Top 6 Security Considerations in Migrating to Microsoft Windows 10

ABSOLUTE™

Whitepaper

Top 6 Security Considerations in Migrating to Microsoft Windows 10

The release of a new Microsoft operating system is always an important event for IT departments, and Windows 10 is no exception. IT organizations and end users have been looking forward to a wide range of new features in Windows 10, with interest particularly high as users of Windows 7 and 8 can upgrade for free.

However, the adoption of a new operating system can also be a period of increased security vulnerability—particularly if the IT department doesn't have the tools, technologies and processes to have comprehensive visibility and control over their endpoints. For IT, one of the top priorities must be ensuring that existing devices are secure and remain secure during and after the transition from one OS version to another.

In addition, many IT leaders view the move to a new operating system as a positive opportunity to re-evaluate their existing security posture and to upgrade where necessary. While Microsoft has equipped Windows 10 with several new security features, such as Device Guard and Windows Hello, organizations still face security gaps that can only be addressed by giving IT centralized visibility across endpoints, whether they are PCs, laptops, tablets or smartphones. In addition to visibility, IT teams need the control and flexibility required to quickly and easily take appropriate actions to mitigate security risks.

To achieve this required level of security, organizations need a trusted connection to each device, regardless of its user, location or operating system version. Persistent endpoint security solutions enable these trusted connections through technology that is built into the core of each device. With persistent solutions, organizations can not only ensure that new devices with Windows 10 are protected from the factory, but they can also leverage the same technology across all of their existing devices, including PCs, laptops, tablets and smartphones. This white paper examines six of the most important IT security considerations in migrating to Windows 10, while describing how utilizing adaptive endpoint security solutions can help you address these challenges and deliver maximum security across all devices.

CONSIDERATION NO. 1: VISIBILITY

A successful migration starts with understanding your current environment and having visibility into all endpoints from a central location that provides accurate information across all stages—before, during and after the migration. IT teams should never lose either visibility or control over any device because that is when security vulnerabilities can occur, especially with users moving from one operating system version to another.

How do you ensure that level of visibility and control? Persistence® technology by Absolute takes a unique approach by embedding technology within the core of most computers, tablets, and smartphones at the factory. Once activated, it provides you with a reliable two-way connection so you can confidently manage mobility, investigate potential threats, and take action if a security incident occurs.

For customers migrating to Windows 10 from an earlier version, this technology ensures you never lose protection. With other security solutions, you need to install a new agent with the new operating system. However, because Persistence is in the core, the Absolute agent it enables is compatible across operating systems, with no administrator input required. This same technology can survive events such as operating system re-installations, hard-drive replacements, or even the firmware being flashed. This extends to ultra-portable devices, which maintain a connection even if a tablet or smartphone is wiped clean to factory settings.

CONSIDERATION NO. 2: CONTROL

Visibility must be accompanied by centralized control. It's not enough to see where there may be security gaps or risks, you need to be able to do something about them, and you need to be able to respond quickly. In a scenario where users are moving to Windows 10, IT needs to maintain control. You don't want rogue users making the upgrade without permission or company support. You also want to move at a controlled pace. For example, there may be areas of the company or specific departments that you have visibility and control over each endpoint, you can make those decisions with the assurance that your security solutions allow you to enforce them. With Persistence technology, the Absolute software agent in each device makes regularly scheduled calls over the internet to a monitoring center that

you access via the cloud. You can obtain realtime information about each device's assets, status and location. You can also define specific conditions and receive alerts so that you can respond immediately to any potential security risk or device incident.

For example, if you were to detect a potential security risk during or after a migration to Windows 10, you could invoke commands such as data delete, device freeze, file retrieval or other remote security measures. If there is an unauthorized user on a particular device security actions can still be performed—regardless of any malicious attempts they may make to bypass the solution.

CONSIDERATION NO. 3: RISK REDUCTION

Even with the enhanced security features of Windows 10, you want to be able to maximize protection on each endpoint to limit your vulnerabilities. Endpoints are particularly vulnerable to data breaches caused by internal incidents, such as malicious employees, theft, lost devices, negligence or human error. In fact, during a recent 12-month-period 67% of breaches were caused by internal incidents, according to a survey by Forrester Research.[1]

Persistence technology offers the highest level of protection against unauthorized or accidental attempts to remove the software agent, allowing you to track and secure devices regardless of the user or location. Because Persistence technology is embedded in the core and can maintain a connection to the device, you will never lose visibility during the migration from one OS version to another. And you can utilize the same level of protection on any new devices you provision or purchase with Windows 10.

CONSIDERATION NO. 4: COMPLIANCE

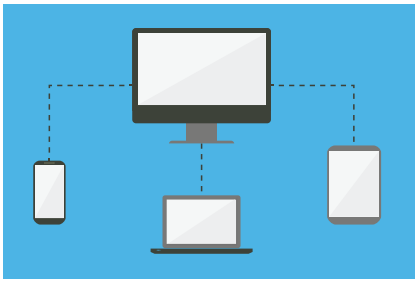
By using Absolute you not only reduce the risk of a damaging breach, but you can also be more comprehensive, efficient and accurate in meeting regulatory compliance requirements. With a persistent endpoint security solution, you can more readily prove to auditors that IT compliance processes are being properly implemented and enforced before, during and after the migration to Windows 10.

For example, if a device is lost, stolen or misplaced during the migration you can:

- Provide proof that sensitive data was not accessed
- Provide proof that data was securely deleted before it could be breached
- Remotely freeze a device to revoke access to the corporate network, regardless of the location of the device
- Provide chain-of-custody proof to show that data was secure when the device was lost or stolen
- Remotely delete data from a device when it is decommissioned or transferred between users

CONSIDERATION NO. 5: COMPLEXITY

Migrating to a new OS is challenging for IT, with many aspects to manage. Because Persistence technology is built into the core, IT doesn't need to deploy a new agent when migrating to a new OS. This is one less thing to worry about. Also, with the centralized visibility and control provided by Absolute, IT can simplify overall management of its endpoint security, while using a wide range of remote functions to enhance security without having to physically handle any devices. This remote connectivity to each device is available regardless of whether it is on or off the network, providing remote data retrieval and deletion no matter where the device is located.



CONSIDERATION NO. 6: CONSISTENCY

Because the same technology can be used across new Windows 10 endpoints along with all other endpoints—including tablets and smartphones, as well as non-Windows devices such as Mac OS X or Android—the organization benefits from a consistency of approach and security processes across all devices. With centralized visibility, control and management, the IT team can design alerts that can be implemented across all devices, or can be tailored to specific devices or users. This consistency of security processes and controls makes it much easier to protect data on mobile devices—while at the same time offering maximum security on new Windows 10 devices or existing devices that are migrating to the new OS version.

TAKING THE NEXT STEP

Moving to a new OS version can be an opportunity for an organization and its users to improve productivity by leveraging innovative new features and functions. But it is also a time of increased security risk if IT doesn't have the right technology to control and monitor the migration with visibility into all endpoints at all times, regardless of their location.

The migration to Windows 10 is particularly challenging because, as a free upgrade, users may feel they can undertake the process without corporate approval. In addition, the ubiquity of mobility in today's era makes the organization more vulnerable during and after the migration, with IT needing to account for a far wider range of endpoints across a much broader and more unpredictable geographic area.

As IT leaders evaluate how to achieve the highest levels of security during and after the migration, they will see clear benefits, including unprecedented visibility and control, while reducing risk, enhancing compliance preparedness, decreasing complexity and providing a platform for consistent security and management across all devices at all locations. Are you ready to take the next step in assuring the safest migration path to Windows 10? Here's where to get started: absolute.com.

FOOTNOTES

[1] Business Technographics Global Security Survey, 2014, Forrester Research, July 2014