Modernizing enterprise IT with 5G

Extract from the Ericsson Mobility Report

November 2025

ERICSSON

Modernizing enterprise IT with 5G

As digital transformation accelerates in the enterprise sector, service providers are well positioned to modernize enterprise IT, shifting from traditional site-bound perimeter models to secure, zero-trust endpoint-centric models that improve user experience while enabling agile, resilient operations.

Key insights

- SoftBank Corp. aims to enhance its 5G network and develop enterprise solutions that leverage 5G standalone (SA) capabilities.
- An endpoint-centric model, built on zero-trust, 5G and cloud technologies, is set to redefine enterprise IT architecture.
- More agile, flexible business practices will be enabled by making 5G programmable networks available to enterprise IT.

SoftBank is advancing its Beyond Carrier strategy – an initiative that guides its efforts to combine mobile network expertise with cloud, security and AI capabilities to support enterprise digital transformation. Within this approach, SoftBank continues to enhance its 5G network and develop enterprise solutions that leverage 5G SA capabilities such as ultra-low latency and massive device connectivity, which are essential for modern enterprise IT environments.

Facing new challenges in enterprise IT management

For decades, enterprise IT has largely revolved around centralized, site-based infrastructure. Data centers, on-premises servers and wired networks formed the backbone of corporate computing and communications. However, the rise of remote work, high-performing mobile networks and 5G laptops, and cloud services is disrupting this model. Enterprises now require greater agility, scalability and mobility to support distributed operations and real-time data processing.

The enterprise IT market encompasses a wide range of technologies and solutions designed to support complex business processes, enhance productivity, ensure security and enable digital transformation at scale. These technologies are typically implemented, managed and maintained by the enterprise's IT department. The trends of cloudification, hybrid working and AI are raising significant challenges for enterprises to cost-effectively and securely manage, maintain and develop existing IT infrastructure to meet future demands:

- **Cloudification:** The current software trends strongly lean toward cloud services driven by their flexibility, scalability, cost-effectiveness and ease of maintenance. As enterprise applications migrate to the cloud, IT infrastructure becomes lighter but also more distributed – requiring consistent management and security across locations and devices.
- **Hybrid working:** Catalyzed by the COVID-19 pandemic, hybrid working has become the new normal for many organizations. Enterprises are now managing users and devices across office, home and mobile environments, requiring seamless and secure connectivity. This shift increases reliance on mobile networks and makes location-based security models less effective.
- **AI:** Enterprises are increasingly integrating AI tools into a wide range of business functions, and even moving beyond pilot initiatives to embed AI in their core operations, such as automating tasks and enabling real-time decision making. These applications depend on continuous, secure connectivity to access data and computing resources distributed between the cloud and edge. In this context, 5G's low-latency and always-on characteristics provide the foundation for secure and responsive AI-driven workflows, while also reinforcing the need for zero-trust security principles.

SoftBank

This article was written in collaboration with SoftBank Corp. (SoftBank), a leading communications and technology company operating one of Japan's most advanced 5G networks. SoftBank aims to drive enterprise digital transformation by combining mobile connectivity with cloud, AI and security innovations.

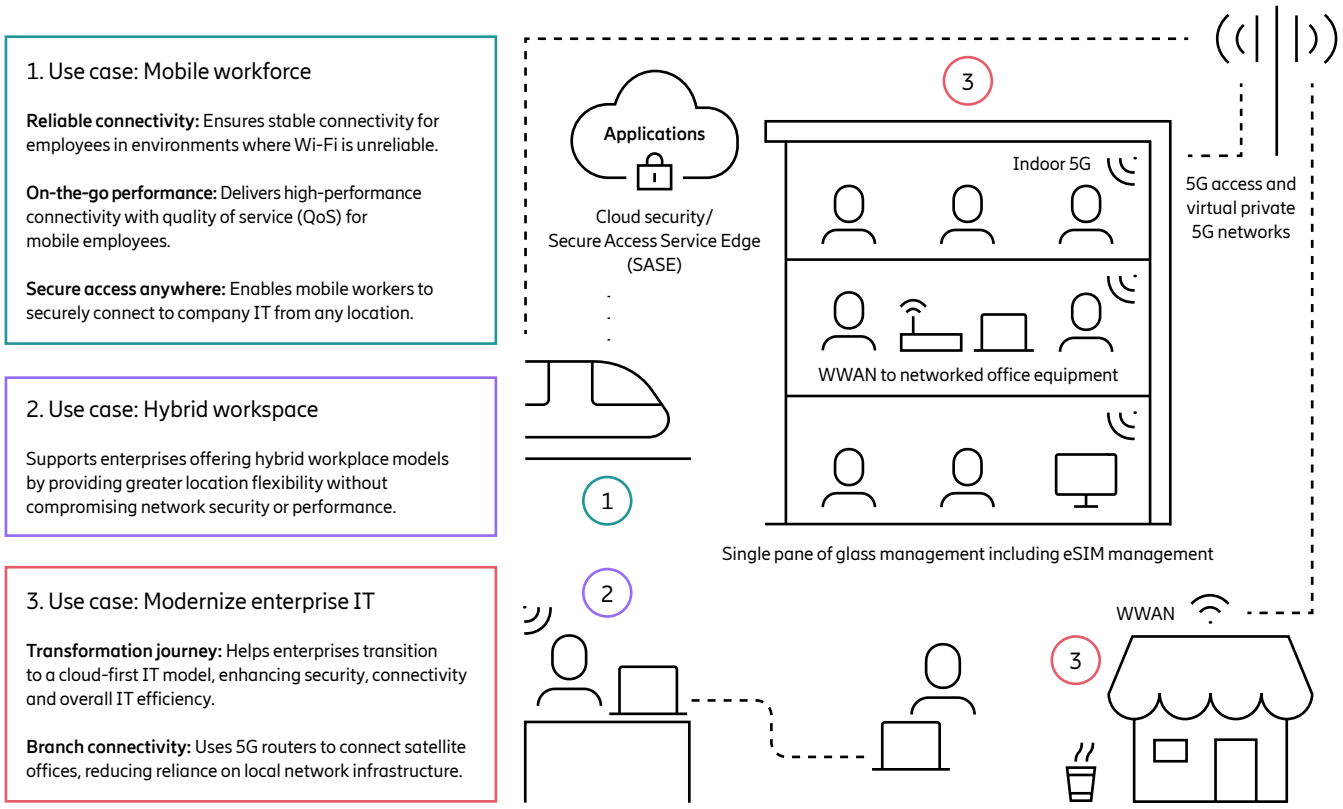
Enterprises face significant IT management challenges in: device selection, procurement and lifecycle management; network design and operations for both on-site and remote locations; and IT asset governance. The shift to hybrid work broadens the scope of these tasks. In environments that mix on-premises and cloud systems, secure operations based on zero-trust principles are increasingly essential. From a management perspective, the ongoing costs of maintaining legacy systems are a persistent concern.

5G laptops: Anywhere is a secure office

Cellular-enabled laptop adoption is expected to grow faster than the overall laptop market. By 2030, the global installed base of 5G laptops is, by some external analysts, projected to approach 100 million, corresponding to a CAGR of approximately 45 percent between 2024 and 2030.[1] The growth of 5G laptops, combined with the migration of enterprise applications to cloud platforms, serves as a catalyst for enterprise IT transformation.

[1] External analyst forecast (H2 2025).

Figure 18: IT infrastructure-light enterprise



This shift indicates that traditional perimeter-based, location-dependent enterprise IT network architectures will become increasingly obsolete, making way for more flexible, cloud-centric and zero-trust networking approaches enabled by seamless 5G connectivity both inside and outside the office.

Traditional, perimeter-based architectures rely on securing fixed physical sites and treating remote access as an exception – typically employing device certificates and virtual private networks (VPNs) to mimic a trusted internal environment. This approach is becoming less cost effective as modern workforces demand secure, seamless connectivity from anywhere, and as new operational models emerge that leverage 5G networks to meet evolving user demands and offer enhanced experiences.

Transitioning to a mobility-first, zero-trust network

A mobility-first, zero-trust network protects enterprise information assets by continuously validating both the user and the device, rather than basing security on physical location. Access rights are determined by identity and the device's security posture. By leveraging persistent device authentication based on non-removable eSIM and SIM credentials managed through the mobile network, and integrating these with enterprise-managed identity systems and device management platforms, organizations achieve a unified, high-assurance security framework that works seamlessly across office, home and mobile environments. With the traditional notion of a "secure location" disappearing, there is no longer a need to centralize assets at specific sites. This new model allows enterprises to provision, manage and secure devices anywhere – creating the foundation for more flexible operational practices. Service providers play a key role in enabling this transformation, as mobile networks provide the trusted, always-on connectivity required to verify users and devices continuously.

In a zero-trust environment built on persistent device identity, even traditionally IT-controlled tasks such as device provisioning can now be performed securely by end users. User-driven onboarding – supported by cloud-based Unified Endpoint Management (UEM) tools and integrated mobile authentication – enables employees to set up corporate devices directly, wherever they are, without compromising security. This approach reduces operational overhead and enhances flexibility in enterprise IT operations.

Enhancing security and policy enforcement across working environments

Cellular laptops maintain continuous connectivity via the mobile network. This ensures remote management functions and security actions can be immediately executed at any time and at any location, such as remote wiping or the removal of connection profiles if a device is lost or stolen. Always-on, network-native connectivity also gives IT administrators increased confidence in managing and responding to incidents by enabling consistent policy enforcement across all working environments within a zero-trust framework. While this consistent policy enforcement is a core benefit, another important advantage of cellular-first connectivity is the reduced dependence on extensive Wi-Fi infrastructure, enhancing both security and operational simplicity.

Transforming enterprise IT with 5G and partners

In collaboration with partners, SoftBank has been exploring new ways for enterprises to build secure and flexible connectivity for remote and hybrid workforces. High-performing 5G networks enable employees to securely access cloud-based services using 5G-connected laptops – whether in the office, at home or on the move. These initiatives illustrate how 5G connectivity can simplify enterprise IT architecture while supporting zero-trust and AI-enabled workflows that enhance both security and productivity.

Improved efficiencies with mobile-first connected laptops

In Japan, enterprises are increasingly looking for ways to improve both security and productivity through mobile-first IT environments. SoftBank conducted an internal study involving employees from the enterprise sales division to evaluate the benefits of equipping employees with cellular-enabled PCs, focusing on the direct impact on users. For example, participating sales employees often need to access company resources while visiting customers. Previously, they had to spend several minutes preparing their devices and completing authentication procedures before each presentation. With cellular PCs providing continuous, secure connectivity within a zero-trust framework, this step was eliminated. Based on internal trials, this improvement translated into measurable productivity gains across the sales organization – the cumulative reduction is estimated to be up to one full working day per month, per employee. This demonstrates how cellular-enabled PCs can enhance both security and employee experience by enabling truly seamless, always-on access to enterprise resources.

Quantifying potential IT cost efficiencies

As enterprises transition their office environments to support hybrid work and accelerate cloud migration, traditional LAN and WAN infrastructures often become underutilized yet still costly to maintain. According to Ericsson internal analysis, replacing parts of these conventional network environments with 5G-based architectures leveraging network virtualization could reduce overall IT infrastructure costs by up to 50 percent, depending on deployment conditions and enterprise size.

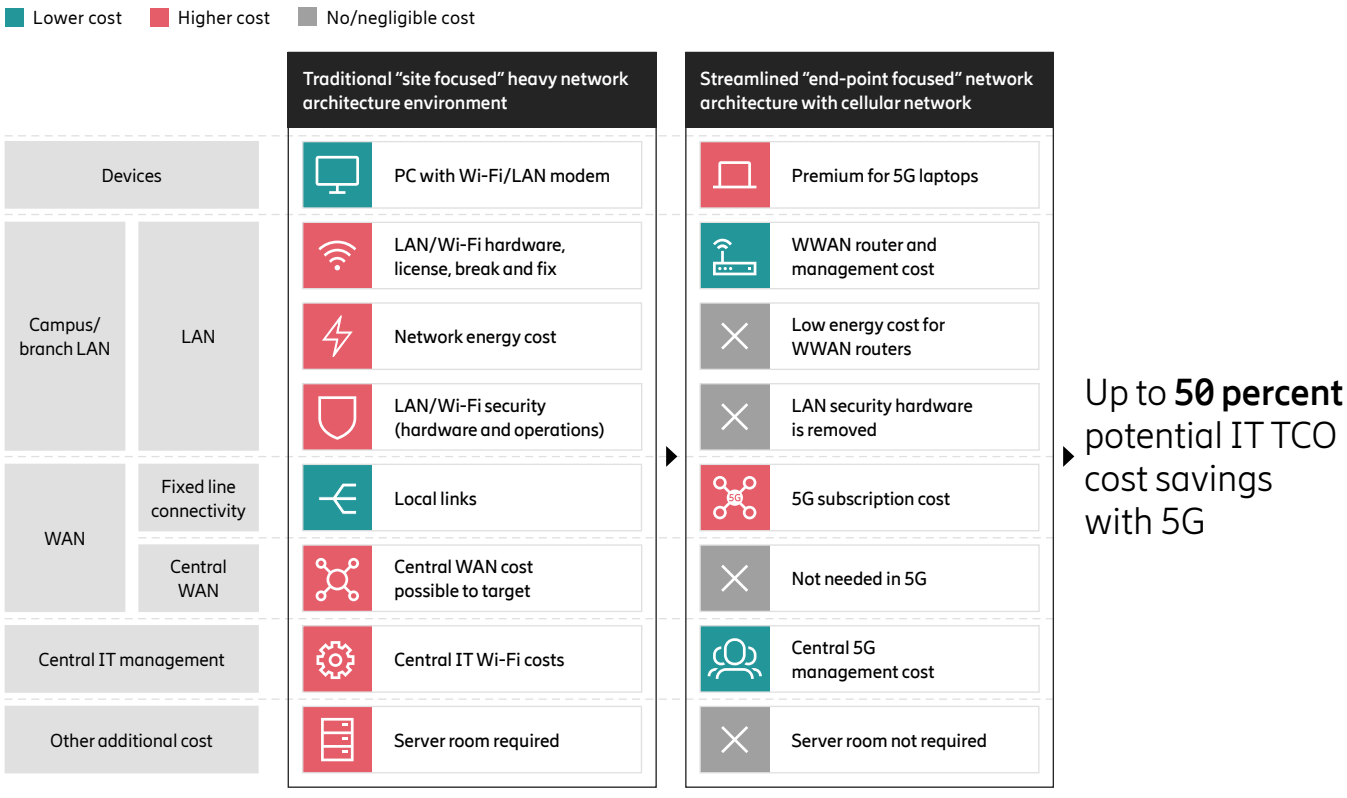
Ericsson Japan has also been implementing this approach within its own offices, gradually replacing local Wi-Fi environments with private 5G networks. Early internal results show reduced operational complexity and improved network reliability, providing a practical demonstration of how 5G can streamline enterprise IT and connectivity management. While the actual savings will vary, such 5G-enabled architectures offer opportunities to simplify network operations, improve agility and future-proof enterprise connectivity.

Evolving to an infrastructure-light enterprise

As enterprises accelerate cloud adoption and hybrid work, a fundamental shift from perimeter-based security to zero-trust models is becoming essential. A mobility-first, zero-trust architecture – powered by cellular-connected secure endpoints – enables service providers to deliver this transformation with capabilities unique to 5G mobile networks. This evolution not only strengthens enterprise security across all workspaces during hybrid working, but also streamlines operations and paves the way for more agile, flexible business practices by making 5G programmable networks available for enterprise IT.

Service providers are uniquely positioned to lead this transformation, integrating secure connectivity, identity management and managed lifecycle services into a cohesive solution offering for enterprise customers. In doing so, they enable enterprises to boost operational efficiency, strengthen security and reduce total cost of ownership (TCO) – while enhancing user experience and laying the groundwork for AI-driven innovation. The endpoint-centric model, powered by zero-trust, 5G and cloud technologies, is positioned to redefine enterprise IT architecture. Service providers who embrace this shift stand to gain not only new revenue streams but also deeper strategic partnerships with enterprises undergoing digital transformations.

Figure 19: TCO comparison: Traditional enterprise IT infrastructure versus 5G



Note: Central IT management includes connectivity procurement, central management of network equipment patches and software updates, and network operation centers for troubleshooting.

About Ericsson

Ericsson's high-performing networks provide connectivity for billions of people every day. For nearly 150 years, we've been pioneers in creating technology for communication. We offer mobile communication and connectivity solutions for service providers and enterprises. Together with our customers and partners, we make the digital world of tomorrow a reality.

www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

EAB-25:009321 Uen/3