White paper

Protection of Production Computers with Windows 7 – Microsoft is Ending Support on January 14, 2020

Author:
Andreas Fuss
Security Product Marketing
Phoenix Contact Electronics GmbH
afuss@phoenixcontact.com

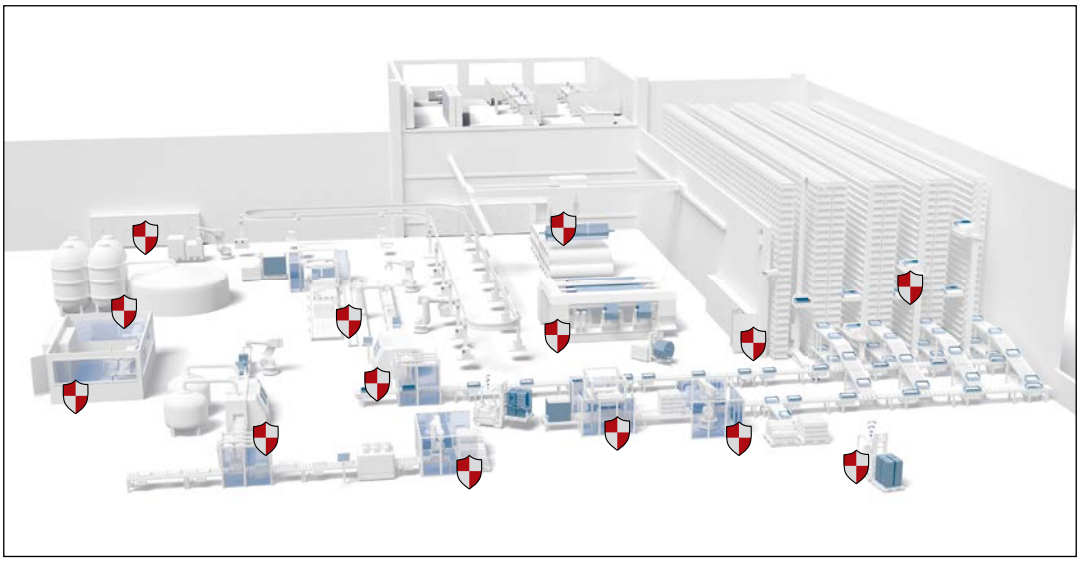
AI 05-19.000.L6

Protection of production computers with Windows 7

Application

Microsoft is ending its extended support for Windows 7 on January 14, 2020, and its support for Windows 7 Embedded will also come to an end on October 13, 2020. After support is ended, Microsoft will no longer provide updates to protect against new security vulnerabilities. The risk of attackers infiltrating production computers with Windows 7 operating system, or of these computers being infected with viruses, trojans or other worms, will therefore increase daily. Since the entire security architecture of these old operating systems no longer corresponds to current state-of-the-art technology, Microsoft – as well as security experts – are warning against unprotected continued operation. However, recent surveys also show, especially in production, that using control computers with Windows 7 may often be unavoidable even after support is ended. The question of how these applications can be protected in the future therefore needs to be addressed.

Solution



IT security for production plants with the mGuard security module

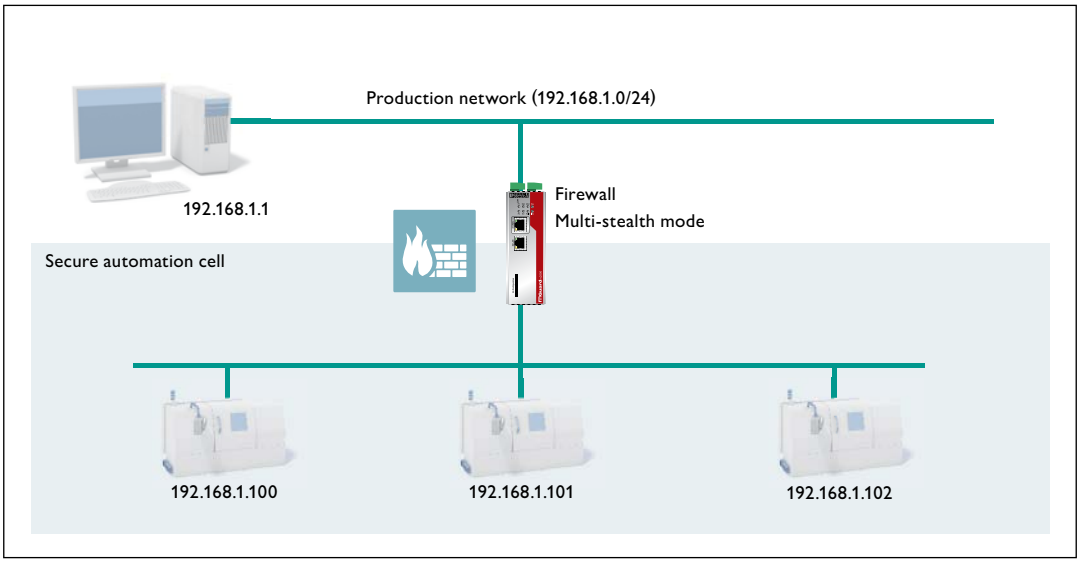
IT security for production plants

It is, of course, essential that only secure systems are connected to the production network. Most companies already have appropriate IT security guidelines. However, for production plants in particular, the principle "Never change a running system" applies. Major changes to the network infrastructure and upgrading the operating system to a newer Windows version is therefore out of the question in the majority of applications. Either the computer systems do not even satisfy the necessary requirements for the new operating system, or the required drivers are no longer available. It is also often the case that the ramifications of a corresponding update on the real-time behavior of the computer are deemed critical or there are no update options planned by the machine manufacturer. In all cases, the potential increase in IT security involves

significant costs and a high degree of risk with regard to the productivity of the machinery. For this reason it is advantageous to implement security measures that work without interfering with the system that is to be protected and can be easily retrofitted.

Retrofitting security appliances for increased protection

A reliable and inexpensive solution is to retrofit an mGuard security module, which is an industrial security appliance. The mGuard security module is simply integrated into the network upstream of the Windows PC that is at risk, and immediately protects this PC by means of several coordinated security functions. Thanks to a patented stealth mode, no changes have to be made to the system that is to be protected, either on the network, or on the Windows computer itself. The mGuard security module can therefore also be integrated into an existing network later on in a completely transparent way. Since it automatically adopts the MAC and IP address of the system to be protected, you do not even have to assign additional addresses for managing the mGuard security modules. Even the network configuration remains unchanged. This allows a production machine with Windows 7 control computer to be protected quickly, easily, and entirely free of risk.



Transparent integration in existing networks thanks to the patented stealth mode

Isolating the Windows computer by means of a firewall

A common feature of many security risks is that they exploit vulnerabilities of protocols or services. Malware then spreads throughout the IP-based network via already infected systems. To be completely on the secure side, communication of unsecure systems with the production network must therefore be entirely prevented. However, this decoupling is not feasible in modern production. However, the security risk posed by a Windows 7 computer can be minimized by isolating this computer as much as possible from the rest of the network. The integrated firewall in mGuard controls and filters communication from and to the systems to be

protected using a configurable ruleset. Communication is thereby restricted to the partners, protocols, ports, and connection directions required in order for the entire plant to work. Connections that are not initiated by the system itself and instead come from outside are prevented in most instances. Even communication from inside the system to the outside can be restricted to the necessary services and partners. At any rate, access to the Internet should be blocked.

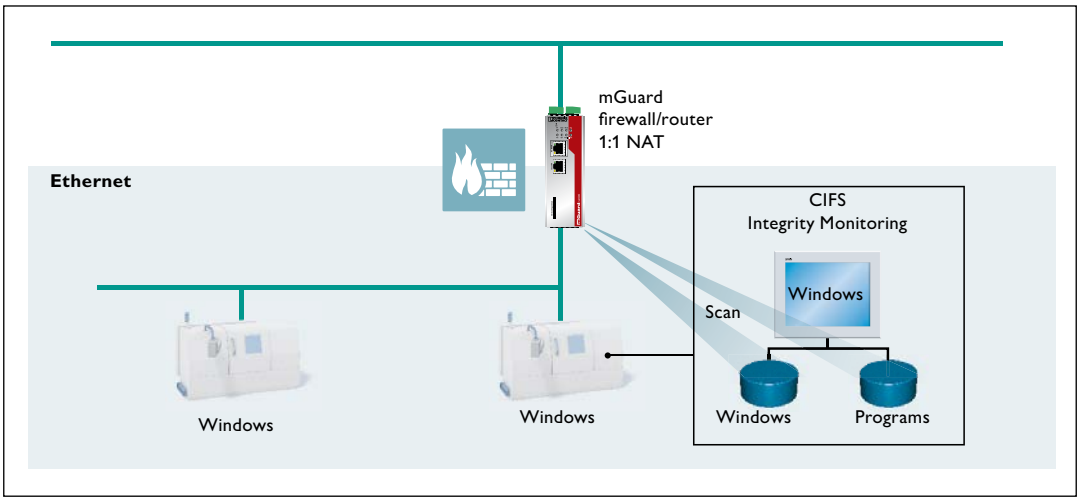
CIFS Integrity Monitoring for protection against viruses

Even the best firewall cannot provide a Windows 7 computer with 100% protection against viruses. After all, malware can also be inadvertently introduced to the PC by a service engineer by means of a laptop or USB stick. It is therefore essential that the Windows 7 computer is continuously monitored for malware infection. However, using a standard virus scanner places high demands on the resources of the control computer, which can significantly impact the real-time properties of the system. In addition, new virus patterns have to be continuously loaded in order to keep the virus scanner up to date.

mGuard's CIFS Integrity Monitoring (CIM) offers a better alternative.

CIFS (Common Internet File System) refers to the file sharing system used by Windows including the Server Message Block (SMB) protocol.

CIFS Integrity Monitoring is a sensor that monitors the file system of the Windows computer for changes and detects whether any changes have been made to the computer. If a change is detected, mGuard generates an alarm immediately notifying the person responsible by e-mail or SNMP trap. CIFS Integrity Monitoring is therefore an alternative solution to conventional antivirus software that is suitable for industrial applications. Its main advantage is that the load on the Windows computer is minimal and the system's real-time properties are unaffected. Regular loading of virus patterns is not required with mGuard.



Industrial virus sensor: CIFS Integrity Monitoring

Our service – your security concept

If required, our specialists will check your network and design an individual security concept for your plant based on your requirements. Furthermore, we provide training for your employees in industrial network security.

Summary

mGuard protects the production computer using several security functions without affecting its real-time capability:

1. The integrated firewall isolates the Windows 7 computer from the rest of the network as much as possible and only allows communication that is actually required.
2. CIFS Integrity Monitoring (CIM) protects against viruses.
3. Thanks to the patented stealth mode, the mGuard security module can be easily retrofitted without making any changes to the network configuration.

Our tip

mGuard is powerful enough to protect a production area with several machines and Windows control computers. It appears to be a very inexpensive solution at first glance. However, production needs to remain flexible and will have to be adapted to new circumstances or products over the years, with the result that machines and their locations may well change. If, therefore, an entire production area is protected using a single mGuard security module, the security concept also needs to be adapted whenever a change is made. That is why we recommend that you protect each machine with a separate mGuard security module. This ensures that the individual machines are still protected in the event of changes to production without incurring any additional expense.

Your advantages

- ☑ No changes to the network configuration or the systems to be protected
- ☑ Conserves the resources of the protected/monitored system (CPU power, network load)
- ☑ Virus patterns do not have to be loaded
- ☑ No false alarms/false positives during the integrity check
- ☑ No impact on the system to be protected

PHOENIX CONTACT Deutschland GmbH
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 (0) 5235 3-12000
Fax: +49 (0) 5235 3-12999
E-mail: info@phoenixcontact.com
phoenixcontact.com