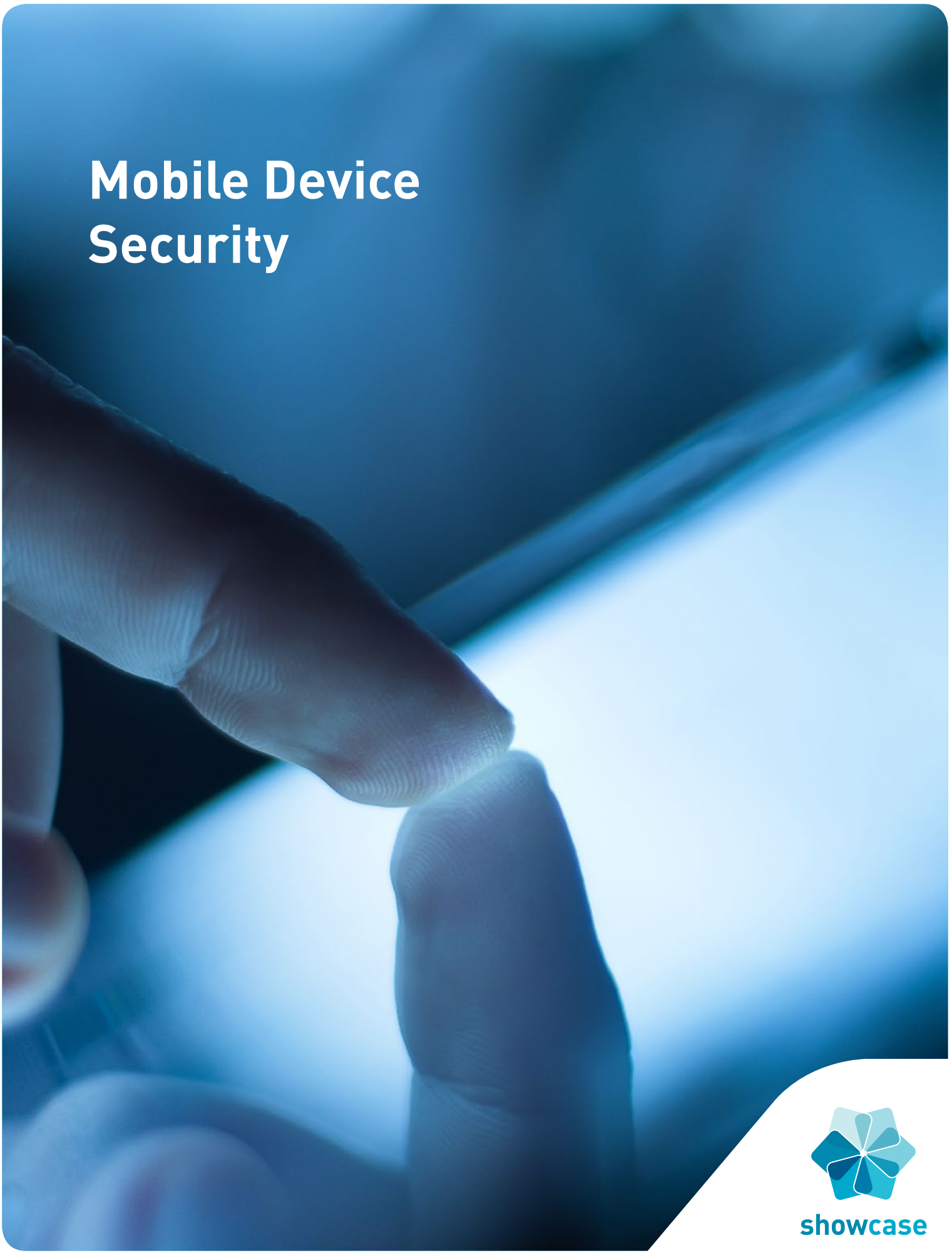
# Mobile Device Security



showcase

# Through no fault of your own, your company has become 2-3x more exposed to data breaches and loss. How? Through mobile devices.

The same tools that are enhancing the way your employees work, communicate, and sell are also revealing new vulnerabilities in your data's security. Every network visited, email opened, and byte of company data stored on these devices constitutes another risk.

And what if the device is the property of your employee? Is this 'free' asset worth the potential liability? Is it subject to your mobile security policy?

## In the next few minutes, we'll explore:

- The foundations of a smart mobile security policy that accounts for the everyday needs of your sales team
- The pros, cons, and tradeoffs of BYOD (Bring Your Own Device)
- The reasons why remotely wiping the device's memory is no silver bullet

Let's review your options before an employee's mobile device strays away.

showcase

# BUILDING BLOCKS

## The smart way to equip your sales teams

**According to a survey by Kensington, in 2010 52% of stolen laptops disappeared in office settings, 24% at conferences, 13% in meeting rooms, and 6% from cars. Given their size and utility, tablets are at even greater risk of theft.**

Help your staff keep their devices and privileges with these suggestions.

### Trust your gut

Though the devices have changed, basic hacker tactics haven't. Following unsolicited links, downloading apps or games from untrusted sites, or opening SPAM SMS/text messages from strangers may infect your device. **If you don't trust the source, don't trust the content.**

### Record serial numbers

For any chance of recovering a stolen device, you'll need to prove ownership with the serial number. Take a screenshot of the device's unique information, and store the image in several safe places.

**iOS devices:**
***Find it: Settings > About > Carrier, Model, Serial Number, IMEI, ICCID.***

***Record it:*** Press the Home and Top buttons at the same time.

**Android devices:**
***Find it: Settings > About Phone > Status > Serial Number***

***Record it:***
If You're Running Ice Cream Sandwich (4.0) and Above: ***Press and hold the Volume Down and Power buttons at the same time for a few seconds.***
If You're Running Android 2.3 and Below: ***It varies by device. Yours may have a built-in shortcut, or you may need to install a screenshot app.***

showcase

## Update regularly Backup automatically

Updates to your device's operating system include patches to exploitable weak points in its security. Make it a habit to back up your files whenever you install a software update.

Even better, back up data from mobile devices more frequently, preferably automatically, onto the cloud.

## Encrypt local data

Customer data is a token of their trust. Never leave it exposed on your tablet after a presentation. Save it, and close the program where you entered their information.

For that matter, devices should be logged off networks, email or websites after use. Imagine how delighted a thief would be if your stolen device granted him access to these password-protected spaces.

Have an automatic timeout in case employees forget to log out manually.

## Wifi and Restrooms: Question the public ones

Since anyone can log on to a public wifi network, anyone could access what you're transmitting. Choose only hotspots that use WPA2 security, which is stronger than the older WPA and WEP. You'll see a network's security system in the box where you enter the login password.

Even then, only trust sensitive information on encrypted sites: look for the **"S"** in the browser between "http" and the colon. E.g. **https://app.showcaseworkshop.com**

For sales people regularly on the road, Virtual Private Network software is a must-have. VPN software wraps your data in an encrypted shell for its trip across the Internet. Many large companies already use VPN to transmit sensitive data over public wifi networks.

The easiest way to secure your mobile device: disconnect it from the Internet.

## Use smart passcodes

Start with a phrase that has personal meaning and is easy to remember. Take the initials of each word in that phrase, convert some of those letters into analogous numbers, and capitalize at least one letter. For good measure, add a non-alphanumerical symbol.

E.g. "Make your own presentation app in minutes" would become MYOPAIM. The resulting passcode (including the period): MyØpa1m.

> **"The easiest way to secure your mobile device: disconnect it from the Internet.**

showcase

## Apps: Another Trojan Horse

Adding an app to your device gives it permission to access certain private information. Free apps generate revenue with popup banners and other forms of advertising. Though the app's developer may be a reputable company, the popup ad banners that fund the app may come from third-party sources whose security may be less robust. Upon downloading the app, malware can corrupt your system and betray your data.

Researchers with the Android Malware Genome Project found more malware families in July 2011 than they'd collected in the final four months of 2010.

By limiting the types of apps that can be loaded onto your device, you'll minimize your exposure. Stick to approved app stores, such as iTunes, Blackberry App World and Google Play.

## Jailbreaking: Resist the Temptation

In an effort to alter their tablets' performance, sophisticated users may intentionally hack their own devices.

'Jailbreaking' iOS devices (aka 'rooting' Android devices) voids the warranty, and increases vulnerability to malware. This has been likened to buying a sophisticated alarm system for your house, and then leaving all the doors and windows open.

### The gates of Troy

Jailbreaking allows users to install apps that don't adhere to the established requirements of the premiere app stores. These requirements help protect users, such as requesting permission before an app can use your location. Circumventing these protections makes users more vulnerable to malicious applications.

### World's costliest paperweight

If something goes wrong in the jailbreaking process, it's possible to completely "brick" the device, rendering it useless.

It's easy enough to prohibit jailbreaking on company-owned devices, but what if the employee paid for the device?

**"If something goes wrong in the jailbreaking process, it's possible to completely "brick" the device, rendering it useless.**

showcase

# BYOD
# 'Bring Your Own Device' blurs the line

## If your company didn't buy the device, can you decide how it's used?

Some salespeople aren't waiting for their employers to invest in mobile devices. They're bringing their personal tablets to work. It's convenient for employees. It's one less cost for businesses. And it's a gray area for data security.

### The Allure: Cheaper and Better

Companies are letting their employees' personal devices onto corporate networks for a variety of reasons:

- **No up-front cost.** Organizations can save on hardware while taking advantage of newer technology faster.
- **More convenient for employees.** They have fewer devices to manage, and more control to choose the technology that best meets their needs.
- **Greater ownership.** Employees are more likely to take better care of their own devices, and organizations often see an increase in productivity.

### The Catch: Liability and Ambiguity

IT departments are reluctant to let employees' personal devices onto corporate networks:

- Personal devices multiply the number of opportunities for proprietary information to meander out of the safe boundaries of the company's network, and for malware to find its way in.
- Employees may balk at your company attempting to impose a data security policy on a device it didn't pay for: i.e "If you want control over my device, you'll have to buy it for me."

showcase

## Compromise

Each side will each need to make concessions for a productive mobile worker program. The agreement should clearly state who is responsible for what. Some organizations require an actual signature to make sure the staff member understands the program.

If the device is going to have access to your company's network, it should be tagged, tracked, logged and backed up.

Since this could affect employees' personal data and privacy, consult your legal advisors before implementing the program.

## Moderate Support

Keep a list of acceptable devices, and declare how long your company will support them.

After the time limit has passed, the user needs to assume responsibility. Gartner offers an alternative to limiting support time: "best effort support." In this scenario, IT will do their best to fix an employee-owned device, but at the end of the day, the device is the user's responsibility.

Encourage staff to help one another with their devices. Provide a space on your company's intranet where they can share experiences, applications and best practices.

Require employees to insure their personal devices. Transfer the risk of losing an expensive device to the insurance company.

**"If the device is going to have access to your company's network, it should be tagged, tracked, logged and backed up.**

showcase

# REMOTE WIPE

# The nuclear option is no silver bullet

**Remote wiping sounds like an appealing fail-safe. If a mobile device is lost or stolen, and proprietary information could be compromised, you can remotely command the device to wipe all of its data.**

## The reality isn't quite so simple

The storage technology that most mobile devices use these days –flash drives- and their integration with a host of embedded controllers present their own set of challenges. Deleting all of the files on a flash-based device is more complicated than simply formatting the drive.

Jailbreaking further muddies the water. To wipe these devices remotely, you first have to detect that they have been modified. For most remote operating systems, the API calls that can be queried about jailbreak status are often the first calls changed by the jailbreak.

Even iOS devices are at risk, since Apple removed a jailbreak detection API in December, 2010. The most common workarounds depend upon tracking the location of users when they switch between cell towers. Even if the technology were to work reliably, many users may raise their civil right not to be tracked by their employers at all hours.

**Deleting all of the files on a flash-based device is more complicated than simply formatting the drive.**

showcase

# SHOWCASE

## Total Security and Complete Convenience For Tablet-Based Sales.

Showcase allows you to control who sees your sales and marketing materials, and how. As a complete collateral management system and sales toolkit, it's a mobile sales platform for tablet devices such as iPad, Samsung Galaxy, and Amazon Kindle Fire.

Our software-as-a-service allows sales and marketing managers to distribute and control their existing collateral within their own branded app. With redundant backups, Internet-standard encryption, and real-time authentication, Showcase's security offering reflects today's standards and best practices for mobile data security.

## Leading brands use Showcase to:

- Control content from any web browser
- Eliminate print and distribution costs
- Coordinate an international sales force

Showcase works closely with IT, marketing, sales and other key decision makers at companies that sell everything from energy to creativity, from heritage to education. With Showcase, salespeople in the field have the product information and secure software integration they need to save time, sell more, and boost revenue.

## Showcase. Selling never looked this good.


**www.showcaseworkshop.com**
info@showcaseworkshop.com
ShowcaseSoftware
NailTheSale

showcase