Whitepaper

5 key considerations for effective security in a mobile world

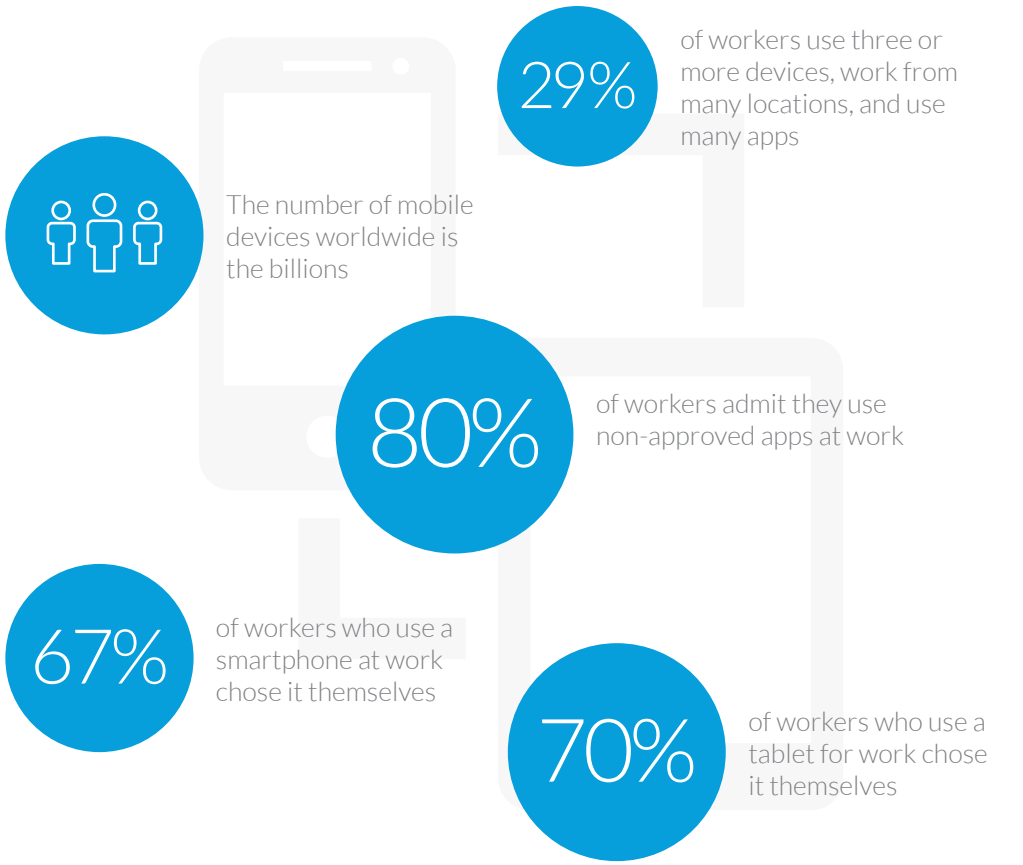
Dilignet
Step into the cloud

The way in which people work has changed. The mobile workforce is a reality. Yet while new ways of working bring many benefits, they demand a new approach to security.

For instance, how do you secure your data and applications on the internet? What happens if a device gets stolen?
How do you ensure documents are secure if they are used in public environments?
Can you provide quality technical support to users who are working from home?
How will your employees ensure that their work and private information remains separate?

A recent survey of global C-suite executives by IBM[1] revealed that 71% of all surveyed CIOs believe mobility is the technology that will most revolutionise business. The report also revealed that IT security is by far and away the biggest risk in the opinion of CIOs.

Despite this, however, many businesses are still investing in very costly, large-scale security solutions that protect their infrastructure and devices, yet neglect their data and people.



Source: Microsoft, Controlling the Uncontrollable, 2016[2]

To shed light on this topic, we spoke with the following mobile security experts:

Gary Smith,
Cloud Practice Lead,
Dilignet

Peter Royal,
Account Manager,
Dilignet

Jason Flynn,
Product Manager,
Enterprise Mobility & Security, Microsoft Australia

Based on their insights, this whitepaper includes our top 5 tips on establishing an effective mobile security strategy.

1 IBM, Redefining Connections: Insights from the Global C-suite Study – The CIO perspective, January 2016

1. Secure your data, not just your infrastructure

"Back in the day, corporate security meant establishing impenetrable perimeters. However, this doesn't really work now there are so many applications and so much data out there. Today, it's about securing the data itself, not just the container."

Gary Smith, Cloud Practice Lead, Dilignet

"Traditionally, a secure business was like a castle with big strong walls, protecting everyone that lived in the castle. Now, the village has extended and people are living outside the castle and so simply securing the four walls isn't enough. Businesses are struggling to keep up with this new scenario."

Jason Flynn, Product Manager, Enterprise Mobility & Security, Microsoft Australia

The weak link in most mobile security solutions isn't the technology. It's the people. If your employees forget to change their passwords, leave their devices unlocked or borrow their colleagues' access, they can leave you exposed to all kinds of security risks. And what's the point of securing your business with a costly solution if there's nothing left inside to protect?

Today, it's no longer enough to implement a robust, on-premise security solution. Now, people need access to their data and information wherever they are, and businesses need to cater for this. Rather than securing their borders, businesses need to focus on the assets they have inside their operation.

Your company data must be protected at all times, wherever it is: whether in the cloud, at your datacentre, or in transit between your office and a client's home. It must also be isolated and protected from a user's personal data.

A recent Forrester report[3] claims that as the ecosystem becomes more complicated, identity-level security is increasingly just a baseline level of business security. The report also suggests that access security is no longer just about privileging at the user level; it must also address the application, file, and data levels.

Ensuring effective level of security, and regulatory compliance over the entire process, has therefore become complex and multi-faceted. Access to data needs to be based on a user's identity and role, and data needs to be classified according to its level of sensitivity and business impact.

There are four key components of a successful mobility strategy: users, devices, apps and data.

3 Forrester, Overcome Security And Identity Management Challenges In Enterprise Mobility With The Right IT Infrastructure, December 2014

2. Turn security from a capital expense into an operating expense

"When it comes to security, we rarely ask our customers to throw away their existing investments. Instead, where appropriate, we help them move their legacy systems into more secure environments."

Gary Smith, Cloud Practice Lead, Dilignet

It's simply no longer the case that businesses need to invest in large, expensive, up-front security solutions that weigh heavily on their capital expenses budget. Instead, businesses should be looking at shifting to service-based security solutions that come out of their operating expenses, which they can scale up or down depending upon their needs.

By switching to a service-based model, businesses can save significantly on their up-front IT costs, as well as their ongoing support costs. Features such as a self-service password reset, for instance, can dramatically reduce help desk calls. If users can do it themselves, the cost of support can be quantifiably reduced. If a business has multiple workers on multiple devices, IT resources can now manage it all, quickly and effectively, from a single pane of glass.

To reduce costs, it's also important for businesses to consider how they can make the most of the investments that they have already made, and simply increase the security of those, rather than starting from scratch.

3. Make self-service and ease of use a priority

"Ease of use is the biggest thing that workers want. If technology is difficult to use, people will just find a way around it."

Gary Smith, Cloud Practice Lead, Dilignet

To work effectively, a business' security solution relies on the cooperation of its people. It must therefore be very straightforward and easy to use.

Once users are comfortable with a solution, they can then drive it – which can considerably reduce the burden on a business' IT team.

"It's about empowerment of the end user experience. It's about giving people the experience they want, and making it secure through multi-factorial authentication and role-based identity, so they can work intuitively and from anywhere. Users therefore get the most powerful user experience rather than the locked-in container experience."

Jason Flynn, Product Manager, Enterprise Mobility & Security, Microsoft Australia

A report by Forrester[4] suggests, for instance, that employee self-service in areas such as password reset, basic troubleshooting and application reset offers business a low-risk way to entrust employees to solve their own issues, assuming they are given the necessary tools and training to do so.

This same Forrester report also suggests that, to make the experience as seamless and as simple as possible, having a single user identity across all devices and applications needs to be a priority. Extending and integrating single sign-on with mobile devices will lead to end user benefits of faster and easier login, as well as simplified password resets and synchronization, the report says.

4 Forrester, Overcome Security And Identity Management Challenges In Enterprise Mobility With The Right IT Infrastructure, December 2014

4. Plan for security from the outset (where possible)

"The mobile workforce is moving fast and the habits of a traditional IT department can be difficult to change at the same rate. Security needs to be considered early on, and by the right people."

Peter Royal, Account Manager, Dilignet

For a business of any size, applying security policies retrospectively can also be a major challenge, though it's certainly not impossible.

According to Forrester[5] in the near future, we will see enterprises in one of two factions for mobile: the "haves" and the "have-nots". The report suggests that the haves will be companies who have made adequate investments in mobile initiatives early on. These companies will reap the benefits of a mobile-empowered workforce, having overcome the growing pains in IT infrastructure before their competition could figure it out. The have-nots will be the late-adopters: companies that dabbled on the fringes of enterprise mobility or never dedicated the necessary resources to refigure their back-end systems to support the mobile ecosystem. The have-nots will be hard-pressed to compete with the much more agile, customer-focused mobile-enabled enterprises, and they may find themselves being pushed out of the marketplace, the report concludes.

To get the best results, security should be a consideration from the outset of any new initiative/business. Businesses need to be proactive about mitigating security threats, and collaborate to achieve their security goals, regardless of what stage they are at. They also need to choose the tools and partners that are best suited to their specific business and technology investment.

5. Put the user at the centre of your strategy

"There is a natural momentum with digital that's changing the way people work. Companies are increasingly realizing that flexible ways of working can mean increased productivity. Organisations need to adapt to meet users' needs rather than the other way around."

Peter Royal, Account Manager, Dilignet

In the past, security innovation happened in the corporate sphere. Once workers became accustomed to new innovations in the workplace, they would then take them into the personal realm. Today, the reverse is true. Now, innovation happens first in the consumer space, and then in the corporate space. As a result, workers have far higher expectations of their workplace environment than ever before. They are used to working from home, on a range of devices, and to getting the information they need, as soon as they want it, regardless of which device they are using. When they come into the office, they expect the same experience and don't want to be bound by any technology constraints.

Therefore, to be effective, any solution must be based upon, and meet, users' needs. By having users' needs at its core, a solution can also deliver upon its productivity and efficiency objectives. Similarly, if a solution is easy for a worker to use, there is far more likelihood that the user will make the necessary upgrades – and self-support – if required.

5 Forrester, Overcome Security And Identity Management Challenges In Enterprise Mobility With The Right IT Infrastructure, December 2014

According to a recent Microsoft publication[6], the most important elements of an enterprise mobility security solution are the users or employees: "Without them, the costs and IT infrastructure to enable enterprise mobility are meaningless…. If an IT administrator finds user identify hard to manage, or if an employee must take overly complicated steps to gain access to devices or resources, [the solution] is not worth whatever you're paying for it."
Federal Group Tasmania is a privately owned family company that operates a significant number of tourism, hospitality, retail, casino and gaming assets in Australia, as well as a sensitive freight company. They also own the oldest continually operating hotel group in Australia, and across all their operations, employ around 2,400 people.

Success story – Federal Group Tasmania

Dilignet worked with Federal Group Tasmania to set up a single sign-on for employees to leverage their Microsoft Cloud Services. As part of this, we implemented Active Directory Federation Services to allow the synchronization of objects from on-premise Active Directory to Azure Active Directory. We also set up tenant access for several Microsoft Online services, including Microsoft Office 365, Microsoft Azure and Microsoft Intune.

Approved Federal Group employees can now login to Microsoft Online Services using single account and setup the building blocks in place so as to execute the company's cloud strategy.

Want to find out more?

To discuss your business' mobile security needs, contact the expert team at Dilignet on **1300 812 512** or **info@dilignet.com**.

6 Microsoft, Controlling the Uncontrollable: Why you need to enable, protect, and manage mobile productivity end to end, 2016