



making sense of the
connected world

The Always-Connected PC in the New World of Work



HIGHLIGHTS

With most businesses now following hybrid working practices, employees are becoming increasingly reliant on constant connectivity to access cloud-based applications and processes and collaboration tools. Breaks in connectivity severely hamper productivity, delay business workflows and cause frustration.

With growing reliance on cloud-based solutions, the laptop remains at the heart of the technology experience and is the most important device in the employee's workday.

Generative artificial intelligence technologies provided with cloud platforms are enhanced

with constant connectivity. As these technologies are adopted at a rapid pace, reliable connectivity becomes a vital opportunity for businesses to embrace the next generation of connected laptops.

The constant connectivity of a 4G- or 5G-connected laptop removes many of the hurdles that inhibit productive working and create frustration for employees.

These devices can help lower the risk to businesses by providing reliable, secure connectivity and substantially reducing the need for employees to connect to unsecured public Wi-Fi hot spots or other potentially unsafe third-party connections.





The Era of Hybrid Work

The pandemic had a significant impact on the way we work. Widespread stay-at-home orders forced businesses not only to shift to remote work overnight, but also to rapidly digitize their processes and re-evaluate long-established cultural and working norms. Although some industries were more severely unsettled than others, every business felt an impact, with the pandemic proving to be the disruptor of a generation.

Most importantly, these effects were lasting. The prolonged period of remote work opened businesses' eyes to the greater flexibility in where and how employees work, and pushed them to adjust their operational practices to support the future workforce. There is no doubt that employees want to retain that flexibility: just 10% of respondents in CCS Insight's 2022 survey research ¹ stated that they wanted to return to the office full-time. However, our 2023 survey ² shows that 56% of desk-based employees have returned to full-time office work in a push to re-establish the office as the epicentre of productivity. Just 37% of employees operate as hybrid workers, combining regular contact with colleagues in an office environment with the benefits of remote working.

The prolonged period of remote work opened businesses' eyes to the potential of greater flexibility in where and how we work

Business leaders believe their desk-based workforce is pushing for greater levels of hybrid working, expecting 60% of the workforce to spend time working outside the corporate office environment ³, bringing significant opportunities for organizations to reduce costs. However, once the focus of work, in the era of hybrid working, the office is just a small cog in a business's operations.

Businesses Face New Challenges and Complexities

It is not just where people work that is driving changes for businesses. Organizations face a raft of operational and organizational challenges driven by the differing expectations of employees and increased digitization, many of which were exacerbated by the shift to hybrid working and global economic slowdown.

¹ CCS Insight Employee Workplace Technology Survey, 2022

² CCS Insight Employee Workplace Technology Survey, 2023

³ CCS Insight Senior Leadership IT Investment Survey, 2023

Employee Experience in a Tech Driven Workplace

One of the biggest concerns is how to hire and retain the best talent that will fuel the innovation needed to grow and remain competitive. A side effect of the health crisis was the weakening of ties between employees and their employers, leading to what was described as “the great resignation”.

Widespread remote working further highlighted the challenge of ensuring a distributed workforce remains not just productive but also engaged and connected, both to their immediate team and to the wider organization. In 2023, with businesses supporting hybrid working practices, the challenges have shifted slightly — the leading concerns for decision-makers are now managing hybrid teams, cited by 36%, and ensuring teams can work collaboratively and effectively, highlighted by 35% ⁴.

These concerns are shining a spotlight on the employee experience, an area that has attracted significant investment as businesses look to reduce attrition and court new talent by improving perceptions of the corporate brand. Although not the only factor, technology plays an important role in the employee experience, ensuring employees have streamlined and integrated access to the information, applications and services they need to do their job, providing automation of manual processes, and keeping them connected to colleagues wherever they are.

However, CCS Insight’s 2023 survey research reveals that employees face a raft of frustrations with their technology experience, from passwords and logins (34%) and poor connectivity (27%) to too many software updates (26%) ⁵. This remains a top focus for businesses, with 25% planning an investment in digital experience monitoring tools over the next 12 months to help resolve these challenges.

⁴ CCS Insight Senior Leadership IT Investment Survey, 2023

⁵ CCS Insight Employee Workplace Technology Survey, 2023



EMPLOYEE FRUSTRATIONS WITH WORK TECHNOLOGY

34%

Passwords and logins

27%

Poor connectivity

26%

Too many software updates

Source: CCS Insight Employee Workplace Technology Survey, 2023

Constant Connectivity Is a Business Imperative

The growth of cloud-based applications and the digitization of processes means that employees are becoming much more reliant on connectivity to carry out their tasks. Influenced by experiences in their personal lives, workers increasingly expect constant connectivity and immediate response times for their cloud applications and services in the business arena. Breaks in connectivity can severely hamper productivity, delay business workflows and cause frustration for employees.

Up from 18% in 2022 ⁶, over a quarter of employees (27%) now cite poor connectivity as a top-three frustration with their work technology, according to CCS Insight's survey research ⁷. As well as affecting the employee experience, this has the potential to expose businesses to additional risk, for example, if employees turn to unsecured connectivity methods such as public Wi-Fi hot spots. Not only does poorly secured

⁶ CCS Insight Employee Workplace Technology Survey, 2022

⁷ CCS Insight Employee Workplace Technology Survey, 2023

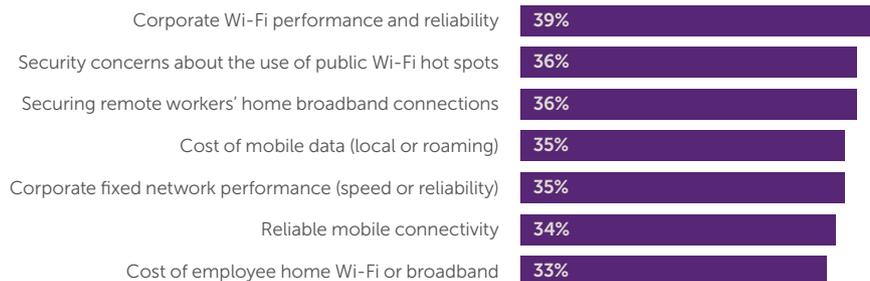
public Wi-Fi pose considerable risks to both the employee and the business by presenting potential hackers with unfettered access to corporate data and applications, the lack of incentive to upgrade these hot spots means they often offer poor performance to users as well.

Breaks in connectivity
can severely hamper
productivity, delay business
workflows and cause
frustration for employees

For businesses under pressure to meet these ever-growing connectivity expectations, the shift to hybrid working further complicates the picture. Not only do employees need consistent, reliable and capable connectivity in the office, but also wherever they are working, be that from home, a customer office, a field location, or even a coffee shop.

Once the primary focus of business connectivity strategy, the corporate fixed network is now just one investment priority of many for IT teams. Business leaders face the challenge of ensuring the performance, reliability and security of corporate fixed connectivity, corporate Wi-Fi, employees' home broadband and Wi-Fi, and mobile connectivity to ensure that employees remain connected at home, in the field, or anywhere in between.

PRIMARY CONNECTIVITY CHALLENGES FOR BUSINESS



Source: CCS Insight Senior Leadership IT Investment Survey, 2023



Traditional Security Models Are Broken

A critical challenge for businesses that has been exacerbated by remote working is security. Security remains the number-one investment priority for businesses over the next 12 months, as shown in CCS Insight’s Senior Leadership IT Investment Survey, 2023, and dominates decision-making across the technology landscape.

The accelerated shift to the cloud, paired with a wave of new devices connecting remotely into corporate networks at the onset of the pandemic, highlighted weaknesses in security models, exposing them as unfit for purpose in the hybrid working environment.

The traditional, perimeter-based approach to IT security, typically enabled through virtual private networks (VPNs), have come under scrutiny as more of the workforce works from home, extending the reach of the network infrastructure and putting pressure on the available capacity. Many businesses have continued to see unsecured personal devices even though most companies have provided laptops and other office equipment to support their hybrid workforce. And IT teams are

still challenged with concerns about the security, visibility and lack of control of employees’ home Wi-Fi networks.

IT teams are still challenged with concerns about the security, visibility and lack of control of employees’ home Wi-Fi

All these concerns remain very real with the adoption of hybrid work, and with workers being more mobile than ever, the security concerns about employees connecting to public Wi-Fi networks are also added to the mix. Most public Wi-Fi networks, and indeed many home and private Wi-Fi networks, lack adequate security to prevent hackers intercepting data sent or received by others logged into the same Wi-Fi network, in so-called “man in the middle” attacks.

Similarly, spoof “evil twin” Wi-Fi networks that trick people into joining them in the belief that they are legitimate access points are another trap for employees. Stories like that of the DarkHotel hackers, who used hotel Wi-Fi to infect business executives’ laptops with malware in order to steal company data⁸, underline the scale of the risks for IT leaders. It is why

⁸ <https://www.theguardian.com/technology/2014/nov/10/hotel-wi-fi-infectedbusiness-travellers-asia-kaspersky>

securing remote workers' home broadband connections was rated as a top priority by 36% of senior leaders, along with security concerns about the use of public Wi-Fi spots and home Wi-Fi or broadband reliability ⁹.

Such concerns are prompting a rethink of enterprise security strategy. There is growing adoption of zero-trust security policies, which promote a shift from a perimeter-based approach to one that constantly verifies identity, operating a least-privilege access policy and layering security across devices, networks, users, applications and cloud infrastructure. Solutions that build security into devices and infrastructure, rather than requiring employees to consider whether their connection is secure, offer a more practical and, in the long term, more effective, approach to securing the workforce.

Pressure Mounts on IT Teams

All these challenges are compounded by the increased pressures on IT teams from the shift to hybrid working, particularly for small and medium businesses with limited IT resources that are already stretched. Many firms experienced dramatic increases in IT support workloads as processes and applications rapidly moved online and workforces transitioned to remote work, and employees often bore the brunt of this impact. Remote work has evolved from being an exception to forming part of the strategic direction; it must be built into IT's processes, policies and investment priorities.

⁹ CCS Insight Senior Leadership IT Investment Survey, 2023

¹⁰ CCS Insight Senior Leadership IT Investment Survey, 2023

¹¹ CCS Insight Employee Workplace Technology Survey, 2023

As a result, although the move to cloud-based services has helped businesses to simplify their IT landscape, hybrid work adds a new dimension of complexity. With many IT employees themselves now hybrid workers, and with the ongoing concerns about the global economic environment, IT teams need new solutions and strategies to help them provision, secure, manage and support employees at scale, wherever they work.



Remote work has evolved from being an exception to forming part of the strategic direction

New Workstyles Demand New Approaches to Employee Technology

Technology played a pivotal role in helping businesses build strongly out of the pandemic, as organizations of all sizes embraced digital transformation to lay the groundwork for innovation and growth. CCS Insight's research shows that 71% of businesses expect IT investment to rise over the next 12 months ¹⁰, even as the economic slowdown weakens.

Equipping employees with the right tools is paramount to a positive and engaging experience. And in the digital, hybrid work era, the laptop is at the heart of the technology experience, especially given the growing reliance on cloud-based solutions to support core business processes and online communications and collaboration tools to support teamwork and employee engagement. Remote employees identify a laptop as the number-one technology used for work ¹¹, and it is by far the most frequently used device for all employees during their workday.

Although some generative artificial intelligence (AI) technologies are provided with cloud platforms, needing constant connectivity, generative AI functionality can be

bundled into a desktop application for use with or without an active connection. Using this requires a high-performance, AI-capable PC, which supports AI model inference on a dedicated GPU or using the inference extensions in a 14th-generation Intel Core CPU.

As employee and business needs evolve and reliable connectivity becomes vital, there is an opportunity for businesses to embrace the next generation of connected laptops, which build in constant, secure connectivity through their own mobile data plan.

Enter the Always-Connected PC

An always-connected PC is a one-stop shop for hybrid working. Like a smartphone, the device has a built-in cellular 4G or 5G modem, in addition to a standard Wi-Fi modem, enabling a constant connection to the Internet.

The cellular modem provides support for a physical SIM card or e-SIM, which must be enabled through a directly associated mobile data plan, providing the device with its own cellular connectivity. Always-connected PCs bring several important benefits over traditional laptop devices that rely on wired connections or Wi-Fi only. However, since the introduction of the always-connected PC, e-SIM has grown as operators worldwide have kick-started support for the technology, making it easier to manage connected PCs and improving security. With Windows 11 now able to emulate 64-bit x86 code and a big jump in Arm hardware performance due in 2024 when Qualcomm's Snapdragon X Elite processor becomes available, this will drive further growth in always-connected PCs.

Simplicity and Convenience

With an always-connected PC, employees no longer need to be aware of how they are connecting their laptop on the move, or to be constantly on the lookout for Wi-Fi connections. Once set up and connected to the cellular



With an always-connected PC, employees no longer need to be aware of how they are connecting their laptop on the move

network, connectivity happens in the background, predictably and reliably, with the laptop switching seamlessly between Wi-Fi and cellular data as needed. The laptop mirrors the connectivity experience employees have come to know and expect — and not even think about — on a smartphone; it just works.

With traditional laptop devices, connecting to cellular data means tethering to a smartphone or to a mobile hot spot. Not only is this clunky, but it is also difficult for less-technically minded employees and an undesirable option for those without a work phone that is paid for by their company. CCS Insight's research shows that only 28% of employees use mobile tethering, while almost half (47%) have an employer-provided smartphone to use for tethering ¹².

Tethering may be useful for quick simple tasks such as sending e-mail, but it is not well-suited to activities requiring reliable

¹² CCS Insight Employee Workplace Technology Survey, 2023



connectivity over a long period, such as extended video meetings, which rapidly drain a phone battery. And because the tethering connection from a laptop to a mobile device uses Wi-Fi, data speeds may be restricted if using older smartphones, or if multiple people are connecting to the same mobile hot spot.

Mobility and Productivity

The constant connectivity of a 4G- or 5G-connected laptop removes many of the hurdles for productive working and a smooth employee experience. The device is connected immediately upon waking, without any effort on the part of the user, and maintains connectivity regardless of the work location, whether in the office, at home or on the move. Software updates can be downloaded and applied to the device when the employee is not working to minimize disruption. App notifications, e-mails and messages are received instantly, ensuring workflow continuity. These capabilities reduce frustration and time wasted, improving productivity and effectiveness as well as employees' technology experience.

New Network Options

Private mobile networks are growing quickly and expanding uses for always-connected LTE and 5G hardware. Active networks more than doubled in 2023 from 2022, to almost 32,000, generating more than \$6 billion in revenue for the telecom infrastructure industry in 2023, according to our research. Leading sectors include national public services such as emergency services, transportation, and manufacturing. Although adoption has proliferated across numerous industries, each has dozens of deployment scenarios and potential uses. Deployments blend elements of three different markets for private 4G and 5G:

- **Cloud and Internet of things (IoT) networks.** This category ties in with trends in cloud and edge computing, AI and machine vision, robots, security cameras and more-general IoT uses. It aligns with digital transformation projects in enterprise IT and operational technology. This area often favours 5G over 4G and complements Wi-Fi and fibre-based Ethernet, with many applications geared toward cloud or multisite wide-area networks. It features a lot of experimentation and innovation, but there are still relatively few large-scale operational deployments.
- **Critical communications networks.** These make up the bulk of larger-scale private network deployments to date, typically by utilities, mining, public safety, airports and military organizations, often in rugged or hard-to-reach environments for communications, and specific automation systems such as remote sensors and monitoring systems.
- **Indoor mobile phone networks.** Local private 2G and 3G networks were present in a few enterprise markets in as early as 2005 to replace DECT cordless phones. Several thousand such networks are still around, including ones updated to 4G and some that run on ships or onboard private jets.

Recent activity has focused on using private 4G and 5G to create neutral host networks for in-building or on-campus coverage. There are many neutral host models, some requiring an entire local network with its spectrum and core and others just relying on the tenant mobile operator's active equipment. In the US, options based on CBRS spectrum have been prominent.

Since 2020, 5G has been accelerating and has overtaken 4G in new private mobile networks. With the shift to newer 5G standards that offer even more new capabilities, 5G is where functionality improvements in private mobile networks will lie. Although private mobile networks for IoT, critical communications and indoor mobile connectivity largely differ when it comes to drivers, models, devices and uses, we expect to see an overlap emerge in the coming years. Adoption of connected PCs will pick up in the next three to five years as hardware prices fall and applications grow, fuelled by 5G connectivity, particularly in enterprise markets, and rising support for e-SIM.



Improved Security and Management

Not only does a connected laptop streamline the experience for employees, it helps dramatically lower the risk to businesses by providing reliable, secure connectivity through an encrypted cellular connection. Employees no longer need to seek out potentially unsecured public Wi-Fi hot spots or other third-party connections, nor do they need to struggle with cumbersome VPN connections.

IT teams avoid the headache of trying to secure employees' private home Wi-Fi network, or preventing use of less secure connection methods when on the move. By having a first-party mobile data plan associated with the device, logging into the cellular network automatically authenticates the user and ensures all transferred data is fully encrypted, protecting both business and employee. The devices can be easily and seamlessly provisioned, supported, updated, managed and

The device is connected immediately upon waking, without any effort on the part of the user

remotely wiped by IT staff using zero-touch processes, wherever the employee is working, easing the burden on IT teams.

Ensuring Employee Devices Are Future-Ready

Always-connected PCs provide an opportunity to ensure employees have the most advanced and attractive tools to meet the needs of constantly evolving workstyles. With built-in connectivity, not only can employees connect using 4G or 5G, with the benefit of improved speeds and lower latency for the best performance of their business applications.

For decision-makers, this new breed of laptop helps to maximize the return on their investment by providing reassurance that the device will not become obsolete before the next upgrade cycle. It also delivers a great experience for employees, helping the business stand out in the competitive battle for talent.

RECOMMENDATIONS FOR IT DECISION-MAKERS

To better support employees in the new world of work, CCS Insight offers businesses the following recommendations:

Get ahead of the curve by equipping employees with 4G- and 5G-connected laptops



Against a backdrop of recruitment and employee retention challenges, always-connected PCs present a way to give your workforce the latest technology and the best experience, while also protecting the organization by reducing the risks from unsecured connectivity alternatives. Instantly available, constant connectivity helps maximize employee efficiency and productivity, but also takes friction out of the employee's workday, making work more enjoyable. In a post-pandemic world and with hybrid working practices now common for most employees, an investment in always connected PCs underlines a business's commitment to remote working and to the employee experience, helping support employee retention and talent attraction.

Invest in a laptop connectivity plan, not just devices that support cellular connectivity



Businesses should now be buying laptops with integrated cellular modems as standard to future-proof their investments. However, to get the most value from an always-connected PC it is critical to purchase a mobile data plan as well as a connectivity-enabled device. This will ensure that hybrid employees can take advantage of the benefits of constant connectivity immediately, allowing access no matter where they are based.

Segment employee roles to determine where an always-connected PC can add immediate value



In the future, every worker will come to expect constant connectivity through their laptop. Some employee roles, though, will get immediate value from these devices today and these groups should be the focus of your initial investment. This includes employees in roles that involve frequent travel or that regularly work in locations other than the corporate office, whether from home, from different branch offices, customer sites or field locations. Examples include those in business development or customer engagement roles or other externally facing positions, such as executives, consultants, sales representatives, field researchers and engineers, as well as hybrid workers.

Take advantage of early-adopter employee groups to shape your long-term needs



Focusing on mobile-centric and hybrid working employee roles now will help you and your employees understand the immediate benefits of the devices, their data requirements, the policies needed to manage and govern them, and the longer-term potential and opportunities that come from always-available cellular connectivity for laptops. This will help maximize the return on investment for your business while showcasing your commitment to the best experience for employees.



[ccsinsight.com](https://www.ccsinsight.com)



info@ccsinsight.com



[@ccsinsight](https://www.instagram.com/ccsinsight)