WHITE PAPER

SECURING THE MOBILE DEVICES OF REMOTE WORKERS

pradeo

INTRODUCTION

To smoothen the activity of their workforce, enterprises are more and more issuing corporate-owned devices or enabling BYOD usages multiplying access points to corporate data.

If some companies are used to this way of working and have implemented all security gates to protect data beyond the enterprise perimeter, others are looking for some guidance on the best practices to protect such a the versatile security context.

You will find in this white paper figures and trends about the current mobile workers usages, the threats surrounding them, followed by some best practices and the security stakes related to the mixing of professional and personal usages arising from mobility.

INDEX

MOBILE WORKERS USAGES, THREAT LANDSCAPE & EXPECTATIONS

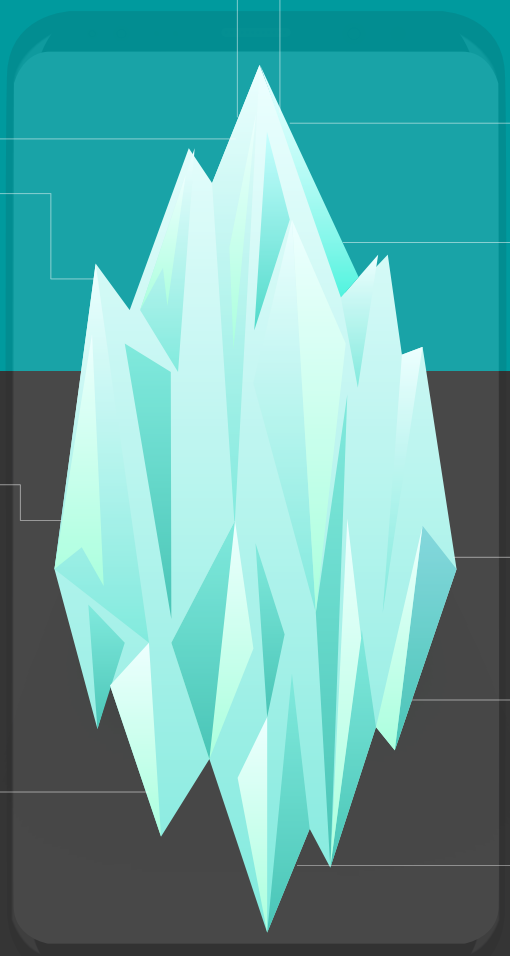
Mobile workers usages

Being the aggregation of all working and often personal tools at once, the mobile device became the privileged media of workers. To make calls, consult emails, access corporate resources but also remain connected with relatives or simply take a break... our mobile device is an integral part of our daily life. The democratization of BYOD and remote working widens the spectrum of mobile usages and constitutes a security challenge that companies have to address.
Now, mobile represents: 89% of **workers**, 80% of **corporate tasks** and 77% of **digital traffic.**

Mobile workers threat environment

Tablets and smartphones came along with the application model where there is an application for every need, always a network to connect to... Mobile devices turn into the perfect swiss knife hiding along the way underground activities that could take place.

THE DOWNSIDE OF MOBILE



DEVICE
Settings configuration, system update, root/jailbreak of the device

NETWORK
Connection to cellular and WiFi networks, corporate and public

CONTACTS
Mix of professional and personal contacts

CORPORATE APPS
E-mails, CRM, business applications…

OTHER APPS
Social networks, news, transport, entertainment, health, tools, banking...

FILES
Business contracts, procedures, documents, pictures, videos, PDF...

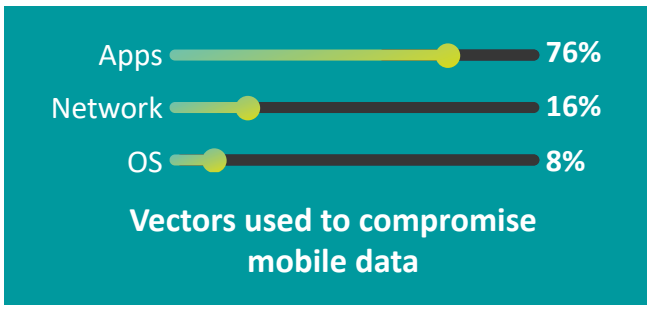
MALWARE
Ransom demand, data theft, eavesdropping (microphone, location, camera…)

OS EXPLOIT
System takeover, vulnerability exploits

NETWORK EXPLOIT
Man-In-The-Middle, rogue cell tower

PHISHING
Credentials theft , identity theft, fraud

LEAKY APPS
Abusive collection of personal and corporate data



Being easy to develop, maximising the outreach and having a direct access to data, applications unsurprisingly represent the principal vector of threats.

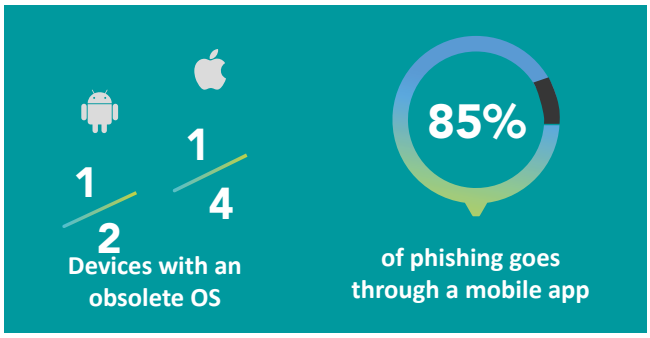
Beyond malwares, data theft and leakage are a prime scourge. The dark web is chock-full of data brokers monetizing active users' data for $4000 USD/month the million.

HIGHLIGHT

In our latest security report, we identified that 2/3 of Android devices and 3/5 iOS devices are hosting an app sending contact information over the network.

On the other end, OS exploits use to be conducted leveraging outdated OS or rooted and jaibroken devices.

Phishing is the most perpetrated network attack and still traps millions of users.



32% of data breaches involve phishing activities

Needs to be balanced

The mobile environment is full of threats to be thwarted in the light of corporate and employees' expectations to preserve business agility. In addition, the spreading of hybrid configurations such as BYOD and work/life separation prevent from a single-sided approach.

- Protection of company data
- Maintaining the productivity of mobile employees
- Implementation of a customized security solution
- Compliance with regulations

- Easy access to corporate data
- Privacy policy
- No impact on personal use
- Blocking access to corporate resources in case of threats

pradeo

Data protection legal framework

Mobile devices are processing and hosting data and as a result fall within the scope of the data protection legal framework. Depending on their industry and the sensitiveness of data manipulated, companies are subjected to more or less regulations.

HIGHLIGHT

Every company is due to comply with personal data protection regulations and is required to set appropriate security measures and report security events within a timely manner in case of a breach. Industry-specific regulations impose predefined security measures to ensure the protection of highly sensitive information such as financial or health data.

» For more information on the data protection legal framework, refer to our white paper dedicated to the mobile data privacy.

Individual best practices

Mobile threats act on 3 different layers, starting with **applications, network and device**. Some simple rules could be followed at the individual level to reduce the attack surface.

APPLICATIONS

Applications are the privileged media for cybercriminals to run attacks because of their outreach and easiness of deployment. Therefore, collaborators must pay greater attention to applications that are hosted on their devices.

Here are the core principles to individually apply:

1. **Banish the download of apps from 3rd party stores**. Malwares, but not only, primarily come from non-official stores.

2. **Watch out for requested permissions**. Users might carelessly grant permissions to applications. Yet, it happens more often than they may imagine, that permissions are not all required for the proper functioning of the application but requested to collect and sell data mainly to marketing companies. When using a mobile device for corporate purpose, users have to be diligent with apps' permissions to prevent from data leakage (contact list, SMS, call logs…).

3. **Rigourously update applications**. Malicious applications can still be downloaded from stores despite security measures implemented by Google and Apple and are usually removed as soon as they are detected. By enabling applications auto-update in the store settings, obsolete apps will be deleted and the user will benefit of new releases right away.

NETWORK

When working from home or traveling, network connection is key to run activities: retrieve and send e-mails, access to corporate resources (files, contracts…) and applications (intranet, CRM, messaging…).
It usually often involves to rely on a network connection other than the cellular one. Here also are some core principles that must be followed:

1. **Use a known private WiFi network**. To prevent from any transaction interception, collaborators have to connect to a trusted WiFi network and avoid any next-door public connection facilitating Man-In-The-Middle attacks.

2. **Do not tweak the connection**. Whatever the bandwidth capacity, it's never enough and users may be tempted to try to improve their network performance downloading for instance a shady application.

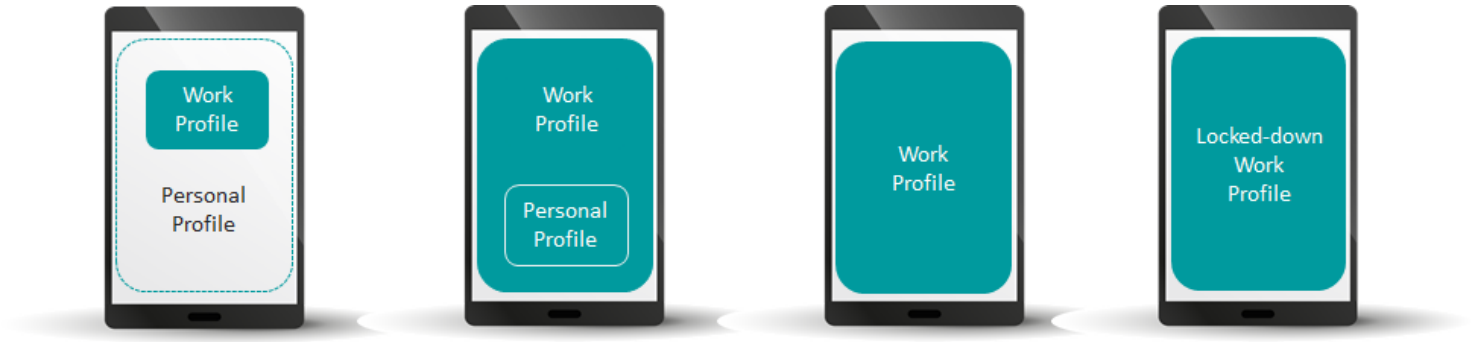
The device itself represents a target for hackers which are looking for breaches to take control on the system. Basic actions can be taken to strengthen the OS:

1. **Do not root or jailbreak the device**. Extra capabilities unlocked when jailbreaking or rooting a device are leveraged by cybercriminals when perpetrating an attack. Thus, 75.1% of applications are checking this status to run advanced commands.
2. **Keep the OS up to date**. Updates have to be strictly applied as they usually embed a security patch fixing known vulnerabilities.

The limits of work and personal profiles

The advent of Android Enterprise sheds the spotlight on **work/life separation** through the containerization of one profile or another. Android Enterprise core objective was to deliver a common set of device management APIs to ensure a consist experience across Unified Endpoint Management (UEM) solutions.

Becoming mandatory with Android 10, any device to be managed through an UEM has to be enabled with one of the 4 setup modes.



In both COPE (Corporate Owned Personally Enabled) and BYOD modes, the separation consists in isolating work/life files, applications and resources (messages, contacts, call logs…). There are taking opposing view with regards to which profile masters the device and put the other part in a sub-area.
The COBO (Corporate Owned Business Only) and COSU (Corporate Owned / Single Use) configurations depict a device fully managed by the company and strictly aimed for work. Kiosk-managed devices are fully locked down to only enable a targeted usage.

With these four specific types of configuration, organizations are free to have more or less control over the user device. With an **ever-growing BYOD landscape**, companies can decide to let employees work on their personal devices, while still having control over the work environment.

The containerisation capability, already available in UEMs for some time, simplifies and unifies Android management but doesn't really add a structuring security piece. Setting up a work/life separation must only be considered as a data privacy measure and not fall into the trap viewing it as a security gate.

CORPORATE APPS

Unexpected behaviors or vulnerabilities of private and public apps distributed

NETWORK

Phishing, Man-In-The-Middle, Unsecure connections, …

END-USER APPS

Malwares or leaky or intrusive apps to jeopardize corporate data security

DEVICE

Vulnerability exploit, system takeover, outdated system…

Corporate data are still exposed, whatever the chosen setup mode, to environmental threats coming from applications, network communications and the device configuration like any other device (Android or iOS). Network and device criteria apply for the entire device and a Man-In-The-Middle threat or a root/jailbreak exploit will injure the work profile the same way.

Looking at applications, if validating the security level of applications prior their distribution to the work area is a must have, the assessment of on-device applications is not to forget. By downloading an application from the store either on the work or personal profile, corporate data are exposed to malware (screenlogger, keylogger…) and intrusive or leaky applications (contacts…) that could hit from one profile to the other.

In sum, a proper security posture requires to be taken to protect Android Enterprise/containerized mobile devices as any other device.

Adapted security measures to mobile workers

If the practices previously mentioned help limiting attacks and enforcing privacy, mobile devices of remote workers are still exposed to threats and endanger corporate data. A dedicated solution is to be implemented to close the gap and ensure the thorough protection of the mobile workforce.

The mobile security ecosystem is no exception and there are plenty of solutions claiming to properly protect mobile devices. As for any solution selection, a careful comparison needs to be conducted to identify strengths and weaknesses of players in the light of their core expertise and the company requirements (for more information, confer our Mobile security solution comparison article).
Below are highlighted the core properties to look for when setting up mobile security.

PRECISE

A successful implementation of mobile security requires to subtly balance protective measures and users' freedom of use. A restriction can only be accepted as long as it is appropriate and measured.
Thus, threat detection accuracy and security response granularity are the two pillars to provide an efficient mobile security posture. False positives would ruin confidence of both the security team and the end-users in the solution and by extension in the security strategy.

REAL-TIME

The vivacity of the mobile context requires to act on the fly through a mobile threat defense agent. Taking the form of a mobile application, it dynamically detects and remediates threats in real-time.
A complete protection has to handle the three vectors of attacks being applications, network and device and offer adapted counter measures.

TAILORED

Mobile workers present various configurations (Bring Your Own Device, remote working, nomadism) and have different roles in the company. The solution has to be highly customizable to define adapted security policies matching users' profile.
The threat detection sensitiveness is to be adjusted according the users' role and threat exposure. On another hand the security response will depend on the mobile context. Intrusive security measures cannot be taken on a personal device and threats have to be mitigated by locking down the access to corporate resources.

EFFORTLESS

Workers are needing an easy to deploy and burden-free solution to embrace the mobile security strategy of the company. Mobile threat protection usually provides pre-configured agents for 0-touch deployment to smoothen the adoption.
When the device is setup with a dual environment for professional and personal activities, the solution needs to be deployed on both profiles to ensure a total protection. The ability of the solution to manage both environment and offer adapted security response with regards to each one is key.

MANAGED OR UNMANAGED

Last but not least, there are two kinds of mobile workers. The managed ones refer to mobile devices that are administrated by the company and enrolled within a Unified Endpoint Management platform. Those usually are COPE, COBO or COSU and, to a lesser extent, BYOD (cf. chapter above).

On principle, managed devices conform to the security policy of the company through the enforcement of security measures and restriction of usages if needed (blocking of applications, networks…).

Unmanaged devices represent external collaborators or partners as well as most of the BYOD users. They must access to corporate resources to fulfil their duties but shall not be restricted in their usages. The security response has to be adjusted and will consist in warning the user and preventing the access to corporate resources until the detected threat is remediated.
Unmanaged devices require a custom mobile security solution to combine security and users' flexibility.

ABOUT PRADEO

Pradeo is a global leader of mobile security. It provides mobile threat intelligence services as well as solutions to protect the data handled through smartphones, tablets and mobile applications.

Pradeo developed Pradeo Security, a patented mobile security technology that uses Artificial Intelligence andmachine learning to automatically detect and ward off known, unknown and advanced mobile threats including zero-days. It provides a reliable detection of mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

Pradeo Security offers a complete and automatic protection of the data manipulated by mobile devices and applications, aligned with organizations' security policy, while preserving business agility.

" Pradeo continues to raise the bar in mobile security. By delivering high quality products that are easy to deploy, automated, highly accurate, user-friendly and compliant with data protection laws, the company has emerged as a clear market leader. With its strong overall performance, Pradeo has earned the 2019 Frost & Sullivan Global Product Line Strategy Leadership Award. " **Vikrant Gandhi, Industry Director, Frost & Sullivan.**

Managed devices

Pradeo Security Mobile Threat Defense solution provides multi-layered security (applications, network, OS) for all devices (Android and iOS) including BYOD devices.

Key takeaways

- Seamless deployment («0-touch»)
- Quick and easy synchronization with device management solutions (MDM/UEM)
- Real-time remediation on the device according to the security policy
- Detailed dashboards

Unmanaged devices

Pradeo's Secure Private Store provides business tools and mobile services without compromising device security and without the constraints of managing personal devices.

Key takeaways

- Installation as a simple application
- Choice of content to be deployed and configuration of the security policy from a single platform
- Real-time security analysis
- Conditional access to business tools and mobile services depending on the device's security level

For more details, visit www.pradeo.com or write to contact@pradeo.com