Mobile Device Management

The modern way of working – BYOD and consumerization

From managers compiling contracts while flying between continents to commuters checking their mails on the subway: Modern business is mobile. In order to keep up, businesses must provide mobile devices that create a comfortable digital workspace – wherever employees set up their office.

Two buzzwords immediately come to mind when it comes to enterprise mobile devices: **consumerization** and **BYOD** (Bring Your Own Device). The former describes the private use of enterprise devices, the latter the enterprise use of private devices. By allowing employees to use their own mobile devices for enterprise tasks, enterprises can significantly reduce their hardware investments. The catch: private devices are not enterprise-owned. Not only can security vulnerabilities on the device affect the enterprise network - productivity may also be reduced if employees are allowed to use any apps they want.

Benefits of defining a BYOD policy:

- A BYOD policy enables employees to be productive anywhere
- BYOD makes sure that users are familiar with the device
- Enterprises can save money by not having to invest in corporate-issued devices

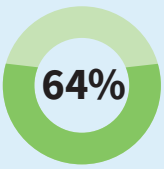
Risks for mobile devices:

- Cyber-attacks on mobile devices (malware, phishing)
- Device loss or theft, leading to data loss
- Productivity loss (excessive app usage)

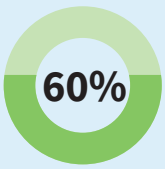
The same problems can occur on company-owned devices as well: when employees install insecure apps or use their phone or tablet for private matters, productivity and security alike can be reduced. Regardless of who owns the mobile device: when a smartphone or tablet gets misplaced or stolen, the company's data are in grave danger. Preying eyes can take advantage of a poor security strategy and view, copy or erase sensitive mails, photos and documents.

However, data loss and malware are not the only threats. When browsing the internet, phishing websites try to convince users to enter personal data into a seemingly innocuous form, stealing sensitive information in the process. Phishing and drive-by-downloads endanger smartphones and tablets the same way they do computers.

"It is essential to make the mobile office a safe space - while guaranteeing a high level of comfort."



of decision makers read their email on mobile devices



of employees access content from outside the office

Source: CyberEdge 2016 Cyberthreat Defense Report

new Android malware instances are discovered every day

Source: G DATA CyberDefense AG

Mobile devices are consistently perceived as the weakest link of enterprise infrastructure

Source: IBM

Maximal security – minimal administrative effort

A management policy enables administrators to enjoy the benefits of the modern way of working while ensuring security. Equipping all enterprise mobile devices with security software has never been easier. Using a unified interface for all aspects of mobile device management maximizes efficiency and reduces deployment and management costs. If the company grows, so does the number of mobile devices - every new smartphone or tablet can easily be incorporated into the mobile device management (MDM). App and policy deployment are centrally managed. Applying security policies and integrating patches into the system becomes a matter of only a few clicks. The communication with mobile devices can be established via an internet connection, cloud-based push messages or SMS. A permanent connection between devices and server is not necessary: devices comply with server policies even if there is no contact to the server.

Mobile Device Management protects mobile devices at all times, even outside the enterprise environment.

What can G DATA do for you?

Mobile Device Management (MDM) is a matter of trust. We assist you with a secure management solution, based on strict German data security laws:

- **Information:** With our clear administration interface administrators can easily keep track of all devices used on the company's network.
- **Deployment:** Administrators can easily deploy software on any mobile device on the network.
- **Security:** The Anti-Theft module makes it simple to track a lost or stolen device. To protect sensitive data, it is possible to remotely wipe the device.
- **Compliance:** Employees get access only to the apps and data they need.

How to get G DATA MDM?

For every need, there is the perfect way to deploy MDM:

- G DATA Mobile Internet Security and G DATA Action Center: Our hosted MDM solution G DATA ActionCenter is ideal for businesses with only a small number of devices. Without any local hardware or software deployment, administrators can easily register and manage mobile devices.
- All G DATA business solutions, such as G DATA Endpoint Protection, include Mobile Device Management. This allows administrators to get a holistic view of all network security aspects, including their mobile devices.
- G DATA Managed Endpoint Security: By using a hosted G DATA business solution, administrators can take advantage of the know-how and infrastructure of a G DATA partner, eliminating the need for hardware investments and building and maintaining expertise.
- G DATA Managed Endpoint Security powered by Microsoft Azure: Our Azure-hosted solution supports the development of new platform-based business models for G DATA partners, allowing them to easily offer their customers scalable infrastructure, high availability and flexibility.

What does MDM do?

- ☑ Keep track of mobile devices
- ☑ Streamline deployment
- ☑ Unified administration
- ☑ Anti-malware/Anti-phishing
- ☑ Theft detection
- ☑ GPS location
- ☑ Locking/wiping devices
- ☑ Productivity management
- ☑ Enterprise policy management
- ☑ Apps blacklisting/whitelisting
- ☑ Corporate contact management (managed phone book)

Administrators should choose a device management solution that integrates with existing management structures in order to minimize their workload. Ideally, mobile devices can be managed using the same kind of interface and reporting capabilities that are available for other device types in the network, in order to support an integrated workflow and consistent configuration.

New company-managed devices should always be equipped with mobile device management features before being handed over to employees. BYOD devices should be denied access to the corporate network and its resources until they have been equipped with mobile device management. Optionally, a guest network can be used for devices that do not meet the requirements or are used by visitors.

More information:

www.gdatasoftware.com

sales@gdata.de

G DATA | SIMPLY SECURE