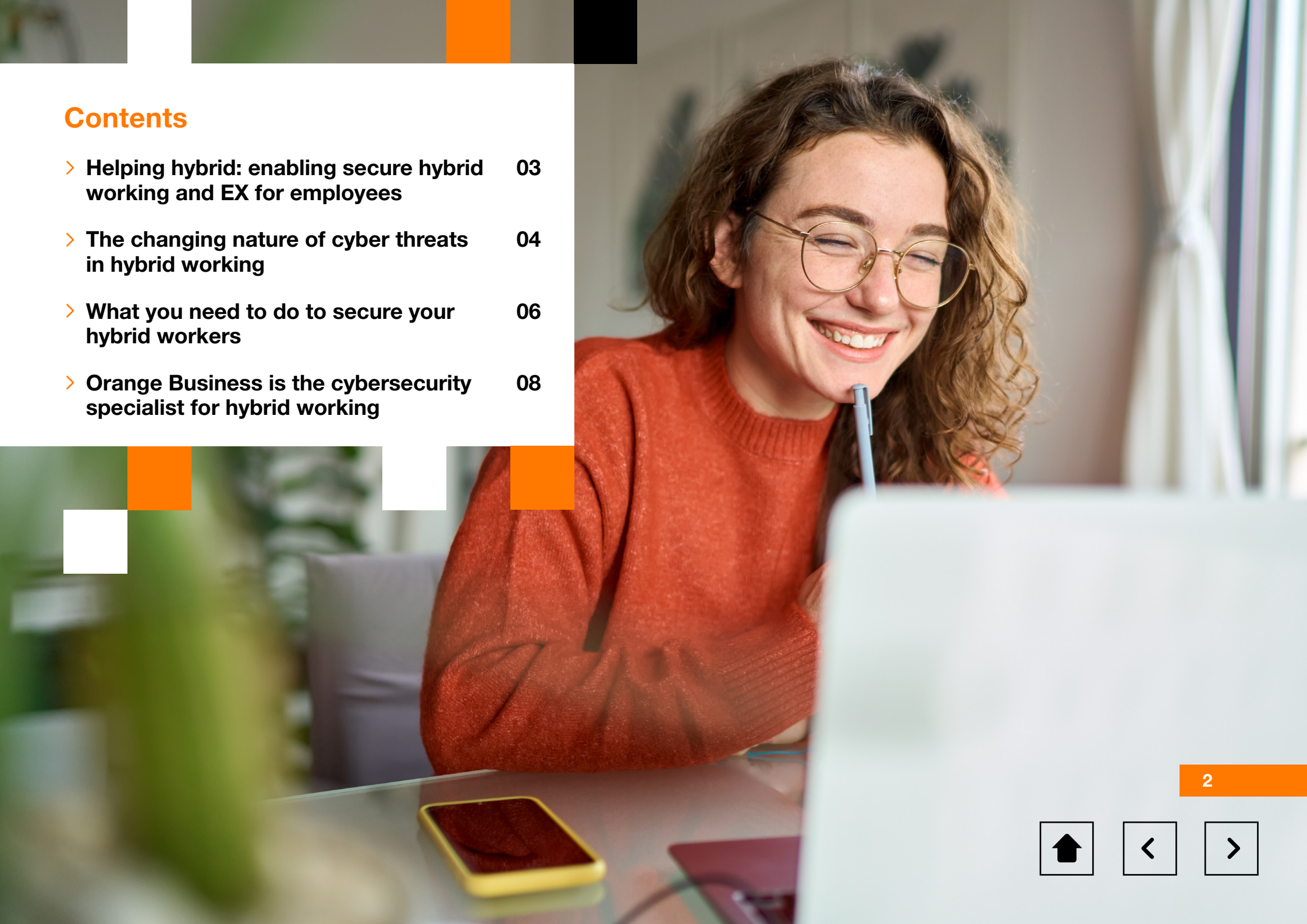

Helping hybrid: enabling secure hybrid working and EX for employees
orange™ Business
Microsoft

Contents



Helping hybrid: enabling secure hybrid working and EX for employees

Cyber threats continue to grow in frequency and variety. Orange Cyberdefense reported a 30% rise in threat detection events in 2023[1], with hacking, ransomware, and malware all on the increase. With more workers working in more places under hybrid working models, enterprises need to know what new cybersecurity steps to take.

Businesses have embraced the hybrid working model and are reaping the benefits it brings. One survey found that 58% of companies have seen improvements in individual productivity from hybrid work[2], and 49% report increases in team productivity[3].

Orange Cyberdefense detected cyberthreat incidents show a 30% increase year on year[4]

But the new ways of working require significant changes to how you approach cybersecurity. You now have a much bigger, very different ecosystem of devices and end-users to manage, in more locations, inside and outside the network perimeter. Typically, you only have limited resources and expertise to do it. Your IT teams and CISOs must work on minimizing risk to acceptable levels while not negatively impacting employee experience (EX) and hybrid working benefits.

Hybrid workers benefit from productivity tools like Microsoft 365, which comes with built-in cybersecurity features - but it needs the right support to help you maximize the ROI on the licenses companies have already paid for.

37% **of detected cyber incidents originate from internal actors, whether deliberate or accidental[5]**

28% **End-user devices were the most cybersecurity incident impacted asset in 2023 with 28%[6]**

The changing nature of cyber threats in hybrid working

The shift to hybrid working models over the past couple of years has meant a lot of adjustments for companies, with cybersecurity particularly impacted.

As ways of working evolve and workers begin to work more regularly from different places, cybersecurity has needed to evolve alongside them.

Under conventional approaches to cybersecurity, rules and practices were established and accepted. It was understood that work devices were configured and provisioned in the company offices, and doing so was safe and secure. There was a clear and defined network perimeter, and devices spent much of their time within that wall.

More than 90% of organizations have BYOD or personal device usage for work[8]

Now, devices and apps have shifted outside of the traditional network perimeter, as solutions like cloud and Software as a Service (SaaS) have grown and become essential to businesses.

With employees working from different remote locations, the traditional corporate network perimeter became a thing of the past. More endpoints in more places outside the network perimeter makes for a bigger, more diverse attack surface.

42% **of business leaders say they are particularly worried about the risks of a cyberattack[9]**

The changing nature of cyber threats in hybrid working

So, your company can be open to new types of threats, such as ransomware, that impact business continuity and cause financial losses. There's the possibility of data leaks that negatively impact your brand and can incur fines and litigation. Plus the always-there threat of hackers probing for ways in and attempting to steal sensitive personal or corporate data.

New technologies emerge and create potential new points of vulnerability, too. Your employees could be experimenting with productivity tools like new GenAI apps, and their insecure nature presents new risks. Indeed, AI and machine learning (ML) are likely to play a growing role in cyberattacks in 2024 and beyond, as cybercriminals leverage AI and ML to automate and enhance attacks to make them more sophisticated and adaptive. For example, in early 2024, a deepfake avatar of a company CFO was used to fool a finance officer into paying out $25 million via a video conference call[7].

There is so much for your IT teams and CISO to manage: all those devices and apps are now outside the perimeter, but you need your hybrid workers to enjoy an enhanced EX and be productive. And tools designed to help your workers be productive, like Microsoft 365, need specialist cybersecurity expertise to get maximized functionality and results, but with minimized risk.

47% **increase in enterprise phishing attacks year on year[10]**

What you need to do to secure your hybrid workers

With new ways of working, you need new thinking around cybersecurity. The Zero Trust model is key to a secure path forward.

Zero Trust cybersecurity starts from a position of not automatically trusting anything inside or outside company perimeters. Instead, it requires verification from anyone trying to access resources on the network, regardless of where the request comes from. Zero Trust assumes that threats can exist both inside and outside the network, thus removing the traditional trust assumption from network architecture. Access to resources is granted based on a strict verification process, following the “never trust, always verify” principle. Implementing a Zero Trust model involves several key steps:

- Identify sensitive data that needs protection
- Understand how data moves across your network
- Design your network with zero trust principles, segmenting networks and implementing strict access controls
- Implement multi-factor authentication (MFA) for strong verification of user identities
- Give users and devices the minimum level of access needed to perform necessary job functions
- Monitor network traffic for suspicious activity and maintain detailed logs for analysis
- Apply real-time threat intelligence to identify and respond to threats quickly

One key security principle is to deploy a detection and response service to monitor networks, systems, and applications for suspicious activity, identify security breaches, and respond to detected threats. Doing this means you can quickly mitigate and manage risks associated with cyber incidents. This approach typically uses advanced technologies and expert analysis to detect hard-to-find threats, and provide organizations with enhanced protection against cyberattacks.

The changing role of the CISO

Furthermore, the role of the chief information security officer (CISO) has evolved. CISOs were typically required to be experts in technical security know-how. Today, their role is that of a vital C-level visionary who is responsible for strategic cybersecurity and business growth.

CISOs need to focus on much more than just keeping viruses at bay: cyber risk management, compliance, and regulatory adoption, strategic business integration, crisis management, incident response, and more are all part of the mix.

Part of the CISO's remit is making security transparent for workers to be productive but risk-free. Zero trust approach can help, as can early detection and response using managed detection and response solutions. It's a big job, and must all be done at a time when there is a general cybersecurity skills and talent shortage worldwide.

As to the types of security technologies in use, CISOs are increasingly adopting Microsoft security solutions over deploying best-of-breed security products. This approach seeks to reduce the number of security tools deployed, streamline operations, and help companies maximize Microsoft 365 licenses they've already paid for.

Securing your hybrid workers: key questions for your IT teams

- How do you know you are using Microsoft security products in line with best practices?
- And how do you align solutions to your desired outcomes and know if they are going to deliver or not?
- How do you securely deploy GenAI chatbot tools that employees want, but also minimize misuse and cybersecurity risks?
- And how do you address the skills shortage around the Microsoft security stack and cybersecurity in general?

73%

of CISOs say when selecting a new security solution it is "extremely important" or "very important" that it enables a seamless EX on any device[11]

Orange Business is the cybersecurity specialist for hybrid working

Orange Business understands that companies need to empower workers without stifling productivity and creativity and so supports Microsoft Teams use with advice and auditing to identify cyberthreats.

Using our expertise in Cyberdefense and on Microsoft security products like Defender, Sentinel, Purview, and Entra, we help stop attacks across all digital assets, endpoints, identities, email, shared documents, multicloud application, OT, and ensure the maximum security baseline. By using Microsoft Security APIs, we offer managed detection and response services to detect threats, respond, and improve security posture.

Orange Cyberdefense is Europe's leading cybersecurity service provider[12]

We also offer security services like incident response retainer, vulnerability management and threat hunting to protect the most exposed enterprises, and our consultancy approach is designed to ensure cybersecurity solutions are tailored to your individual company need.

60bn logs and events tracked daily by Orange Cyberdefense threat detection

We have over 150 Microsoft Security certified experts and over 3,000 cybersecurity experts on hand to support you, and you have the peace of mind of knowing Orange Cyberdefense is a Microsoft security solution partner and one of only 40 MXDR vetted companies.

Steps to building positive productivity

- Create a digital workplace centered on users, their needs and how they want to work
- Develop an attractive employee experience to enhance satisfaction with digital tools
- Deploy a high-performing, flexible, scalable hybrid work environment that optimizes work/life balance
- Manage devices, operating systems and applications in a modern and efficient way and free your IT teams for more business-valuable work
- Work to build a responsible company every day, aligned with environmental, social and governance issues

To find out more about Orange Business and Employee Experience, please visit: https://www.orange-business.com/en/business-needs/digital-work-experience/provide-outstanding-employee-experience

And to learn more about secure hybrid working, please visit: https://www.orange-business.com/en/business-needs/digital-work-experience/enable-efficient-hybrid-working

Sources

1. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024
2. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work
3. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work
4. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024
5. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024
6. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024
7. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
8. https://techtoday.lenovo.com/sites/default/files/2023-08/IDC%20Whitepaper.pdf
9. https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year
10. https://newsroom.orange.com/ocd-harris/?lang=fr
11. https://www.securitymagazine.com/articles/99200-sixty-three-percent-of-cisos-predict-hybrid-or-remote-work-to-remain
12. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024

orange™ Business

Microsoft