SECURING NEXT-GENERATION BUSINESS IN THE SUPERFAST MOBILE AGE

1. INTRODUCTION

Fear has always been the stick that has driven traditional IT security investment. Fear of virus infections, fear of hackers, fear of costly and headline-grabbing data breaches. It has, to date, been a necessary cost of doing business in the digital world.

In the superfast mobile age, that is all about to change. Security is set to evolve from this 'locking down' approach to become a positive enabling layer that unlocks the potential for what we call Total Enterprise Mobility.

In this whitepaper we will show how superfast connectivity and consumerisation create an unprecedented opportunity for next-generation businesses to leap-frog their competition and the key security challenges and threats this brings. More importantly we will discuss the suite of security toolings, known collectively as enterprise mobility management (EMM), that are key to organisations being able to realise the benefits of fully mobilising the workforce. This means providing secure mobile access to the corporate data, applications and content employees need to do their jobs.

Consumers are driving an unstoppable mobile revolution that is transforming the way we live and work. This tsunami of mobile consumerisation has now made the internet a mobile-first medium, but UK businesses are lagging dangerously behind the curve.

"SUPERFAST CONNECTIVITY AND CONSUMERISATION CREATE AN UNPRECEDENTED OPPORTUNITY FOR NEXT-GENERATION BUSINESSES TO LEAP-FROG THEIR COMPETITION."

"MOBILE SECURITY PROVIDES A WAY FOR ORGANISATIONS TO EMBED MOBILE PROCESSES ACROSS THEIR WORKFORCE, CUSTOMERS AND OPERATIONS."

Total Enterprise Mobility is a holistic strategy for next-generation business to seize the opportunities of superfast mobile infrastructure and this consumer-led revolution.

We break down the future opportunities of Total Enterprise Mobility into three key areas that cover your employees, your customers and your operations. These are:

- Enabling a genuinely mobile workforce
- Engaging with customers through mobile channels and devices
- Connecting machines and information

Businesses cannot afford to ignore this mobile watershed if they want to survive and succeed in this fast-changing digital business environment.

At the heart of delivering the promise of Total Enterprise Mobility lies mobile security and the EMM tools that provide it. Mobile security provides a way for organisations to embed mobile processes across their workforce, customers and operations and gives businesses confidence to securely enable business data and applications across mobile channels and devices. EMM enables the IT department to centrally manage and remotely secure these devices and applications as well as their data and content. In doing so it frees up your data and enables it to flow freely but securely wherever and whenever your people need it.

2. WHAT'S CHANGED IN THE SUPERFAST MOBILE AGE?

Connectivity
The leap to 4G means that people now have cellular connectivity on their mobile device that is often faster than in the office or at home. 4G already covers over 70 per cent of the UK.[1] This marks a huge step change in making the mobile device far more than just a tool to make calls and access emails on the go. Superfast mobile broadband and cloud-based applications enable employees to access business and customer data in real-time, download and upload large files and do other high-bandwidth tasks such as video conferencing. It is also changing customer behaviour as they embrace mobile channels as well as driving a new wave of machine-to-machine (M2M) applications as we head towards the Internet of Things.

"4G ALREADY COVERS OVER 70 PER CENT OF THE UK. THIS MARKS A HUGE STEP CHANGE IN MAKING THE MOBILE DEVICE FAR MORE THAN JUST A TOOL TO MAKE CALLS AND ACCESS EMAILS ON THE GO."

Smart mobile devices
Devices have got a lot smarter and more portable. The average smartphone or tablet today is more powerful than your desktop PC of just a few years ago. We have also passed a mobile tipping point. PC sales suffered their worst decline in history in 2013[2] and the installed base of smartphones and tablets was estimated to have overtaken PC and laptops by the end of 2013.[3]

Consumerisation
Corporate IT trends used to come from innovations in military and academic labs filtering down to the business environment. Today it is consumers who are bringing these technology trends into the workplace and this will only accelerate as Generation Y enters the workforce and eventually becomes the next generation of entrepreneurs and leaders. What started with employees bringing their own mobile devices (BYOD) into the workplace is now evolving into more sophisticated choose your own device (CYOD) and corporate-owned, personally enabled (COPE) programmes for enabling a mobile workforce.

Customer behaviour
In addition to the impact of consumerisation on corporate IT and the workplace it is also having a profound and dramatic effect on customer behaviour. We only need to look at the retail sector to see this in action, where mobile has completely disrupted the traditional linear customer discovery and purchase cycle. Retail analyst Verdict is forecasting online spend in the UK via mobile devices to rise from £7.9bn in 2013 to £23.1bn by 2018.[4] Consumers are seeking to maximise the convenience and speed that mobile brings to their lives and are increasingly using smartphones and tablets at home, on the go and even in-store to discover, browse, compare prices and buy products. This is forcing businesses -- small and large -- across all sectors to embrace a mobile-first mindset.

[1]Coverage for EE alone.
[2]http://www.idc.com/getdoc.jsp?containerId=prUS24129913
[3]http://futurethinking.ee.co.uk/byod-and-the-post-pc-mobile-device-tipping-point-for-the-workplace/
[4]http://www.verdictretail.com/shopping-on-the-go-mobile-and-tablet-spending-set-to-soar/

3. KEY SECURITY CHALLENGES AND THREATS IN THE MOBILE-FIRST ERA

This exciting mobile-first world presents new challenges for corporate IT, expanding the network perimeter and increasing the potential for sensitive corporate data to be compromised through lost or stolen mobile devices. Some of the key threats and challenges that must be tackled include:

Lost and stolen devices
Theft and loss of a mobile device remains the biggest cause of security incidents for businesses. According to the Information Week 2013 Mobile Security Survey, 78 per cent of organisations said stolen devices is their top mobile security concern.[5] More than 20,000 mobile phones were handed in to Transport for London (TfL) in 2012, and incidents of lost tablet devices on TfL transport have risen 2,786 per cent in the five years to 2013.[6] And some 264 mobile thefts per day were reported in London in 2012.[7]

"MOBILE DEVICES AND CLOUD-BASED DATA STORAGE AND SHARING SERVICES, SUCH AS DROPBOX, HAVE MADE IT VERY EASY TO MOVE CORPORATE INFORMATION AND FILES FROM THE DEVICE TO CLOUD SERVICES OUTSIDE ENTERPRISE IT CONTROL."

Unsecure networks
Employees accessing sensitive business information from their devices over unknown or unsecured Wi-Fi or other networks potentially puts that data at risk. It is a key security concern for almost two-thirds (62 per cent) of IT managers, according to a survey by industry analyst Forrester Research.[8]

Data leakage
Mobile devices and cloud-based data storage and sharing services, such as Dropbox, have made it very easy to move corporate information and files from the device to cloud services outside enterprise IT control. Email attachments are one of the key ways that company data gets on to a mobile device. Features such as iOS' 'open with' allow the user to use third-party file readers or document management apps such as Box, Dropbox or Google Drive to open email attachments and save them or distribute them without the knowledge of IT, in effect leaking the data out of company control.

Standardisation versus employee choice
Unlike the desktop environment, the mobile world embraces a variety of major operating systems (OSes) that include Android, BlackBerry, iOS and Windows. Many businesses are no longer able to standardise around one OS. The pace of change in the mobile world makes it impossible for one size to fit all. Very often highly mobile executives want the convenience of carrying around an iPad while other users want to retain the physical QWERTY keyboard experience of BlackBerry or take advantage of the latest Android or Windows features.

It's not only business needs that are shaping the company mobile fleet, however. The rise of the BYOD trend, where employees want to use their own personal devices in the workplace for business, creates a significant challenge.

[5]http://reports.informationweek.com/abstract/18/10935/Mobility-Wireless/Research:-2013-State-Of-Mobile-Security.html
[6]Source: Freedom of Information request by McAfee: http://www.mobilenewscwp.co.uk/2013/12/12/londoners-have-handed-in-nearly-16000-mobiles-to-tfl-this-year/
[7]http://www.independent.co.uk/news/uk/crime/264-mobile-phones-stolen-every-day-8296811.html
[8]https://www.lookout.com/static/ee_images/figure-1.png

"ORGANISATIONS FAILING TO PROPERLY SECURE THE DATA HELD ON AND ACCESSED VIA EMPLOYEE MOBILE DEVICES FACE PROSECUTION AND SANCTIONS UNDER THE UK'S DATA PROTECTION LAWS."

Ignoring it can lead to uncontrolled devices gaining access to email and other applications without the knowledge of the IT department. Embracing it creates the challenge of how to control company data and applications while also respecting the privacy of the personal elements on the device.

Smart organisations are moving on from basic BYOD (with its potential for hidden costs) and onto more sophisticated choose your own device (CYOD) and corporate-owned, personally enabled (COPE) programmes for managing the provision and use of mobile devices among the workforce. These typically allow employees to choose a supported mobile device from a pre-approved list, instead of giving them the freedom of using any device and mobile OS as under BYOD.

Analyst Aberdeen Group also warns that the typical BYOD programme can cost a third more than allowing staff to use company-owned devices across a corporate wireless network.[9]

With CYOD the employee still gets a degree of choice but for the company this ownership gives it more control over the security of the devices and means it can standardise to some degree with the mobile operating systems and devices it supports. SAP is one company that has gone down the CYOD route, giving its users the choice of 10 devices across three mobile platforms.[10]

Regardless of the policy chosen, most businesses now have the challenge of keeping up with the pace of multi-OS change driven by the relentless march of consumerisation.

The insider threat

The human factor, whether deliberate and malicious or accidental, is still one of the biggest security headaches for IT departments and it is no different in the mobile era. Insiders were identified as the main cause in almost a quarter of security breaches in a CERT CyberSecurity Watch survey.[11]

There are tangible costs associated with failing to tackle all these mobile-related security threats. Organisations failing to properly secure the data held on and accessed via employee mobile devices face prosecution and sanctions under the UK's data protection laws.

The UK data protection watchdog, the Information Commissioner's Office, has issued a warning to businesses, particularly around the use of employee-owned devices for work, saying "it is the employer who is held liable for any breaches under the Data Protection Act".[12]

A global survey by security company Check Point also found that almost 80 per cent of businesses admitted to having a mobile security incident in the past year. Just over half (52 per cent) of large companies said the cost of mobile security incidents in the past year exceeded $500,000, while 45 per cent of small-to-medium sized enterprises (SMEs) reported mobile security breach costs exceeding $100,000.[13]

[9]http://www.cio.com/article/703511/BYOD_If_You_Think_You_re_Saving_Money_Think_Again
[10]http://www.zdnet.com/cyod-to-rise-amid-death-of-byod-in-2014-forecasts-idc-7000023676/
[11]http://www.cert.org/archive/pdf/CyberSecuritySurvey2012.pdf
[12]http://ico.org.uk/news/latest_news/2014/new-years-resolution-to-have-a-clear-personal-device-at-work-policy-08012014
[13]http://mobileenterprise.edgl.com/news/The-High-Cost-of-Data-Breaches88246

4. SECURITY AS A BUSINESS ENABLER IN THE SUPERFAST MOBILE AGE

As we move into the post-PC era and from the traditional desktop environment, IT security is a critical layer in what we at EE call Total Enterprise Mobility.

The network is the foundation of this, with 4G opening up mobile devices as genuine corporate business tools.

In the US, which is ahead of the UK in terms of 4G rollout, businesses are already seeing the benefits. In a study by Arthur D Little of US businesses using 4G, just over two-thirds (67 per cent) said they had seen increased productivity, almost half (47 per cent) said it had helped them cut costs and 39 per cent said it had helped them win more business.[14]

"MOBILE SECURITY IS THE LAYER THAT ENABLES ORGANISATIONS TO REMOTELY CONFIGURE DEVICES TO USE SECURE NETWORK CONNECTIONS, TO DEPLOY SAFE APPLICATIONS AND GIVE EMPLOYEES SECURE ACCESS TO CRITICAL BUSINESS CONTENT."

Here in the UK, business adoption of 4G continues to rise significantly across a wide range of organisations small and large, including the likes of Expedia, Foxtons, IKEA, RAC and London Air Ambulance.

"4G OPENING UP MOBILE DEVICES AS GENUINE CORPORATE BUSINESS TOOLS."

Construction company Kier is rolling out 4G across its sites as an alternative to traditional fixed line connections, while London estate agent Foxtons is using 4G to allow its agents to update its property database remotely.

These are just some early adopter examples and it is clear that 4G will boost employee productivity by giving them reliable immediate access to high-bandwidth corporate data and content on the go.

Mobile security is the layer that enables organisations to remotely configure devices to use secure network connections, to deploy safe applications and give employees secure access to critical business content.

[14]http://business.ee.co.uk/ad-little

5. MANAGING SECURITY IN THE MOBILE ENTERPRISE

The many benefits of mobilising the workforce include boosting productivity and agility, enabling flexible working and improving employee engagement. To fully reap these rewards organisations need to allow mobile access to the critical content, data and applications that employees need for their job. From a security perspective this requires a comprehensive approach that covers the network connection, device, application and content.

"SECURING THE DEVICE, APPLICATION AND CONTENT FOR A MOBILE WORKFORCE REQUIRES A COMPREHENSIVE STRATEGY THAT DEMANDS A SPECIALIST SET OF TOOLS."

There are a number of approaches to securing network access that ensure only trusted devices can gain access. These include virtual private network (VPN) services that provide a private network access point that only registered devices can access and the secure connectivity option provided by the BlackBerry Enterprise Server infrastructure.

Securing the device, application and content for a mobile workforce requires a comprehensive strategy that demands a specialist set of tools. Originally such tools were referred to as mobile device management (MDM) but as these have evolved to also manage applications and content, they are increasingly referred to as EMM. These tools go far beyond simple configuration tasks such as the set up of a password. Such a toolset needs to work across multiple mobile OSes, be managed through an easy-to-use central management console and allow settings and policies to be grouped to make it easy to apply security to users with similar security needs. An effective EMM solution should include:

Mobile Device Management (MDM)
MDM gives IT departments a way to control and protect both employee-owned and corporate-owned mobile devices. MDM tools enable security settings on devices to be centrally configured and then remotely managed by the IT team. As we have already revealed earlier in this white paper, loss and theft of mobile devices remains one of the biggest reasons for corporate data being compromised. MDM allows organisations to set and enforce password policies, encrypt data and remotely lock or wipe handsets or tablets in the case of them being reported lost or stolen. These settings can be grouped and applied to segments of users with similar security needs.

Mobile Application Management (MAM)
MAM focuses on the mobile application layer and controls the provisioning and access to apps -- whether internally developed or from a commercial apps store -- to the workforce. Secure access to business apps is a critical element in realising the full benefits of mobilising the workforce by giving employees access to data wherever and whenever they need it. MAM is designed to keep company

"MDM ALLOWS ORGANISATIONS TO SET AND ENFORCE PASSWORD POLICIES, ENCRYPT DATA AND REMOTELY LOCK OR WIPE HANDSETS OR TABLETS IN THE CASE OF THEM BEING REPORTED LOST OR STOLEN."

apps and data secure, using techniques such as containerisation, while also providing distribution and configuration mechanisms so employees can quickly and easily access those apps and data. Containerisation creates a secure container on the device that keeps company apps and data secure and separate from the employee's personal apps and data. This allows for the company-owned apps and data to be remotely wiped in the event of a security breach while still leaving the employee's personal data intact. MAM also enables organisations to track usage patterns of apps, which can be useful in analysing which corporate apps are delivering value and which aren't.

Mobile Content Management (MCM)
With superfast mobile networks and cloud-based applications supporting more flexible and productive ways of working, MCM enables organisations to control the content layer when it goes mobile and allow employees to securely access, share, collaborate, edit and send documents, presentations, sales reports and other information from their mobile devices. In this way MCM is another critical element in helping organisations realise more benefits from enabling a mobile workforce. It means they no longer need to rely on email to distribute content. Instead services such as Microsoft SharePoint enable organisations to create secure access to content repositories. Securing this content when it is at rest on the device is key. MCM will also typically allow email attachments to be secured and support restrictions on what can be done with that content in terms of tasks such as saving, copying, pasting and editing.

"MCM ENABLES ORGANISATIONS TO CONTROL THE CONTENT LAYER WHEN IT GOES MOBILE AND ALLOW EMPLOYEES TO SECURELY ACCESS, SHARE, COLLABORATE, EDIT AND SEND DOCUMENTS, PRESENTATIONS, SALES REPORTS AND OTHER INFORMATION FROM THEIR MOBILE DEVICES."

6. SECURITY AND TOTAL ENTERPRISE MOBILITY

Total Enterprise Mobility is far more than just improving workforce productivity. It is also about engaging with customers better, driving innovation and revenue growth and new business opportunities. Total enterprise mobility is a holistic integrated strategy that builds on a superfast network to join the pillars of workforce, customers and connected machines.

The security layer is a key enabler of this and it relies on working with the right partner. We offer a range of security tools for all major operating systems to secure devices, the network, applications and content, ensuring your data stays your data. Here at EE we know that one size does not fit all and we take a flexible and collaborative strategic approach to your business needs. As suppliers of devices across all major manufacturers and OSes we are agnostic and in a unique position to advise on both devices and an appropriate security solution to deliver on the Total Enterprise Mobility vision.

"TOTAL ENTERPRISE MOBILITY IS A HOLISTIC INTEGRATED STRATEGY THAT BUILDS ON A SUPERFAST NETWORK TO JOIN THE PILLARS OF WORKFORCE, CUSTOMERS AND CONNECTED MACHINES."

Our trained, accredited security specialists look forward to working with you to enable Total Enterprise Mobility for your organisation.

Contact us on 08000 790853 to discuss how we could help your organisation.