Windows Information Protection (WIP) price, marketcap, chart, and fundamentals info

Microsoft Windows Information Protection Policy is effective in securing corporate data, Windows Information Protection does not overwhelm the user experience on the computer.

The need for data protection and security is growing, especially with the increasing number of frontline employees working remotely and the adoption of the BYOD trend (bring your own equipment to the company). work) quickly.

Windows laptops and desktops are very popular among businesses as well as personal use spaces. The security of company data on BYO PCs (Windows computers and laptops owned by employees) is at risk when these devices operate outside of the corporate network and infrastructure. This is where the Microsoft Windows Information Protection Policy comes into play in corporate data security.

In this article, let **TipsMake** learn more about Windows Information Protection (WIP) in protecting enterprise data.

What is Microsoft Windows Information Protection (WIP)?

Windows Information Protection is a set of policies that help organizations and technology groups secure corporate data on employee-owned devices, without impeding the overall user experience, which is the main reason. to apply Windows a lot in enterprise environments.

Microsoft Windows Information Protection (WIP), formerly Enterprise Data Protection (EDP) was introduced with the Windows 10 Anniversary Update in an effort to support and complement Windows 10's modern management system.

When determining the meaning of Windows Information Protection or WIP, it is often associated with the Windows desktops and laptops owned by the employee. But it's important to understand that Windows is a non-proprietary operating system, which means that Windows Information Protection (WIP) can also be used to secure corporate data on managed devices. company, 100% owned by the company.

Why use WIP - Windows Information Protection?

The number of personal Windows devices used for work is growing exponentially. While some organizations rely entirely on employees using their personal devices for work, many allow and depend on partial employee use - perhaps for work. Complete missions over the weekend, resolve emergencies or while working remotely.

The proliferation of employee-owned devices at work (either locally or remotely) has led to concerns about corporate data security. The growing risk of data accidentally being leaked through one of the many websites or applications employees visit on their PCs is the main reason businesses need Windows Information Protection. It also secures company data against employee's intentional breaches while accessing company data on devices on which they simultaneously have access to social media, sharing, and public cloud storage.

The advantage of the Windows Information Protection policy is that it does not overwhelm or overlap with the user experience on the computer. Unlike managed device, fully controlled by enterprise mobile management tool, where technology administrator blocks / restricts access to non-enterprise and unauthorized applications , Windows Information Protection policy works synchronously with control and privacy in employees' personal devices.

In summary, the benefits of WIP are:

1. Protecting corporate data on employees' devices
2. Ensure no changes to existing enterprise and application environments
3. Facilitates the original Windows user experience

Protect enterprise data with Windows Information Protection (WIP)

The main idea of ??Windows Information Protection is to not only protect corporate data on employees 'devices, but also divide corporate data and personal data on employees' devices, selectively apply key policies. data protection books for corporate data. This ensures that while corporate data is protected to maintain the confidentiality of the business, it does not affect employee personal data.

Let's see the impact of Windows Information Protection will be like offline!

Company data

Windows Information Protection adds corporate or identity tags to company data on employees' devices and automatically encrypts the data when it is downloaded, saved, or retrieved from predefined company sources. These resources include corporate applications, corporate networks, and protected business domains. Any data entering from these sources is encrypted with Windows Information Protection.

Technology administrators can define a Windows Information Protection policy and prevent corporate data from being copied, pasting it into personal applications / data. Corporate data files can only be accessed through protected applications and cannot be accessed from unprotected applications.

Personal data

Employee personal data remains unaffected when the Windows Information Protection policy is applied. When organizations disable the Windows Information Protection policy on deprecated devices or employee devices are no longer associated with the organization, the personal data remains the same. Even when performing remote wipe on these devices using MDM, personal data remains intact. This is one of the main advantages of Windows Information Protection.

Enlightened and Unenlightened Applications

We need to understand the two basic types of applications and the terminology used with Windows Information Protection. Two commonly mentioned types of applications related to Windows Information Protection are Enlightened and Unenlightened applications.

Enlightened application

These are the applications that can differentiate between corporate data and personal data. Microsoft Office 365 ProPlus applications such as MS Word, MS Excel, MS PowerPoint, MS OneNote, and MS Outlook are Enlightened applications.

Unenlightened application

These are applications that cannot differentiate between corporate data and personal data. Common examples of unenlightened apps are Gmail and the Google Chrome browser. Although technology administrators create a Windows Information Protection policy, they choose unenlightened applications as allowed applications, corporate data can be accessed through these applications.

The unenlightened app treats all data on the device as corporate data and encrypts it. This also includes employee personal data. The Windows Information Protection policy ensures that when an application has not been confirmed as necessary for business, data is always encrypted.

You should only allow enlightened applications in the WIP settings to ensure that only company data is encrypted. This addresses a general concern about how to protect customer information on Windows 10 or how to protect confidential information in Windows.

Managed application

These are applications that run on the device in an enterprise context. These are not employee-enabled personal applications and must be authorized by the technology administrator. These applications are also known as corporate apps or business apps.