10 TIPS
TO IMPROVE MOBILE DEVICE AND ENDPOINT SECURITY

wireless watchdogs
A DATAPRISE COMPANY

Mobile devices offer a world of benefits to employees, but chief among them is the ability for employees to stay connected to their work without being tethered to a desk. Yet as this use spikes, the need for bolstered security to defend against external threats rises with it. This report examines what's at stake and offers security leaders a lens into developing an airtight endpoint management and mobile device security program.

Why is mobile device security so important?

Two words, "Extremely Concerned." This is how 71% of CEOs answered a recent study when asked about cyber threats and rightfully so when you consider:

- The average data breach costs $3.86 million.
- 70% of successful breaches start at the endpoint and around 70 million mobile devices are lost every year with only 7% recovered.
- 40% of all CEOs see mobile device security as their biggest IT security threat.

The last bullet is fascinating, especially when you consider that investment in mobile device security is dwarfed by investment in their less portable counterparts. While we are starting to see a shift in how budgets are spent, much of the focus remains on traditional devices.

Leveling the Endpoint & Mobile Device Security Field

Here are 10 actionable steps to help secure your mobile devices and endpoints.

#1: Plan and build a mobile device policy that can be enforced through MDM

Mobile device management (MDM) is sometimes thought of as another security tool, but it might serve CXOs better to think of it as a policy enforcement tool. You set the rules for what is acceptable and what is not, and these parameters make it easier for employees to slip into better habits. It also takes considerable responsibility off individual employees to stay on top of corporate security.

#2: Enroll ALL mobile devices – no exceptions

This is another way of saying that all endpoints matter. In general, there are two major faux pas that companies are guilty of making:

- BYOD: Bring your own device is popular for businesses because it cuts down on the amount of equipment they must buy. The reality, though, is that every device has its own quirks and characteristics.
- Executive: The more responsibilities someone has in a company, the more likely they are to be exempt from standard protocol. This is a mistake that can cost a business more than they're willing to spend.

Even the most carefully planned MDM platform will fail if select devices aren't enrolled in the program. Employees at every level might be used to breaking the rules, but organizations play with fire every time someone makes an exception.

#3: Only use industry-leading MDM/UEM platform solutions

Unified Endpoint Management (UEM) includes all endpoints, which can be useful for a company that wants to bring every device under a comprehensive security umbrella. This tip refers to industry leaders' ability to evolve faster than competitors, making it more likely you'll stop threats long before they have a chance to reach a device.

If you're using an UEM or MDM platform that's both vetted and well-known, you're far less likely to experience a breach.

#4: Leverage tools for enrollment

Apple Business Manager, Android Enterprise Enrollment, Microsoft Autopilot: these tools are designed to streamline the platform enrollment process for users. Ultimately, it makes for a more positive experience for an employee while still protecting the organization. Bypassing the laborious setup process for anyone can be a huge weight off their backs. It's an incredibly simple way to get people up and running without the endless back and forth.

#5: Device encryption – screen unlock passwords and disk encryption with PC/MAC

Encryption is a key component of any MDM or UEM platform, one that can be easily overlooked until it's too late. This tip encourages companies to set rules that ensure these steps are taken without delay. Whether it's prompting a passcode change every 90 days or the encryption of the latest data on a disk, it can make a big difference. By taking the responsibility off the user, it makes it that much easier to ensure that all endpoints are properly secured.

It is worth noting that lost mobile devices are a common exclusion on cybersecurity insurance however some insurance companies will modify this policy if the devices are encrypted.

Benefits of Mobile Device Management

- ✔ Centralized remote policy distribution
- ✔ Remote management with no manual configurations after initial enrollment
- ✔ System structure allows easy application updates and content distribution
- ✔ Helpdesk with expert knowledge
- ✔ Improved Security
- ✔ Simplified application management
- ✔ Streamlined communications
- ✔ Easy to follow process across all markets

#6: Simple Mobile Device Security Dos and Don'ts

The lines between professional and personal technology have never been more blurred. And while this might cause a few ruffled feathers, it's one that needs to be addressed:

- Don't allow employees to use Apple IDs or Gmail accounts for any corporate-owned devices.
- Do use Managed Apple IDs, Federation, and Android Enterprise Enrollment.

This tip essentially boils down to ownership. What does the company have access to when an employee leaves the organization? Simultaneously using capabilities like federation and banning personal accounts on corporate-owned devices means that a company can still control their information regardless of what happens to an individual employee.

#7: Centrally manage applications, including email, on mobile devices

Centrally managed applications are something like a secret weapon for security sticklers. If an employee wants to have a feature on their device, such as email, then they'll automatically have to take part in the MDM or UEM platform the company has provided. Once a device is enrolled, the critical functions can be pushed immediately to the employee based on their role. It's an added layer of mobile device security, of course, but it also ensures employees get all the tools they need to do their jobs.

#8: Encourage use of corporate repositories for backup

It's not uncommon for employees to back up their information to personal cloud accounts, a fact that leaves untold troves of data vulnerable. Encouraging everyone to backup to a corporate repository keeps your data under the right lock and key. This is a simple solution that can have strong results for any organization.

#9: Regularly push out OS updates to user endpoints

Organizations often can't force employees to update their devices, which means that there are plenty of people out there running older versions of their OS. However, constant and consistent prompts to update an endpoint (in combination with regular reporting) has been shown to vastly increase compliance. As with many of the other mobile device security points listed here, it applies to all devices.

#10: Deploy antivirus software / threat detection software

Organizations today are known to make big investments in their cybersecurity but make major mistakes on the execution. Antivirus and threat detection software can be centrally managed, allowing employers to push the program to all endpoints and ensure all threats are monitored. An endpoint detection and response (EDR) software can keep mobile devices every bit as protected as their other corporate device counterparts including servers, laptops and desktops.

Executive Summary

There are three key takeaways to keep in mind from these mobile device security tips:

- If you haven't deployed an MDM or UEM platform, it needs to be done today.
- If you do have an MDM or UEM platform, make sure that it's used to its full capabilities.
- Merge your security worlds together so you get the best possible protection of all endpoints.

Wireless Watchdogs and Dataprise are known for helping companies deploy tools that work for their employees. Our team can also assess your current protection to see if and where it can be adjusted. By both empowering users and protecting ALL endpoints, we've found that we can have the best all-around impact on corporate mobile device security.

About Wireless Watchdogs

Whether you're looking for managed mobility services, MDM, UEM, or IoT device management, having all of the facts is critical when it comes to deciding how to manage all of the deployed devices across your organization. With twenty years of experience in managing all aspects of mobility for companies large and small, Wireless Watchdogs, a Dataprise company, has a depth of knowledge that's unmatched -- and we're happy to share that knowledge with you.

Learn More

www.wirelesswatchdogs.com

sales@wirelesswatchdogs.com

(310) 943.3400