Sys
Hardeni
valid
Refurbishing + updating Hardware
phys. cleaning of machines
visual inspection
Part tracking
Removal games + unused compilers programs
Close unused ports
Restrict access to USB + D
mentation

XP Mitigation Techniques

FoxGuard Solutions®

White Paper
FoxGuard Solutions, Inc.
January 2014

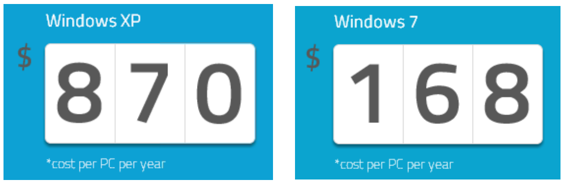
The End of XP Extended Support

Today's critical infrastructure sectors will soon be faced with new challenges as Microsoft® ends extended support for Windows® XP on April 8, 2014. What does this mean for industrial control environments? No more additional patches or service packs will be released, and users will no longer have access to free or paid technical support. This doesn't mean that systems running Windows® XP will suddenly stop working on April 8, but they will become increasingly vulnerable.

> *"No more additional patches or service packs will be released, and users will no longer have access to free or paid technical support."*

Operational Costs

The cost to keep running an outdated system will increase operational expenses. If an organization has not begun the migration process, they may be late, as the full deployment process can take 18-32 months[1]. The yearly expense of running Windows® XP will also increase operational costs, which can be as much as $870 per PC each year[2]- compared to running Windows® 7 at $168 per pc each year. Upgrading to a newer operating system could save companies 31% in hardware and labor costs alone[3].



IDC White Paper sponsored by Microsoft® Corporation

Security and Reliability

The continuous use of Windows® XP will decrease the reliability of operations and increase vulnerability to hackers and cyber-attacks. With a long list of documented vulnerabilities and rootkits already available, the end of extended support will open up even more exploit opportunities[4]. Upgrading to a newer Operating System offers an immediate increase in security such as:

- Support by Microsoft®
- Greater system speed and stability
- Increased user account flexibility and control
- Enhanced system protection
- Wider third-party application integration
- Improved system health and analysis

[1] www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx
[2] IDC White Paper sponsored by Microsoft Corporation, Mitigating Risk: Why Sticking with Windows XP is a Bad Idea, Doc #234690, May 2012
[3] CCS Case Study: Consoles For First Responders
[4] CCS Case Study: Support Plus New Technology Equals Better Security

XP Mitigation Techniques

Industrial users should have already begun migrating towards newer operating systems, due to the often long lead times for maintenance or operational outage. For those operations that are not able to migrate right away and that need a temporary solution, there are mitigation techniques which can be implemented. FoxGuard Solutions has developed three XP Mitigation techniques to serve as those temporary solutions.

Refurbishing and Upgrading Hardware

How old is the machine? Are all components still working and will continue to work in the future? Questions such as these are what industrial users should ask to determine if hardware needs to be refurbished. As part of the FoxGuard mitigation process, a full-scale maintenance check on XP-installed machines will be performed, and can include:

- Running backup
- Running a meticulous visual inspection of the machine
- Physical cleaning of machine components and additional memory added if possible
- Replacing or upgrading power supply, fans, DVD's and hard drives as needed
- Part stocking programs available to assist end-users
- Documentation of all changes made, and how they improved system performance

System Hardening

Once XP patches become unavailable, industrial users will have to find new ways to secure systems and data. One approach is to harden current systems. By disabling all non-operational ports, thus making it harder for malicious actors to access the system, industrial users help prevent potential threats. Additionally, security can be increased by continuous monitoring, whitelisting/antivirus, installing Intrusion Detection System (IDS), and by removing unused programs to lower the threat footprint without impacting operational reliability or stability.

An effective hardening system should be one that can mitigate the loss of OS patches, and includes but is not limited to:

- The removal of games, unused compilers, and unused programs
- The closing of all unused ports and unnecessary services
- Policies to restrict access to USB and DVD services
- Implementation of flexible, but strong user authentication
- Bringing the system to the final patch level
- Documentation detailing all changes and updates made, for NERC CIP compliance
- Patching and validation testing for required software on system

Virtualization

Currently, industrial users often have hardware that is custom designed to meet their control system needs. What happens when a machine crashes? Can additional pieces of hardware still be purchased? Is there a way to rebuild from scratch if needed?

Typically, when the hardware or operating system malfunctions, both have to be replaced. For older operating systems, this possibility is an extremely large risk. With virtualization, a middle layer can be added between the hardware and the software, giving the industrial user an easy way to purchase new hardware without affecting the software load. By virtualizing the Windows® XP operating system, industrial users have an effective and easier way to replace the hardware through:

- Taking faster backups of the system
- Rolling system changes back, if the changes cause adverse effects
- Running an older operating system on modern hardware

Migrate or Mitigate?

The answer is typically “both”. Many will need to mitigate until they can migrate. The two most important considerations when planning an operating system upgrade, such as one from Windows XP to Windows 7, are software and hardware compatibilities[5]. Once these have been confirmed, the update process can begin:

> *“The two most important considerations when planning a system upgrade…software and hardware compatibilities.”*

- Define the upgrade process
- Configure of OS and settings
- Test procedures
- Create a deployment schedule

[5] http://www.ccs-inc.com/xp/how-to-upgrade

About FoxGuard Solutions, Inc.

FoxGuard Solutions develops innovative programs and services to improve the cybersecurity and compliance posture of industrial control systems in critical infrastructure markets.

To reduce the likelihood of system downtime related to cyber incidents, FoxGuard provides assistance with patch validation and distribution, software updating, and system hardening for control system devices. Additionally, FoxGuard offers research and development services, engineering services, and field implementation services to support these programs.

Contributor

Scott Hudson

Scott joined the FoxGuard team in 2009 as a Product Manager with a background in Mathematics. In his role, he is responsible for defining product solutions to meet security and compliance requirements for FoxGuard customers.

Contact Information

To discuss which mitigation path best fits your operational needs, contact a FoxGuard Solutions representative.

www.foxguardsolutions.com

requestinfo@foxguardsolutions.com

877-446-4732

@FoxGuardInc