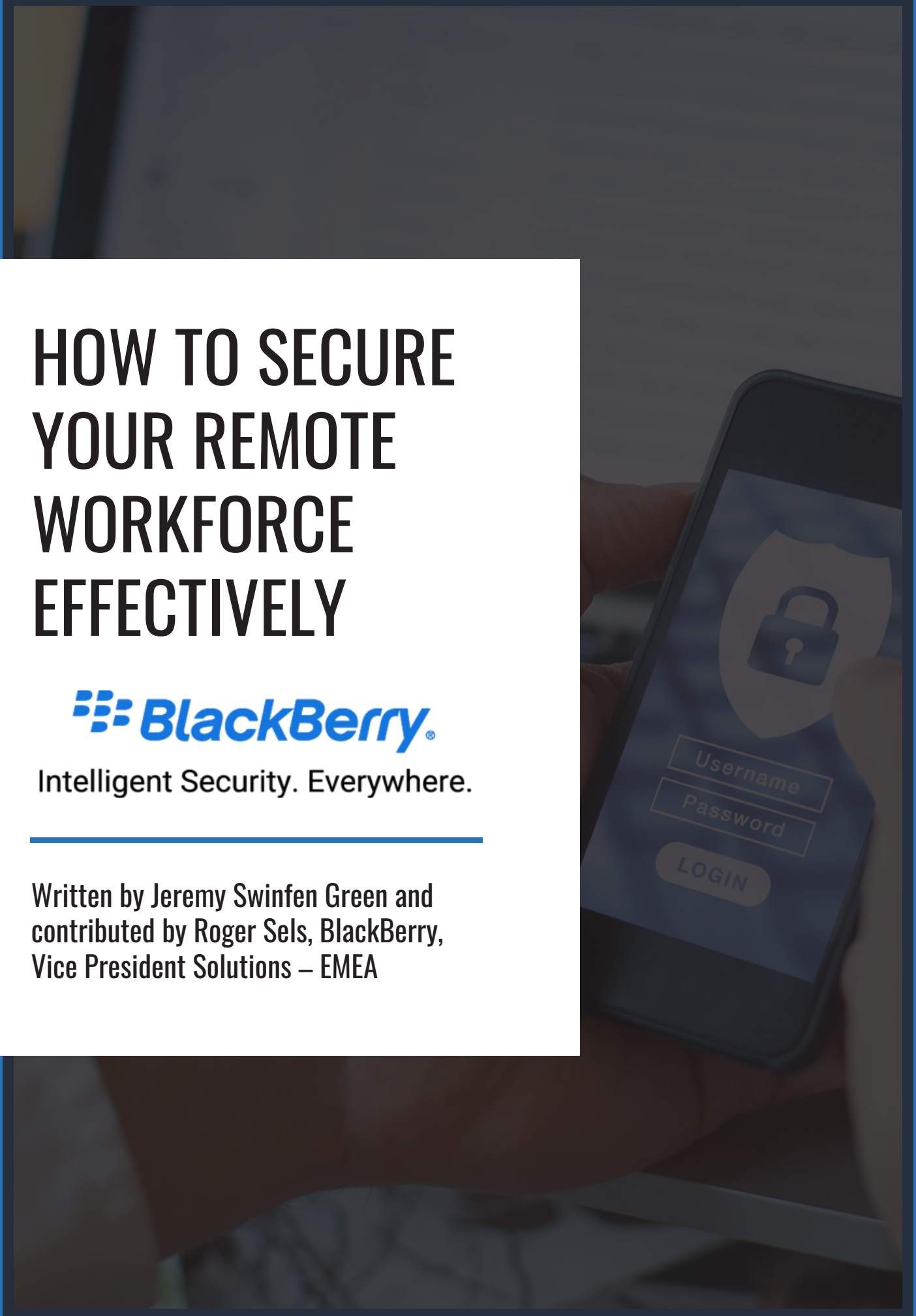
HOW TO SECURE YOUR REMOTE WORKFORCE EFFECTIVELY

BlackBerry

Intelligent Security. Everywhere.

Written by Jeremy Swinfen Green and contributed by Roger Sels, BlackBerry, Vice President Solutions – EMEA



HOW TO SECURE YOUR REMOTE WORKFORCE EFFECTIVELY

The Rise and Rise of Remote Working

Remote working is increasingly common. In 2019, over two-thirds of U.K. companies said they had a flexible working policy, allowing at least some of their employees to work remotely. For many workers, especially flexi-workers, remote working is the new normal. People on flexible contracts increase their efficiency by becoming digital nomads, taking their work with them wherever they go.

In some cases, remote working is caused by people having to visit several different places for work. Mobile workers hot-desk in different buildings as well as staying online and in touch when travelling between locations.

Remote working is often down to managers recognising that workers who are allowed to work from home on occasion tend to be more productive,[1] less stressed, and happier at work. It's unsurprising then that more and more of us are working from home. Between 2008 and 2018, the number of people working from their own home in the U.K. rose by 74%.[2] By 2019, around 20% of the U.K. workforce, over 5 million people, were sometimes working from home.[3]

1. http://assets.regus.com/pdfs/iwg-workplace-survey/iwg-workplace-survey-2019.pdf
2. https://www.bbc.co.uk/news/business-48180804
3. https://www.merchantsavvy.co.uk/remote-working-statistics/

Making Remote Working Work

The advantages of remote working are clear. People can work anywhere, which makes them more time efficient. Away from a normal office environment, they may well have fewer distractions, which can result in greater productivity. And remote workers save the time commuting to and from offices.

There are, of course, concerns that managers need to address if remote working is to be beneficial for an organisation. Many of these are cultural issues. If people aren't used to working from home, they may find the discipline required difficult. Colleagues may be less likely to interrupt, but family members can demand attention. And to many people, especially in the U.K., the office is a key part of their social life: working remotely can cause feelings of loneliness.

Management culture is also important. Without trust, managers may be tempted to micromanage remote workers, causing frustration and disengagement. And special techniques are needed to manage people working away from the office; handled badly, teams that include remote workers may fall apart, and individual remote workers may find it hard to prioritize or make decisions.

There may also be technological issues to deal with. Unless remote workers are provided with corporate computing equipment, which can be a very expensive thing to do, organisations are reliant on the technology used by their employees. Any required standards around security and licensing will be difficult to impose. And, home Internet connections may be slower.

However, the major issue for organisations relying on technology provided by their employees is security.

Not Remotely Secure

Personal Devices

Some home computers run older operating systems like Windows® 7 that are no longer supported by security updates. This is clearly a problem. And even with more up-to-date operating systems, the security provided may be inadequate. Any endpoint protection provided as part of a home computing package may not be turned on, or may be inadequate or not up-to-date

To make things worse, any work-related activity on a personally owned device can be hard to audit, while work files that have not been transferred to a corporate IT environment are at risk of being lost or deleted.

Security in the Cloud

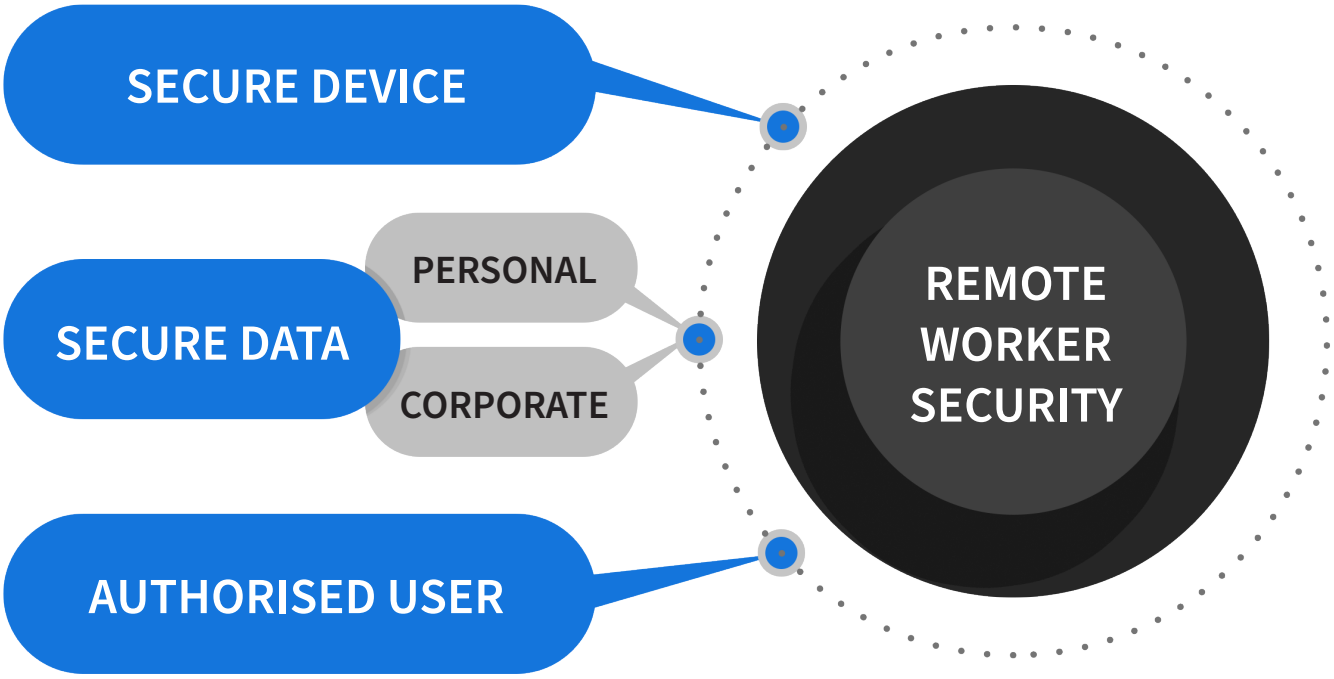
In recent years, there has been a strong trend to move data and applications to the Cloud, computer storage that is accessed over the Internet. This is often because the Cloud can bring major cost savings, although it also provides many benefits around flexible working.

The Cloud makes remote-working and home-working far easier. But as far as security goes, it has its downsides. This is in part because the Cloud has driven an important change: where organisations used to keep their data within a secure IT perimeter, the Cloud has led to a world where secure IT perimeters are at best virtual and at worst impossible to create or maintain.

People working outside a secure corporate IT perimeter, for instance in hotels and cafes, may connect to corporate data held in the Cloud through unsafe Wi-Fi connections. They may be exposed to malware or man-in-the-middle attacks. It is fairly simple to protect against these risks if the employee installs and uses VPN (virtual private network) software, but it is harder for the employer to know that a VPN has been installed or is being used correctly.

Making Remote Working Safe

Organisations that allow employees to work remotely need to focus on three things if they are to secure confidential information: securing the devices that are being used, securing the data on those devices, and making sure the people who use those devices are authorised to access the data.



Personal Devices

The first step to security is to ensure that all devices used by remote workers to access corporate data are protected. Supplying corporate laptops to remote workers is expensive, perhaps unnecessarily so when so many workers already take their own devices to work, whether formally allowed or not.

Where bring your own device (BYOD) is happening, organisations need to take steps to keep personal devices, and the corporate information on them, safe, while at the same time ensuring the privacy of personal data stored on these devices is maintained.

Policies need to be written, and then explained to workers, that define the security steps they should be taking. These may include using anti-malware services that update automatically, using secure web browsers, avoiding public Wi-Fi or installing VPNs that activate when Wi-Fi is used.

Some workers will be confident about installing anti-malware and VPNs, but many will need help, either with the cost or with set up and use. Inevitably, this is complex and expensive.

A better solution is to use a standardised security system, like BlackBerry® Desktop, which can be rolled out across multiple devices and which can be centrally controlled. This gives the enterprise confidence that remote workers really are secure as well as making it far easier to implement security for new employees and deny access to confidential data for ex-employees.

Another advantage of using a standardised security package is that it is far easier to ensure that workers understand how they should be using it. If security software is being applied to personal devices, the experience of the end-user is key. Any software that interferes with a worker's ability to undertake normal tasks, especially personal tasks, is likely to be uninstalled. By using standardised software, common user problems can be identified and appropriate help to overcome them given.

Securing Data

The next step is to ensure that data on devices used by remote workers is kept confidential and accessible. If the device is secure, then the data on it should be secure from external attacks. But there is still the problem of internal breaches.

Remote workers may share data inappropriately, perhaps with clients to make projects work more slickly, or even with competitors if they are hoping to move jobs.[5] Organisations need a way of preventing this.

Implementing centralised "data loss prevention" (DLP) controls can prevent this either by warning workers that a particular file may be inappropriate to share, or by physically preventing it being shared outside an authorised group of people. However, most DLP solutions only protect files from leaving an organisation; once a document has been shared externally (for a legitimate purpose or having been smuggled out) the control is no longer in place. And crucially, this is precisely where and when it is needed the most.

5. It's generally a very bad idea to employ someone who offers you data from their current employer. If they are willing to do this then they are very likely to be untrustworthy to handle confidential information appropriately.

There is also an important issue around personal data on personal devices. It is not appropriate for an employer to have access to all the content on a worker's private laptop or phone. Personal documents and emails should remain private, inaccessible to the employer.

But they should also remain accessible to the employee. Accidental deletion of personal data should not be possible. For instance, when a remote worker leaves their employment, corporate data must be deleted from their private device. But personal data like family photographs must not be deleted at the same time. The solution here is to "containerise" the work-based data so that it is separate from personal data and documents and can be managed separately.

Authorising users

Securing devices and the data on them is rarely sufficient. There is also a need to ensure that the person who is accessing corporate data on the device is authorised to do so. A personal tablet computer might be used by different family members, for instance. If a remote worker logs on and then leaves the room for some reason, data on the device may be open for all to see.

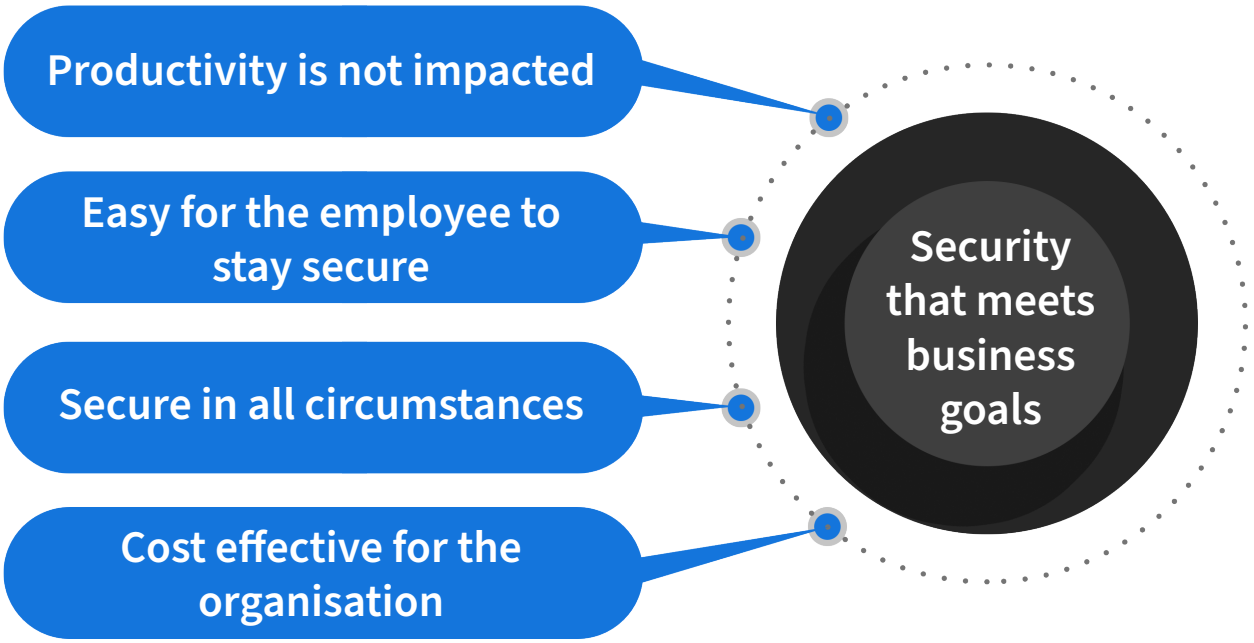
Authenticating the user, periodically, is therefore essential. Security managers should have a "zero trust" philosophy where things like the identity of a user are not taken for granted. Artificial Intelligence (AI) has an increasingly important part to play here. Digital "footprints" can be built up so that over time AI systems can recognise typical and atypical behaviour and react accordingly.

For instance, if a user (or rather a device) suddenly tries to access data from an unusual geographic location, or if they try to access a set of files that they would not be expected to have an interest in, the security system might deny them access until they have been able to re-authenticate themselves in some way.[6]

6. A demonstration of how AI can enable reauthentication is available at: https://pages.cylance.com/en-us-2020-12-RSASneakPeek2020-OnDemand.html

Managing the risk

Security solutions for remote working must not have a damaging impact on productivity. They must deliver security in all circumstances. They must also be user friendly and allow flexibility. And they must be cost effective for the organisation. In other words, security needs to enable achievement of organisational goals. Achieving this is not a trivial challenge.



Security that promotes productivity

It's important for employees to stay secure and productive. This is a non-trivial challenge. Staying secure but only half as productive makes little sense. Unfortunately, there can be tensions between security and productivity:[7]

- 92% feel increased security has noticeably impacted productivity at their organization
- 58% prioritize strict security controls over ease of use and convenience for employees

7. IDG survey of 400 IT Professionals in the US, Canada & UK – Dec 2019 - Jan 2020

Over-strict security solutions that make it hard for employees to do their day job effectively are likely to result in well-intentioned security workarounds. It's very important to take account of this when evaluating endpoint security solutions.

Usable security

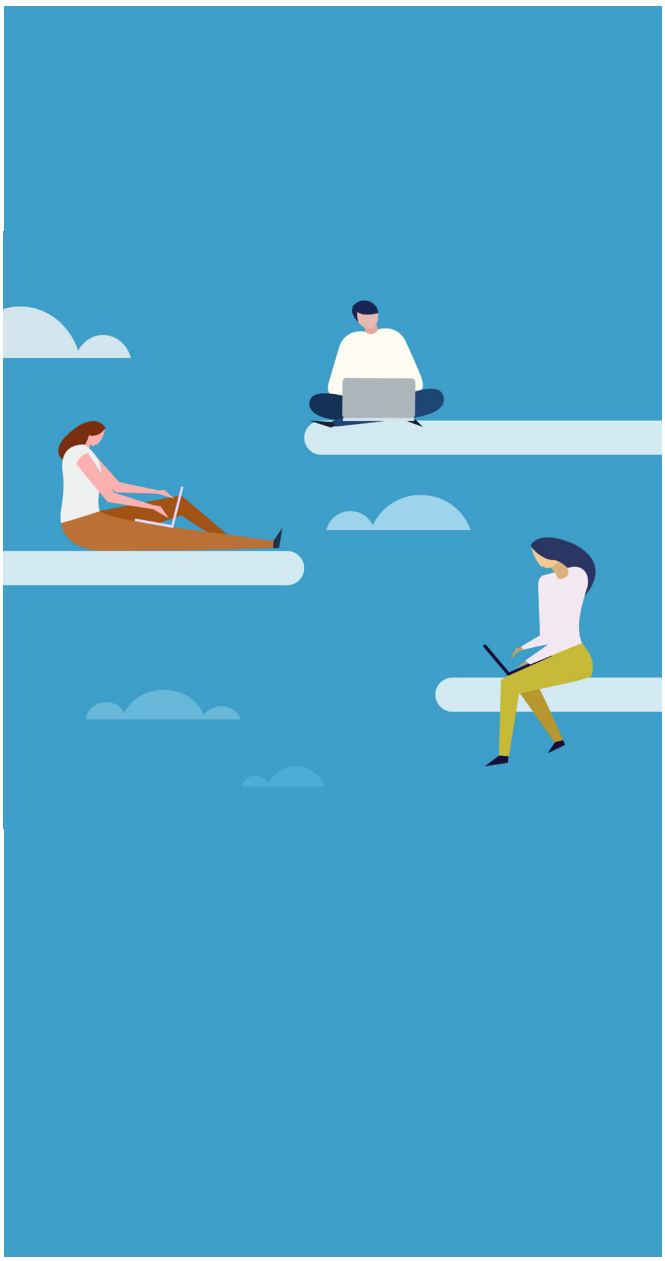
Effective security is also usable security. If security systems are easy to use and don't hinder efficiency, then mobile employees won't try to work around them.

For employees, usable security means security that does not make their life difficult by subjecting them to complex login and authentication requirements including complex passwords, time outs for slow logins and lock outs after a small number of failed logins). In addition, from a user perspective, usable security will enable, or at least not obstruct, easy collaboration between people working on projects together.

For managers, usable security enables the efficient onboarding, promotion and offboarding of employees, ensuring that they are only able to access appropriate content or restricting the locations, times and devices that content can be accessed. In addition, it enables employee access privileges to be reviewed from time to time.

One important consideration is scalability: a good solution will work well for large teams, enabling security to be managed without unwieldy requirements such as having to review, on an individual basis, permissions which are common to the whole team.

Usable security should also enable the monitoring and remote wiping of computers, and where personal devices are being managed ensuring "absolute personal data privacy": that only the corporate data, held in a containerised part of the device, is affected.



Effective security in all circumstances

For mobile workers, smarter security is more effective: security must adapt with the circumstances and with the risk associated with different circumstances.

Cyber security risks vary in likelihood and impact for many reasons. Likelihood may depend on who is accessing data (Are they trusted? Do they have the right experience? Do they need to access this data?), where are they accessing from (Is it a secure location like a branch office or somewhere less secure and private like a café or airport terminal?), what device they are using (Is it a corporate laptop or a personal phone?), or when are they accessing (Is it at a suspicious time such as 4 am, if that user is rarely connected at that time?). Impact may depend on what are they accessing or how much data they want to download.

Flexible security is the way forward. As the risks change then, based on real time risk scoring, the security requirements may change with perhaps more stringent login processes being demanded. The user privileges may also vary with perhaps certain files only available when they are within the employer's offices, a known working-from-home location or a pre-authorised mobile location such as a hotel.

Effective security in all circumstances

Naturally enough, security always comes with a cost but there are very few organisations where security-at-any-cost would be acceptable. (Some mission specific environments where cost is of little importance include military and anti-terrorism systems and potentially catastrophic infrastructure such as nuclear power stations.) The cost can be measured as a cost per user licence or "seat"; but there are also costs involved with managing security systems, including updating them and testing them.

In addition, it's important to take account of the fact that organisational requirements change. This means that it is important to use security systems that are easy to scale, up and down, and flexible enough to adapt to changing circumstances such as mergers or a change in the regulatory landscape. In a fast-moving world, agile and flexible security is essential.

Secure, private, usable and efficient

Remote workers need to be confident that they are working securely, and that security isn't getting in the way of them doing their day jobs. At the same time they need to be confident that, by using their private devices, they are not exposing themselves to snooping by employers or to the risk of losing valued personal documents.

And in their turn, organisations need to be confident that their mobile workforce is keeping confidential corporate data safe and that they systems that enable this safety are cost effective and flexible.

JARGON BUSTER

Artificial Intelligence (AI)	The ability of computers to perform tasks that would normally require a human being. There are different types of AI relevant to security including Machine Learning (qv) and Natural Language Processing (qv)
Bring Your Own Device (BYOD)	The practice of allowing employees to use personal laptops and smartphones to access corporate data and documents, in the office and also when working remotely
Cloud computing	The storage and accessing of documents, data and software in remote computers that have to be accessed over the internet rather than over cables within company locations
Containerisation	An essential tool for securing the personal devices of remote workers, where personal data and documents are separated from corporate data and documents
Data Loss Prevention (DLP)	Software that restricts the external sharing of documents that have been marked as sensitive, or that prevents them from leaving an organisation's corporate IT network
Hot desking	The practise of using any desk that is available in a workplace; hot desking reduces the number of workspaces within an office that need to be provided. However, it can be unpopular with people who frequently work in the same office location
IT perimeter	Part of the traditional architecture of an organisation's IT structure, the perimeter can be likened to a wall around an organisation's data, within which it is secure and outside which it is at risk. Increasingly as BYOD (qv) becomes popular, the perimeter is less like a wall and more like a Swiss cheese
Machine learning (ML)	The ability of a computer to change the way decisions are made based on the result of previous decisions
Malware	Software that is designed with a malicious intent; examples include ransomware (software that locks users out of computer systems until a ransom is paid), key-loggers (software that logs keystrokes including login details such as passwords and sends it back to a hacker), and viruses (software that is capable of copying itself with a detrimental effect, such as corrupting an IT system or destroying data)
Man in the Middle	A way of intercepting data (such as passwords) that is input to a website when public Wi-Fi is being used. The data is sent to the desired destination but travels via a hacker's computer where a copy is taken
Natural Language Processing (NLP)	NLP involves a computer analysing the meaning of words in documents based on how they are being used, for instance within a sentence, rather than simply on dictionary definitions; this can enable the sensitivity of the document to be assessed automatically
Shoulder surfing	A method on spying on people, and perhaps discovering passwords, by simply watching what they type by looking over their shoulder or even through a window
Virtual Private NetworK (VPN)	A private network that uses the public internet to send and receive data securely
Zero Touch	The installation of a computer or other device onto an IT network without the need for someone with IT skills to configure it locally.
Zero Trust	The principle that organizations should not automatically trust anything or anybody inside or outside its IT perimeter

For more information visit
www.blackberry.com

BlackBerry.

Intelligent Security. Everywhere.