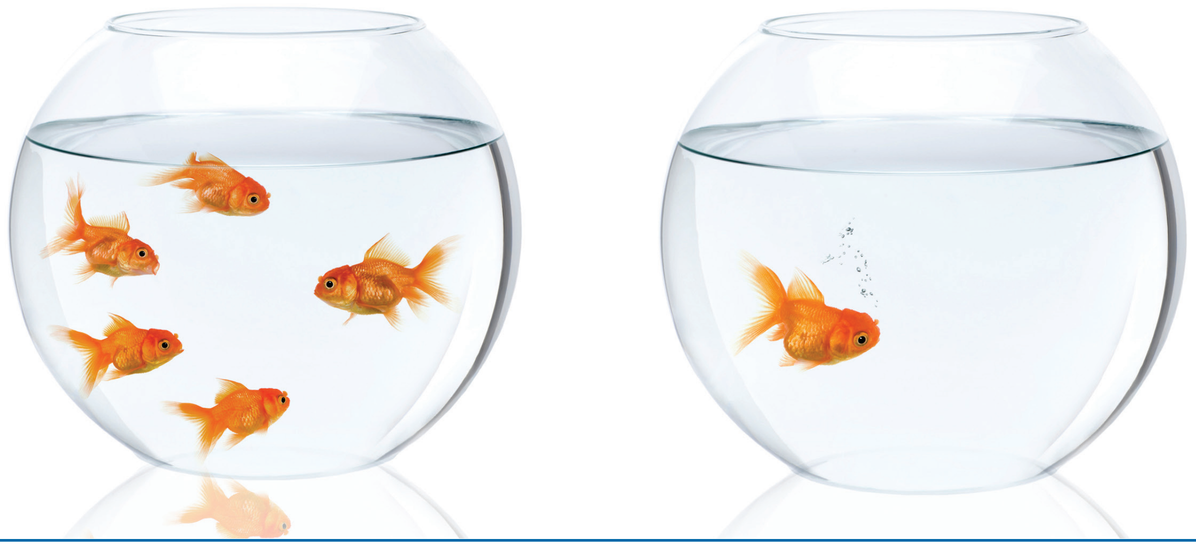
STEALTH by UNISYS

XP in Quarantine

Isolate and Protect Your Mission Critical Systems



Isolate XP with Unisys Stealth

Support for Windows XP ends April 8, 2014. Some organizations cannot migrate. Mission critical systems such as process control, point of sale, ATMs, Electronic Health Records, and other critical environments are vulnerable to security compromise.

Unisys Stealth™ is innovative software-based security that makes endpoints virtually invisible on a network to users or systems not explicitly authorized into the same secure community group, called a Community of Interest (COI).

Stealth-protected endpoints running Windows XP are designed to be undetectable, visible only to the specific users that require access. The endpoints continue to execute the same applications and control the same instrumentation or other downstream devices with no network reconfiguration and no creation of “air-gap” network segments. The endpoints can be prevented from reaching any other network locations, particularly the Internet, or can be allowed access to specific resources, such as the enterprise’s core IT services.

Authenticated network users, if not authorized into the appropriate COI, would not be able to detect or access the set(s) of XP endpoints, regardless of network topology.

With Stealth, cyber attackers and malware cannot interact with the XP workstations in any way. These XP workstations can be cordoned off from the enterprise and external network without requiring any physical network changes.

Value of Stealth Isolation and Protection

Isolating XP systems from the remainder of the network greatly reduces the attack surface for the entire enterprise. XP systems are predicted to be under heavy cyber scanning when security patches terminate. Removing these systems from hacker visibility will drive hackers to move to easier targets. Additionally, if an XP endpoint is compromised, the breach would be limited to only those systems in the same COI, similar to quarantine. The remaining enterprise network is not impacted.

A Few Use Cases

Unisys Stealth isolates mission critical systems to foster secure, continuous operations.

- **Automation and Process Control Systems** - Systems that monitor and control industrial and critical infrastructure processes including manufacturing, power generation and transmission, chemical processing, and water treatment are under strict regulation for security, compliance and availability. For stability reasons and because instrumentation devices downstream of the control systems may not have upgrade capability, these environments are not candidates for timely OS upgrades.
- **Point of Sale or Payment Card Systems** - Merchants utilizing Point of Sale or other payment card systems running Windows XP will be challenged to remain compliant with the Payment Card Industry Data Security Standard (PCI DSS) which states merchants must ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. With Windows vendor supplied patches terminating for XP, Unisys Stealth can be used to cloak Point of Sale devices and PCI processing systems to facilitate compliance.
- **Automated Teller Machines** - ATMs running unsupported XP may become non-compliant with PCI requirements.
- **Electronic Health Records** - Electronic Health Record and HIPAA regulations require specific protections to ensure the security and confidentiality of electronic health information and mandate that action be taken to properly safeguard this data. Unisys Stealth proactively controls access to servers and applications based on COI keys.

You Can’t Hack What You Can’t See

Unisys Stealth is innovative software-based security technology that is designed to:

- **Segregate assets** running unsupported Windows OS’s from the rest of the network
- **Mitigate risk** associated with connectivity to the enterprise network when no longer receiving security updates for legacy OS’s
- **Darken the segregated systems** from would-be attackers so they are not discoverable via typical network scanning techniques
- **Allow access to core IT services** if required, while restricting access to the Internet

Contact

stealth@unisys.com

For more information visit www.unisys.com/stealthxp

Printed in the United States of America 01/14 14-0013-B