Enterprise networks in the “new normal”

Business
Services

Enterprise networks in the “new normal”

What is the long-term impact on enterprise networks of the new working practices necessitated by the Coronavirus?

We examine how it affects four areas: the home, network technology, the office and connected objects. The impact of the coronavirus pandemic is unprecedented in the modern age. The total lockdown of industries worldwide has created millions of new homeworkers. Collaboration technologies and networks have been the key to enabling some businesses to operate even through the most stringent restrictions.

While homeworking has been thrust upon most of us, will the change precipitate a revolution in working practices when we reach the end of the pandemic? Will businesses think that offices in central business Districts are expensive overheads, and will employees be reluctant to waste hours every week commuting?

In this paper we examine the long-term impact these changes in working practices could have on the network and enterprise infrastructure. We look at four different areas: homeworking, software-defined networks, the ‘new normal’ in the office and connected objects in the workplace.

Contents

Key takeaways

- Greater oversight on standards, equipment and behavior is required in the home office
- Adoption of software-defined networks (SDN) will accelerate, while integrating security and remote access
- Expect further consolidation in the SDN vendor market
- Offices should consider adopting zero-trust security along with ubiquitous high-speed Wi-Fi
- There will be a divergence of networks connecting objects and people in all working environments

The rise and rise of homeworking

Homeworking is one of the success stories of COVID-19 business continuity. Millions of employees are working from home connected to their organization via virtual private networks (VPN) and using cloud-based collaboration applications.

As we move through the pandemic, it's likely that many of these workers will want to continue to work from home and avoid the commute. Companies may also want to avoid spending heavily on large city center offices, particularly when governments are encouraging homeworking where possible.

What does this significant working change mean for home networks in the long run? Currently the typical arrangement with employees is that the employer provides the device and secure connection to the workplace, while the employee provides wireless hub and internet connection. But is this unsustainable if homeworking becomes more widespread?

Focus on security

The lack of control over home networks, particularly in terms of security, will motivate many enterprises to provide their employees with home networking connectivity, just like they do with laptops. This should include network equipment that they can remotely manage, and in some cases provide an additional internet connection dedicated to work use.

By exerting control over network equipment, companies can ensure that correct passwords and configuration are observed, and that employee network performance can be effectively managed for work use. It will also require that employees are subject to an audit of their home office environments to ensure their device and workspace is secure. This can be combined with a more thorough assessment of the home office to ensure that workers have enough space and an ergonomic workstation.

This is vital because the increase in homeworking could represent an increased risk for the organization. For example, hackers could unearth the home addresses of high-ranking employees and sit outside to compromise their network access. They could do this by spoofing the network name and harvesting the passwords quite easily.

Already COVID-19 has seen a massive spike in criminal activity[1] particularly around phishing and related scams. Therefore, it’s quite clear that companies need better oversight of their employees’ network infrastructure to limit this risk.

Potential of edge computing

The continued popularity of homeworking will see its adoption by job roles that have previously struggled to work effectively at home. In some cases, there is a cultural or practical reason why this isn’t possible, for example leisure services or veterinarians. But in others, technology is a barrier, particularly in terms of processing capacity.

Here, edge computing could help if it were implemented in the home environment. This would support specialist, high-performance applications, by allowing some processing to be done locally as an extension of the hyperscale platform.

The sort of roles this could support include traders in the financial services industry who have high processing requirements for trading desks with multiple screens[2]. Others include industrial designers who have a requirement to work on high-bandwidth CAD files, and even medical professionals who have high processing requirements for applications like scans. All of these roles would have previously been unable to work from home – but advances in technology promise to revolutionize their experience.

Key points

- Growth in enterprise-controlled home network infrastructure
- Technology audit and governance of home offices
- Deployment of edge computing to support demanding job roles

The future network is software defined

Digital services are proving themselves invaluable during the coronavirus challenges. Rapid deployment of new services requires an agile and flexible network infrastructure that can be deployed on demand. This will accelerate the move towards software-defined networking (SDN).

One impact of the coronavirus pandemic is the need to limit the reliance on human management to build and operate network platforms. At the peak of the pandemic many enterprises struggled to ramp up capacity quickly to deal with the increase in home users, partly because there was a need for some network services to be installed by an engineer.

This is driving a need for plug-and-play equipment to allow self-installation by non-technical staff and remote provisioning of network functions. Because SDN allows for automation and centralization of many key network functions, it will be perceived as providing mitigation for future disruption and potential lack of availability of staff.

SDN allows for the automation and centralization of many key network functions to protect enterprises against disruption

Security, network convergence

In addition, because remote access has emerged as one of the most vital network services in the pandemic, SDN vendors and service providers are increasingly including remote access functionality as standard[3] within the technology. In some cases, homeworkers will be candidates for SDN deployment, particularly in senior roles where high-performing network connections are vital. Here the traffic management ability of the technology is key in ensuring corporate application performance.

In parallel, there is also a push from security vendors who are looking to include networking capabilities in their security devices. They can realize strong synergies by converging their security technology with SDN. Networking vendors are already on the lookout to acquire challenger SDN such as Palo Alto's acquisition of Cloudgenix[4].

In fact, further consolidation in the market is highly likely. Challenger vendors will face venture capital funding issues in a constrained economy, which will make enterprises reluctant to choose them for their long-term technology roadmap.

Also, on the technology side, there is an increasing convergence of SD-WAN and SD-LAN functionality on the same device[5]. This type of SD-Branch appliance will handle all network, security, and related functionality for the site. It will effectively enable end-to-end security and performance management for network traffic and applications.

Commercial models

Enterprises will also be looking to take advantage of the flexibility of SDN and ask for commercial models that are more utility-based and able to reflect the ability to dial down or switch off network services. For example, if the SDN network is extended to home offices, enterprises might want higher bandwidth when the office is being used, and the ability to turn it off when it isn't.

Key points

- Enterprises look to SDN for zero-touch provisioning and plugand-play installation
- Convergence between SD-LAN, SD-WAN, remote access, and security
- Further consolidation in SDN market expected
- Demand for commercial models that can turn bandwidth off as well as on

Network and security in the “new normal” office

The modern office has seen many changes over the past 50 years. What long-term impact will the pandemic have on the office and its infrastructure when the lockdown ended?

Many industries have successfully deployed homeworking, even in functions that previously were wholly office-based. However, even with increased homeworking in the long term, there is an important role for the office to play in face-to-face collaboration and meetings.

In addition, a significant number of employees will be keen to return to the office once the lockdown is over. For them, the social aspects of the office environment will be attractive after months of self-isolation. Questions will be asked, however, at the highest levels of business as to the real benefit of expensive office locations and what the post-COVID office should look like.

‘Starbucksification’ of the office

Many enterprises are already starting to consider the Starbucksification of the office. One aspect of this is changing the layout of the office away from fixed desks into something more like a café. This will support the nature of modern work where ever-shifting multidisciplinary teams collaborate on different projects.

Supporting this way of working will require a total overhaul of the office IT and network architecture. In this context, Starbucksification applies to the wide availability of high-speed open Wireless Local Area Network (WLAN) with Wi-Fi. Just like in a café, access to the Wi-Fi network will be provided on a zero-trust basis. Essentially this means that every device would be responsible for its own authentication – regardless of physical location or IP address.

Why zero-trust security?

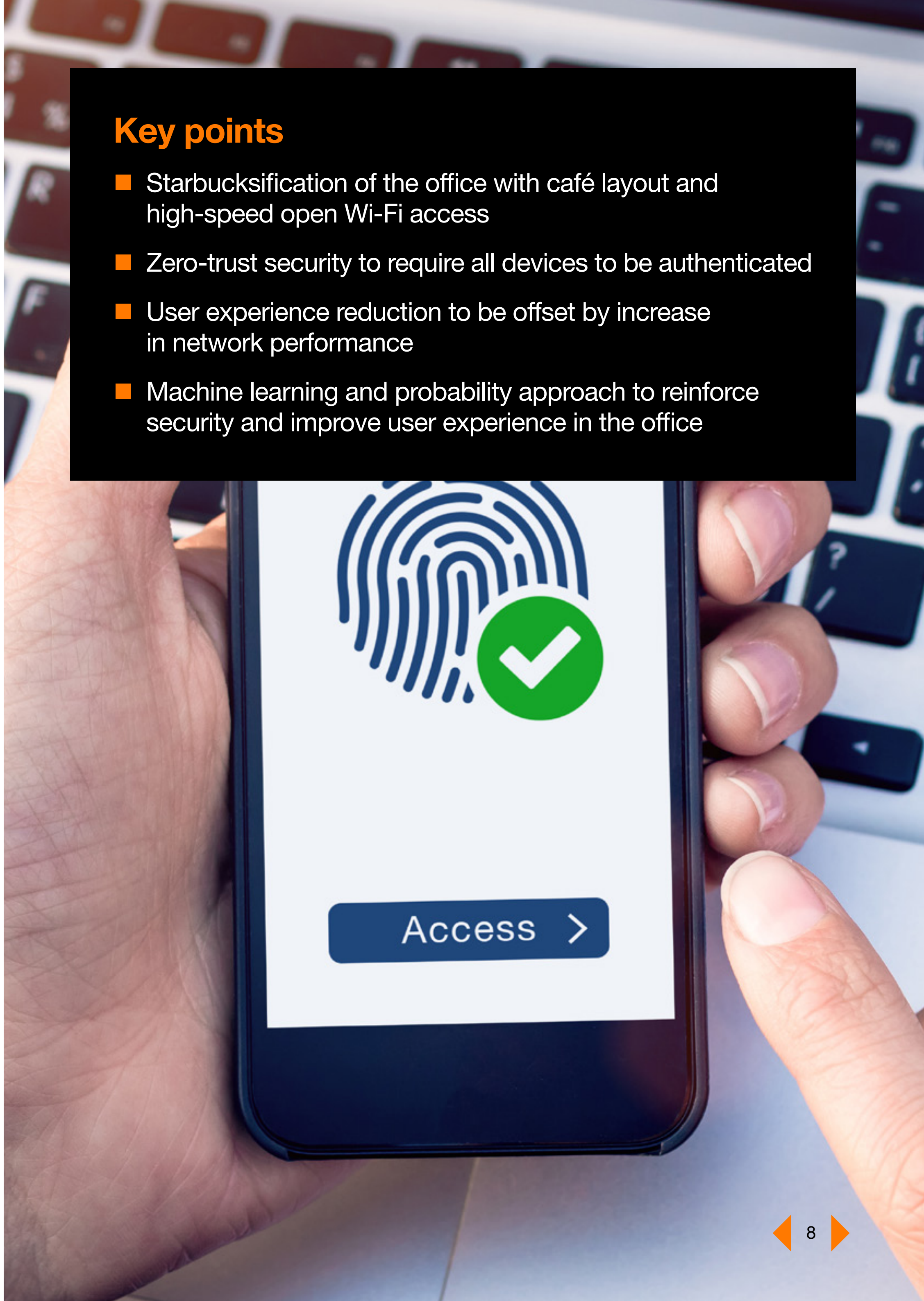
This is quite different from the traditional approach, where a company-owned device would automatically access the Wi-Fi network in the office. The key advantage of zero trust is that it increases security significantly[6]. Because every device is responsible for its own security, the network controller does not trust it until the user has established credentials – irrespective of whether the device is work-owned or personal. Zero trust also provides one of the components of building a software-defined perimeter (SDP) for access to the cloud.

The reason this level of security has not become more established in the office is that it degrades the user experience. However, it is also quite similar to the experience of working from home and logging in to a VPN. After a period of homeworking, many employees will be more accepting of this leveling up of security in the office. The *quid pro quo* of zero-trust security from the user's viewpoint is that they will also expect to enjoy better bandwidth and network coverage in the office. The integration of SD-LAN into the network infrastructure will contribute to this by improving end-to-end network and application performance.

Risk-based analysis

In time, the user experience in a zero-trust office can be improved. The way to do this is to combine risk-based analysis and machine learning to make probability-based decisions on users. In other words, look at the context of the user and device to assess if they are who they say they are. Authentication is a key element of this[7], and a probability model would assess the time of day they are logging on, what sort of device it is and how quickly are they making requests? This can be combined with the behavior of the user, such as are they downloading files, or copying, and does their activity look like a script or a user?

This type of probability model can give the system a level of confidence that the user is who they say they are and reduce the security requirements. Or conversely, it can ask for additional levels of credentials if there is low confidence in the user. This approach is already widely used in other security applications, such as biometrics, so it is practical to roll out in the office environment.



Key points

- Starbucksification of the office with café layout and high-speed open Wi-Fi access
- Zero-trust security to require all devices to be authenticated
- User experience reduction to be offset by increase in network performance
- Machine learning and probability approach to reinforce security and improve user experience in the office

Operational technology and automation in the workplace

Automation of services in offices will become increasingly important in the post-pandemic world. Operational technology will play a key role in managing the large numbers of connected objects that this will require.

The coronavirus pandemic will lead to more devices and services in offices needing to be remotely managed. This is because having on-site maintenance and facilities service employees for locations that are not fully occupied will make less sense. Deploying connected office solutions can help automate systems to organize meeting room bookings, control reception areas and manage all the connected devices in an office environment.

Operational technology (OT) will be key to successfully managing connected objects and automated systems in offices and other workplaces. Most people think of OT as an issue that only affects big production lines of factories, but it also plays a key part in managing any connected objects in the workplace. Enterprises wanting to remotely manage devices such as printers, coffee machines and thermostats will need to include them in their OT strategy and infrastructure.

Operational technology will be key to successfully managing connected objects and automated systems in offices

Security requirements

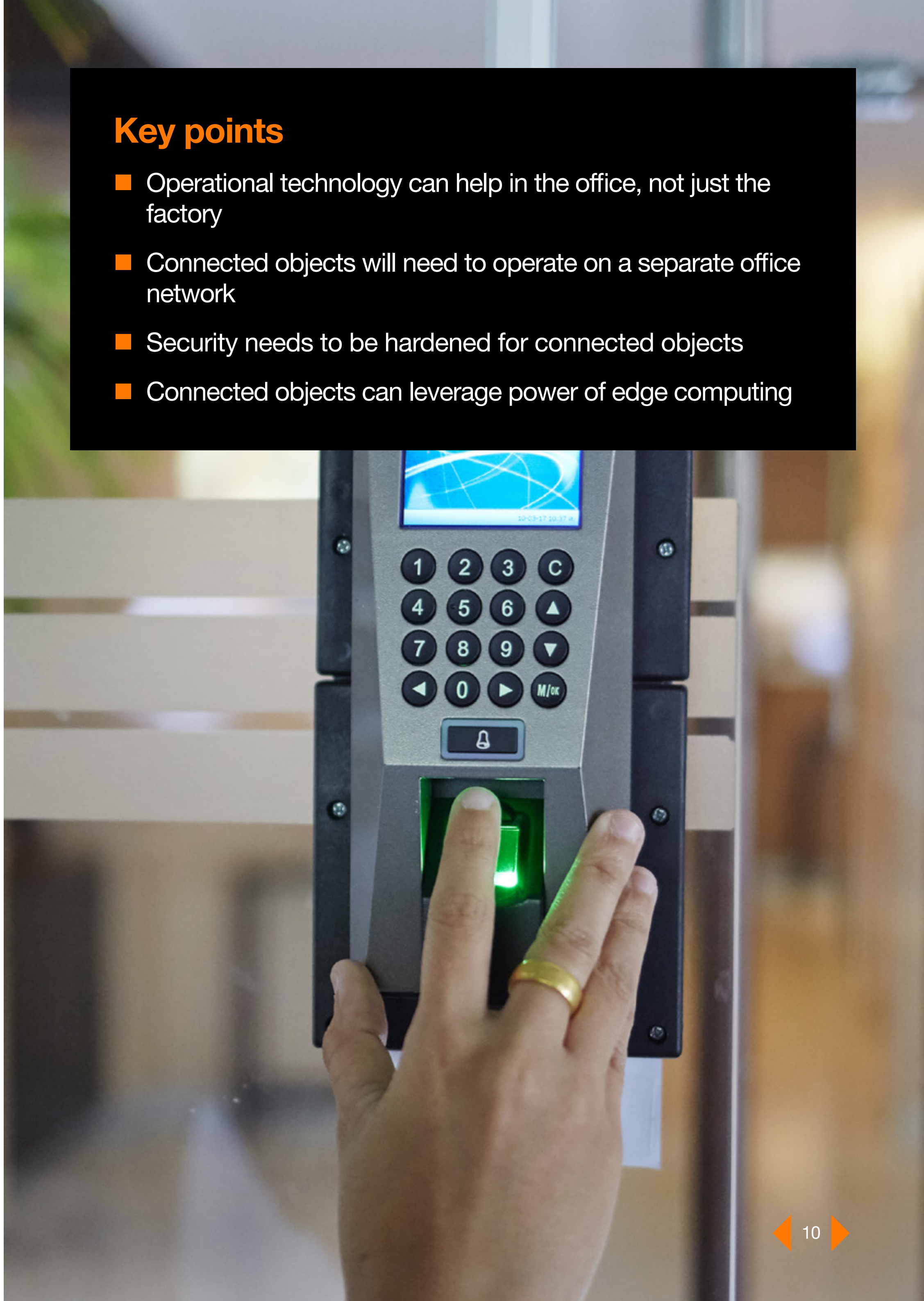
Security is one of the most important factors in managing the connected office. Applications run by these objects are, in general, more sensitive and cybercriminals will target them because they could open doors or set off the fire alarm. Connected objects on the network also offer entry into the corporate network and security breaches to these networks can be costly. This happened in the Target attack[8], where hackers gained access to credit card details through the air conditioning system.

Enterprises will need to treat the security differently for connected objects compared to the zero-trust approach outlined for employee devices. For example, connected objects are frequently fixed in position, so this can help dictate their security. One approach is to harden the OT network for initial sign-on, because these objects are permanently connected to the network. This means that once it is connected, the object can be trusted more.

Furthermore, the objects themselves will need to be more secure, with effective patching and security policies. Enterprises will be much more attracted to procuring objects that are secure by design and have a clearly documented patching process.

Role of edge computing

Applications for the connected office are also typically provided by specialists in vertical markets. Because they are fundamental to workplace safety, these applications often run on premise, rather than the cloud. However, edge computing could provide a way for the enterprises to leverage the power of the cloud in OT apps, with their dual benefits of proximity and scalability.



Key points

- Operational technology can help in the office, not just the factory
- Connected objects will need to operate on a separate office network
- Security needs to be hardened for connected objects
- Connected objects can leverage power of edge computing

If you are considering changes to your network, network security and the impact of the connected office on your organization please get in touch with the author at tom.gavin@orange.com

Sources:
1. COVID-19 and Cyberdefense (https://orangecyberdefense.com/uk/covid-19-and-cyberdefense/)
2. Coronavirus Forces Change for Sales and Traders Working from Home (https://www.finextra.com/blogposting/18658/coronavirus-forces-change-for-sales-and-traders-working-from-home)
3. Secure remote access-as-a-service is now a critical requirement (https://www.fiercetelecom.com/telecom/industry-voices-doyle-secure-remote-access-as-a-service-now-a-critical-requirement)
4. Palo Alto Networks Completes Acquisition of CloudGenix (https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-completes-acquisition-of-cloudgenix)
5. The convergence of networking and security at the edge (https://searchnetworking.techtarget.com/tip/The-convergence-of-networking-and-security-at-the-edge)
6. What is Zero Trust? A model for more effective security (https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html)
7. How risk-based authentication has become an essential security tool (https://www.csoonline.com/article/3271134/how-risk-based-authentication-has-become-an-essential-security-tool.html)
8. Target breach happened because of a basic network segmentation error (https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html)

orange™ Business Services