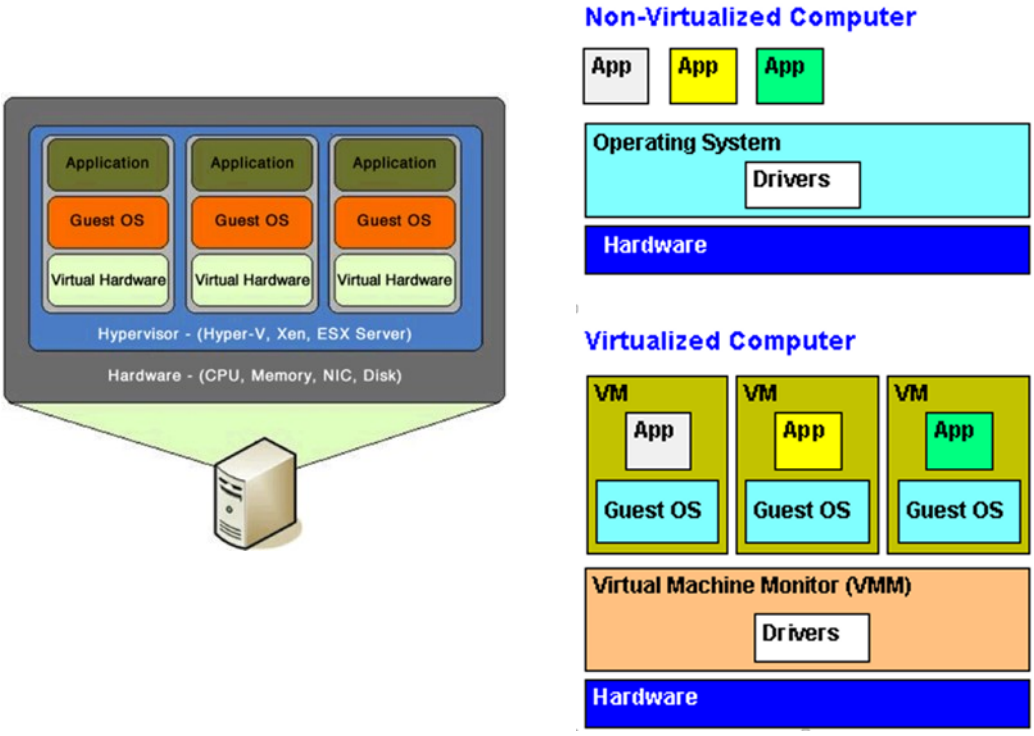
Active Directory features include:

- Support for the X.500 standard for global directories
- The capability for secure extension of network operations to the Web
- A hierarchical organization that provides a single point of access for system administration (management of user accounts, clients, servers, and applications, for example) to reduce redundancy and errors
- An object-oriented storage organization, which allows easier access to information
- Support for the Lightweight Directory Access Protocol (LDAP) to enable inter-directory operability
- Designed to be both backward compatible and forward compatible

VIRTUAL MACHINE

Virtual Machine (VM)	A virtual machine (VM) is a software-based emulation of a computer. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer.
System VM	A system virtual machine provides a complete system platform that supports the execution of a complete operating system (OS). It is also known as a Hardware Virtualization.
Process VM	A process virtual machine (or language virtual machine) is designed to run a single program, which means that it supports a single process.

A **Virtual Machine** is a PC (operating system and application software) that exists in a set of files on a server. This allows a company to allocate several dedicated virtual PCs that can be used by individuals even though they are located on the same server. The image below illustrates this concept.



A virtual machine (VM) is a software implementation of a machine (i.e. a computer) that executes programs like a physical machine. Virtual machines are separated into two major classifications based on their use and degree of correspondence to any real machine:

System Virtual Machine provides a complete system platform which supports the execution of a complete operating system (OS). These usually emulate an existing architecture and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use, or of having multiple instances of virtual machines leading to more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization, the key to a cloud computing environment) or both.

Process Virtual Machine (or language virtual machine) is designed to run a single program, which means that it supports a single process. Such virtual machines are usually closely suited to one or

more programming languages and built with the purpose of providing program portability and flexibility.

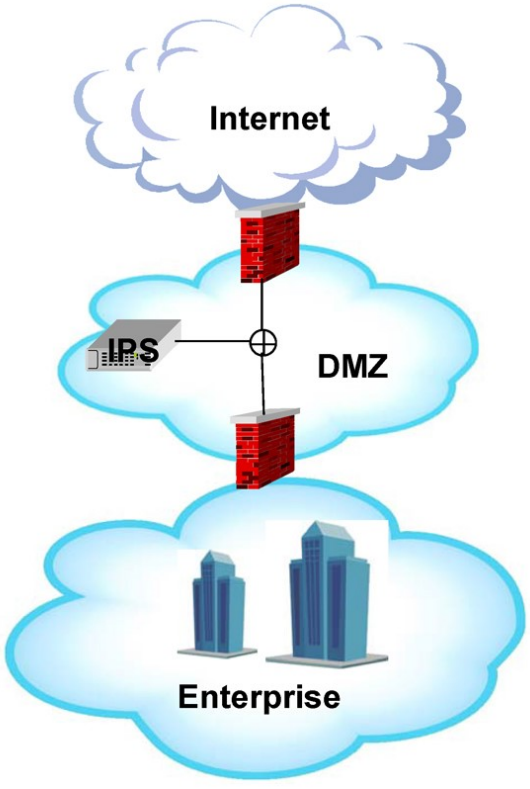
Some advantages of Virtual Machines are:

- **Lower power usage:** Having the same number of hosts on fewer computer units with power supplies cuts down excess power consumption and heat from intermittently idle machines.
- **More effective crash recovery:** Virtual machines that experience a critical failure can simply be redeployed to other hardware and resume current operations.
- **Ease of maintenance:** Hardware that needs to undergo servicing can be taken out of circulation without requiring the host to be shut down.
- **Greater ability to tune:** Virtual machines can be allocated only the resources they need. Should it be discovered that more CPU or memory is necessary, these can be quickly expanded without touching hardware.
- **Greater ability to scale:** Identical virtual machine configurations may be deployed in multitude to service a large number of users, and just as easily retracted.

INTRUSION DETECTION SYSTEMS (IDS/IPS)

Intrusion Detection System	An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
IDS vs. IPS	Although similar, the difference is IDS watches a copy of the traffic and IPS watches the real traffic.

Most modern firewalls also include technology such as an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). Both technologies are similar and can be standalone devices separate from a firewall, if needed. However, **Intrusion Detection Systems** only detect possible network intrusions and **Intrusion Prevention Systems** can actually stop a network intrusion once it is detected. Network intrusions can be detected by these systems only after they are properly configured. There are two configuration types for Intrusion Detection and Intrusion Prevention Systems: Anomaly-Based and Signature-Based.



IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place—but not to prevent it. An IDS essentially reviews your network traffic and data and will identify probes, attacks, exploits, and other vulnerabilities. An IDS can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event, or even paging an administrator. In some cases, the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion.

Anomaly-Based Intrusion Detection and Intrusion Prevention Systems require a large amount of administrative overhead as they must be left running on the network to build a historical baseline. An administrator then has to examine the data collected to set alarm/action conditions for anything that

is out of the ordinary. This requires a long lead-time for setup as well as for when significant changes are made to the network. Anomaly-Based Intrusion Detection and Intrusion Prevention Systems are best suited to static networks that do not change often with administrative staff that is well-educated in network forensics.

Signature-Based Intrusion Detection and Intrusion Prevention Systems operate in a similar manner as an anti-virus client on a PC. Signature-Based Intrusion Detection and Intrusion Prevention Systems require a subscription to download common definitions of network attacks. These "definitions" carry with them default alarm/action conditions that will work "out of the box." However, if a required ICS communication triggers one of these definitions, it is referred to as a false positive. An administrator familiar with what should be standard ICS network communication can then customize the definition, if needed. Signature-Based Intrusion Detection and Intrusion Prevention Systems are best suited for dynamic networks that have limited administrative staff.

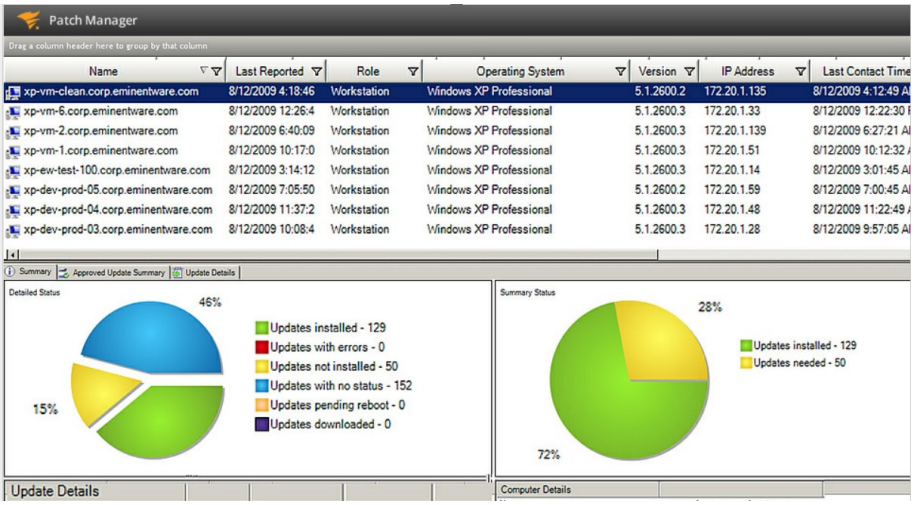
An IDS/IPS can send out alerts on its own to the parties that need to be notified, or it can send all of its status updates to a logging system, which can aggregate this and other information before sending an alert.

PATCHING

Patching	A patch is a piece of software designed to update a computer program or its supporting data by fixing or improving it. This includes fixing security vulnerabilities and other bugs and improving the usability or performance.
Clientless	No additional software should need to be loaded on systems to support remote installation of patches from a patch management device.

Patching is also an important part of keeping a network secure. Patching closes security holes in applications that computer hackers and viruses can exploit. On the other hand, for an ICS, operating system and common software patches must be treated more carefully than patches applied to corporate network computers as they could have an adverse impact on operations. The following are some best practices recommended by Invensys. All of these practices are part of a good change management program:

1. Invensys has a certification process that all Microsoft patches must go through before they are applied to computers running Foxboro I/A software. Customers should check this listing on the Foxboro support website before installing patches.
2. Backups should be performed on all systems to be patched before patching begins in case a patch disrupts proper operation and uninstalling the patch does not fix the issue.
3. Patch a small subset of computers first that are less critical to operations (such as a testbed environment) and observe for adverse impacts.



There are many software solutions available to automate patching; however, Invensys recommends looking for a solution that has the following attributes:

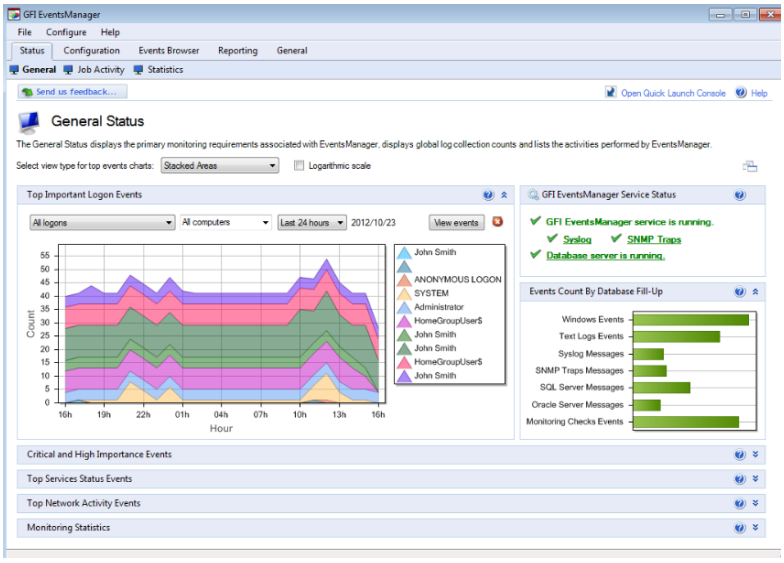
- **The solution should be clientless.** No additional software should need to be loaded on systems to support remote installation of patches from a patch management device
- **The device that manages sending patches to other devices should have the ability to act as a *relay host*.** A relay host is a PC/server that gathers information from the internet or another outside network location so that individual devices do not require internet access.
- **Personnel should be able to schedule activities to run during off-peak usage times.** These activities could include scanning systems to determine what patches are missing and/or installing patches to systems.
- **The solution should have built-in or "canned" reports for common patch management and regulatory requirements.**

LOGGING

Logging	Log management (LM) comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, and event-logs).
Clientless	No additional software should need to be loaded on systems to support remote installation of patches from a patch management device.

Logging is integral in ensuring an ICS is secure and stays secure. It is the "burden of proof" to show when, where, and how a security intrusion was attempted and if it was successful. Logging is also a company's necessary audit trail that is required for regulations such as NERC CIP. An effective yet easy- to-manage logging system supports the following features:

- **The logging system should be clientless.** No additional software should need to be loaded on systems to support the gathering of logs.
- **The logging system should support Windows Event Logs** and be able to connect to Microsoft Windows-based systems and gather event logs using supplied administrative credentials.
- **The logging system should support SYSLOG information.** UNIX-based systems as well as some network devices (firewall, IDS/IPS, network monitor) should be able to forward their logs to the system.
- **The logging system should support SNMP information** and be able to receive broadcasts of network device status updates.
- **The logging system should generate the necessary alerts when needed.** Administration/ configuration of the alerts should be easy to maintain and support *clipping* levels. Clipping is where logged information is gathered and an alert is only sent once the number of a certain type of event exceeds a maximum value.
- **The logging system should have built-in or "canned" reports for common security and regulatory requirements.**



NETWORK MONITORING

Network Monitoring	Network monitoring describes a system that continuously monitors a network and notifies a network administrator though messaging systems (usually e-mail) when a device fails or an outage occurs.
Network Management System (NMS)	A Network Management System (NMS) is a set of hardware and/or software tools that allow system administrators to supervise the individual components of a network within a larger network management framework.

Network Monitoring goes hand-in-hand with Logging. For logging to be successful, the network must be monitored. Intrusion Detection and Intrusion Prevention Systems are essentially monitoring external access to a network that touches the firewall. Network Monitoring systems are used to observe conditions inside the firewall on the ICS.

Very basic network monitoring systems simply try to contact all devices on a network, record their response time if one is received, and send an alert if a device does not respond. More advanced network monitoring systems contact devices as well as read the same SYSLOG and SNMP (Simple Network Management Protocol) information gathered by the logging system.

Most modern implementations of Network Monitoring systems are configured to be “aggregators” of all SYSLOG and SNMP information for the internal network. However, only a limited amount of this information is kept in the Network Monitoring system for troubleshooting recent events. In turn, the Network Monitoring system forwards a copy of all information it gathers to the Logging system for long term audit storage.

Network management system components assist with:

- Network device discovery - identifying what devices are present on a network.
- Network device monitoring - monitoring at the device level to determine the health of network components and the extent to which their performance matches capacity plans and intra-enterprise service-level agreements (SLAs).
- Network performance analysis - tracking performance indicators such as bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other SNMP-enabled devices.
- Intelligent notifications - configurable alerts that will respond to specific network scenarios

HARDENING

Hardening	Hardening is usually the process of securing a system by reducing its surface of vulnerability. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.
Baseline Server Hardening	After new servers are installed. A baseline hardening sets all servers at a common known level. Important when looking for unintentional configurations.

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

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 must 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.

Baseline Server Hardening:

- The base install of all operating system and post-operating system software comes from a trusted source.
- Servers are only connected to a completely trusted network during the install and hardening processes.
- The base install includes all current service packs and is reasonably current with regard to post-service pack updates.
- After the base install finishes, you must update the target servers.

Typical steps taken to harden a server:

- 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

MALICIOUS SOFTWARE

Malicious Software	Malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems; viruses and malware
Anti-Virus	Anti-virus software is all about prevention. It is used to prevent files that contain viruses from being downloaded onto your computer.
Anti-Malware	Malware may exist in a variety of forms, such as a file, a hidden file, or a partially corrupted file; it can hide the mechanisms that initiate the virus, such as a start-up service or a registry item. In the worst-case scenario, the malware is working for a third party that aims to steal valuable information.

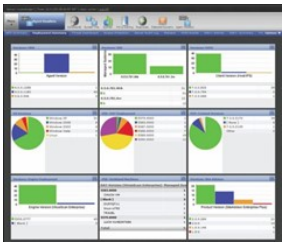
Malicious software is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc. The damage done can vary from something slight as changing the author's name on a document to full control of your machine without your ability to easily find out. Most malware requires the user to initiate its operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks OK on a pop-up, and from vulnerabilities in the operating system or programs. *Malware is not limited to one operating system.*

Viruses are a specific type of malware (designed to replicate and spread), while malware is a broad term used to describe all sorts of unwanted or malicious code. Malware can include viruses, spyware, adware, nagware, trojans, worms, and more. However, because viruses (and to a lesser extent, trojans and worms) made headlines a few years ago, most security companies focused their marketing on them, which is why they're called "anti-virus."

Anti-Virus Software is all about prevention. It is used to prevent files that contain viruses from being downloaded onto your computer. It also tries hard to prevent the virus from being activated, should it somehow get downloaded to your computer, placed in memory or in a file-like location. If the virus-laden file is never downloaded, no problem. And if the file is downloaded, but flagged by anti-virus software as malware and prevented from being activated, it won't cause any damage to your system—though the infected file still needs to be contained and deleted. Some anti-virus software may have rudimentary tools to remove active viruses, but modern malware is sophisticated in hiding on the infected computer where it can be re-initiated at a later time, so these rudimentary tools may not completely remove infections. Malware remover provides tools that are used to specifically take malware out of an infected computer, should a virus somehow pass through an anti-virus software check. Malware includes active viruses, contained viruses and inactive malware that may be hidden and lurking on the infected computer.

Malware may exist in a variety of forms, such as a file, a hidden file, or a partially corrupted file; it can hide the mechanisms that initiate the virus, such as a start-up service or a registry item. In the worst-case scenario, the malware is working for a third party that aims to steal valuable information like bank account numbers or personal identifiers without calling attention to itself. With modern malware, it is usually not enough just to remove a single virus file. Instead, multiple location checks and virus scanning techniques are needed to completely remove the package of malware.

Malware types can be categorized as follows: viruses, worms, trojans, and backdoors seek to infect and spread themselves to create more havoc. Adware and spyware seek to embed themselves to watch what the user does and act upon that data. Root kits seek to give full access of your machine to the attacker to do what they want.



ePOLICY ORCHESTRATOR (ePO)

ePolicy Orchestrator	ePolicy Orchestrator is a network application that works with the ePolicy Orchestrator Agent installed on a workstation to schedule McAfee products such as VirusScan installations, virus scans, and virus definition updates.
ePO Services	Additional ePO services include anti-virus software, HIPS, Whitelisting, and Device Control, to name a few.

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.

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. The necessary ePO policies control USB drives, host firewall policies, rogue system detection setup, and policy implementation. An ePolicy server can receive AV DAT updates from a centralized proxy server (if available). You can also determine alerting requirements and set up ePO Alerting.

ePO features:

- 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

Whitelisting	Application whitelisting is a computer administration practice used to prevent unauthorized programs from running. The whitelist is a simple list of applications that have been granted permission by the user or an administrator.
Blacklisting	Blacklisting works by maintaining a list of applications that are to be denied system access and preventing them from installing or running. However, because the number, variety, and complexity of threats are constantly increasing, a blacklist can never be comprehensive -- and as a result is limited in its effectiveness.

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. Whitelisting is not meant to be a replacement for a substitute for anti-virus software.

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.

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.

Whitelisting features:

- 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

SIEM	Security Information and Event Management (SIEM) is a term for software and product services combining security information management (SIM) and security event manager (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.
SIEM vs. Log Management	SIEM products typically provide many of the features required for log management but add event-reduction, alerting, and real-time analysis capabilities. They provide the layer of technology that allows one to say with confidence that not only are logs being gathered but they are also being reviewed.

Security Information and Event Monitoring (SIEM) provides system administrators with the ability to gain real-time visibility into all activity on their network. Real time situational awareness and the speed and scale required to identify critical threats, respond appropriately, and ensure continuous compliance monitoring is key to defending against network threats. 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).

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 is 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.

SIEM systems collect logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment and even specialized security equipment like firewalls, anti-virus software, or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions.

Different SIEM vendors license their products differently. Some of the most common licensing modes are:

- Number of monitored computers/devices
- Number of events per day/hour/minute and log volume size (in MB). If you have a baseline of the logs you wish to monitor, you should already know most (if not all) of this information beforehand.

At the most basic level, a SIEM system can be rules-based or employ a statistical correlation engine to establish relationships between event log entries. In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. The danger of this approach, however, is that relevant events may be filtered out too soon.

The SIEM detects and alerts for attempts at or actual unauthorized accesses, where technically feasible.

- 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—DATA LOSS PREVENTION (DLP)

DLP	Data Loss Prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
Device Control	Device Control is a protection component designed to ensure protection by restricting user access to devices. You can open or block access to the following devices: data storage media such as hard disks, removable devices, tape carriers, CD/DVD disks; data transfer devices (modems, external network adapters)

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. The lines can get blurred between Device Control and Data Loss Prevention (DLP). Data loss/leak prevention solution is a system that is designed to detect potential data breach/data ex-filtration transmissions and prevent them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. The terms "data loss" and "data leak" are closely related and are often used interchangeably, though they are somewhat different. Data loss incidents turn into data leak incidents in cases where media containing sensitive information is lost and subsequently acquired by an unauthorized party. However, a data leak is possible without the data being lost in the originating side.

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.

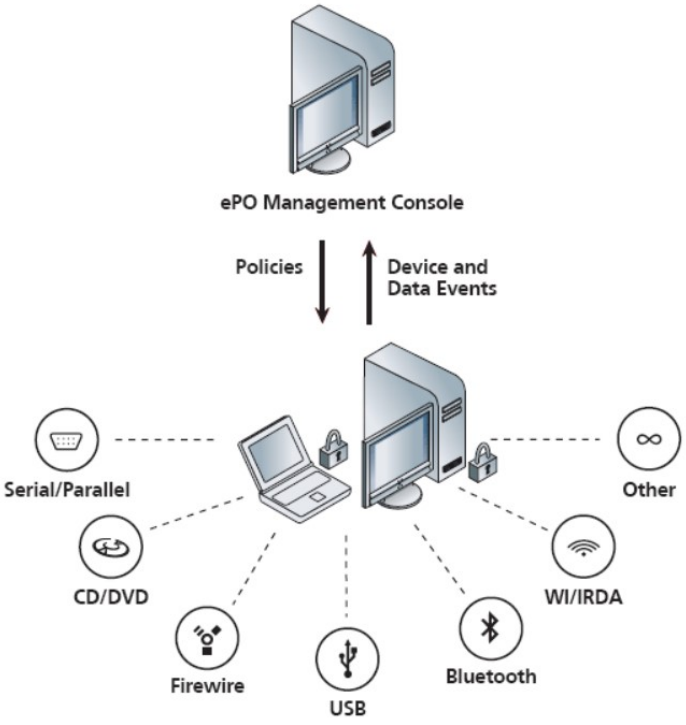
- Support for plug-and-play devices and removable storage devices
- Removable storage devices can be blocked or made read-only
- Content-aware protection for removable storage devices
- File access protection for files that reside on removable storage devices
- Non-system hard disks rule blocks and monitors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

Data Loss Prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

- Discover confidential data wherever it is stored and identify data owners to make data cleanup easy.
- Monitor how confidential data is being used and where it is going to provide visibility into broken business process and high-risk users.
- Protect confidential data by automatically enforcing data loss policies, educating users about data security, securing exposed data, and stopping data leaks.
- Manage data loss policies, incident remediation, and risk reporting from a single, web-based management console.

Features of the McAfee-supported Data Loss Prevention solution include:

- 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



DISASTER RECOVERY

Disaster Recovery (DR)	Disaster Recovery (DR) is the area of security planning that deals with protecting an organization from the effects of significant negative events.
Disaster Recovery Plan (DRP)	Disaster Recovery Plan (DRP) is a plan for business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data records, and the physical space of an organization.
Backup Recovery	Backup Recovery, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. There are multiple techniques for providing Backup Recovery.

Disaster Recovery (DR) is the process, policies, and procedures that are related to preparing for recovery or continuation of technology infrastructure that is vital to an organization after a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems that support business functions, as opposed to business continuity, which involves planning to keep all aspects of a business functioning in the midst of disruptive events.

Disasters can be classified into two broad categories. The first is natural disasters such as floods, hurricanes, tornadoes, or earthquakes. While preventing a natural disaster is very difficult, measures such as good planning that includes mitigation measures can help reduce or avoid losses. The second category is manmade disasters. These include cyber attacks, hazardous material spills, infrastructure failure, and bio-terrorism. In these instances, surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events.

Disaster Recovery Plan (DRP) documents policies, procedures, and actions to limit the disruption to an organization in the wake of a disaster. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of actions intended to minimize the negative effects of a disaster and allow the organization to maintain or quickly resume mission-critical functions.

Disaster recovery steps may include restoring servers or mainframes with backups, or provisioning Local Area Networks (LANs) to meet immediate business needs.

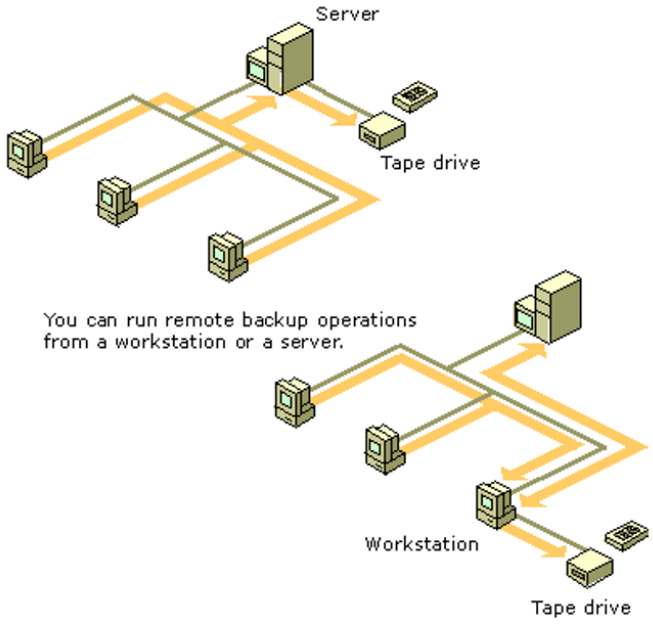
Business continuity describes the processes and procedures an organization must put in place to ensure that mission-critical business functions can continue during and after a disaster. The emphasis is more on maintaining business operations than IT infrastructure. Because business continuity and disaster recovery are so closely related, the two terms are sometimes combined as Business Continuity and Disaster Recovery (BCDR or BC/DR).

Backup and **Recovery** in general refers to the various strategies and procedures involved in protecting your database against data loss and reconstructing the database after any kind of data loss. A backup is a copy of data from your database that can be used to reconstruct that data. Backups can be divided into physical backups and logical backups.

- Physical backups are backups of the physical files used in storing and recovering your database, such as data files, control files, and archived redo logs. Ultimately, every physical backup is a copy of files storing database information to some other location, whether on disk or some offline storage such as tape.
- Logical backups contain logical data (for example, tables or stored procedures) exported

from a database with an export utility and stored in a binary file to later re-import into a database using the corresponding import utility.

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss can be a common experience of computer users. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required. Though backups popularly represent a simple form of disaster recovery and should be part of a disaster recovery plan, by themselves, backups should not alone be considered disaster recovery. One reason for this is that not all backup systems or backup applications are able to reconstitute a computer system or other complex configurations such as a computer cluster, active directory servers, or a database server, by restoring only data from a backup. Below are a couple of basic “remote back-up” architectures.



Some of the most common strategies for data protection include:

- Backups made to tape and sent off-site at regular intervals
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized), often making use of storage area network (SAN) technology
- Network-Attached Storage (NAS) is a dedicated hard disk storage device that is set up with its own network address and provides file-based data storage services to other devices on the network.
- Hybrid Cloud solutions that replicate to both on-site and off-site data centers. These solutions provide the ability to instantly fail-over to local on-site hardware, but in the event of a physical disaster, servers can be brought up in the cloud data centers as well.

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."

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).

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

CYBER SECURITY BEST PRACTICES

Cyber security best practices are intended to provide guidelines on network security that will not only reduce external threat vectors, but also internal. Items are presented in order of priority.

⇒ **Always apply and maintain the latest Invensys-authorized Operating System (OS) and application patches.**

- Download updates directly from the patch source or via secure file server.
- Assess which patches are required for each individual asset and apply as necessary, ensuring deployment does not impact operations.
- Ensure all required patches have been successfully applied.
- WITHOUT applying the current Invensys-authorized patches, individuals will be increasing the attackable surfaces of individual DCS workstations and servers.

⇒ **Always use current anti-virus definitions.**

- Ensure that the latest anti-virus definition files have been downloaded and run from the Invensys Support Website.
- Verify through the McAfee client that the update was successfully installed.
- Test new DAT in a test bed environment, prior to release into production environment.
- WITHOUT keeping anti-virus current, the servers and workstations will not have the current malware signatures, leaving the equipment vulnerable to current attacks.

⇒ **Update authorized application software.**

- Ensure application software such as Adobe, if authorized, is updated. File types such as *.pdf* are one of the top distributors of malware if not routinely updated.
- WITHOUT updating third party software on the inventoried system, additional vulnerabilities will remain in place.

⇒ **Enable Network Anti-Virus / Intrusion Prevention System.**

- Ensure that the most current anti-virus definition files and Intrusion Prevention System policies are enabled on all capable network appliances protecting the second Ethernet networks.
- WITHOUT using a device that incorporates intrusion detection system (IDS), you will not have a baseline of normal network activities versus an attack. Antivirus module will provide an alert and a secondary screen for network malware.

⇒ **Do not use a USB stick unless it has been scanned and confirmed that it is free of problems with the latest *dat* file.**

- Designate and use specific USB equipment where required.
- If using USB equipment to bridge air-gaps, always use a specific designated station in conformance with DCS security policies.
- WITHOUT restriction on USB devices, their portable nature can be used to compromise your security perimeter.

⇒ **Harden Servers and Workstations. Hardening Non-DCS assets is a requirement and typically will not have negative effects on the DCS. Hardening DCS assets may be performed and will vary from Non-DCS asset hardening.**

- Ensure all software and hardware patches and updates are current.
- Run A/V scans.
- Disable all unused ports and services.
- Harden Bios.
- Use static IP addresses, disable DHCP on the interfaces, and disable unused interfaces.
- Disable NetBIOS, unless specifically mandated by the IT department; disable NetBIOS over TCIP/IP (via WINS tab).
- WITHOUT hardening servers, there is greater risk for attacks. Hardening reduces the attackable profile of the system.

⇒ **Change default "admin" passwords.**

- Use strong passwords consisting of more than 6-8 characters using special characters when applicable.
- WITHOUT policies to ensure that "admin" passwords are changed, individuals can use "admin" passwords to escalate their privilege levels. Automated attacks by malware using "admin" passwords are prevalent.

⇒ **Control User Rights.**

- Verify that only authorized accounts are members of the local system administrators group.
- Do not use accounts across domains.
- When applications cannot use special characters, a service account should be created with authentication compatible with the application.
- Wherever Group Policies are in use:
  - Change local system administrator passwords.
  - Implement password aging, history, and complexity requirements.
  - Ensure that Restricted Groups policy is enabled and used.
- WITHOUT policies that specify user privilege criteria, individuals can receive privileges beyond those required for the task at hand. If too many users have elevated privileges beyond their needs, malware can use this as threat vector.

⇒ **Always implement Backup and Restoration.**

- Use a network backup repository.
- Back up the network repository to a geographically disperse secondary storage site for disaster recovery or to removable media that can be stored off site.
- If removable media is elected, then a rotation policy should be implemented to ensure that multiple copies of the backup exist off site.
- Periodically conduct recovery exercises using test bed equipment.
- Determine relative storage capacity available and automated a backup schedule for individual workstations and servers.
- WITHOUT implementing a back up policy, customers will have no recourse to restore to a condition prior to an attack date if required.

⇒ **Take inventory of network assets.**

- Keep inventory current of all network assets and status.
- Update inventory as network changes are made to both hardware and software.
- Run network scans to collect asset information (log files, etc.) where authorized. Non-DCS assets typically may be scanned without issues but DCS asset scanning should incorporate a limited tuned methodology for scanning DCS assets.
- Run regular network audits to ensure all systems are up to date.
- WITHOUT a network inventory, you do not have a baseline of what normal network assets are and that goes towards the network scan, complicating what are known devices and what are known patches. Knowledge of what specific network firmware is running and what network security equipment is present can be critical in determining whether or not vulnerabilities exist.

⇒ **Use physical network isolation when possible**

- WITHOUT using physical network isolation, cross contamination of the DCS platform is possible from the corporate system.

⇒ **Use logical network segmentation (secure zones) when possible with strict Firewall Rules.**

- Isolate and control flow of information between Business Network(s) from PCN through use of firewalls.
- Require strict firewall rules with specific (/32) source, destination, port, and protocol.
- Use DMZs
- WITHOUT using a secure zone, there will be no buffer before the network traffic traverses into the DCS network.

⇒ **Enable Firewall Logging.**

- Ensure that all firewall policies protecting the Process Control Networks (PCN) and supporting infrastructure have logging enabled.
- Monitor firewall logs as appropriate, paying special attention to locate potentially malicious or abnormal traffic.
- WITHOUT firewall logging, you will not have visibility into dropped traffic or attacked traffic.

⇒ **Use Network Management Systems (NMS).**

- Implement NMS to provide system audit and logging.
- Monitor system logs for failed login attempts.
- Generate and review reports for abnormal events.
- WITHOUT using NMS, there will not be a consolidated location for viewing all logs. The NMS system reports provides consolidated insight to all systems, which is invaluable for day-to-day operations and in the event of a cyber attack.

⇒ **Don't click links or files that aren't verified.**

- DCS assets should not have internet access; some Non-DCS assets may have outside DCS access to business network website interfaces. Even business networks could be compromised, so verify all access leaving the DCS network to un-trusted networks.
- Ideally, the DCS network should be isolated from internet connected networks.
- WITHOUT policies restricting web access, users can potentially comprise the security perimeter by clicking on malicious links and installing unauthorized software.

⇒ **In the event of a Cyber Incident:**

- Create an Incident Response Plan before an Incident so that you are prepared in the event of an Incident. Steps that are typically part of incident response plans are:
  - *Do not* start updating anti-virus.
  - *Do not* start running anti-virus patches.
  - *Do* get a triage team together.
  - *Do* get copies of all the logs.
  - *Do* make a VM image of the affected system.
- WITHOUT an incident response team and procedures, the opportunities to collect the forensic evidence required to determine the attack vector and point of origin can be lost or compromised, depriving the client the opportunity to work with the antivirus vendor and other agencies.

⇒ **Download and run latest McAfee Stinger tool.**

- WITHOUT collecting the necessary forensic evidence to work with the antivirus vendor, the client may not detect the variant that was not completely remediated by the Stinger tool.

CYBER SECURITY TERMS

ACCESS CONTROL	The procedures for specifying the use of system resources by only authorized users, programs, processes, or other systems. Controls cover access and flow enforcement issues such as separation of duties, least privilege, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination.
ACCESS CONTROL LIST (ACL)	A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.
ANTI-VIRUS TOOL	Software products and technology used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system.
AUTHENTICATION	Verifies the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
AUTHORIZATION	A right or a permission that is granted to a system entity to access a system resource.
BACKDOOR	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.
BUFFER OVERFLOW	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.
CHALLENGE/ RESPONSE AUTHENTICATION	Challenge/Response Authentication requires that both the service requester and service provider know a “secret” code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider.
CLEAR TEXT	Information that is not encrypted.
CONFIDENTIALITY	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
DENIAL-OF-SERVICE (DOS)	The prevention of authorized access to a system resource or the delaying of system operations and functions.

DISASTER RECOVERY PLAN (DRP)
A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

DOMAIN CONTROLLER
A server responsible for managing domain information such as login identification and passwords.

DOMAIN NAME SYSTEM (DNS)
Domain Name System (DNS) is primarily used to translate between domain names and IP addresses. For example, a DNS could map a domain name such as control.com to an IP address such as 192.168.1.1.

ENCRYPTION
Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

FILE TRANSFER PROTOCOL (FTP)
FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download Web pages, graphics, and other files between local media and a remote server that allows FTP access.

FIREWALL
An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

FTP AND TRIVIAL FILE TRANSFER PROTOCOL (TFTP)
FTP and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. They are implemented on almost every platform including many SCADA systems, Distributed Control Systems, PLCs, and RTUs because they are very well known and use minimum processing power.

HUMAN-MACHINE INTERFACE (HMI)
The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

HYPERTEXT TRANSFER PROTOCOL (HTTP)
HTTP is the protocol underlying Web browsing services on the Internet. It is seeing increasing use on the plant floor as well as an all-purpose query tool.

IDENTIFICATION
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in a system.

IDENTIFICATION AND AUTHENTICATION

Authentication describes the process of positively identifying potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions (e.g. when an automatic teller machine asks for a PIN). Based on the authentication determination, the system may or may not allow the potential user access to its resources. Authorization is the process of determining who and what should be allowed to have access to a particular resource; access control is the mechanism for enforcing authorization.

INTRUSION DETECTION SYSTEM (IDS)

A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

INTRUSION PREVENTION SYSTEM (IPS)

A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

MALWARE

Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Malware can be a virus, worm, Trojan horse, or other code -based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

NETWORK ADDRESS TRANSLATION (NAT)

Network Address Translation (NAT) is a service where IP addresses used on one side of a network device can be mapped to a different set on the other side on an as-needed basis. For example, a control network device may need to establish a connection with an external, non-control network host (for instance, to send a critical alert e-mail). NAT allows the internal IP address of the initiating control network host to be replaced by the firewall; subsequent return traffic packets are remapped back to the internal IP address and sent to the appropriate control network device.

NETWORK INTERFACE CARD (NIC)

A circuit board or card that is installed in a computer so that it can be connected to a network.

PASSWORD

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

PASSWORD AUTHENTICATION

Password authentication technologies determine authenticity based on testing for something the device or human requesting access should know, such as a PIN number or password. Password authentication schemes are thought of as the simplest and most common forms of authentication.

PHYSICAL TOKEN AUTHENTICATION

Physical Token Authentication is similar to password authentication, except that these technologies determine authenticity by testing for a secret code or key produced by a device or token the person requesting access has in their possession, such as security tokens or smart cards.

PORT SCANNING

Using a program to remotely determine which ports on a system are open (i.e. whether systems allow connections through those ports).

RESOURCE STARVATION

A condition where a computer process cannot be supported by available computer resources. Resource starvation can occur due to a lack of computer resources or the existence of multiple processes that are competing for the same computer resources.

RISK

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals) resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

RISK ASSESSMENT

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses.

RISK MANAGEMENT

The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

ROLE-BASED ACCESS CONTROL (RBAC)

Under RBAC, security administration is simplified through the use of roles, hierarchies, and constraints to organize user access levels.

ROUTER

A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets.

SECURE SHELL (SSH)

SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web servers and other types of servers.

SECURITY CONTROLS

The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY PLAN

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

SECURITY POLICY

Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g. remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

SMTP is the primary e-mail transfer protocol. Outbound SMTP mail messages from the control network to the corporate network are typical examples of use for SMTP.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or "hard-coded" in the MIB, while others are dynamic values calculated by agent software running on the device.

TECHNICAL CONTROLS

The security controls (i.e. safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

TELNET

The telnet protocol defines an interactive, text-based communications session between a client and a host. It is mainly used for remote login and simple control services to systems with limited resources or to systems with limited needs for security.

TRANSMISSION CONTROL PROTOCOL (TCP)

TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TROJAN HORSE

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

UNAUTHORIZED ACCESS

A person gains logical or physical access without permission to a network, system, application, data, or other resource.

VIRTUAL LOCAL AREA NETWORK (VLAN)

VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches.

VIRTUAL PRIVATE NETWORK (VPN)

One method of encrypting communication data is through a VPN, which is a private network that operates as an overlay on a public infrastructure, so that the private network can function across a public network.

VIRUS

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e. inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

VIRUS DEFINITIONS

Predefined signatures for known malware used by anti-virus detection algorithms.

WIDE AREA NETWORK (WAN)

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

WIRELESS DEVICE

A device that can connect to a manufacturing system via radio or infrared waves to typically collect/monitor data, but also in cases to modify control set points.

WORKSTATION

A computer used for tasks such as programming, engineering, and design.

WORM

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

To learn more about Schneider Electric Cyber Security Services, contact your sales representative or visit:
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

Schneider Electric • 1650 W. Crosby Rd Carrollton, TX 75006 • Tel: 1 (972)-323-1111 • www.schneider-electric.com

Rev. 201507