TECHNOLOGY HORIZONS

atlantic-IT.net

Aligning Information Technology With Business Strategy

Jan./Feb. 2014

Time to Move Beyond XP

As support for operating system ends, organizations must migrate any remaining desktop systems to avoid security risks and gain benefits.

On April 8, Microsoft will end support for Windows XP and several other products, which means that security patches and other updates will no longer be available. Although the "sunset" date has been well publicized for almost six years, organizations continue to drag their feet up to the eleventh hour. The highly popular operating system still commands nearly thirty percent of the desktop OS market — a share that actually rose slightly in January.

There are a number of reasons why organizations are clinging to XP, including familiarity with the system and the potential business disruption associated with replacing it. With less than two months to go, however, organizations must move quickly to migrate any remaining XP systems to another platform.

"It is absolutely critical that organizations eliminate XP from their environments," said Michael Stenger, IT Director, Atlantic-IT.net. "Failure to do so will leave you exposed to substantial security risks and support challenges, while also wasting budget dollars that could be put toward updating your IT environment."

Organizations have several alternatives to consider when migrating from Windows XP. An obvious path is to upgrade to

Time to Move Beyond XP

continued from page 1

either Windows 7 or Windows 8, the more recent versions of Microsoft's desktop OS. To date, most organizations migrating from XP have decided to go with the four-year-old Windows 7 platform, which has a similar look and feel to XP with greatly improved performance. Windows 7 now owns nearly half of the desktop OS market share, compared to about 10 percent for Windows 8, according to NetMarketShare.

"Other options include Apple platforms or a cloud Desktop-as-a-Service solution," Stenger said. "The important thing is to develop an XP migration strategy and move forward with it as quickly as possible."

What's at Stake

Security is the most obvious risk facing XP users. Not only will Microsoft stop providing security patches and other updates, but security software vendors will almost certainly stop patching, updating and supporting products designed to work with XP. Many industry analysts have predicted that organized hacker and criminal groups are developing attacks in anticipation of unpatched XP systems.

More information is available in Atlantic-IT.net's Microsoft End-of-Support Resource Center. Visit www.atlantic-it.net/microsoft-end-of-support

Regulatory compliance also becomes a major concern. For example, regulators have warned financial institutions that they will be liable for lost or stolen credit-card data if they fail to upgrade from XP. Healthcare organizations responsible for protecting sensitive patient data and health information face similar compliance mandates.

"The newer versions of Windows mitigate these security and compliance risks. Windows 7 provides dramatic security improvements over XP with kernel patch protection, service hardening and data execution prevention," Stenger said. "Windows 8 goes even further, adding enterprise-grade data encryption, better tools for enforcing network access policies, and Secure Boot to prevent malware from hijacking boot processes and concealing itself from the OS."

Beyond the security risks and compliance issues, organizations maintaining an XP environment are at a competitive disadvantage. Because it is two full generations behind Microsoft's current desktop OS technology, XP either does not support or poorly supports features that have become commonplace on the latest PCs — including integrated wireless networking and Bluetooth adapters, more memory and faster USB performance.

"Microsoft's newest operating systems are loaded with tools and features that save time and make workers more productive," said Stenger. "For example, Microsoft's Hyper-V virtualization technology embedded in Windows 8 Pro provides a readily available foundation for internal virtualization efforts and private-cloud initiatives."

Rethinking Costs

Organizations that have yet to begin migration often cite costs as a reason for delaying the platform change. But Stenger says they should consider the potential for lost revenue, decreased productivity and image damage.

"The truth is that, on the whole, a move to Windows 7 or Windows 8 delivers key business improvements that have a demonstrable financial benefit in the form of investment versus cost avoidance," he said.

Support and remediation costs for XP machines are likely to rise rapidly over the next few years, significantly increasing the total cost of ownership (TCO) for those who don't migrate. In a recent study, Intel found that repair costs for older PCs typically exceed the purchase price of new machines. The Intel Small Business PC Refresh Study released in October 2013 found that older PCs have 50 percent more problems with 30 percent higher repair costs.

"It's really a simple formula: a new Windows 7 or Windows 8 PC is going to be more cost-effective because it is easier to manage, it operates more efficiently and it reduces remediation costs by keeping you more secure," said Stenger.

After a rough start when it was launched in 2001, XP eventually evolved into what most consider the most user-friendly and stable version of Windows ever produced. However, it wasn't designed for today's computing needs, and its continued use will bring substantial risk after April 8. Organizations can alleviate those risks and create substantial IT and business benefits by acting now to retire XP and migrate to a platform built for today's more demanding requirements.

The Sound of Malware

Network security researchers in Germany have proven that it is possible to use inaudible audio signals to spread malware to computers, even if the machines aren't directly connected to a network.

For years, so-called "air gap" security measures were considered the safest way to protect computer systems. Such measures involve physically isolating systems from unsecured networks, such as the public Internet or an unsecured local area network.

However, researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics have proved it is possible to jump the air gap using high-frequency audio signals. They were able to use the built-in speakers and microphones of computers to transmit passwords and other data at a rate of 20 bits per second over a distance of more than 60 feet.

In an experiment involving a host of Lenovo laptops running Debian Wheezy, the researchers were also able to send stolen keystrokes to a remote email server using a mesh network.

Cloud Risk Assessments Off Target, Study Says

Organizations are creating policies to guide their adoption of cloud services without enough information to fully understand and mitigate a broader set of risks posed by the use of those services, according to a recent report intended to gauge cloud adoption and risk.

According to the report from Skyhigh Networks, this lack of information is causing organizations to block trustworthy services but not more uncertain services. The report found that familiar services are blocked 40 percent more than high-risk services. Broken up by industry segment, some of the most common blocked services in the familiar category include Apple iCloud, Skype, Google Drive, Dropbox, bitly and PayPal, while high-risk services such as CloudApp, SockShare, RapidGator or MovShare are rarely blocked.

"What we are seeing from this report is that there are no consistent policies in place to manage the security, compliance, governance and legal risks of cloud services," said Rajiv Gupta, founder and CEO at Skyhigh Networks, the cloud security firm that conducted the study. "Our cloud usage analytics suggest that enterprises are taking action on the popular cloud services they know of and not on the cloud services that pose the greatest risk to their organization. Lack of visibility into the use and risk seem to be crux of the problem."

Technology Horizons

Editorial Correspondence:

7360 E. 38th St., Tulsa, OK 74145

Phone (800) 726-7667 • Fax (918) 270-7134

Change of Address: Send updated address label information to the above address.

Technology Horizons is published quarterly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

Next Stop: The Cloud

Atlantic-IT.net serves as a trusted guide on the journey to cloud computing.

Companies of all sizes are expanding their use of cloud computing to realize greater agility and efficiencies. Small to midsize businesses (SMBs) in particular find that cloud services enable them to reduce costs, become more productive and gain better access to information.

The move to the cloud would suggest that SMBs no longer have to worry about their IT infrastructure or technology strategy. That could not be further from the truth, however. The cloud can be a beneficial addition to the IT environment but it has to be approached strategically.

There are a lot of misconceptions associated with cloud computing. It is not some sort of silver bullet. Despite industry hype and promises, cloud services can be fraught with pitfalls and drawbacks for those who don't do their homework.

From a technology perspective, organizations need to look at service levels, performance, data access, security and flexibility. Cost is another consideration — because cloud services generally are priced on a per-user, per-month structure, organizations must be comfortable with moving IT services from the capital budget to an operational budget. Licensing, tax implications, data migration, IT skills sets and a host of other issues also come into play.

Furthermore, not every IT function is suitable for the cloud. SMBs need sound advice in developing a cloud strategy and selecting the appropriate cloud solutions to execute that strategy. This can help organizations avoid moving mission-critical applications to cloud services that are not up to the task, and otherwise maximize benefits of the clouds without the downsides.

In-House IT Still Matters

There is a tendency to overlook the internal IT environment when considering a move to the cloud. The in-house IT infrastructure does not go away with cloud computing, however. The cloud merely shifts the emphasis from one area to another.

For example, when applications are hosted in-house, IT staff are often focused on keeping those applications up and running and protecting the associated data. If those applications are moved to a Software-as-a-Service (SaaS) solution, network performance and availability become paramount.

"With SaaS, the network becomes the lifeline to applications and data," said Krystal Triumph, IT and Telecom Advisor, Atlantic-IT.net. "Because employees connect to a cloud application via the Internet, any network bottlenecks are amplified. It is important to ensure that the network is operating optimally and that there is failover to a secondary Internet provider in case of an outage.

"Atlantic-IT.net has skilled network engineers who can help organizations increase the performance of their LANs,

WANs and wireless networks, thereby boosting the productivity of SaaS users. We also provide managed services that can help ensure the network remains available."

Even if applications are running in the cloud, organizations still need skilled technicians to ensure that in-house equipment and the network stay up and running. Atlantic-IT.net proactively monitors the network using remote support software. All critical events are identified within minutes and resolved as quickly as possible so that access to the cloud is not interrupted.

In addition, an Atlantic-IT.net technology consultant meets periodically with each customer in a "virtual CIO" format to discuss network performance and ways to improve IT operations. This offers a golden opportunity to discuss the impact of cloud services on the business.

Bringing IT All Together

Cloud-based applications generally are faster to deploy, easier to use and have a lower upfront cost than traditional enterprise applications. But not every application can move to the cloud.

"We have seen a lot of success moving clients to cloud-based email, collaboration, backup and disaster recovery, customer relationship management, and office productivity tools," said Michael Stenger, IT Director, Atlantic-IT.net. "But core business applications that require high network performance may not be suitable because access via the Internet isn't going to be as fast as access via your local network. You may also have some legacy or custom-developed applications you don't want to update, or an application that is specific to your industry that requires a specialized infrastructure."

An often-overlooked aspect of cloud computing is software integration. Cloud applications by nature exist outside the IT infrastructure and, as a consequence, outside of the general flow of data among business processes. Application "silos" impact productivity and limit the return on the software investment. Because most organizations wind up with a hybrid environment, the integration of SaaS with traditional applications and data sources becomes imperative.

"At the end of the day, it's about getting the most from your technology investment, whether that's a cloud service or traditional on-premises solution," said Triumph. "The cloud is an attractive option for smaller organizations — it helps to level the playing field by giving them cost-effective access to enterprise-class tools, and enables them to adapt more quickly to changing business requirements. But proper planning and management of the IT environment remain very relevant. Atlantic-IT.net can help customers move to the cloud in a thoughtful, beneficial way."

How to Protect Sensitive Data

Storage encryption helps prevent embarrassing and costly data security breaches.

The data breaches suffered by Target and other major retailers have many businesses worried about the threats posed by hackers. The ongoing adoption of cloud computing and storage raises concerns about the security of data on third-party systems. And more and more employees are transmitting and storing sensitive information on mobile devices — devices that could be lost, stolen or compromised.

While there is no foolproof way to prevent a data breach, one technique comes very close: encryption. Encryption effectively "scrambles" data, which cannot be read without access to the correct encryption key. As a result, encryption can dramatically reduce, if not eliminate, the security risks associated with the loss or theft of stored data.

That has led a number of analysts to proclaim 2014 as the "year of encryption." Experts predict that organizations will begin to encrypt data within the data center, on endpoint devices and at all points in between.

"Storage, backup and archival solutions are designed only to preserve data; they don't protect against unauthorized access. Only data encryption can effectively safeguard so-called 'data at rest.' As a result, organizations should consider incorporating encryption into their storage and backup environments," said Michael Stenger, IT Director, Atlantic-IT.net.

"Strong encryption using 128-bit or longer keys make it impractical to try to decipher the text through brute force. A 2012 report by the National Institute of Science and Technology estimates that AES-128 encryption should be secure through to 2031."

Growing Requirement

Organizations in certain regulated industries have very real incentives to encrypt data. The HIPAA Final Omnibus Rule requires covered entities to provide notice to affected individuals, the Department of Health and Human Services and in some cases the media if there is a breach of unprotected — that is, unencrypted — data..

The healthcare sector isn't the only industry that promotes encryption. Under California's Security Breach information Act and similar regulations enacted by more

than 20 other states, companies must disclose even suspected security breaches to the media and all customers potentially affected. Encrypted data is exempt, however.

The Payment Card Industry (PCI) Data Security Standard mandates the encryption of stored data, including data on backup tapes — a rule that potentially impacts any merchant that accepts credit cards. Noncompliance can result in financial penalties ranging from $5,000 to $50,000 per month.

Regulatory requirements aside, the need to secure data is clear: a single data security breach incident costs $5.4 million, according to the Ponemon Institute. Still, the price tag for data protection can cause sticker shock for many companies.

In addition, many organizations have operated under the theory that encryption makes finding and retrieving information more difficult, increasing the complexity of storage and backup process. Indeed, traditional software-based encryption solutions required companies to make painful tradeoffs to achieve data security: performance degradation, operating system and application dependency or changes in workflow.

A Better Way

The good news is that today's encryption devices can be so tightly integrated with the storage environment that they avert the unacceptable performance slowdowns of the past. Several vendors offer appliances that sit on the network, encrypting and digitally signing data on the fly. Because they sit "in-line" — that is, in the network data path rather than within application software or storage devices — they operate independently. They can be deployed with storage-area network (SAN), network-attached storage (NAS) or direct-attached storage (DAS) solutions.

These solutions also provide better key management than traditional storage encryption solutions. Encryption rules can be used to minimize the number of keys to be managed and master keys can be used to protect the encryption rules. Centralized security management provides user authentication and role-based privileges. Encryption appliances can also monitor the physical access to the device itself and automatically lock down all encryption keys.

According to the Ponemon Institute's 2012 Global Encryption Trends Study, released early last year, about 35 percent of U.S. businesses had an encryption strategy applied consistently across the enterprise. Experts expect that proportion to increase dramatically due to the threats posed by hackers and malware, along with cloud and mobility risks. Encryption can help organizations meet regulatory requirements and prevent a costly and embarrassing security breach with little impact on IT operations.

Rise above your technology limitations

Keeping up with the multitude of new developments in hardware, software and infrastructure can be overwhelming for IT staffs that are already stretched thin. Atlantic-IT.net can help.

Atlantic-IT.net is a full-service IT solutions provider that designs, implements and supports integrated voice and data communication solutions for businesses and government agencies.

Gain the advantages of "one-stop shopping" plus our 15+ years of experience. Call Atlantic-IT.net for all your voice and data needs, including:

- IP Phone Systems
- Mobility and Wireless
- Contact Centers
- Backup and Disaster Recovery
- Networking and Security
- Cloud Computing

atlantic-IT.net

Aligning Information Technology With Business Strategy

Contact us at 877-936-3328 or go to www.atlantic-IT.net to learn how we can help with technology initiatives that can push your business to new heights.