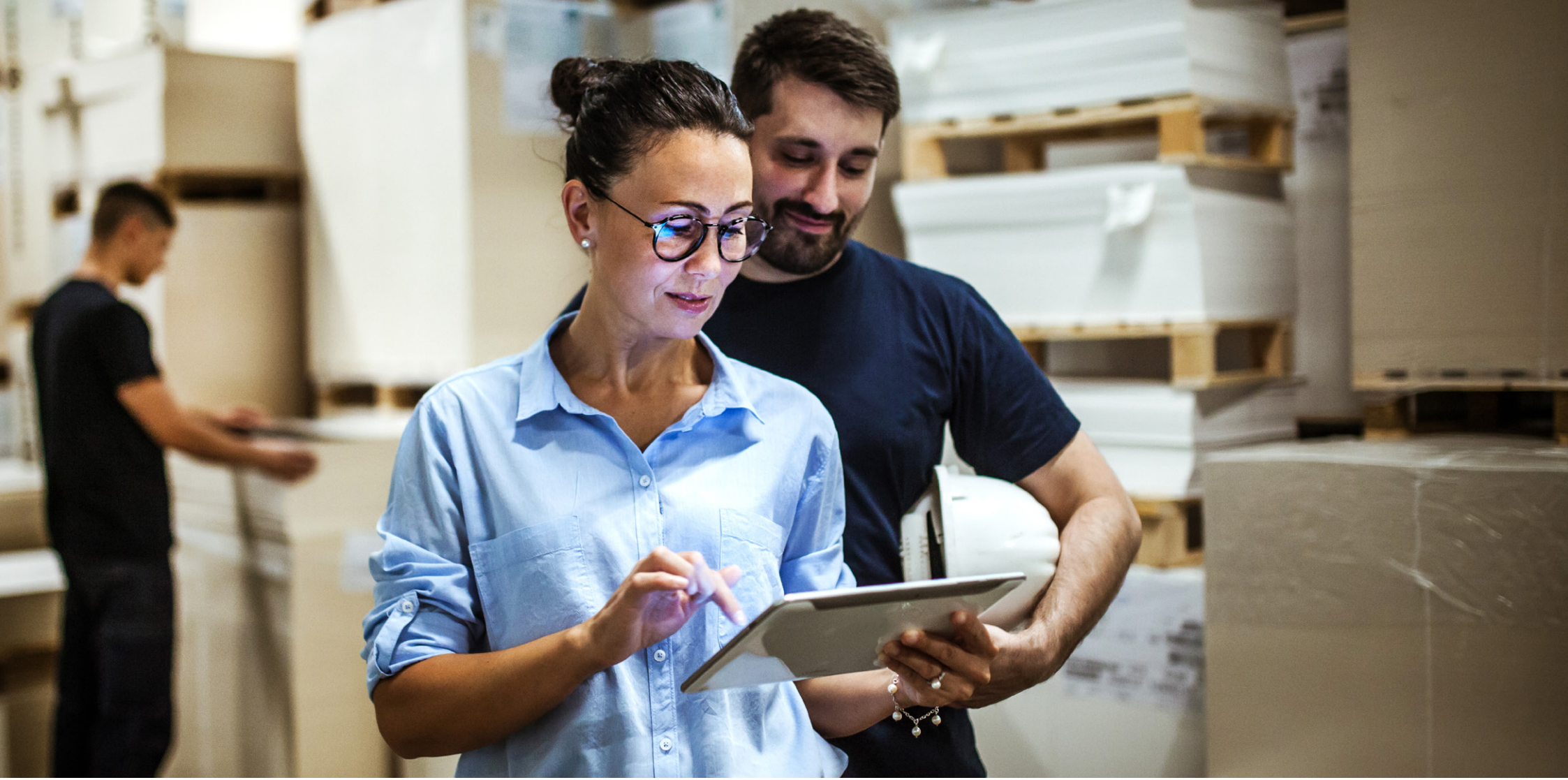


Bridging the gap between IT and Operations for successful digital transformation

White Paper

Alcatel·Lucent Enterprise

Table of contents

- IoT drives IT and Operations collaboration
- New use cases and opportunities
- A shared vision and foundational technologies
- The right technology partner

IoT drives IT and Operations collaboration

Until recently, it typically made sense for IT and Operations teams to function as separate units within enterprises. The two worlds didn't overlap. While IT teams focused on deploying and maintaining the company's network infrastructure and increasing cybersecurity, Operations focused on day-to-day activities, such as facilities management, manufacturing management, sales and marketing, and building security.

Now, as Operations teams increasingly rely on IoT solutions to achieve their goals and digitally transform the business, there's a new, and urgent, need for the two teams to collaborate and share expertise. IoT solutions are an ideal way to automate and accelerate operations to increase business agility and continuity, and improve the customer experience. But these solutions require hundreds or thousands of new devices to be connected to the corporate network, which falls under IT's domain.

Enterprises that break down the walls between IT and Operations and encourage the two teams to collaborate in a natural way can significantly reduce these risks. They can also maximise the benefits that IoT and other digital transformation initiatives bring to the business.

Disconnected teams increase risks

IT and Operations teams that aren't aware of each other's activities, or that don't coordinate and collaborate, put digital transformation initiatives, and the company, at risk from multiple perspectives:

- **Cybersecurity.** When IT doesn't know about new IoT devices being implemented by the Operations team, they can't ensure the devices comply with corporate security policies. IoT devices come with highly variable levels of cybersecurity features and may not implement the latest best protection practices. These unauthorised "shadow IT" devices could be running any software, and could already be infected with viruses and malware. Left unchecked, they can easily introduce new vulnerabilities and attack vectors into the network.
- **Financial and operational efficiency.** When IT and Operations teams implement technology solutions without the other's knowledge, they may be duplicating costs and effort. For example, Operations staff may purchase an IoT device monitoring and management solution, not knowing that IT already has a solution in place that can perform these tasks. A single solution that can meet IT and Operations needs is always the most cost-effective and operationally efficient option.
- **Performance and reliability.** IT teams understand how the corporate network can be optimised and fine-tuned to meet specific requirements, such as quality of service (QoS) for IoT deployments. If Operations teams can't benefit from that expertise, there's greater risk that business-critical digital transformation initiatives will be implemented with performance and reliability weaknesses that may have been prevented.

New use cases and opportunities

Because IT and Operations teams have different focus areas and expertise, each group brings unique and important capabilities to the table. Operations teams understand which IoT solutions can best help the company increase efficiency and reduce costs. IT organisations have the tools and know-how to automate and simplify every aspect of those solutions, from deployment and monitoring to maintenance and upgrades — advantages that multiply as IoT deployments increase in scale.

Together, the two teams have the knowledge, skills and tools companies need to take advantage of new use cases and opportunities that increase business success. At the same time, IT becomes a key strategic resource that helps Operations as well as the business, achieve its financial and operational goals.

When IT and Operations collaborate to put secure, cost-effective and reliable IoT solutions to work for the business, the possibilities are unlimited. Following are just a few examples that can be easily adapted to meet the needs of different industries and organisations.

Increase agility and responsivity with real-time communications

IoT solutions that automatically connect people and systems based on real-time events bring new speed to business operations.

In airports, baggage handlers can be notified that planes are about to land so they can have belt loaders and transport vehicles in place. If there's an emergency situation, the solution can automatically connect airport management, security teams and law enforcement personnel so they can coordinate to address the situation. In schools and cities, real-time notifications let people know when buses are about to arrive and help officials swiftly respond to unexpected events.

Reduce costs by automating routine tasks

Many businesses and public facilities still rely on time-consuming manual inspections to perform mundane tasks, such as checking whether garbage bins are full. With sensors that monitor garbage levels, the right person or system is automatically notified when each bin reaches the predefined threshold. No time or money is wasted on manual inspections, maintenance staff can spend more time on higher value tasks, and the cost of garbage bags and disposal are reduced as bins are only emptied when necessary.

Increase efficiency with asset tracking

Knowing the precise location of business-critical assets at all times helps people work more efficiently and effectively.

In medical centres, the ability to pinpoint the location of the nearest available oxygen tank, crash cart, wheelchair and other equipment, enables more responsive care and streamlines workflows. At airports, the same asset tracking technology lets staff know where ground support equipment, such as pushback tugs, pallet loaders and catering vehicles, are located to accelerate aircraft turnaround time.

Improve the customer experience with a smooth journey

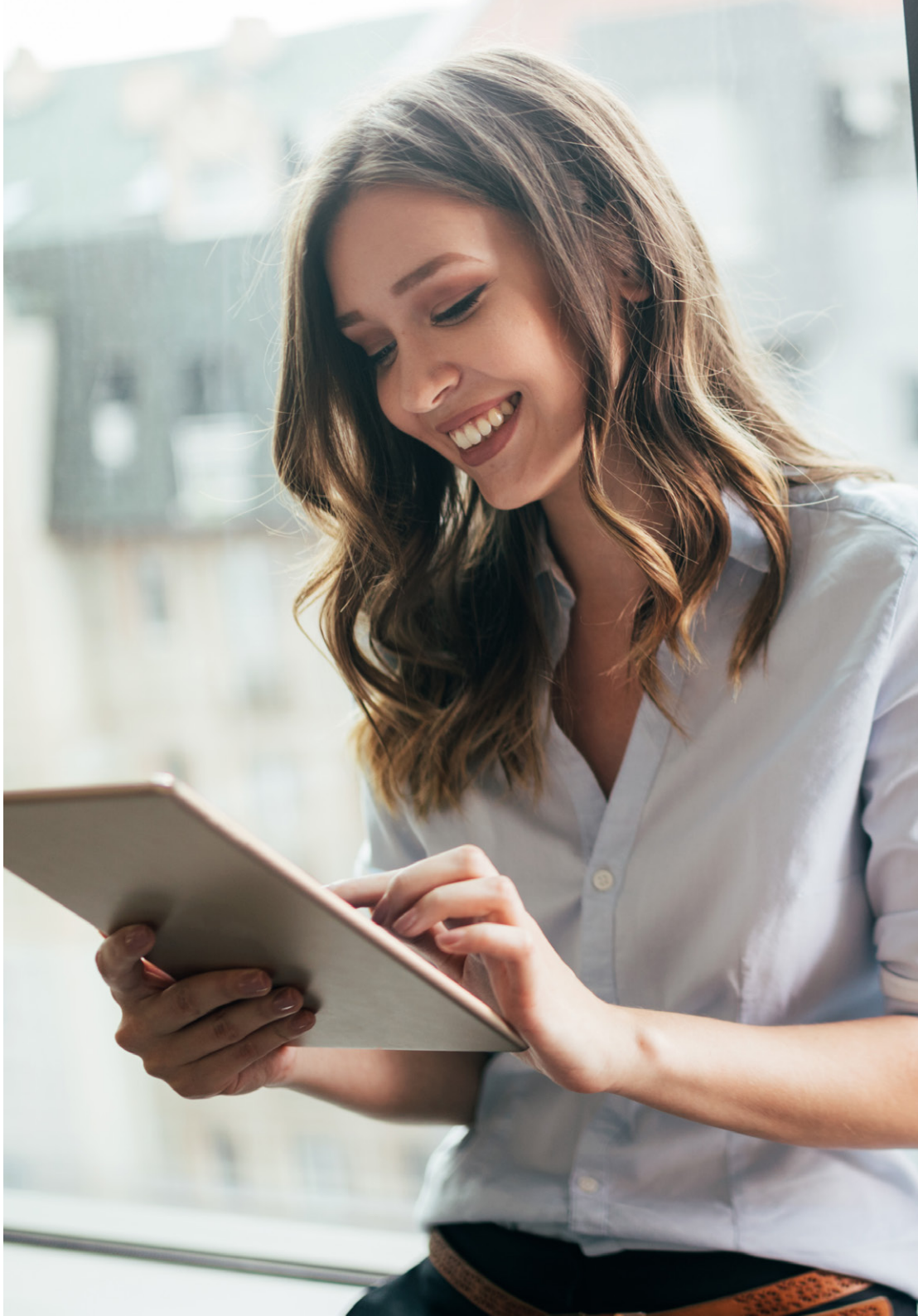
Location-tracking technology can also be used to improve the customer journey end-to-end. For example, a hospital can use data collected from IoT-enabled patient bracelets to analyse the amount of time patients spent in each stage of care, including the emergency departments, admissions, waiting rooms, radiology, operating rooms, recovery, physiotherapy and discharge. They can then use the results to optimise processes and workflows to improve the patient experience and satisfaction.

At airports, enhanced location technology can help travellers take the most efficient routes through sprawling terminals. With an app that outlines the fastest path from their current location to their gate, passengers are far less likely to get lost or follow a slow, convoluted path that increases the risk flights will be delayed.

Increase resilience by monitoring critical systems

Secure and reliable IoT solutions are an ideal way for utility providers and businesses to proactively monitor the performance of critical infrastructure and systems, such as gas, water and electricity distribution systems.

In these types of deployments, sensors automatically send alerts when thresholds for key performance indicators (KPIs) such as temperature, pressure, vibration, torque and moisture are crossed. With immediate notice of performance degradation, maintenance personnel can proactively address issues to prevent equipment damage, breakdowns and service disruptions.



Increase sustainability with smart building solutions

Smart building solutions help businesses and government organisations optimise their use of energy and resources so they can achieve green objectives and reduce operational costs.

There are any number of smart building solutions that rely on connected IoT devices, but some of the most common include solutions that automate lighting, water, and heating, ventilation and air conditioning (HVAC) systems based on time of day, demand levels and human presence.

Reduce pollution with smart traffic solutions

As cities work to reduce air pollution, they're increasingly adopting IoT solutions that help them monitor vehicle emissions along the busiest roads and at intersections that experience congestion. They can then analyse the data collected and use the resulting insights to target improvements that help streamline traffic flows.

Smart cities are also taking advantage of IoT technologies to implement smart parking solutions that help citizens find parking spots faster to reduce traffic congestion and vehicle emissions.

Improve compliance with full visibility of all devices

Finally, when IT and Operations teams collaborate on IoT deployments and the supporting network technologies, they can implement solutions that provide visibility and management of all devices that access the network. This complete view makes it easier to prove compliance with regulatory standards, corporate policies and cybersecurity best practices. There are no unsettling surprises revealed through audits. Devices with out-of-date firmware or security patches are immediately identified, and the risk of incurring industry fines is significantly minimised.

A shared vision and foundational technologies

Every organisation is at a different stage in its evolution and digital transformation, so there is no one-size-fits-all approach to increasing collaboration between IT and Operations teams. While some organisations are further along their digitalisation journey than others, most are still using a combination of modern and legacy technologies that reflects their unique history.

No matter where an enterprise is at today, there are common topics and technology considerations for IT and Operations teams looking to collaborate. Discussions should start with networking and cybersecurity requirements for the proposed IoT solutions, including:

- The types of devices that will access the network and the connection medium each will require, such as wired or wireless, indoor or outdoor. Additionally, environmental factors such as extreme heat, cold, vibration, winds, rain, snow, or ice should be considered.
- The cybersecurity policies each device type should adhere to and the applications with which each device type can communicate
- How information from each device type should merge with information from the network and corporate systems to ensure the right insights and data gets to the right people at the right time

Once the shared vision for IoT solutions is defined, it's time to evaluate the technologies needed to successfully implement the vision.

For many IT teams, new requirements to support high demands for IoT connectivity from various departments can seem overwhelming. However, leading network solutions available today were designed to securely support and simplify every aspect of even the largest IoT deployments. With the right approach to network infrastructure and management platforms, IT teams can smoothly evolve from being a potential roadblock to IoT deployments to being a business-critical enabler.

Secure, automated networks simplify IoT deployments

Modern networks automatically detect new IoT devices, and can classify and segment each type of device based on cybersecurity policies. They also support a Zero Trust Network Architecture (ZTNA) that establishes a "no trust premise" to any user, device, or application, no matter where it is located — on-site, in the cloud, or off-site — to minimise cybersecurity risks. The most advanced network solutions support macro- and micro-segmentation to enable a granular approach to cybersecurity:

- Macro-segmentation segregates users, devices and applications on the network according to their functional domain. For example, desktop and IP telephony are one macro-segment while video surveillance is a different macro-segment.
- Micro-segmentation defines how the users, devices and applications within a macro-segment can interact with each other, and is typically governed by very specific security policies.

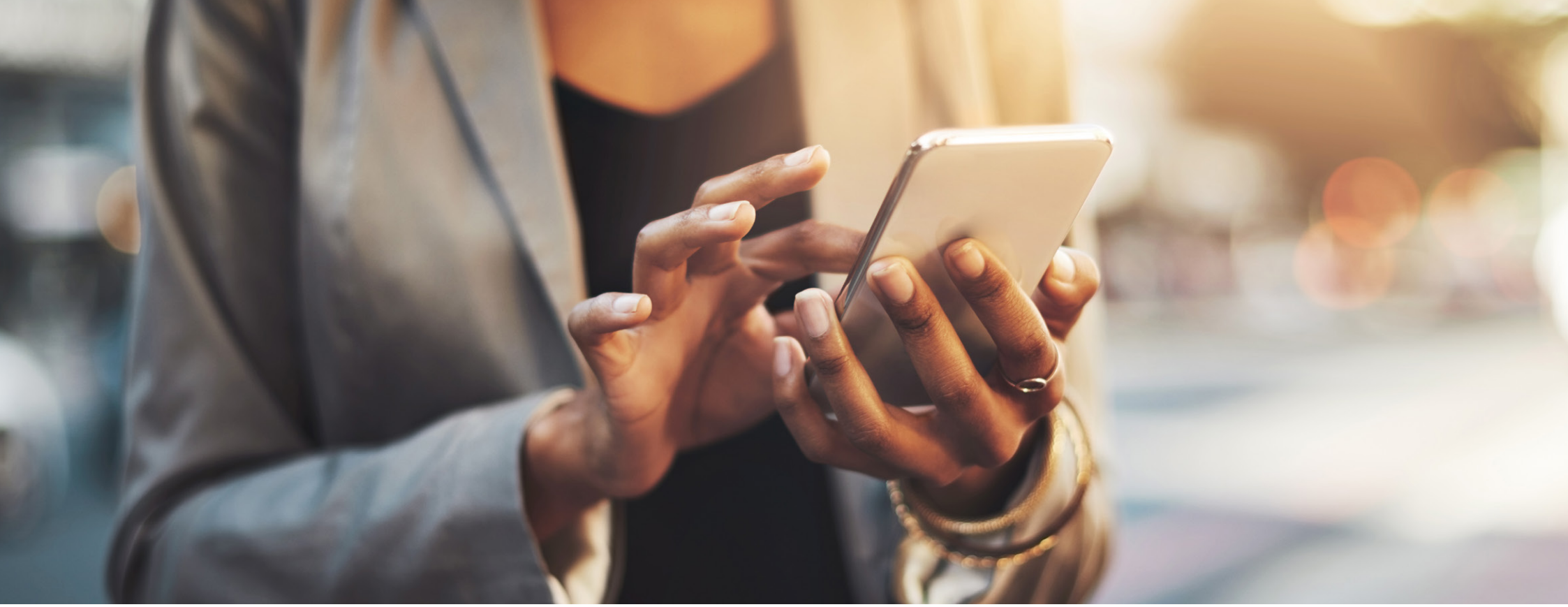
In a hospital, a macro-segment could be dedicated to medical equipment, such as patient monitors, and to a specific group of users. The macro-segment can also be used to ensure network access is provided with specific quality of service (QoS) and security parameters. Sensors and controls for lighting and HVAC systems would be mapped to a distinct macro-segment, as would security-related technologies, such as CCTV cameras and door-lock systems. With this type of segmentation, a compromised thermostat would not be able to communicate with a patient monitor or a door-lock system.

Micro-segmentation regulates the activities within the macro-segment. For example, a surveillance camera should not be allowed to interface with a door lock, despite the fact they are in the same security-related macro-segment.

Unified network management increases efficiency and consistency

Using a single management and analytics platform that provides an end-to-end, holistic view of all wired and wireless network and IoT devices makes management and troubleshooting faster, easier and less risk-prone compared to using multiple, disparate management systems. For example, if an IoT device is experiencing connectivity issues, the network operator can determine whether the root cause of the issue is the device itself or the wired or wireless network equipment to which it connects.

The business can also avoid the extra costs associated with purchasing and operating multiple management systems for wired, wireless and IoT devices. And cybersecurity policies are applied consistently across all device types, reducing the risk that security vulnerabilities will be introduced into the network.



New innovations connect people and information

IT and Operations teams should also evaluate new technologies that help them make the best possible use of data from IoT devices.

Asset tracking applications that identify the location of assets and people in real time are a good example of recent advances that should be considered. These applications use GPS-, BLE-, or RFID-enabled tags to quickly and easily track and find assets or people. They also include analytics that help enterprises optimise use of their assets, including:

- How long people had to wait to access equipment
- Which departments use each type of equipment most often
- Which equipment is used least
- How often equipment is moved on the premises and how far it travels each day
- When equipment was last serviced

Workflow engines are another good example. These platforms combine data from IoT devices, network infrastructure, business applications and other systems and communicate it to people when they need it most. For example, if an IoT sensor reports a carbon monoxide leak in a public building, the workflow engine can instantly and simultaneously notify internal maintenance teams, external experts, building management and building security teams. It can also enable all notified parties to spontaneously join a chat room, voice, or video conference to discuss the issue. Each party benefits from the real-time information coming from the IoT sensors and can simultaneously see a video surveillance feed that helps them better assess the situation.

The right technology partner

As IT and Operations teams look to increase collaboration, they'll need an experienced technology partner to provide guidance, expertise and solutions throughout their journey.

Alcatel-Lucent Enterprise recognises the financial and operational advantages enterprises gain when IT and Operations teams collaborate on digital transformation initiatives. We also understand how IT and Operations teams can leverage modern technologies and solutions to increase cybersecurity, reliability and efficiency while reducing risks and costs. Our solutions simplify and accelerate digital transformation, no matter what stage of evolution organisations are at today:

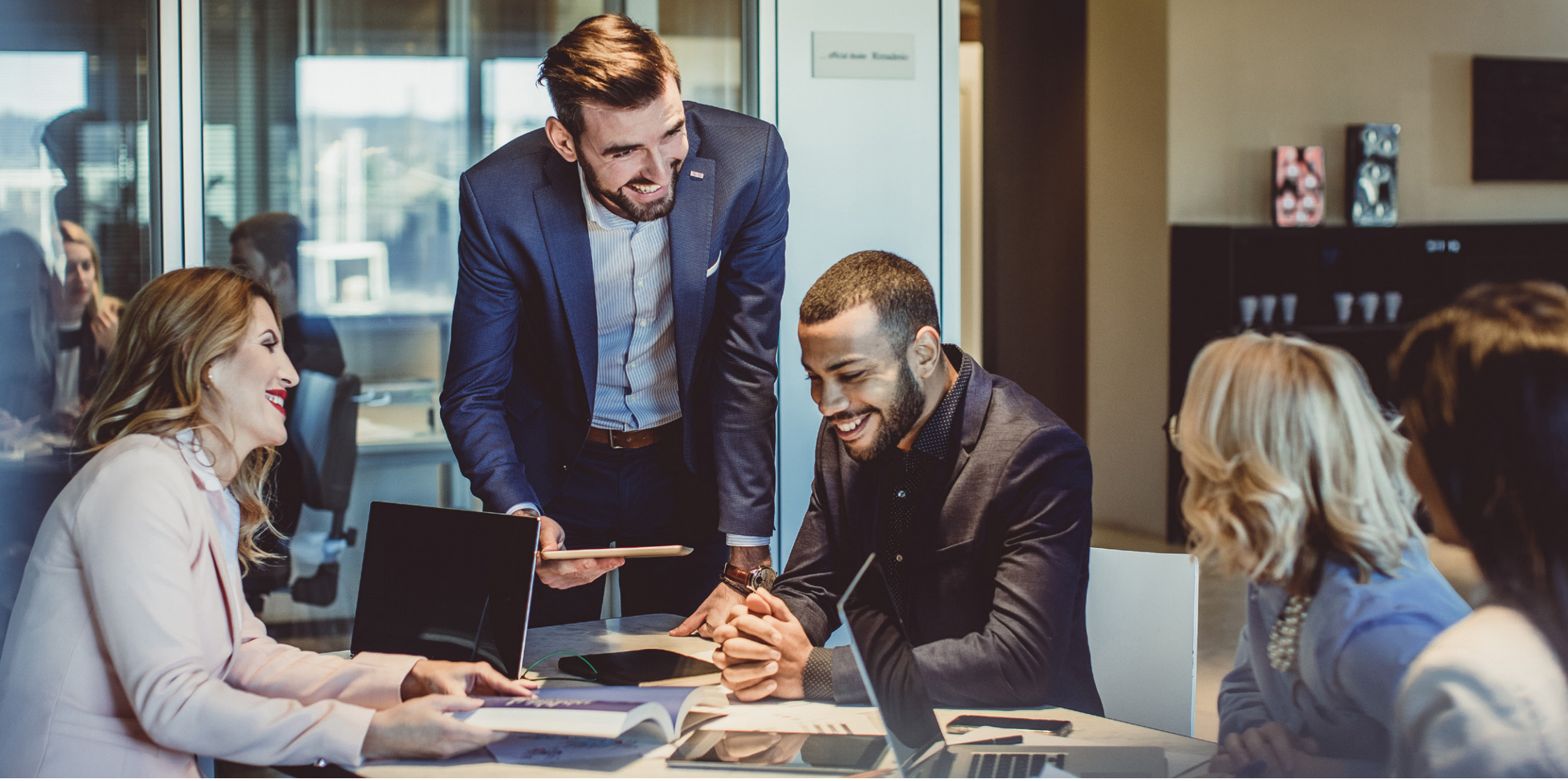
- Wired and wireless network solutions with built-in, automated IoT connectivity simplify deployments and provide full support for ZTNA security strategies
- Unified network management solutions provide cohesive management and network-wide visibility of all wired and wireless devices that access the network
- Asset-tracking solutions use BLE technology for highly accurate yet energy-efficient location tracking
- The Rainbow™ by Alcatel-Lucent Enterprise workflow and cloud communications platform connects people, machines and processes using chat, voice and video

We support our solutions with expert services that help our customers realise their digital transformation goals in an efficient and cost-effective way.

Supporting customers' digital transformation goals

With our unique combination of technology solutions and expertise, leading organisations around the world and across industries, partner with us, including:

- Liverpool City Region Combined Authority in the UK, using ALE network, management and communications solutions to improve traveller experiences and operational efficiency. Our solutions support mission-critical IoT devices for CCTV, traffic management, fire and smoke detection, and supervisory control and data acquisition (SCADA) systems as well as toll services such as Automatic Number Plate Recognition (ANPR) and intercom system integration. The organisation also supports planned enhancements such as ship-to-shore communications, connectivity for river ferries and a smart ticketing expansion for public transportation.
- Bangkok Metropolitan Administration in Thailand, are using ALE network and management solutions to develop a high-speed, redundant network for smart city IoT devices that will help improve citizens' quality of life and economic opportunities. As Thailand's capital, Bangkok's modern network and smart city innovations play a key role in helping the national government meet its Thailand 4.0 objectives.
- Aster DM Healthcare in the United Arab Emirates (UAE), are using ALE network, management, communications and collaboration solutions to give hospital staff 24/7 access to medical data and critical healthcare applications whenever and wherever needed. The converged solution also allows Aster staff to seamlessly and securely connect and collaborate across sites, even when they're on the move, so they can spend more time with patients. And it gives patients reliable access to Wi-Fi so they can stay connected with family and friends while at Aster facilities.
- California State University in the U.S., are using ALE network solutions to improve security, provide Wi-Fi everywhere, and deliver open, shared cloud services to enhance the overall campus experience. The highly reliable and flexible network securely supports more than 500,000 users across the university's 20-plus campuses and has helped save more than $100 million USD in infrastructure costs.
- Energy One in Australia, are using ALE network and management solutions to automate and simplify network management and maintenance across its sites in Sydney and Melbourne. The autonomous network makes it easy to onboard new sites, frees IT staff to focus on priority tasks, and improves network performance and Wi-Fi coverage so employees can work more productively with increased mobility and a consistent user experience across locations.



Learn more

To learn how we can help your organisation digitally transform in an efficient and cost-effective way, check out our website or contact us today to discuss your specific needs.

DID2303301EN (April 2024)

Alcatel·Lucent Enterprise