# WHITEPAPER

## How Windows 10 will be a Game Changer for Enterprises

By 42Gears Team

# Table of Contents

In modern enterprises, knowledge workers work on a multitude of devices – either company or employee-owned. Security and management become complicated with the addition of new devices, requiring the use of complex tools by IT teams. With Windows 10, enterprises can now experience streamlined device management and evolve from a PC-centric culture to modern enterprise architecture.

## Introduction

Over the years, **Microsoft Windows** has evolved from a PC OS (*Windows 3.1, Windows 95, 98*) to a LAN/Network OS (*Windows 3.11, Windows NT*) and then to an enterprise-centric OS (*Windows 10*). Currently, Windows is the dominant operating system in enterprises across the world, with many organizations upgrading to Windows 10 for security and privacy reasons. Especially with support for Windows 7 ending in 2020, enterprises will have to make this shift immediately. However, more importantly, organizations must embrace Windows 10 to offer the modern workforce a smooth enterprise mobility experience.

With Windows 10, organizations can effectively shift from a legacy infrastructure to a modern architecture that offers a highly secure and unified experience across multiple devices. Because Windows 10 converges separate Windows OS versions across devices onto a single platform, IT teams can effectively manage a variety of Windows devices in the organization. They can rely on a single **EMM (***Enterprise Mobility Management***)** platform to manage any Windows 10 device - PCs, tablets, phones - be they corporate or employee-owned. Taking a unified approach to PC management, Windows 10 is paving the way for a new era of enterprise mobility.

## How Windows Became the Dominant Operating System for Organizations

Perhaps the most significant reason for Windows' popularity is how user-friendly the operating system is. It features a smooth user interface that is easy to adjust. Because of its massive user base, Windows enjoys a broad ecosystem and supports a universe of software and hardware. This means that users can select software according to their need; most software programs are also built keeping Windows in mind. The latest release, Windows 10, features minimal bugs as highly trained professionals thoroughly test it.

As modern workers bring a growing number of devices to work, security and privacy of data take center stage. How do various operating systems fare? When it comes to **iOS**, security flaws have been detected

in iOS 10 recently. As for **Android**, its popularity makes it especially vulnerable to malicious attacks. Moreover, devices with the old OS don't feature the latest security updates.

When Windows 10 was released for PC last year, Microsoft immediately updated their mobile OS for security. It features device encryption for local content, secure access to resources, and strong authentication with multi-factor credentials. With a new feature **Device Guard**, only trusted applications are allowed to run on the device.

Windows 10 is a superior enterprise mobility option for organizations, especially since Windows continues to be the dominating operating system. Moving to Windows 10 from Windows 7 is a logical transition (on any number of devices) instead of adopting a different OS.

## Unified Endpoint Management with Windows 10

Rapidly evolving technology (and the deployment of diverse technology solutions over the years) has resulted in multiple challenges with mobility management, such as managing heterogeneous devices with diverse operating systems, ensuring security and compliance, and policy enforcement when company data is present on employee devices. In the past, organizations tried to solve such challenges using traditional client management tools (**CMT**) and Enterprise Mobility Management (**EMM**) tools. Because these tools were expensive and were designed when desktops and other devices were stationary and connected to the enterprise LAN users could not configure and upgrade their own devices.

The next phase in the evolution of mobility management, **Unified Endpoint Management** (**UEM**) combines the capabilities of **CMT** and **EMM**. It is a security and management architecture allowing enterprises to secure and manage data across operating systems easily. **Mobile Device Management** (**MDM**), **Mobile Application Management** (**MAM**), and **Mobile Content Management** (**MCM**), which are constituents of UEM — offer a secure and scalable architecture for modern organizations, prioritizing the user experience with advanced security and management capabilities.

In the past, enterprise IT architecture rested on Windows' desktop model, which essentially involved an open file system and OS kernel vulnerable to security threats. Devices were governed by a set of **Group Policy Objects** (**GPO**), which control a user's interaction with a system. However, this model functioned

well when all devices were connected to a LAN and lacked the flexibility a modern enterprise needs to manage intermittently connected devices.

With Windows 10, a unified approach to PC management is paving the way for a new era of enterprise computing. It converges separate OS versions on PCs, tablets, and phones onto a single platform managed by an **Enterprise Mobility Management** (**EMM**) provider. IT teams no longer need a variety of desktop management to manage legacy Windows PC clients.

With **BYOD** (**Bring Your Own Device**) now a norm in enterprises, mixing data between employee and corporate-owned devices presents a real risk to organizations. Windows 10 enables partitioning via **Digital Rights Management** (**DRM**) and encryption of all apps and data, such that corporate and personal data on each device is separate. With a UEM designed to work with it, Windows 10 can drive other critical management features such as:

- Passwords and encryption on downloaded data
- Policy-based updates
- Self-enrolment of new devices through Azure Active Directory
- Managing corporate provisioned apps separately from user installed apps
- Blocking access to dangerous websites

## Windows 10 – A Game Changer for Enterprise Mobility

In the past, IT teams employed separate tools to manage and secure these devices: EMM for mobile devices and CMT for PCs. UEM brings these siloed management systems together. With Windows 10, enterprises can effectively implement UEM and realize many efficiencies. Windows 10 is pioneering a new era of enterprise mobility. Apart from converging operating systems on different devices, Windows 10 is also converging UIs to give users a unified interface on every device. Perhaps the most crucial pillar that modern enterprise architecture will eventually rest on, Windows 10 prioritizes security and user experience. With a single OS and a unified set of MDM APIs, it truly empowers IT teams to manage devices securely.

This is how Windows 10 enables UEM:

**Improved employee experience (EX)** - A UEM platform must allow enterprises to enable critical business processes through easily accessible apps. Windows 10 makes the job of IT teams easier by simplifying access control and authentication, allowing users to manage multiple devices and troubleshoot problems on their own. IT teams can deploy UEM to grant employees access to enterprise data through granular policy control or through contextual authentication.

**Enhanced Security and Compliance** – Windows 10 offers a common baseline of device protections through mobile device management (MDM) profiles and a unified approach to prevent, detect, and respond to security threats on mobile and PC endpoints. Microsoft also limits the impact of malware and software exploits on its operating system, adding key features such as BitLocker, Windows Defender, and virtual smart cards.

**Backward compatibility** – Support for both traditional and modern management techniques is enabled by Windows 10. It allows users to move to cloud-based practices at a comfortable pace. Apart from traditional capabilities for PC and mobile such as patching, software distribution, and mobile OS containerization, it supports modern approaches that leverage MDM APIs, automation, and conditional access.

**Contextual identity and access management** - Conditional access and risk-based authentication (RBA) methods improve security and user experience. While most UEM providers support conditional access based on one or two criteria like device posture, Windows has a greater breadth and look at additional variables, such as location, network risk, and user behavior.

**Analytics for decision making** – Advanced UEM platforms such as Windows collect an abundance of device usage and behavioral data, analyzing it to highlight operational or security issues. Windows 10 can even suggest potential remediation actions or policy changes, such as blocking a compromised device from accessing the corporate network.

**Serves highly regulated needs** - Some industries have unique compliance needs that dictate which UEM solutions will be shortlisted. Windows 10 has multiple certifications that give it the flexibility for deployment in many environments.

## Embracing Windows 10 for a Modern Enterprise Architecture

Modern work is about transforming the business to drive productivity in exciting new ways. To do so, enterprises must migrate their device management policies from older EMM tools to modern UEM tools that oversee employee and corporate-owned devices in a unified, efficient manner.

Windows 10 comes with powerful UEM capabilities, allowing enterprises to deploy modern device management approaches. By offering a unified platform and a set of MDM APIs, it is a mighty weapon in the arsenal of modern enterprises. When deployed with the right UEM platform, Windows 10 can help organizations deliver unified device and security management. In doing so, enterprises can embark on a shift from ineffectual legacy infrastructure to productivity and security-focused modern enterprise architecture.

Organizations will need the latest Windows PC deployments to take advantage of its unified policy and configuration platforms. Those with large legacy Windows 7 deployments will require legacy PC life-cycle management and software distribution tools. However, support for Windows 7 is scheduled to end in 2020. Enterprises looking to streamline endpoint management must waste no time in adopting Windows 10 for its powerful UEM capabilities.

## References

1. The Forrester Wave™: Unified Endpoint Management, Q4 2018
2. Windows 10 Finally Delivers On Microsoft's Security Promises, Forrester, Oct 2017
3. https://www.computerworld.com/article/3199570/microsoft-windows/how-windows-10-changes-enterprise-mobility-management.html
4. https://blog.voiceplus.com.au/unified-endpoint-management-to-displace-mdm-and-cmt-says-gartner
5. https://www.qolcom.co.uk/wp-content/uploads/2018/10/Ultimate-UEM-Guide_US_EN_V4.pdf
6. https://www.parallels.com/blogs/ras/what-is-byod/
7. https://www.thewindowsclub.com/microsoft-windows-open-source-operating-systems
8. https://www.nextlogik.com/which-mobile-os-is-most-secure-ios-android-or-windows-slideshare/