Supporting BYOD and Windows in a Remote Setting

IBM Security MaaS360 with Watson puts endpoint management concerns to rest

Remote work and work-from-home initiatives have already made a home in the enterprise and many analysts predict that this is not a blip.

In other words, there will continue to be an increase in personal devices adapted for work, corporate devices being treated as personal ones, and laptops acting as the central productivity hub for most employees.

In fact, in early 2020, a 40% jump in U.S. laptop and desktop sales was directly attributed to the massive shift towards remote work.

This growth prompts a few important questions:

- *How are you managing laptops that are not on the corporate network?*
- *How do you maintain security when personal devices are used for work* and *work devices are used for personal matters?*

Beyond window dressing: granular support for Windows devices

A client management tool (CMT) isn't going to patch devices that reside far outside of the company perimeter. IBM has the answer in MaaS360, a unified endpoint management (UEM) solution with API-based policies to secure Windows 10 endpoints, as well as native granular patch management and application distribution for those same devices or even those still running Windows 7.

No need for a VPN or enterprise network – as long as the devices have an IP address and an internet connection, enrollment can be completed and patches, updates, and applications can be distributed all over-the-air (OTA).

Additionally, MaaS360 Windows policy allows for the configuration of application blacklists and whitelists, Wi-Fi and VPN profiles; Windows Information Protection to secure and encrypt corporate applications and data; and an impressive list of other highly specific functions to support any laptop use case. Additionally, administrators can be alerted if a device does not meet organizational security standards (A/V installed, etc.). More information can be found here.

BYOD security: a new world for an established concept

To enforce BYOD policies and help maintain user productivity, MaaS360 offers a three-tiered approach to preserve the security of your corporate data at the network, user, device, application, and content level.

- ***Identity and access management (IAM)*** – single sign-on (SSO) and conditional access come standard and out-of-the-box for all MaaS360 administrators, ensuring only authorized users get access to appropriate resources.
- ***Mobile threat defense (MTD)*** – Through a partnership with leading MTD provider, Wandera, MaaS360 comes equipped to detect and remediate threats—from man-in-the-middle attacks when a user is on an improperly configured network to phishing, a risk vector present in 91% of all cyberattacks.
- ***Data loss prevention (DLP)*** – MaaS360 can separate corporate data from personal data in two ways: 1) via its own encrypted sandbox for company apps and resources, or 2) through manufacturer programs such as Android Enterprise. Through workplace policies, users can be blocked from copying or otherwise transporting data outside of this containerized space, and all corporate content can be wiped from a compromised device without touching personal data.

You may have more questions, and we welcome them. See MaaS360 in action today.

MaaS360 is a leader in UEM and prepared for any endpoint management pressures your organization may be facing. Request a demo here.

Please reach out to your IBM Security representative with any questions or to discuss further.

To see how else IBM Security is responding to modern demands on businesses, go here.