WHITE PAPER – **OCTOBER 2017**

HOW TO EMBRACE A ZERO DAY COMPLIANCE MODEL FOR WINDOWS 10 PATCH MANAGEMENT

vmware® | TechTarget® | Custom Media

Table of Contents

Windows Updates Cost Elements

- Management and reporting servers
- Server licenses
- Distribution points
- Network switches and VPNs
- Third-party management tools
- Validation, testing and reporting

Windows 10 is now a fact of life for most enterprises, offering a wide range of improvements and benefits over legacy Windows systems. But Microsoft has changed the rules of the game when it comes to delivery and management of OS updates. These changes have big implications for IT organizations looking to ensure endpoint security and restore order in Windows patching within a rapidly changing OS framework.

Managing Windows updates has always been a critical requirement for OS security, but there's little debate that the traditional method of dealing with regular OS updates and patches was inefficient, time consuming and one of the least favorite tasks of IT administrators. This legacy approach also didn't scale well across all users, devices and locations, putting endpoint security at risk and increasing costs. Some analyst estimates put the cost of managing OS patches at $150, or 2.9 hours, per user per year. The prospect of consuming larger portions of administrators' time with Patch Tuesdays and other update-related tasks was maddening to IT executives and baffling to business leaders who worried about IT responsiveness and rising management costs.

The good news is that Microsoft has flipped the patch deployment model by moving away from legacy, on-premises, network-centric patching and upgrades in favor of a Windows Updates as a Service model. Much like updates for mobile operating systems, the new threats in the mobile-cloud era require organizations to update the OS faster and more reliably than in the past. On the downside, this much faster cadence comes with its own set of challenges. These include:

- Keeping endpoints up to date with far more frequent updates
- Ensuring application compatibility across each update, especially with third-party security services
- Delivering OS updates, which are much larger than traditional service packs and place added burden on branch office bandwidth
- Deploying all-or-nothing cumulative roll-ups combining a large number of patches that need to be tested and delivered at once.

Windows 10's new approach to OS patching centers on two new types of updates: branch upgrades and cumulative updates.

And, it's not like this approach is unique to Windows 10. Microsoft is instituting this patch management philosophy for all of its most popular applications, such as Microsoft Office 365, that are now being updated via the same Windows Updates service. This is the new reality for the Windows IT community, so deferring and delaying adoption of Windows Updates as a Service is not an option. Instead, the goal should be to embrace this new paradigm without adding to complexity and putting a greater management burden on an already stretched IT organization.

Servicing Channels and Cumulative Updates—Challenges and Implications

Windows 10's new approach to OS patching centers on two new types of updates: branch upgrades and cumulative updates.

Servicing Channels

Microsoft rolled out release channels in order to give IT professionals more say in how frequently and extensively to update their devices. There are three types of servicing channels:

- Insider Preview: Insider builds are released continuously by Microsoft, and are designed for early adopters, IT professionals and developers to get ahead on usability and testing of upcoming versions.
- Semi-Annual Channel (formerly Current Branch and Current Branch for Business): This is the default branch for Windows-based endpoints, and is designed for use across a wide range of devices for consumers, enterprises and educational institutions. The Semi-Annual Channel (SAC) is released twice a year, in March and September.
- Long-Term Servicing Channel (formerly Long-Term Servicing Branch): This is designed for use with "specialized or mission-critical systems," such as endpoints often seen in Internet of Things (IoT) environments like medical, retail and industrial. As the name suggests, they are serviced by Microsoft for about 10 years.

As endpoints proliferate in number and diversify in format and use case, managing those devices in a cohesive, efficient manner becomes more essential—and, at the same time, more difficult.

Servicing channels create challenges for IT professionals for a variety of reasons. For instance, these updates are as large as a new OS image, and updating all devices over company networks will be taxing on bandwidth and backbone infrastructure. These updates are more frequent than traditional service packs, further stressing resources required in testing and rolling out across the entire user base. Additionally, deploying new branch updates for Windows 10 will also require IT to keep updating their existing PC Lifecycle Management (PCLM) tools (e.g. ConfigMgr) to the latest releases.

Organizations can then take the Insider Preview and SAC to create their own distribution rings internally for testing. While every organization may have different requirements, for most use cases, VMware recommends the following:

- Have a few people in IT constantly test Insiders Preview
- Once SAC is released, distribute to IT for ongoing testing
- Roll out to a small portion (about 5%) of the broader organization
- Scale to 20% of the organization for final testing
- Distribute SAC to the rest of the organization
- Distribution LTSC to any mission-critical devices

The role of enterprise-grade UEM: restoring choice and flexibility

As endpoints proliferate in number and diversify in format and use case, managing those devices in a cohesive, efficient manner becomes more essential—and, at the same time, more difficult.

As a result, demand for unified endpoint management (UEM) solutions has surged. The global UEM market is predicted to surpass $3.7 billion by 2020, a compound annual growth rate of nearly 43%.[1] The increasing hybridization of IT is another key driver for UEM, supporting endpoints that are both physical and virtual, as well as on-premises, offsite and in the cloud.

1 "Unified Endpoint Management Market by Deployment Mode, (Cloud, On-Premise, Hybrid), Vertical, Region – Global Forecast to 2020," MarketsandMarkets, February 2016

IT professionals crave more control and don't want to wade through countless unnecessary updates.

Now, endpoint patches and updates are increasingly delivered by Microsoft as a cloud-based service—and those updates are finding their way onto a new wave of mobile platforms from notebooks and tablets to smartphones and IoT devices. This heightens the need for UEM solution built around the concepts of mobility and cloud, while addressing the shortcomings of Windows Updates as a Service in such areas of limiting control and choice by IT to accept or reject updates as appropriate.

As good an idea as cumulative updates and patch roll-ups can be, IT professionals crave more control and don't want to wade through countless unnecessary updates. The ideal UEM solution would allow administrators to see only the updates that apply to their relevant devices, instead of everything Microsoft may want you to see at that time. Administrators also would like to be able to go into a dashboard and view the applicable knowledge base for an update as it relates to a particular class of device. They would then be able to pre-approve groups of updates, based on what they learn from the Microsoft knowledge base.

And, even more attractive would be the ability to assign policies and updates not just on a particular type of device or user, but also for specific brands of devices or versions of operating systems.

How VMware AirWatch modernizes and eases Windows 10 patch management

As enterprises struggle with the challenges and intricacies of Windows Updates as a Service, they have looked for UEM solutions optimized for the mobility/cloud operating model. These solutions must help them overcome concerns over such issues as:

- Losing control over which knowledge bases are distributed or deferred with faster and more frequent updates.
- Dealing with the inevitable demands on network bandwidth in delivering updates over corporate wide-area networks, especially with so many users and devices located off-premises and using multiple devices and multiple identities.

Forced upgrades from Windows Updates as a Service—an issue that otherwise makes IT administrators shudder—are easily overcome in the AirWatch management console...

- Fear of the potential for OS glitches and service interruptions caused by an inability to sufficiently test updates internally before releasing them to users in production environments.

VMware's AirWatch UEM is designed to address these concerns, while giving enterprises the ability to properly support Microsoft's new service model for updates. AirWatch gives administrators tighter, more customizable control over the management and distribution of updates.

Among the specific capabilities and functionality AirWatch offers for Windows 10 environments are:

- Eliminating network dependencies that often result in diminished performance, availability problems and a degraded user experience, particularly for those who work off the backbone network.
- Flexibility for enterprises to embrace Windows Updates as a Service in the manner they feel is most appropriate for their organization. Whether their choice is to move aggressively or cautiously adopt iterations of the new service model, AirWatch can be adapted—and be changed quickly—as conditions warrant.
- The ability to pick and choose the most appropriate branches and updates to go to different devices.
- AirWatch smart group assignment, which handles policies and updates on a highly customizable basis. Not only can policies and updates be assigned on a per-device or per- user basis, but they also can be implemented on a far more granular level—say, only for specific brands of notebooks or certain smartphone operating systems.
- Bandwidth optimization with robust, secure, over-the-air management and security framework.
- Visibility for administrators into all available updates and the status of machines, without resorting to writing custom scripts based on large SQL queries.

AirWatch also allows administrators to deploy and/or defer appropriate operating system branch updates based on device priority and desired maintenance windows. Forced upgrades from Windows Updates as a Service—an issue that otherwise makes IT administrators shudder—are

Windows Updates as a Service is a new model for patching and updates that makes Patch Tuesdays a thing of the past.

easily overcome in the AirWatch management console, giving control over updates and patches to the IT professionals most familiar with requirements on a device and user level.

Additionally, peer-to-peer caching for delivering optimization of updates helps to avoid potential network congestion that otherwise arises from large cumulative updates.

Finally, the increasingly prevalent scenario of off-network patching is greatly facilitated with AirWatch's instant, push-based management feature.

Conclusion

After decades of deploying Windows based on an on-premises, network-dependent paradigm, IT professionals now are coming to grips with Windows as a service (WaaS)—particularly the important requirements of patch management. Windows Updates as a Service is a new model for patching and updates that makes Patch Tuesdays a thing of the past. But it also carries significant challenges for IT professionals who may not find the management demands of continuous updates and service branches to their liking.

In order to regain control over the entire range of endpoint lifecycle management using over-the-air policy and modernized configuration management, application management and real-time security, enterprises should consider a purpose-built UEM solution.

VMware's AirWatch is a cloud- and mobility-optimized UEM platform that lets IT professionals enjoy the many benefits of a WaaS model, while controlling how, when and where to implement updates and patches without constraining budgets, manpower and network bandwidth.

For more information on how AirWatch addresses the many issues associated with Windows Updates as a Service, please visit www.vmware.com/products/airwatch-enterprise-mobility-management.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

10/17