White Paper

Security

Balancing Mobile Security and User Productivity

MICRO FOCUS

Table of Contents

It's your job to protect corporate data. It's your users' job to get their work done wherever they happen to be on whatever device they happen to be using. Too often those goals seem to be at cross-purposes and you get caught in the middle of the conflict, especially when it comes to the use and security of mobile devices.

Mobile Device Management (MDM) solutions do a great job of giving you the control you need to protect the corporate data that resides on and flows in and out of those devices. Unfortunately, that level of control can feel overly intrusive to users and can even impact their productivity and experience using their mobile devices. That might be okay when it comes to company-issued devices since there's an inherent expectation that you can secure and manage those devices in whatever manner you deem necessary. But in bring-your-own-device (BYOD) scenarios, users will often push back against that level of control and simply choose not to allow you to secure their smartphone or tablet.

In a BYOD world, how do you find the balance between keeping your corporate data safe and keeping your mobile users happy and productive? The answer lies with ZENworks® Mobile Workspace from Micro Focus®, a Mobile Application Management (MAM) solution that delivers the right balance between mobile security and mobile usability.

Keeping Corporate Data Safe and Mobile Users Happy

ZENworks Mobile Workspace is a simple, highly secure MAM solution for organizations that want to secure and simplify mobile device use for their internal or external workforce. It lets users access your sensitive corporate data from within a mobile workspace that uses unique, independent security mechanisms that you control. That workspace exists on the device within a secure encrypted container that provides a separate, fortified location for corporate email, calendars, contacts, apps, documents, and pictures.

As a result, your business assets stay protected—regardless of the configuration or ownership of the device. Plus, your users can keep their mobile habits, apps, and privacy without having to deal with frustrating device restrictions.

Comparing Mobile Security Use Case Outcomes

MDM solutions allow administrators to implement strong policies and restrictions to keep corporate data safe on company-issued smartphones and tablets. Such policies and restrictions might include requiring strong passcodes, expiring passcodes after a certain period of time, wiping device data after multiple incorrect passcode attempts, disabling voice commands, restricting camera use, blocking YouTube and social media apps, preventing copy and paste of email contacts, and many more. These policies make

sense for the company-owned devices your users use. But implementing them on your users' personal devices will disrupt your users' way of life and simply drive them crazy, causing large-scale resistance against your security mandates.

ZENworks Mobile Workspace also allows you to implement strong security controls and policies, but they only affect the secure isolated workspace container that the solution creates on your users' mobile devices. That way, users don't experience negative impacts on their personal device use and you still control the security of your corporate data.

To better understand the benefits that ZENworks Mobile Workspace offers your BYOD initiatives, it's helpful to compare the different outcomes between a ZENworks Mobile Workspace implementation and an MDM implementation in different use case scenarios.

Simple Tasks Need to Stay Simple

Even minor inconveniences created by MDM policies can cause big headaches for your users of personal-owned devices. While driving their car during or after work hours, users might want to change the music playing on their phone or activate GPS navigation. Asking Siri or Google for help with these small tasks becomes impossible if your MDM policy disables voice commands. So, they wait for a stoplight to unlock the device with their passcode. But instead of having an easy 4-numeral pin, they have to enter a 6 or 8-digit strong alphanumeric code that takes a little more focus and effort to enter. By the time they manage to punch in the right code, the light turns green and they still can't change their music playlist or turn on their GPS without putting themselves or others in danger.

ZENworks Mobile Workspace eliminates this inconvenience since corporate security policies only apply to the secure corporate container that the solution creates on the device. No more blocking the device's voice commands. Corporate can't even require a passcode to unlock users' devices. But corporate can still employ strong measures for access to its assets stored in the containerized workspace by requiring a strong alphanumeric passcode to access that workspace.

Corporate Policies Shouldn't Jeopardize Personal Data

Certain MDM policies can create even more severe disruptions for your users. Even though requiring strong passcodes on corporate-owned devices is a common best practice, it can be disastrous on user-owned devices when combined with other policies.

A real-life example of this occurred on a couple's sightseeing trip in Europe. After two days of taking pictures on his personal device, the user experienced problems logging into his phone. Moisture on the screen from an evening rain caused a few failed attempts with fingerprint recognition. Next, he had failed attempts entering his 6-digit passcode. It wasn't until after the final and fatal attempt that he remembered that corporate had just recently forced a change to a stronger 8-digit passcode. But by that time it was too late. The corporate policy to wipe device storage after six failed attempts had already kicked in and the couple had lost all their once-in-a-lifetime sightseeing pictures from the last two days.

ZENworks Mobile Workspace is a simple, highly secure MAM solution for organizations that want to secure and simplify mobile device use for their internal or external workforce.

This sightseeing disaster could have been easily averted with ZENworks Mobile Workspace. Policies to wipe data only apply to the secure workspace container. So, if a mobile device gets lost or stolen, you can still protect your corporate data and wipe it clean after a predetermined number of failed attempts. But only the data within the container is wiped. So, if the rightful owner of the device gets the workspace container's passcode wrong, causing a data wipe, their own personal data outside the container will remain intact.

No More VPN Chaos

Attempting to access corporate data over the web isn't always easy for mobile users. Maybe they receive an email from a team leader to a look at certain documents stored on the innerweb. The users click on the link in the email, but they get an error message preventing them from accessing the web page. Multiple clicks on the link return the same fruitless and frustrating results until they remember that they have to use the corporate VPN to access that particular corporate site.

Trying to remember when they do or don't have to use the VPN might not be that big of a deal for your mobile users, but it can be a bigger deal for you if they forget to turn it off, which happens frequently. Once they click the email link to get to the files they needed, they often go back to whatever they were doing before. Maybe it's back to social media, online shopping, or streaming a movie, with all that traffic going through your corporate VPN and using up network bandwidth. Depending on your network infrastructure—such as if you happen to be using leased lines—running all that personal traffic through your VPNs could create some unwanted costs for your organization. Depending on your location, it even could inadvertently put your organization in violation of local regulations that prohibit you from monitoring personal browsing data.

Those VPN related problems go away with ZENworks Mobile Workspace. It comes with its own secure, encrypted browser that eliminates the need to use a corporate VPN. When using the workspace browser, all user traffic flows through a secure gateway. That makes it easy for your users to get secure and easy access to your corporate content from the workspace browser. It also lets you control what websites your users can access from within the secure Mobile Workspace.

Safeguarding Photos with Sensitive IP

Cameras have become an indispensable aspect of mobile devices. The ease at which you can quickly take pictures with your smartphone or tablet has dramatically expanded the ways we use cameras. Did you forget your shopping list at home? No, problem. Have one of your kids take a picture of it and text it to you. Can't ever seem to remember the class schedule at the gym? Take a picture of it. Don't want to lose any of the details from your business planning meeting, take a picture of the whiteboard.

The quick click snapshot of the whiteboard has become a frequent occurrence in the corporate world, but it can also become a security liability if those snapshots stored on users' mobile devices contain any confidential information. The inclusion of a secure camera in ZENworks Mobile Workspace can help make sure those sensitive photos get stored within the devices' secure corporate workspace rather than in personal storage.

Staying Productive and Secure

Some of your organization's most valuable intellectual property roams through the emails, contacts, and calendars on your mobile devices. Those also happen to be the tools most vital to the productivity of your mobile users. Keeping that IP safe in a BYOD world can be a struggle, but not with ZENworks Mobile Workspace. It makes it easy by making the secure and encrypted workspace container home to corporate email, corporate contact lists, and the corporate calendar with its schedule of employee, client, and partner meetings.

Certain MDM policies can create even more severe disruptions for your users. Even though requiring strong passcodes on corporate-own devices is a common best practice, it can be disastrous on user-owned devices when combined with other policies.

Securing Mobile User Productivity

Users want the freedom to use their personal mobile devices the way they want. ZENworks Mobile Workspace gives them that freedom while giving you the mobile security you need. You keep users happy with no disruptions to their personal use of their mobile devices. And you keep corporate assets safe with controls on how users interact with corporate resources.

SECURE MOBILE PRODUCTIVITY

- **Email, calendar, and contacts**—Enable mobile users to conveniently access corporate Office 365, Exchange, GroupWise® or Lotus Notes email accounts, calendars and contact information from within secure workspace container on their mobile devices.
- **Local document access**—Provide convenient and secure access to a repository of corporate files and messages within the workspace.
- **Network repository access**—Provide convenient and secure access to corporate documents on SharePoint, CMIS, or CIFS repositories.
- **PIM task management**—Let users easily create, edit, and delete tasks from their Exchange, GroupWise, and Notes task lists.
- **Document viewing**—Allow users to review Office and PDF files from their email or document repository with the built-in viewer.
- **Intranet and internet browsing**—Without the need for a VPN, automatically secure user access to all websites through the workspace browser's secure gateway, including your corporate intranet and other websites you allow.
- **Push notifications**—Alert users when they have new emails, calendar alerts, and tasks with NPNS and GCM push notifications.

Users want the freedom to use their personal mobile devices the way they want. ZENworks Mobile Workspace gives them that freedom while giving you the mobile security you need.

Simplifying and Strengthening Mobile Security

It's a given that users want the freedom to use their mobile devices the way they want, but that can't override your responsibility to make sure corporate data remains protected. Rather, it simply makes your job that much harder to do. ZENworks Mobile Workspace is all about making it easier for you to do your job, while at the same time keeping your users productive and happy. It does that by making sure personal and corporate workspaces on mobile devices not only stay separate, but that users retain control of personal mobile use and workspaces, while you control corporate mobile use and workspaces.

To help you more easily secure and stay in control of your corporate mobile environment, ZENworks Mobile Workspace gives you the following:

SIMPLIFIED MANAGEMENT

- **Centralized workspace management**—Centrally manage the resources and capabilities available to users within their mobile devices' corporate workspaces.
- **Web-based administration**—Manage devices from anywhere with the web-based management console.
- **Easy user and group management**—Leverage current users, passwords, and groups from within your existing corporate directory (Active Directory or eDirectory™).
- **Self-service apps management**—Allow users to download corporate-approved apps from a simple landing page that eliminates the need for intrusive management agents.
- **Self-service enrollment**—Using over-the-air configuration, let users enroll their devices with the workspace server and gain access with nothing more than an email that includes the enrollment URL.
- **Controlled time of content to sync**—End users and administrators control time of content to sync.
- **Multi-tenant architecture**—Support multiple organizations or departments from a single server with our multi-tenant domain-based architecture.

STRONG, INDEPENDENT SECURITY

- **Workspace-specific security controls—**ZENworks Mobile Workspace uses its own keystore and encryption to remove potential vulnerabilities and to allow you to enforce workspace policies that secure corporate data without having to control the entire device.
- **Sensitive data isolation—**Isolate and encrypt all corporate data in the secure container workspace to keep it safe and secure.
- **Dedicated data-at-rest encryption—**Rely on dedicated, banking-grade encryption for local workspace storage, rather than the device's underlying OS encryption.
- **Data in-transit protection**—Encrypt all communication between the agent and the server at the data level and over the HTTPS transport.

- **Strong two-factor authentication**—Use Java Authentication and Authorization Service (JAAS) to implement two-factor authentication with access management systems such as NetIQ® Access Manager™ and Active Directory Federation Services (ADFS).
- **Secure user activation**—If desired, require users to request access or require an administrator to manually enable user enrollment.
- **Device integrity control**—Enforce rules that control access to the workspace based on hours and days, location, jailbreak status, and more.

POLICY ENFORCED THREAT PREVENTION

- **Data sharing controls—**Manage and control what data users can share outside of the workspace, including restricting sharing of screenshots, calendars, and contacts, as well as not allowing copying from and pasting outside the container.
- **Cache controls**—In addition to securing the local data store with banking-grade encryption, control whether the workspace allows offline access or only allows online access.
- **Remote workspace wipe**—To prevent data theft on lost devices, you can wipe a device's workspace contents if an employee loses a device or leaves the company.
- **Jailbreak access control**—Restrict access to the workspace if a user jailbreaks his or her device.

BETTER GROUPWISE INTEGRATION

- **Simple GroupWise access**—Eliminate the need for GroupWise Mobility Server in providing secure mobile access to GroupWise.
- **Expansive GroupWise capabilities**—Remove ActiveSync limitations by interacting directly with GroupWise through the Simple Object Access Protocol (SOAP).

It's a given that users want the freedom to use their mobile devices the way they want, but that can't override your responsibility to make sure corporate data remains protected.

Bringing Mobile Security Management Closer to UEM

Helping you secure mobile devices is a critical aspect of our Unified Endpoint Management (UEM) vision. At Micro Focus, our goal is to deliver tightly integrated tools that enable you to easily manage all your devices in a similar manner—tools that work together to simplify, streamline, and automate every part of your workspace infrastructure. ZENworks Mobile Workspace represents a major step in delivering on the promises of UEM. As we work to further enhance ZENworks Mobile Workspace and tie it into ZENworks Configuration Management, the benefits of complete UEM will come even closer within your reach.

ZENworks Mobile Workspace enables you to take advantage of BYOD cost benefits, give users secure access to corporate resources and data in a safe and easy fashion, and boost the productivity for your mobile users and IT personnel.

Strike the Right Balance

Micro Focus ZENworks Mobile Workspace lets you strike the balance between mobile security and usability. It enables you to keep your corporate assets safe without implementing controls that negatively impact users' personal use of their mobile devices. That makes it easier for you to roll out a BYOD strategy since users know their personal habits and behaviors in using their mobile devices don't need to change. ZENworks Mobile Workspace enables you to take advantage of BYOD cost benefits, give users secure access to corporate resources and data in a safe and easy fashion, and boost the productivity for your mobile users and IT personnel.

Learn more about how ZENworks Mobile Workspace delivers the right balance between mobile security and mobile usability.

Learn More At
www.microfocus.com/products/zenworks/mobile-workspace/

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com

162-000141-001 | M | 03/18 | © 2018 Micro Focus. All rights reserved. Micro Focus, the Micro Focus logo, eDirectory, GroupWise, and ZENworks, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. NetIQ and Access Manager are trademarks or registered trademarks of NetIQ Corporation in the USA. All other marks are the property of their respective owners.