Life Is On | Schneider Electric

Protect your automation assets

Foxboro Evo continuously secure design

Product at a glance

Foxboro Evo™ protects your plant with the following designed-in features:

- ePolicy orchestrator (ePO)
- Virus scan
- Host intrusion detection (HIDS)
- Data loss prevention (DLP)
- Active directory (A/D)
- Hardened OS
- Whitelisting
- Station assessment tool (SAT)
- Backup exec system recovery (BESR)
- Data loss prevention (DLP)

Secure process automation

Schneider Electric offers a continuously secure control infrastructure and cybersecurity program designed to help you meet regulatory compliance and protect your facility's most critical assets — your people, your intellectual property and your equipment. The Foxboro Evo system helps you establish a secure foundation for your process and extend cybersecurity beyond the control system.

As the need to secure critical infrastructure becomes more important, no element is more critical than the Foxboro Evo process automation system. Foxboro secure-based features include the ability to centrally manage antivirus scans, DAT file updates, HIDS, and DLP from one central location on all Foxboro secure based systems.

Protect your automation assets

Foxboro Evo continuously secure design

Secure connections throughout your plant

ePO is a unifying security management open platform by McAfee. ePO makes risk and compliance management simpler, enabling you to connect security solutions to your enterprise infrastructure to increase visibility, gain efficiencies, and strengthen protection.

Prevent an incident before it happens

Virus scans prevent, detect, and remove malware, including but not limited to system viruses, computer viruses, computer worms, Trojan horses, spyware, and adware. Early prevention and detection eliminates the threat and potential damage to equipment, safety, and resources.

Enable fast response to intrusion

A host intrusion detection system (HIDS) monitors and analyzes the internals of a computing system. A host-based IDS monitors all or parts of the dynamic behavior and the state of a computer system. Besides options such as dynamically inspecting network packets targeted at a specific host, an HIDS might detect which program accesses which resources. It might then discover that a word processor has suddenly and inexplicably started modifying the system password database. Similarly, an HIDS might look at the state of a system and its stored information to check

that its contents appear as expected, i.e. have not been changed by intruders. Think of an HIDS as an agent that detects whether anything or anyone, internal or external, has circumvented the system's security policy.

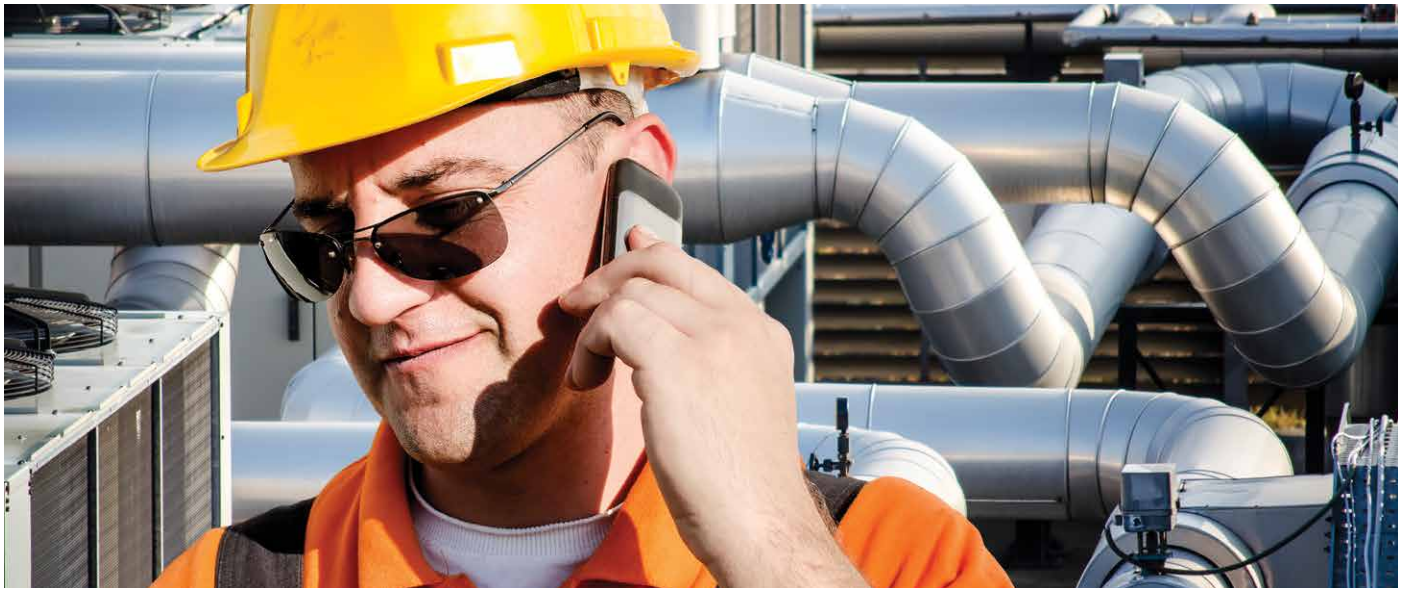
Safeguard your physical and intellectual property

Data loss prevention systems enable organizations to reduce the corporate risk of the unintentional disclosure of confidential information. These systems identify, monitor, and protect confidential data while in use, in motion, and at rest through deep content inspection, contextual security analysis of transaction and with a centralized management framework.

Active Directory (AD) is a directory service created by Microsoft® for Windows® domain networks. Active Directory provides a central location for network administration and security. It 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. Foxboro secure systems utilizing A/D now have the ability to tie ePO policies into

Protect your automation assets

Foxboro Evo continuously secure design



the Foxboro A/D deployment for controlling Foxboro computers as well as Foxboro account management.

Harden OS with Factory Hardening is a procedure that updates patches and antivirus software and disables unused ports and services. System hardening is necessary because default operating system installations focus more on ease of use rather than security. Foxboro systems include hardening, removing basic levels of unneeded services and Windows software.

Whitelisting permits only those programs to which you wish to grant access. This makes security less labor intensive because you only have to keep up with the applications you know about.

Maintain security throughout your plant's lifecycle

Foxboro Station Assessment Tool is a Windows-based application automatically installed on all Foxboro workstations and servers running the Windows operating system Foxboro software V8.5 and later. Backup Exec System Recovery enables easy management of backup and recovery tasks for multiple desktops across the network. Schedule backups to run automatically, including event triggered backups with disrupting network usage. Built-in software encryption of backups ensure security of critical data.

Change is a constant for our customers — adding a new employee, a new software release or bringing up a new unit and even the smallest change can be exploited. Keeping your plant current and protected during day-to-day operation is a challenge. The Foxboro Evo process automation system and Schneider Electric cybercecurity practice will help you meet cybersecurity compliance requirements, protect your investments, and keep your production operations safe and secure for whatever the future may bring.

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On Schneider Electric