

# Press Kit

# pradeo

September 2015



**? Do you know what an Appsberg is? ?**

**Do you trust your smartphone ?** **What future for Antivirus software?**

**? Why should you be suspicious of gadgets such as the flashlight app? ?**

**?**

**?**

# SOMMAIRE

<a href="#">Cybersecurity and mobile applications: danger !</a>	p.4
<a href="#">Mobile applications, more and more present in our daily lives</a>	p.4
A booming sector	p.4
Corporate and/or private context	p.5
<a href="#">A growing threat</a>	p.6
Cybersecurity at the heart of current events	p.6
A growing number of cyber attacks	p.6
Unexpected risks	p.6
<a href="#">Pradeo reveals mobile apps' behavior</a>	p.7
<a href="#">Pradeo, an unprecedented technology to face new challenges</a>	p.7
A thesis: “ traditional Antivirus is dead ”	p.7
Trust Revealing, the app analysis engine unique in the world	p.8
Pradeo security's solution suite	p.9
Case studies	p.10
<a href="#">An entrepreneurial success story</a>	p.13
Once upon a time there was Pradeo	p.13
A recognized player, repeatedly awarded	p.13
Strong partnerships	p.14
Pradeo is conquering the world	p.14
<a href="#">For more information...</a>	p.15
<a href="#">Annex</a>	p.16

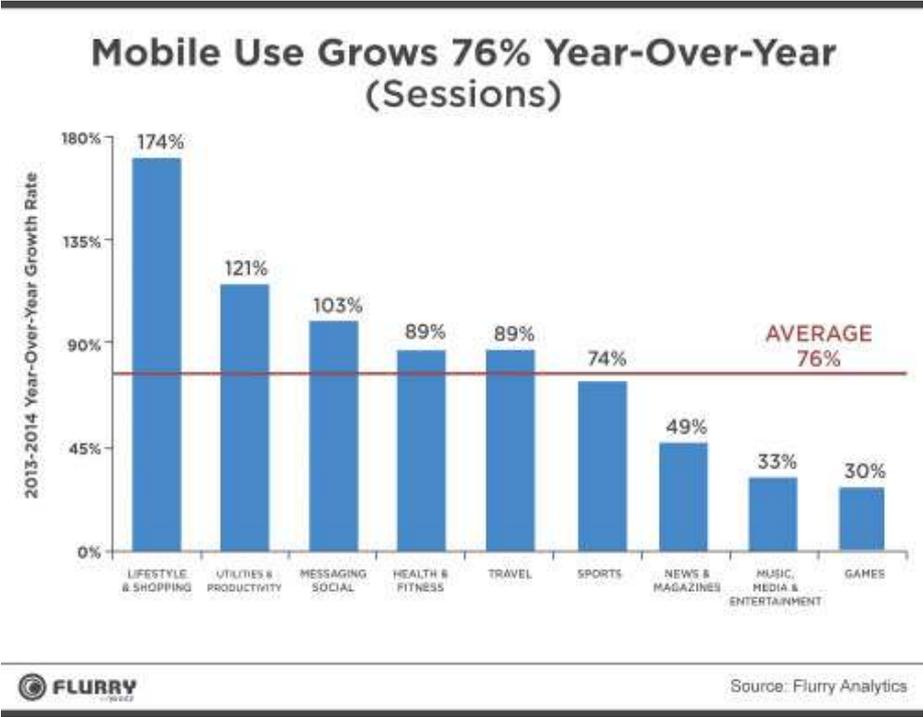
# CYBERSECURITY AND MOBILE APPLICATIONS: DANGER!

Mobile applications, more and more present in our daily lives

## A booming sector

The mobile applications market is booming: The turnover generated by **the global mobile app market is estimated to increase from more than 20 billion dollars in 2013 to more than 70 billion dollars in 2017** (Source: Digi-Capital, April 2014). In 2013, an average number of 197 000 apps was downloaded per minute. It is estimated that 518,000 downloads per minute will be reached in 2017 (Source: Gartner, September 2013).

Another striking figure: according to Flurry Analytics, **mobile application use has increased by 76% in 2014.**



Still according to Flurry Analytics, **86% of the time spent on mobile internet is generated by apps, which is 6% more than in 2013.**

The mobile app market is expected to grow even more and exponentially, especially with rising markets that are entirely based on the apps model, such as IoT. (watches, cars, domestic appliances...). The IDATE DigiWorld Institute (formerly the *Institut de l'audiovisuel et des télécommunications en Europe*) estimated in June 2014 that approximately 15 Billion objects were

connected to the internet, compared to only 4 million in 2010. And the number won't cease to grow especially after such a great launch. According to a report by Gartner and the IDATE Institute, **the estimation of connected objects on the globe will reach new heights in 2020, - between 50 to 80 billion units**. Basically, this means that everyone will own at least 6 connected objects.

#### Corporate and/or private context

Applications on smartphones are taking more and more space in economic terms. **Not only within a private context: daily news, gaming, sports, cooking, weather forecast... but they are also more and more used in a corporate sphere.**

The number of mobile apps within enterprises has increased significantly. This phenomenon is due to the **creation of internal app stores within companies and also due to the development of business-apps**. This trend can also be explained by the growing practice of BYOD (Bring Your Own Device), which facilitates the coexistence and indeed the integration of personal apps into corporate IT systems.



Personal life and professional life are linked via mobile applications!

## A growing threat

### [Cybersecurity at the heart of current events](#)

Cybersecurity is a topic that concerns people, which provokes strong reactions and which fuels journalistic debate. Economic, political, military and social issues are at the heart of this matter, because it affects everyone.

**The regulatory frame around this subject remains blurry, which causes the current complications not only in Europe but in the US as well.** In France, the next Digital Technology and Communications Act is planned for autumn 2015, and an advice and support platform for victims of cyber-attacks will go online in 2016. In Europe, an obligation for companies to declare the cyber-attacks they have faced will be implemented. In the US, cybersecurity is a priority for the Department of Homeland Security and a great awareness of the dangers of criminal actions on the internet can be observed.

Nevertheless, **large parts of this topic remain unclear and protection is difficult, on one hand because of the mobility of the actors, victims and objects,** on the other hand due to the fact the general awareness of the reality of the threats is not yet entirely established, for both the professional and the private sphere.

### [A growing number of cyber attacks](#)

Another factor which puts cybersecurity in the spotlight: the victims of cyber attacks are diverse and heterogeneous, and they make a lot of noise.

The latest attack which was extensively covered by the media (August 2015): The Ashley Madison hacking scandal during which the hackers revealed detailed personal information of several millions of users of this extramarital affairs dating service. Another prominent hacking scandal, in April 2015: the Francophone international channel TV5 Monde (TV, website and social networks) endured a cyber attack and was entirely unable to broadcast.

**Cyber attacks multiply, they surprise and they scare. They point out that we are not protected, and that we could all possibly be a victim one day.**

### [Unexpected risks](#)

But there are risks that we speak less of, and of which we are less aware. According to a study conducted in May 2015 by OpinionWay for CapGemini, **85% of employees estimate that their**

**company is well protected against cyber attacks and hackers.** But hacks are not limited to the computer... The revelations made by Edward Snowden on cyber-spying implemented by the NSA via popular mobile apps (Twitter, Facebook, Angry Birds..) have allowed the public to **be aware of the potential danger coming from a mobile app and especially provoked by its behavior.** And with the growing number of downloaded apps, protecting private or corporate users becomes increasingly complex.

Furthermore, **mobile apps handle very crucial data**, due to the growing number of banking-apps, payment-apps, health-apps or social media...

The risks for consumers are multiple and concern three spheres:

- **Respect of privacy** (data theft...)
- **Financial loss** (stealing of banking data...)
- **Mobile devices Security** (virus...)

In order to really understand the threats related to mobile apps, you have to consider an app as an iceberg. **The visible part corresponds to the clearly declared actions of the app which are legitimate and allow for a proper functioning. The hidden, non-visible part corresponds to unknown and potentially malicious behaviors, which are performed without the user's knowledge.** The issues related to this "Appsberg" phenomenon are crucial for the consumer market. They are even more crucial to enterprises which engage in strategic development in the m-business universe and who have to adapt their security policy to the new mobile devices and their particularities.

## PRADEO REVEALS MOBILE APPS' BEHAVIOR

### [Pradeo, an unprecedented technology to face new challenges](#)

A thesis: " traditional Antivirus is dead "

A traditional Antivirus software isn't the solution of choice in order to address these new threats. This is Pradeo's conviction, as well as it is the conclusion of security experts. "Antivirus software is dead", said an expert of one of the global leaders in IT security in the Wall Street Journal on May 4 2014.

More than just a statement, this is henceforth a reality: **the "apps model" has rendered obsolete the approach made by antivirus software.** Indeed, **this model imposes above all an immediateness in security analysis and response:** once a user has downloaded an app, he uses it immediately afterwards. It is thus pointless to know about an app's malware status only weeks later. The cycle used by antivirus systems - detection of a malware, creation of a viral signature and at last the protection of the user - is simply too long to efficiently face the threats posed by mobile apps.

**The "apps model" also demands a subjectivity in security analysis:** The fact that a mobile app could retrieve a phone number can be considered acceptable by some users, and inadmissible by others. The characterization of a potential security breach is thus subjective. Regarding this complexity, antivirus software does not provide any answers.

**The workspace, providing historical ground for the success of antivirus software, is also subject to an in-depth transformation, following more and more the logic of the "apps model"** (such as Windows 8 and Windows 10). All of this accelerates the announced death of the traditional solutions to protect the workspace and its related IT systems with antivirus software.

[Trust Revealing™, the app analysis engine unique in the world](#)

Since antivirus software has become obsolete, new technologies become indispensable, in order to warn users from malicious behaviors coming from mobile apps for smartphones and other devices. **Even if some applications seem harmless, they can be the perfect vector for hacking and data theft, while profiting from the global distribution system through the globally accessible app stores.** This is the case for online payment apps, but not exclusively: so-called gadget apps such as the phone flashlight could be used as a hacking medium and retrieve saved contact data, documents or diaries. Behind seemingly inoffensive actions such as sending automatic text messages could be hidden a malware system which carries out hacking activities without the user's knowledge.

**Detecting and identifying suspicious or malicious app behavior is a real challenge, and Pradeo follows this objective.** In order to effectively face the aforementioned threats, and after 6 years of research and development, **the company has established its own technology: A behavioural mobile app analysis engine called Trust Revealing™, which enables user to reveal hidden actions carried out by an app, and to identify those which translate into malicious behaviour.**

Trust Revealing™ analyzes within one minute the hidden actions carried out by a mobile application and reveals:

- what connections are established by the app,
- what kind of data are manipulated: user data, mobile device data, app data,
- what operations are carried out: data transfer to a distant server, automatic sending, unsecured payment connection, etc.

Every threat is then classified according to three categories: privacy, financial loss and security. Out of 1.1 million analyzed apps, Pradeo states that 50.9% of the threats are in relation to the user's privacy, and 46.5% are related to the user's security.

Trust Revealing™ allows to discern secure apps, which don't pose any risk, from those who pose real risks. This is an **innovation in the field of security, for enterprises and organizations that develop their own corporate apps as well as for employees and external users.**

This technology, protected by two patents, is unique in the world.



#### [Pradeo's security solution suite](#)

Based on the Trust Revealing™ analysis which constitutes an innovation unique in the world, Pradeo has developed a portfolio of products dedicated to the security of mobile apps, ranging from the app development phase to the end consumer.

(Detailed description, see Annex p.16)



CheckMyApps™, CheckMyApps API™ and AuditMyApps™ are tools deploying a technology based on the Trust Revealing™ app analysis engine. They enable the user to **analyse and manage the personal level of app security** on their devices.

- **CheckMyApps™** allows companies to evaluate the security level of mobile apps that are already installed on mobile devices, based on a security policy predetermined by each company. This allows to take control over mobile app security.
- **CheckMyApps API™** is a security solution dedicated to secure “critical” apps (such as m-payment, health, security-apps...) as soon as they are executed on a non-secure device.
- Last but not least, **AuditMyApps™** is a web platform dedicated to enterprises who wish to perform a security diagnosis and a behavioural analysis of their mobile apps.

Pradeo has also developed a store of secure apps, called **MyCompanyStore**, in 2015. This store's objective is to assure a secured and focused distribution of mobile apps to the company's clients.

### [Case studies](#)

Pradeo's technologies answer to a real need for mobile app securisation systems and are recognized for their efficiency. Big names from different domains trust Pradeo to secure their mobile apps and protect them against hacking. Among them are for instance La Poste Group and Sanofi.



Protection of a mobile fleet of 100,000 smartphones <a href="http://bit.ly/1EPKyOT">http://bit.ly/1EPKyOT</a>	
Client	La Poste: historical French mail service, approx. 100,000 postmen
Project	<ul style="list-style-type: none"> <li>• Equip postmen with a smartphone in order to optimize their daily round and to deploy new services</li> <li>• Modernize and transform mail distribution thanks to the capacities of the new mobile devices</li> <li>• Integrate the "Apps + Store" model into the information system</li> </ul>
Challenges	<ul style="list-style-type: none"> <li>• Define and deploy a security policy which then evolves according to the user profiles</li> <li>• Security control of the apps downloaded by the users in order to determine their compliance with the security policy</li> <li>• Supervise the security of all apps installed on the mobile fleet</li> </ul>
Opportunities	<ul style="list-style-type: none"> <li>• Security initiatives made by companies wishing to develop their mobile projects destined to their employees</li> <li>• Secure the implementation of the BYOD concept within enterprises that open up their information systems to their employees</li> </ul>



Apps Factory: Automatic security control	
Client	Sanofi: global leader in the pharmaceutical sector, more than 110,000 employees
Project	<ul style="list-style-type: none"> <li>• Ensure app security control before their distribution to public or private stores</li> <li>• Automatize the security controls as much as possible in order to accelerate the validation process of the apps, due to tight project deadlines</li> </ul>
Challenges	<ul style="list-style-type: none"> <li>• Accelerate the process of app validation</li> <li>• Prepare for large-scale deployment of the "Apps + Store" model</li> <li>• Make app security controls accessible for internal teams in order to facilitate the work of Corporate Security Officers implementing mobile projects</li> <li>• Reduce workload for experts so they can dedicate to more crucial issues</li> </ul>
Opportunities	<ul style="list-style-type: none"> <li>• Enterprises which deploy "mobility" programs dedicated to their employees and/ or their clients</li> <li>• Enterprises which wish to attribute a certification to their apps before distribution</li> </ul>

## An entrepreneurial success story

### Once upon a time there was Pradeo

Pradeo is the result of three key steps: in 2008, Clément Saad, founder and president of Pradeo, presents his PhD thesis to the French Ministry of Defence. **Considering the success of mobile apps, he is convinced that soon there will be more mobile apps than websites.** He is sure that the "historical" approach to app security (deployed for instance through antivirus software) is outdated and he has the idea to develop an app analysis engine in order to protect "producers and consumers" of mobile apps. He decides to explore this domain through an entrepreneurial approach. Several years of research and development are necessary in order to bring the technology to perfection and to obtain the first marketable versions of the technologies based on the Trust Revealing™ analysis engine. In 2013 the Pradeo suite of security solutions are launched on the market.

The etymology of the name "*Pradeo*" says a lot about the company and its competences: "*Praedo*" means "pirate" in Latin. This choice was made on purpose, because in order to create a reliable security solution, we have to know perfectly the different techniques used by hackers to avoid their technological traps. Pradeo can be considered as a "white pirate".

### A recognized player, repeatedly awarded

**Numerous juries and expert committees have honoured Pradeo for its innovation and its potential of international development. They have furthermore confirmed Pradeo as an expert in the field of app security.** During the International Forum of Cybersecurity (FIC 2015), which took place on January 20 and 21 2015 at Lille, Axelle Lemaire, French State Minister for Digital Affairs, has awarded Pradeo with the **Award of the Innovative SME.**

**Pradeo also benefits from significant institutional support:** Pradeo has been rewarded twice by the French Ministry of Research in the **Contest for Innovative Companies** in 2010 and 2011. This national distinction is the highest award for the creation of innovative companies. It values Pradeo's research and development activities. Furthermore, Pradeo has won the **Tremplin Enterprises** Award

**Pradeo has won numerous other awards:** "Prix Coup de Coeur French Tech Montpellier" during the Big Up 4 Startup event (2015), winner of the of the Trophies from the International Digital competition (2014), the Innovation Award during the IT Innovation Forum Event (2014), the Special Award of the CCI Paris... Pradeo convinces experts thanks to its unique technology.

In addition to this, Pradeo is listed in **Gartner's "Magic Quadrant for Application Security Testing"**. Published every year by the American information technology research and advisory firm, this "Magic Quadrant" positions the major players of the application security testing market according to different categories. Pradeo has first been listed in this report in 2014, recognized for specialization and the original approach to analyse mobile apps.

### [Strong partnerships](#)

**Major partnerships mark Pradeo's development and contribute to establishing the company as a major actor in the field of mobile security.**

**A global partnership has been signed with the South Korean giant Samsung in April 2015, which authorizes Pradeo to broadcast their mobile app security solutions via Samsung's BtoB platform the "Knox Marketplace".** Knox allows for the user to virtually divide a mobile device into two spheres: A personal sphere and a professional sphere. This implies a real security challenge regarding the separation of these two spheres. Pradeo enables the user to verify that the applications he/ she downloads don't display malicious behavior and don't retrieve personal data. The signature of this partnership implies for Pradeo the opening of a market of approximately 100 million mobile devices in the world, using the Knox system.

**The most recent partnership has been signed between Pradeo and the American company MobileIron, a leader in the global MDM market.** The MobileIron platform is built to secure and manage modern operating systems while incorporating identity protection, context and privacy enforcement. **With this MDM solution, IT departments can secure corporate information no matter where they are, and thanks to the partnership with Pradeo, customers can benefit from a particularly innovative anti-malware protection to conduct security checks on the mobile apps running on their fleet.** This partnership with Pradeo complements MobileIron's security and management capabilities and constitutes a major step for Pradeo on the American market.

### [Pradeo is conquering the world](#)

While major national and international players engage in ambitious programs to develop their mobile services, the issues around security, data protection and privacy have become crucial.

These developments confirm Pradeo's international ambitions. The company has developed a unique technology, which is useful and needed across borders. Pradeo's main international markets are: **USA, UK, Germany, Thailand and Singapore**. Pradeo is currently present in **22 countries across the globe** and has recently opened an office in San Francisco and in London. The next opening is planned in Germany. To be continued...

[For more information...](#)

**Customers:** La Poste Group, French Ministry of Foreign Affairs, French Ministry of Defence, Radio France, Samsung, Sanofi, Société Générale...

**Workforce:** 20 employees

**Awards and contests :** laureate of the contest of the Ministry of Research, winner of the Tremplin – Senate contest, winner of the innovation award "Enterprise Mobility" - IT Innovation Forum, winner of the "International Digital Trophy" award – Business France and IE Club, laureate of the Pass French Tech.

**Turnover 2014:** 1 Million Euros.

**Present in 22 countries:** Europe, Thailand, Singapore, China, India, Russia, South America, United States.

**Website :** [www.pradeo.net](http://www.pradeo.net)

**Media Contacts :**



Mélanie DA RUI – 01 44 94 95 64 – [melanie@escalconsulting.com](mailto:melanie@escalconsulting.com)

Maria SCHUBOTZ – 01 44 94 95 75 – [maria@escalconsulting.com](mailto:maria@escalconsulting.com)

## ANNEX

### Description of Pradeo's security solutions :

- **AuditMyApps™** : web platform of Application Security Testing (AST) with an objective to provide the user with a full security report for one or several mobile apps he uploads on the platform.

**AuditMyApps™** is available as a Cloud service on <https://www.auditmyapps.com> or as an On-premise appliance.

- **CheckMyApps™** : next-generation antivirus able to check in real time the security of the entire personal (BYOD) and professional mobile applications installed on a mobile fleet of Smartphones & Tablets by ensuring their compliance with any company's security policy.

**CheckMyApps™** allows companies to define their own security criteria and to automatically manage the authorization or blocking of an apps running either on Android, iOS and Windows by making sure they respect the security policy.

**CheckMyApps™** is available as a Cloud service on <https://www.checkmyapps-cloud.com> or as an on-premise appliance.

- **CheckMyApps API™** : security solution dedicated to publishers of “critical” apps (example of critical apps: m-payment, health, security...). Through the analysis of third-party apps present on a mobile device (native and downloaded apps), the jailbreak detection..., the Pradeo's API is able to reveal if a “critical” app is executed in a secure environment.

**CheckMyApps API™** also offers to telecom operators and smartphone or tablet manufacturers the possibility to ensure the security of the apps pre-loaded for their clients.

- **CheckMyApps Mobile Security™** : free public mobile application available on Google Play and Amazon Appstore. CheckMyApps Mobile Security™ gives the opportunity to users to evaluate the risk level of the Android apps present on their handset from 3 main perspectives: privacy, financial losses and their device security.

To learn more about PRADEO, visit the website [www.pradeo.net](http://www.pradeo.net)