SOLUTION BRIEF

FALL IN LOVE WITH WINDOWS ALL OVER AGAIN

By Keeping It Where It Belongs: In the Data Center or Cloud

When it comes to endpoint computing, Windows is no longer the only game in town. From x86 operating systems like MacOS, Chrome OS, and Linux to full-featured mobile operating systems like iOS and Android, there are more ways than ever for people to access corporate applications.

But Windows desktops are here to stay.

As of April 2019, Windows still holds 87 percent market share on desktop and laptop devices. And this isn't just a product of a large legacy Windows installed base. Windows 10, the latest version, eclipsed Windows 7 in December 2018 to become the world's most popular operating system.

But all is not perfect in the Windows desktop ecosystem! Wider use of non-Windows operating systems is opening desktop IT administrators' eyes to a world without the Windows management and security challenges. They see potential for tremendous efficiency gains and improved security through reduction or elimination – not of Windows, but of Windows installed locally on endpoints. But for most, doing so is perceived as impractical.

Windows is deeply embedded into how many organizations work. There are many specialized business applications in use that require Windows. Moreover, even as Microsoft Office support on non-Windows operating systems improves, many still view the Office application suite experience on Windows as superior and throughout many enterprises, expected.

Fortunately, there is a way to both continue to enjoy the many benefits of Windows desktops while eliminating management and security headaches at the endpoint.

The answer is to keep Windows where it belongs: ***in the data center*** or, alternatively, ***in the cloud***.

Source: NetApplications report, retrieved May 2019.

Windows Endpoint Management Challenges

The breadth of supported options and sophistication of Windows is what makes it so useful as a general-purpose operating system for a wide variety of enterprise computing activities. But these same attributes also make Windows extremely unwieldy to update and maintain. This includes both Microsoft's ability to create, test, and distribute updates reliably and IT teams' ability to apply updates to devices in a reliable and timely manner. It's worth noting that Windows 95 debuted in 1995 with RAM and free disk space requirements of 4 MB and 120 MB respectively. The current Windows 10 RAM requirements are 1000X greater at 4 GB, and required disk space has grown over 130X to 16 GB. As each subsequent update of Windows 10 occurs, the system sizing requirements continue to expand.

Users Suffer Data Loss as a Result of Windows 10 Update

Both of Microsoft's bi-annual feature updates to Windows 10 in 2018 encountered significant issues. In fact, Microsoft was forced to pull the October 2018 update after some users reported that files in their C:/Users/[username]/Documents/ folder were deleted by the update. Users also encountered Intel driver issues and oddities like incorrect CPU utilization values in the task manager after the update.

Major Windows version upgrades are particularly daunting for organizations with many devices. In many cases, they have turned into multi-year projects and consumed considerable IT resources while delivering very little value beyond maintaining Microsoft support coverage. Microsoft is attempting to reduce these major hits to IT productivity by declaring Windows 10 "the last version of Windows" and shifting to a more iterative development approach. But this places even greater pressure on the wave of monthly updates that organizations receive from Microsoft.

Moving forward, Microsoft will release two Windows 10 "feature updates" per year in addition to the traditional "Patch Tuesday" security and stability updates that IT teams are accustomed to receiving on a monthly basis. The problem is that the increased density of these updates is putting additional pressure on an already imperfect, time-consuming, and labor-intensive update process.

Regardless of whether updates are frequent or infrequent, the fact remains that upgrading an operating system as large and complex as Windows at scale is a complex endeavor that is prone to errors and quality issues. In some cases, these errors may originate with Microsoft. In other cases, IT teams may encounter localized patch failures due to situational issues.

While Microsoft deserves credit for rethinking the update process with Windows 10, the new process has been far from issue-free and continues to be a major resource drain for desktop IT teams.

Windows Security Challenges

A major side effect of the difficultly of Windows endpoint management is ongoing security exposure. Many successful attacks exploit known software vulnerabilities. The industry's Common Vulnerabilities and Exposures (CVE) database reports 255 distinct Windows 10 vulnerabilities discovered in 2018 alone. Even organizations that are highly adept at applying Windows patches to their endpoints quickly find themselves in a near-constant state of vulnerability.

Most organizations attempt of mitigate this risk by deploying endpoint security products. While these products do bring added protection, it generally comes at the cost of even greater complexity on the endpoint and even more management burden for desktop IT teams.

Conflicts Between Windows Update and Endpoint Security Products Lead to Boot Failures

Following the installation of Microsoft's April 2019 "Patch Tuesday" updates, many users of popular endpoint security products found that they could no longer boot their Windows machines. Security vendors scrambled to communicate workarounds, and Microsoft acted quickly to block updates from being performed on systems with conflicts. But it's a perfect example of the perils of managing a complex endpoint operating system laden with third-party security products. Quite simply, the more purpose-specific software loaded onto an endpoint device, the greater the chance that something may go wrong, either within any single software component or between any two or more. Not to mention the greater the number of processes (anti-virus, etc.) running on an endpoint, the greater the performance burden on that device's CPU.

The Incredible Growing Hardware Requirements

Along with the operational inefficiency and security risks that come with Windows endpoint management, organizations are also likely to face ever-increasing hardware costs when they run Windows on endpoints. For as long as Windows has existed, there have been unrelenting increases in the system resources required to deliver an acceptable Windows experience on the endpoint. Even as the ways that typical users use their computers remains fairly constant, organizations face ongoing pressure to refresh hardware to meet Windows' increasing demands.

This resource creep is no longer limited to new operating system releases. In an April 2019 advisory, Microsoft warned users that they would need up to twice as much free storage to install its major update than previous upgrades required. These unplanned hardware requirements put desktop teams in the unenviable position of choosing between new hardware purchases or new security risks and feature trade-offs.

Windows in the Data Center: The Best of Both Worlds

While the challenges described above may seem like an argument against continued Windows usage, they are not. They are an argument against deploying and attempting to manage and secure Windows on endpoints. For years, organizations have successfully delivered Windows desktops and applications from the data center using virtual desktop infrastructure (VDI) and remote desktop session hosts technologies from vendors like Citrix and VMware. More recently, it has become even easier to deploy and manage Windows desktops centrally using desktop-as-a-service (DaaS) offerings from Amazon Web Services and Microsoft.

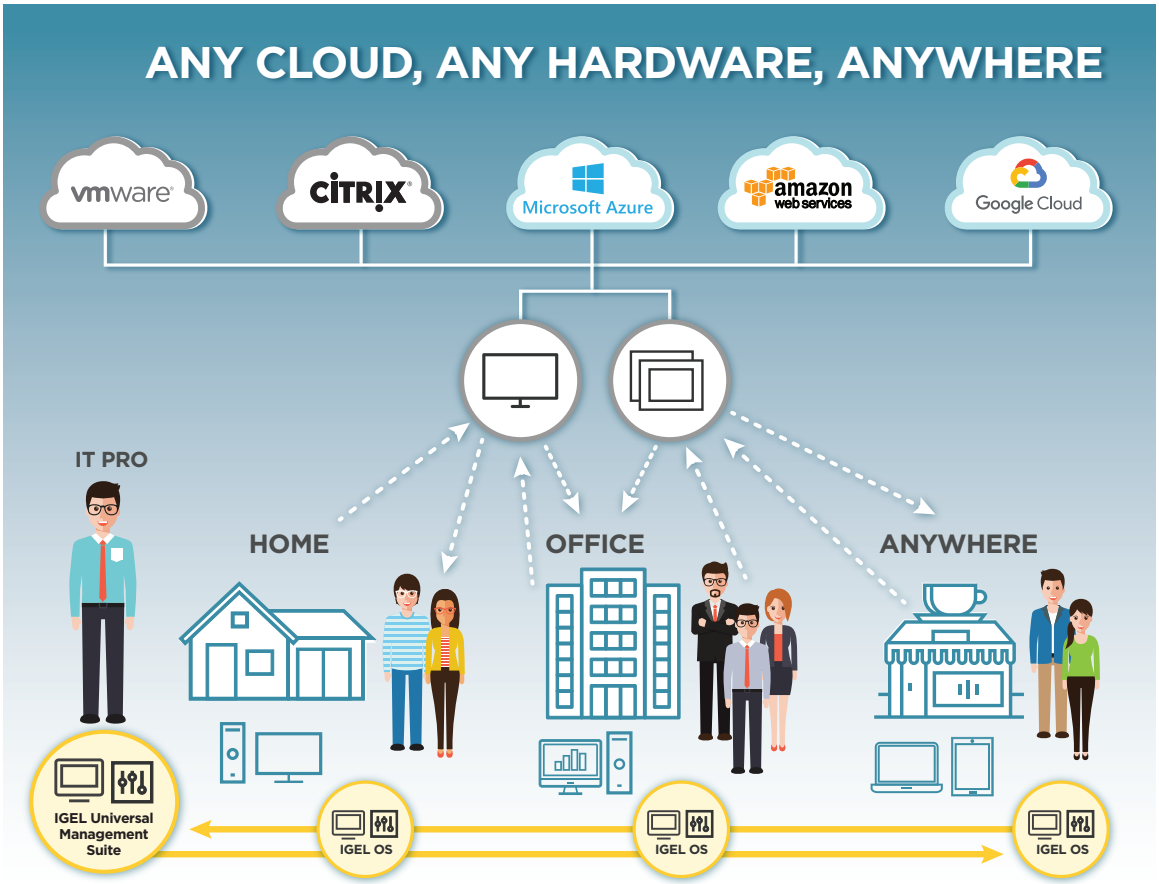
In the past, centralized desktop delivery was often viewed as a niche use case, with the majority of users continuing to run local instances of Windows on their endpoints. The time has arrived to reverse these roles, and for multiple reasons.

Centralized Windows management with a VDI or remote desktop session hosts dramatically improves both manageability and security. Virtualization platforms include superior capabilities for separating user settings and data from the underlying operating system. They also have advanced features like non-persistent desktops, linked clones, snapshots, and rollback that aren't easily replicated on an endpoint running Windows natively. In addition, centralizing Windows execution on server hardware in a controlled environment inherently eliminates many of the hardware- and environment-specific factors that complicate endpoint patching. And it's in the data center where backup and redundancy of compute resources and data is an inherent design requirement.

Windows in the cloud via DaaS takes this a step further by allowing organizations to eliminate data center and virtualization platform management requirements as well. It is worth noting the incredible recent growth of cloud-based Office 365. According to Gartner, in January of 2019, 91% of enterprises were already using or planning to use Office 365. This portends a similar move to the cloud for Windows desktops in the form of DaaS as a logical next step.

By moving Windows to the data center or cloud, IT teams can:

- Offer users a much more performant and reliable Windows experience
- Greatly improve IT efficiency by simplifying the Windows update and patching process
- Improve their security posture by eliminating the need to remotely patch Windows endpoints and implement complex and costly third-party endpoint security products
- Avoid or defer endpoint hardware refresh expenditures for huge CAPEX savings, freeing up IT budget for more strategic uses



Minimizing Endpoint Management Complexity

IGEL OS was designed to function as the next-generation edge OS for cloud workspaces. It was designed to be managed remotely through seamless integration with IGEL's Universal Management Suite (UMS) software. Together, IGEL OS and UMS make it simple and efficient to manage up to tens of thousands of non-Windows endpoints from a single console. With IGEL, IT teams have precise, centralized control over how endpoints are configured and which features and customizations are available to end users.

Any required firmware updates are delivered in a fast and ultra-reliable manner using an efficient "buddy update" approach that reduces the impact of bandwidth bottlenecks. This includes on-premises devices, as well as remote devices, which are seamlessly provisioned and updated through the IGEL Cloud Gateway (ICG) function. Updates are performed with speed and reliability, and unlike most alternative approaches, the IGEL UMS always validates that updates have been completed.

IGEL's efficient and reliable endpoint management approach, when combined with VDI, remote desktop session hosts, and/or DaaS, eliminates the cost and inefficiency of traditional Windows PC imaging, patching, and updates. IT teams are immediately rewarded with much more time to get strategic work done while sleeping much better at night.

Don't Accidentally Replace Windows with Windows

When an organization shifts Windows desktops to the data center or cloud, its end users still need an endpoint of some kind to remotely access desktops. A common mistake that organizations make is replacing their Windows endpoints with "thin clients" running a "Windows Embedded" OS that are actually just new Windows machines in disguise. This approach completely undermines the value of moving Windows to the data center. Even if an operating system comes with a slightly different name, like Windows Embedded or Windows 10 IoT, it is still Windows. It still needs to be patched and secured in much the same way that a locally executing copy of Windows 10 would.

Achieving Superior Endpoint Security

Replacing the large and porous attack surface of Windows on endpoints with IGEL OS delivers immediate security benefits. Linux-based IGEL OS is dynamically configured by UMS with only the capabilities that are necessary per user, and trusted execution ensures the integrity of the endpoint at all times.

IGEL OS also includes support for a wide range of multi-factor authentication and single sign-on technologies, enabling support for general security best practices and industry-specific requirements. In addition, an optional secure browser can isolate high-risk web browsing activity from a user's primary computing activities in VDI, remote desktop session host, and DaaS environments.

IGEL OS also enables centrally executing Windows desktops to be delivered to unmanaged and/or highly mobile "bring your own device" (BYOD) endpoints through its unique UD Pocket deployment option. By giving users the ability to boot IGEL OS from a USB device no larger than a couple of paper clips, UD Pocket can securely deliver remote Windows desktops to unmanaged devices, wherever they may be, without exposing the environment to a potentially non-secure, user-managed operating system.

Whether you deploy IGEL OS on a managed or unmanaged device, all user session activity is performed remotely using compute resources and storage in the secure data center or cloud. No sensitive data is ever stored locally on the endpoint which vastly reduces the probability of costly and potentially embarrassing data breaches.

Fall in Love with Windows Again

Change is a constant in enterprise IT. Most experienced IT professionals understand the perils of radical changes to their mission-critical environments. But there is also risk in continuing processes and practices that are proven to be detrimental to IT efficiency, security, and end user satisfaction.

In fact, Microsoft itself is embracing the evolution of Windows into a centrally managed OS. The most notable example of this is the introduction of ***Windows Virtual Desktop*** (WVD), a Microsoft Azure-based DaaS offering that was released as a preview in early 2019. WVD offers Microsoft customers an easy migration path to Windows in the cloud, including simpler virtual desktop licensing and new DaaS-friendly features like multi-session Windows 10. It also provides Microsoft with an ongoing Windows licensing model as customers shift their end user computing resources to the cloud. Finally, according to IDC Linux has already surpassed Windows as the leading endpoint OS for thin clients, and this is not a trend that is likely to reverse with Linux adoption growing rapidly for VDI deployments and likely to be well received as DaaS offerings mature – see Gartner on WVD adoption.

Adopting VDI, remote desktop session hosts, or DaaS with a highly efficient and secure endpoint management approach from IGEL strikes an ideal balance. Users continue to enjoy a familiar Windows desktop experience and the proven application capability that comes along with it. IT teams become much more efficient. Unnecessary hardware expenses are avoided. And the organization's overall security posture can be vastly improved.

Download IGEL Workspace Edition to Get Started Today

Are you ready to reboot your relationship with Windows? **Download IGEL Workspace Edition for free** to experience the simplest, most cost-effective, and most secure way to deliver Windows desktops to your users.

Your IGEL Workspace Edition download will include 3 IGEL OS licenses and complete access to IGEL UMS for management, all of which are free to use for up to 90 days.