BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

Windows XP End of Service: Practical Options for Industrial Applications

Frank Williams
Senior Manager Security Initiative
frank.williams@belden.com

Scott Howard
Technical Sales Manager
scott.howard@belden.com

Table of Contents

Executive Summary

Nobody likes the job of replacing a good team member when they retire. Yet, that is the job the manufacturing industry is faced with as a trusted component of the industrial application ecosystem steps down from active duty. That component is the Windows XP operating system (OS), a workhorse of a product that is pervasive in factories, energy facilities and many critical infrastructure systems around the world.

You may be shocked to learn just how pervasive Windows XP-based systems are in your operation. Think about it. It's easy to identify the white box PCs running important manufacturing, process or production applications on the plant floor and in control rooms. But don't forget those white box PCs in engineering offices at your site and other locations.

Next, consider the PCs that don't look like PCs. For example, the ruggedized PCs running PLC, DCS and other device configuration/monitoring applications in your processes.

Now, think harder. Did you know that a version of Windows XP is also used in embedded components in thousands of devices that control many factory automation and process control operations? Do you even know which devices to check? Indeed, one large manufacturer of pharmaceuticals actively seeking to identify Windows XP-based assets was surprised to keep uncovering them in groups of hundreds.

There are three options for addressing the risk caused by the End of Service (EOS) of Windows XP for industrial applications. The first is to maintain the status quo and do nothing. If you do this, you need to be comfortable with the fact that when an unexplained event happens, you will no longer be able to call Microsoft or other software vendors and get a patch or a driver.

The second option is to upgrade to a new version of Windows. While this will ultimately be required, it's not a quick project. That's because upgrading an OS triggers a "domino effect," which entails:

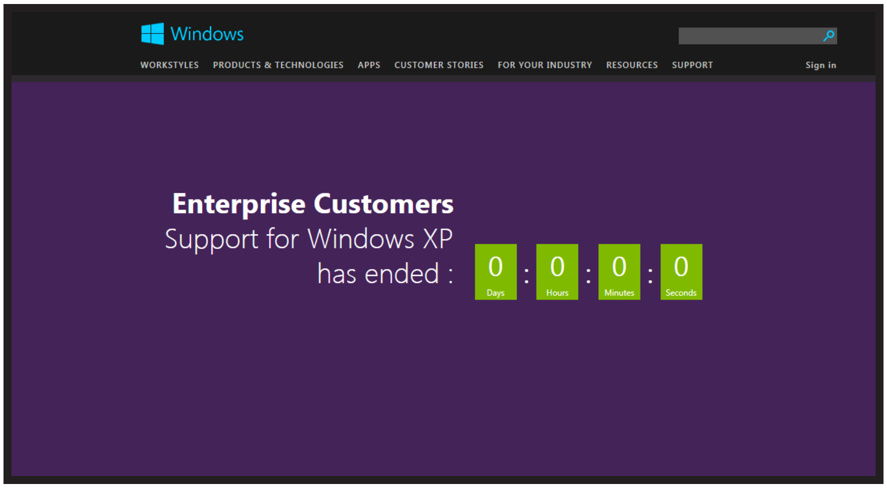
- Upgrading the operating system…
- Requires new PC hardware and/or automation devices…
- The new equipment requires new software…
- The new software requires new drivers…
- Some automation devices don't work with the new software and drivers and may need to be replaced….
- Now your mission critical applications behave differently and system integration work needs to be done….
- The modified applications need to be deployed…
- Extensive testing of the new systems is required…
- Meanwhile operational productivity is lost to the migration project…
- And user training and support for the new systems are required ….

Multiply that times all the Windows XP installs you have, and you can easily see how a "simple" operating system upgrade can take several man years of effort.

The good news is that there is a third option, which is much easier. If you love Windows XP and don't want to leave it, or you are not prepared to upgrade today, you can simply implement industrial firewalls to protect your Windows XP-based systems. This provides you with the time you need to go through the upgrade process, while immediately securing your facility.

Industrial firewalls have the advantage of being able to be deployed into live networks without disrupting production and they are simple to install and configure. They do not require any of the actions included in the OS upgrade "domino effect." In short, they are a cost effective and time efficient way to protect your systems as you plan and execute a migration away from PCs and machines running Windows XP.

This white paper looks at what the EOS for the Windows XP OS means for those responsible for keeping industrial processes up and running. It provides the information you need to know on this topic, and it details the advantages and disadvantages of the three options for addressing this development.



Enterprise Customers
Support for Windows XP
has ended : 0 : 0 : 0 : 0
Days Hours Minutes Seconds

Figure 1. A Microsoft web page notifies enterprise customers that support for Windows XP had ended . Source: Microsoft.com[1]

The End of Service for Windows XP

Microsoft Ends Support for the Windows XP Operating System

On April 8, 2014 Microsoft ended support for the Windows XP OS[2]. This was not news, Microsoft had made this date known years ago and they actively reminded people about it in the year leading up to it.

However, in the days surrounding the end of support date there was significant media attention about it. This might have been a wake-up call for you or your organization to examine the computer and equipment life cycle issues raised by this development.

What Does the End of Support for the Windows XP OS Mean?

The end to extended support for the Windows XP OS refers to the date when Microsoft no longer provides automatic fixes, updates or online technical assistance.

It doesn't mean the Windows XP OS will stop working. However, it does mean Microsoft will no longer release security updates and 'hot fixes.' These were routinely made available before April 8, 2014.

Microsoft itself stated, "If you continue to use Windows XP now that support has ended, your computer will still work, but it might become more vulnerable to security risks and viruses."

Leaving the Windows XP OS unsupported will expose systems to growing risks as the number and severity of security exploits increases.

Consider this fact:

70% of Microsoft's security bulletins in 2013 affected the Windows XP OS .

There is no reason to assume that this will change (unless it increases) in the near future.

While Microsoft may provide limited support for companies that pay for extended support – an option that costs a minimum of $100,000 USD/year – alert organizations should develop a plan to immediately secure their systems and migrate away from the Windows XP OS over time.

How Big Is the Issue?

For more than 12 long years, the Windows XP OS has been a stable and significant workhorse of an operating system. Some experts estimate that the Windows XP OS is still running on 28 percent of PC desktops worldwide. Other market studies show the Windows XP OS holding only a 20 percent market share. In either case, this represents at least one out of every five PCs worldwide.

For industrial applications, the market share is believed to be much higher. It is the first version of Windows that engineers trusted for industrial applications and it is widely deployed.

The result is that Windows XP has been used as the operating system for important industrial applications for multiple generations of automation equipment – with relatively few maintenance or interoperability issues. Many plants use specialized application software that, in a lot of cases, cannot run natively, or hasn't been thoroughly tested on any operating system, except for Windows XP.

Even having said this, you will likely be surprised to learn how heavily the Windows XP OS is employed in your facility. Look for it in these areas:

- PCs running important manufacturing or process and production applications on the plant floor in control rooms or in engineering offices
- Ruggedized PC's running PLC, DCS and other device configuration / monitoring applications

Windows XP Embedded

The Windows XP OS also shows up in another form called "Windows XP Embedded."

This is a lightweight version of the OS that was developed by Microsoft specifically for use in branded OEM devices and systems, such as machine tools, instrumentation and operator interface terminals.

These devices are not "computers" in the traditional sense of the word. You may not even be aware that the Windows XP OS is running inside them and that they present the same security risk as a desktop or laptop computer.

Thus, another place to check for Windows XP-based devices is:

- Embedded components that control and monitor many factory automation and process control operations or power, water or transportation systems.

Even if you are aware that you have devices that use the Windows XP OS, there is typically no practical way to upgrade or patch them without completely replacing them.

When doing a Windows XP inventory

Take care to look beyond white box PCs in the factory/mill/production site(s).

Inspect the different areas described above and make sure your audit is thorough so you identify ALL your Windows XP based assets.

Upgrading Industrial Systems to a New Version of Windows Is Not Easy

The EOS of the Windows XP OS places industrial users in a very uncomfortable position.

The risk of security issues and resultant downtime will steadily increase over time. Yet the cost of upgrading or replacing Windows XP-based systems (particularly the cost of the associated disruption to operations) is often prohibitive.

As you know, mission-critical networks are designed, deployed and managed with a razor-sharp focus on safety, reliability and uptime. Outages of even just a few minutes are unacceptable. Any type of plant outage has an immediate and very significant financial impact. For many plants, the cost of an outage can easily be hundreds of thousands of dollars per hour.

In addition, many industrial facilities run safety-critical processes, which could put the lives of employees or the surrounding communities at risk, or cause significant environmental impact, if not managed properly.

These considerations have led operators to focus on stable systems.

The prevailing mindset in the plant is "if it isn't broke, don't fix it."

Once a plant control system has been tested and commissioned, engineers are very reluctant to make any changes to a working facility – and for good reason!

Practical Options for Industrial Applications

Option 1 – Maintain the Status Quo and Do Nothing

Let's say you love the stability of the Windows XP OS and don't want to upgrade. Perhaps you have never implemented any Windows XP patches over the last 10 years and you don't recall having a serious problem with computers, devices or applications over the time the OS has been in service.

However, you've probably seen a few situations where the computer or the application had some unexplained problem. Resolving them required a call to Microsoft or a software vendor to provide a patch, new driver or some other software reload to return your system to normal.

Likely and thankfully, there have been relatively few incidents for Windows XP in comparison to other operating systems. Plus, up until now, you've always had the peace of mind that support was available when needed.

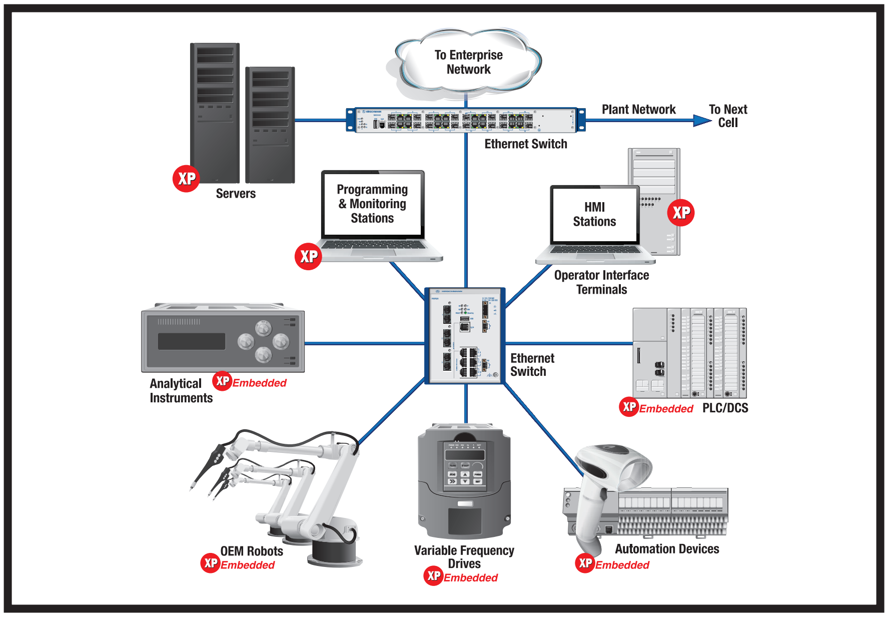


Figure 2. Simplified drawing of an industrial network showing the types of equipment that may be part of your Windows XP and Windows XP Embedded inventory.

Now, you need to decide if the risk of an incident and having no support available is a situation that fits with your operation's uptime requirements.

Don't forget that any USB or laptop connecting to the industrial network going forward could accidentally introduce a virus or malware that could impact a Windows XP-based system.

In addition, overall cyberattacks on industrial systems have increased dramatically over the last five years, and the EOS for Windows XP may trigger malware attacks directed at it.[3, 4]

Option 2 – Migrate to a New Version of Windows

Now let's take a look at securing your applications by upgrading to a new version of Windows.

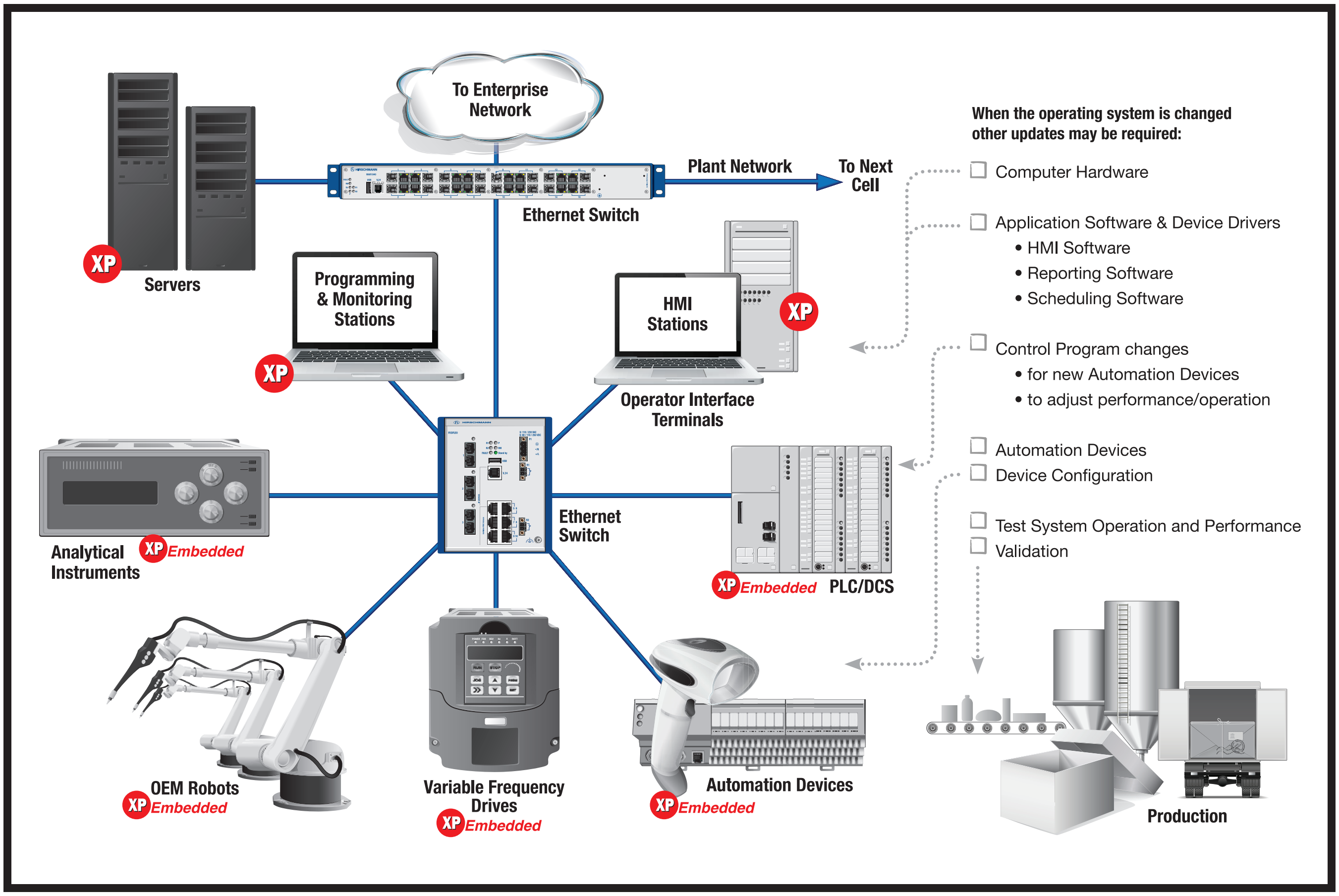
Most industrial firms that choose to migrate to a new operating system know it takes planning and time. The timeframe could be 12-24 months for a complete change out to ensure everything works as it should once it's put back together.

To begin, create an inventory of the Windows XP and non-XP OS assets in your plant network. Remember to include all of the places where Windows XP-based assets might be, as described earlier. Keep in mind that one large manufacturer of pharmaceuticals actively seeking to identify Windows XP-based assets was surprised to keep uncovering them in groups of hundreds.

Next, consider the Windows XP upgrade "domino effect" and identify the areas in it that will present the biggest challenges to your organization.

The Windows XP upgrade "demo effect" is:

- Upgrading the operating system…
- Requires new PC hardware and/or automation devices…
- The new equipment requires new software…



When the operating system is changed other updates may be required:

□ Computer Hardware

□ Application Software & Device Drivers
- HMI Software
- Reporting Software
- Scheduling Software

□ Control Program changes
- for new Automation Devices
- to adjust performance/operation

□ Automation Devices

□ Device Configuration

□ Test System Operation and Performance

□ Validation

Figure 3. To upgrade just 1 computer running Windows XP to a new OS leads necessitates many other updates that then require testing and validation before being put into operation.

- The new software requires new drivers…
- Some automation devices don’t work with the new software and drivers and may need to be replaced….
- Now your mission critical applications behave differently and system integration work needs to be done….
- The modified applications need to be deployed…
- Extensive testing of the new systems is required…
- Meanwhile operational productivity is lost to the migration project…
- And user training and support for the new systems are required ….

Taking into account all of the challenges, dominoes and timing conflicts with other operational or IT initiatives, create your plan. Be sure to include the right budget and people to get the job done. In regards to timing estimates, be generous. Unfortunately, with these projects it often turns out that the actual time taken is 3-5 times longer than what was planned.

Then take a deep breath and remember that OS migration, while necessary, won’t get done overnight.

Option 3– Reduce Downtime Risk Using Industrial Firewalls

To provide immediate protection while you deploy your longer-term plan of migrating away from Windows XP and for those devices that cannot be migrated from the Windows XP OS to a supported platform, you may want to deploy industrial firewalls.

These devices can be easily configured to block network traffic, which can exploit vulnerabilities in Windows XP-based systems, while still allowing them to perform their primary functions without interruption. The advantages of industrial firewalls are that they:

- Can be deployed into live networks without disrupting production
- Are simple to install and configure

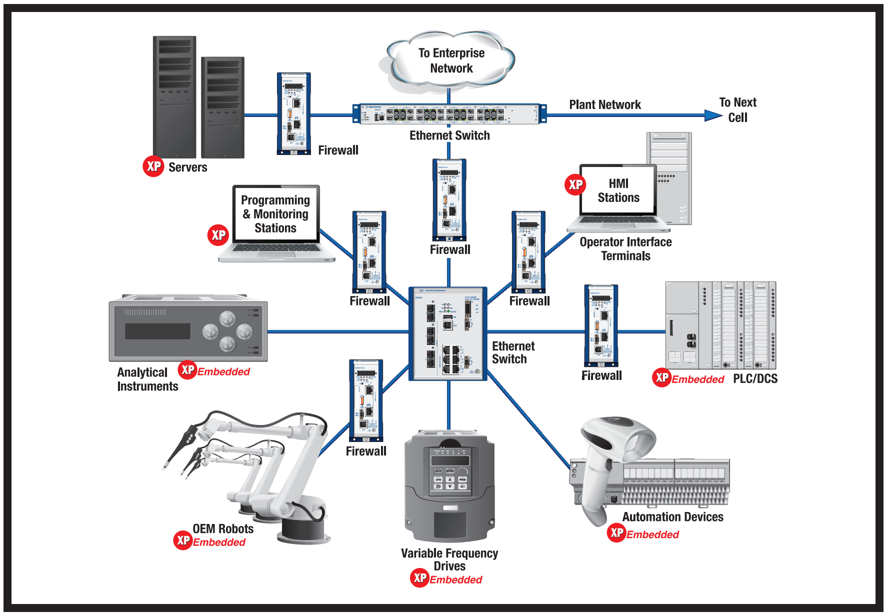


Figure 4. Simplified industrial network diagram showing Belden firewalls protecting Windows XP-based computers and devices.

Impacts	Option 1: Do Nothing	Option 2: Upgrade to a New Version of Windows	Option 3: Install Industrial Firewalls
Downtime Risk	Significant	Significant until the upgrade is complete	Minimized
Calendar Time Required	None – until an incident occurs	Significant	Short
Operational Productivity Impact	None – until an incident occurs	High	Low
Cost	None – until an incident occurs	High	Low
Windows XP Domino Effect:	None – until an incident occurs	Requires Action	Does Not Exist
OS upgrade	“	“	“
PC hardware upgrades	“	“	“
New hardware requires new software	“	“	“
New software requires new drivers	“	“	“
Application system integration work	“	“	“
Automation device replacements	“	“	“
Extensive testing	“	“	“
Modified applications need to be deployed	“	“	“
New user training and support	“	“	“
Lost operational productivity	“	“	“

Table 1. Comparison of Options for Securing Industrial Applications with Windows XP EOS

- Are designed for industrial deployment from the ground up, including being appropriately ruggedized and certified
- May have built-in intelligence about industrial protocols and be able to provide superior protection through technology called Deep Packet Inspection
- Can be implemented without requiring action on any of the Windows XP upgrade dominoes

Conclusion

Unfortunately, the EOS for Windows XP means we need to say good-bye to a trusted component of the industrial application ecosystem. It is not going to be easy or fast to replace this component. While your Windows XP upgrade planning and execution is underway, you need take immediate steps to secure your operations.

We recommend installing industrial firewalls as an immediate security solution that takes minimal staff time, can be completed quickly, has low training and support requirements, does not involve upgrading or replacing other systems, and is cost effective.

Using industrial firewalls gives you immediate peace of mind regarding cyber security plus the freedom to migrate away from Windows XP on your own schedule.

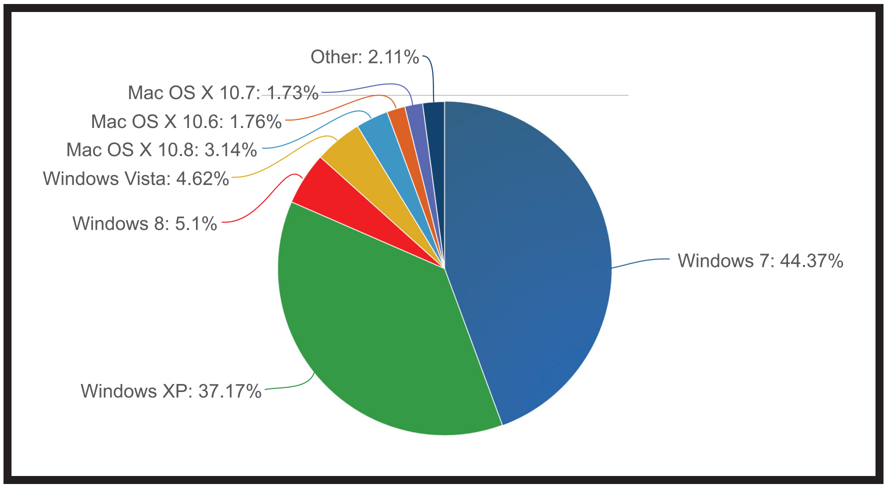


Figure 5 Chart shows the global share of Windows XP OS as of April 8, 2014. Source: Net Market Share[5]

Additional Resources

1. Contact a Belden representative for assistance:
    - Call **1-800-BELDEN1 (1-800-235-3361)** if you are in the U.S. or Canada.
    - Alternatively, complete the form at www.belden.com/contact
2. Belden industrial firewall and network management product information:
    - **EAGLE One Security Router**
http://www.belden.com/products/industrialnetworking/routers/eagle-one-security-router.cfm
    - **Tofino Industrial Security Solution**
https://www.tofinosecurity.com/products/tofino-security-appliance
    - **Industrial HiVision Network Management Software**
http://www.belden.com/products/industrialnetworking/software/industrialhivision.cfm
3. Find out about the Belden Certified Industrial Network Program, which provides expert network design services, outstanding warranties and flexibility for the future, at:
    - www.belden.com/certified-industrial-network

How Belden Can Help

While you may know Belden for our wire and cable, we are also the maker of:

- Hirschmann and Garrettcom switches, routers, and industrial firewalls
- Tofino industrial security products

Our industrial firewalls specifically address the Windows XP obsolescence issue. They use the same leading-edge technologies that are deployed in IT and enterprise networks, but adapted for the special requirements of industrial control and SCADA networks.

These firewalls are:

- Deployed into live networks without disrupting production
- Simple to install and configure
- Designed for industrial use from the ground up, including being appropriately ruggedized and certified
- Some models have built-in smarts about industrial protocols and are able to provide superior content inspection protection for critical applications.

We also provide the Industrial HiVision line of advanced network management tools that make it very easy to build an inventory of network assets, track changes, and monitor the performance of the plant network. These tools allow our solutions to scale easily from single point solutions to plant-wide and even worldwide deployments.

Finally, Belden has developed an ecosystem of partnerships with companies who have the experience and capability to deliver complete solutions including:

- Safety and security risk assessment
- Network design, deployment and certification
- Training services

This ecosystem enables us to deliver fast and cost-effective solutions to our industrial customers.

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Endnotes

1. Microsoft Webpage: "Enterprise Customers, support for Windows XP has ended"
   https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

2. Microsoft Webpage: "Enterprise Customers, support for Windows XP has ended"
   https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

3. Belden Presentation: "ICS Security: What's Happening and What are the Challenges", (Byres, Eric J.)
   http://info.belden.com/ics-security-whats-happening-pr-lp-bc

4. Belden Blog: S4 SCADA Security Symposium Takeaway: Time for a Revolution (ICS Security is in Worse Shape than I Thought)
   https://www.tofinosecurity.com/blog/s4-scada-security-symposium-takeaway-time-revolution

5. Netmarketshare Webpage: "Market Share Reports" (For the Windows XP numbers, select it under "Operating Systems" in the top middle of the page.)
   http://www.netmarketshare.com/

Reference Materials

- Norton by Symantec Webpage: "Is my Windows XP computer still protected after Microsoft stops supporting it?"
  https://support.norton.com/sp/en/us/home/current/solutions/v95977279_EndUserProfile_en_us
- Belden White Paper: "7 Steps to ICS and SCADA Security", Feb 16, 2012 (Byres, Eric. J. and Cusimano, John)
  http://web.tofinosecurity.com/download-7-steps/
- Belden Blog: Industrial Networking: Easy Security Risk Assessment
  http://www.belden.com/blog/industrialsecurity/Industrial-Networking-Easy-Security-Risk-Assessment.cfm
- Belden White Paper: "Understanding Deep Packet Inspection for SCADA Security", Dec 20, 2012 (Byres, Eric J.)
  http://info.belden.com/dpi-tk-lp
- Belden White Paper: "Using ANSI/ISA 99 (IEC 62443) to Improve Control System Security", Jan 2012 (Byres, Eric J.)
  http://web.tofinosecurity.com/download-the-white-paper-using-ansi-/-isa-99-standards-to-improve-control-system-security
- Belden Blog: Why Industrial Networks are Different than IT Networks (and What To Do About IT)
  http://www.belden.com/blog/industrialsecurity/Why-Industrial-Networks-are-Different-than-IT-Networks-and-What-to-do-About-It.cfm
- Belden Blog: Why Patching for SCADA and ICS Security is a Broken Model
  http://www.belden.com/blog/industrialsecurity/Why-Patching-for-SCADA-and-ICS-Security-is-a-Broken-Model.cfm
- Belden Blog: ICS Security: How Your IT Dept. Can Help
  http://www.belden.com/blog/industrialsecurity/ICS-Security-How-Your-IT-Dept-Can-Help.cfm

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

Belden, Tofino and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions.

Belden and other parties may also have trademark rights in other terms used herein.

About Belden

Belden Inc., a global leader in high-quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets.

With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world.

Founded in 1902, the company is headquartered in St. Louis and has manufacturing capabilities in North and South America, Europe and Asia. For more information go to www.belden.com or @BeldenInc.