Windows 10

Enforce acceptable use, prevent excessive data usage and eliminate content threats.

Complete your data policy management and content security
Windows devices are highly productive tools, but data costs can skyrocket. Background processes alone can consume 0.3GB per day, this is 6.5GB per month. Conferencing tools like Skype or Zoom can use 1-2GB/hr and with the ability to multitask it is easy to consume data. With more staff working outside the office than ever before businesses need control.

Cost control
Prevent bill shock with highly customizable and contextual controls. Create end user behavioral changes with real-time app notifications.

Acceptable use
Enforce acceptable behaviors and web usage with intelligent filtering rules. Ensure compliance by preventing access to unauthorised tools and websites.

Content security
90% of data breaches start with a phishing attack. Complement existing Windows 10 security solutions with additional content threat protection.

Unified management
Improve business flexibility and reduce administrative overhead by using a single portal to manage iOS, Android and Windows 10 devices. Understand data consumption with real-time analytics and detailed reporting across your entire mobile fleet.

Benefits
Cap and limit non-business data usage
Reduce roaming costs with controls per country
Apply policy based on connection type including: tethered, eSIM or Wi-Fi
Reduce legal exposure from illegal or unacceptable use
White or blacklisting cloud services and websites
Apply rules to any browser and application, including in-house programs
Prevent phishing attacks from any source
Protect browsing with DNS request encryption
Block commands from C&C servers

Copyright © 2020 Wandera
How it works

The on-device client works on any Windows 10 device, across any network connection and any application by employing the use multiple filtering layers simultaneously. The client monitors data usage, filters content, and applies other contextual policies. Wandera’s cloud based in-network intelligence communicates cost control and acceptable use policies, as well as the latest content security threat information. Administrators can easily create policies and do reporting with their security cloud portal.

Features

Flexible policies
Flexible application-based policies can be defined by admins on a by-network basis

Dynamic policy updates
Dynamically update policy based on the types of network in use and whether it is restricted or through a metered connection, such as an internal SIMs or external Mi-Fi

Extend policies
Extend policies or set usage caps based on: IP, carrier, country plus whether the device is connected in roaming or domestic model

Proxy & VPN ready
The product seamlessly co-exists with existing enterprise VPN or proxy settings

Flexible policies
Flexible application-based policies can be defined by admins on a by-network basis

Dynamic policy updates
Dynamically update policy based on the types of network in use and whether it is restricted or through a metered connection, such as an internal SIMs or external Mi-Fi

Extend policies
Extend policies or set usage caps based on: IP, carrier, country plus whether the device is connected in roaming or domestic model

Proxy & VPN ready
The product seamlessly co-exists with existing enterprise VPN or proxy settings

Global enterprises protected by Wandera

Trusted by the most security conscious enterprises.

The Wandera Security Cloud protects enterprises at the new edge, where data is in the cloud and users are remote. Unified security capabilities include threat protection, content filtering and zero-trust network access.

For more information, get in touch with one of our security experts at www.wandera.com/contact-us/