The Internet of Things in the Enterprise

Build a secure foundation to leverage IoT business opportunities

Solution brief

Alcatel·Lucent Enterprise

IoT fundamentally changes the business equation

The Internet of Things (IoT) has the potential to transform business by profoundly altering how organisations gather data and information by bringing together the major technical and business trends of mobility, automation and data analytics. IoT refers to the networking of physical objects using embedded sensors, actuators, and other devices that can collect and transmit information about real-time activity in the network. The data amassed from these devices can then be analysed by the organisation to:

- **Optimise products and processes,** by reducing operating costs, increasing productivity and developing new products and services
- **Learn more about customer needs and preferences,** enabling businesses to offer more personalised products and services
- **Make businesses smarter and more efficient,** by proactively monitoring critical infrastructure and creating more efficient processes
- **Improve user experiences,** by offering new or enhanced products and services to differentiate a data-driven business from the competition

IoT deployment continues to grow

IT professionals in a variety of industries are already planning for increased use of IoT solutions in the near future. In 2022, the market for the Internet of Things is expected to grow 18% to 14.4 billion active connections. It is expected that by 2025, as supply constraints ease and growth further accelerates, there will be approximately 27 billion connected IoT devices.

Source https://iot-analytics.com/number-connected-iot-devices

IoT deployment challenges

IoT brings unprecedented flows of data, presenting performance, operational and management challenges to the network infrastructure along with increased security risks from all endpoints. To address these issues, organisations need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

Organisations need a cost-effective network infrastructure that can securely handle vast flows of data, but that is also simple to manage and operate. The infrastructure must:

- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems can contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error prone. Automated onboarding enables the network infrastructure to dynamically recognise devices and assign them to the appropriate secured network.
- **Supply the correct network resources for the IoT system to run properly and efficiently.** Many devices in the IoT system deliver mission-critical information that requires a specific level of QoS. For example, some use cases require proper bandwidth reservations on a high-performance network infrastructure to ensure service delivery and reliability.
- **Provide a secure environment against cyberattack and data loss.** Because the many networked devices and sensors in the IoT lead to a corresponding abundance of potential attack vectors, security is critical for mitigating risks of cybercrime. Security is necessary at multiple levels, including segmentation of the IoT networks themselves.

IoT compounds exposure to cybercrime

With the growth of IoT also comes an explosion of cybersecurity threats, as the proliferation of sensors and connected devices greatly expand the network attack surface. IoT is especially susceptible because many IoT devices are manufactured without security in mind or built by companies that don't understand current security requirements. Consequently, IoT systems are increasingly the weakest link in enterprise security.

Forrester analyst Steve Turner said his own research suggested a relatively even distribution of ransom attacks across verticals. However, ransomware incidents in certain industries, such as critical infrastructure and healthcare, tend to result in the most headlines.[1]

IoT devices pose risks to assets across the entire network. By establishing segments using virtual network segmentation, IoT devices and the applications that control them are isolated, thereby reducing threats without the cost or complexity of separate networks.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Building a secure IoT network infrastructure

Protecting IoT traffic and devices is a challenge that can't be solved by any single security technology. It requires a strategic approach that takes advantage of multiple security safeguards.

To help organisations take advantage of the benefits and mitigate the risks of IoT deployment, Alcatel-Lucent Enterprise (ALE) provides a zero trust network strategy with multi-level security.

ALE's strategy delivers protection at every layer of the infrastructure, from the individual user and device to the network layer itself. The macro- and micro-segmentation of the network guarantees a simple and secure approach to securely onboard devices and deliver the right network resources to run the system properly and efficiently, all in a secure environment to safeguard organisations from cyberattacks.

IoT segmentation

To enable IoT segmentation, all users, devices and applications within the ALE network are assigned profiles. These profiles, which define roles, access authorisations, QoS levels, and other policy information, are relayed to all switches and access points in the network.

- With macro-segmentation, devices are placed in "virtual segments," using network virtualisation techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network
- With micro-segmentation, different QoS and security rules can be applied to the devices within each virtual segment. This adds higher granularity and increases network security, preventing different types of devices in the same segment from interacting with each other when they are not intended to do so.
- By segregating the network with macro and micro-segmentation, if a device is compromised in one part of the network, not only does the breach not affect devices or applications in other virtual segments, but it cannot propagate within the affected segment to other types of devices
- When a new IoT device is connected, the network automatically recognises its profile and assigns the device to the appropriate virtual environment
- Communication is limited to the devices within that virtual environment and to the application in the data centre that controls these devices
- Because all users also have profiles within the ALE network, access to the IoT virtual segments can be limited to authorised individuals and groups

In-depth security

- In addition to IoT segmentation, ALE networking technologies provide layered security across multiple levels of the network
- At the user level, profiles ensure users are authenticated and authorised with the appropriate access rights
- At the device level, the network ensures that devices are authenticated and compliant with established security rules
- At the application level, the network can establish rules regarding each application or group of applications, including blocking, limiting bandwidth and controlling who can access which application
- At the network level, ALE switches benefit from secure diversified code. It protects networks from intrinsic vulnerabilities, code exploits, embedded malware and potential back doors that could compromise switches, routers and other mission-critical hardware.
- ALE smart analytics use deep packet inspection and other technologies to detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorised activity and network intrusions

End-to-end operational and network management

ALE network solutions also provide significant operational and management advantages.

- ALE enables multiple separate virtual networks to operate on a single, common infrastructure, eliminating the need for CAPEX investment in multiple physical infrastructures
- ALE's Unified Access solution allows wired and wireless technologies to work together as a single, robust network, with a common set of network services, a policy framework, a common authentication scheme and a single authentication database
- ALE networking solutions also have a single management system for all elements of the infrastructure, including unified management of both wired LAN and wireless WLAN networks. The Alcatel-Lucent OmniVista® 2500 Network Management System and Alcatel-Lucent OmniVista® Cirrus Network Management as a Service for cloud-based management provide a single pane of glass to manage virtual environments, switches, access points and all other network components.

A high-performance network portfolio

ALE switches, access points and controllers support the latest generation of high-bandwidth and low-latency capabilities and can manage large numbers of devices in high- density environments. ALE networking products and solutions address the networking needs for organisations of all sizes. ALE also provides a selection of ruggedised switches, access points and routers for network deployments outdoors or in harsh environments.

IoT scenarios in key industries

IoT solutions promise to make organisations smarter and more successful at what they do. These benefits are especially notable in certain verticals.

Healthcare

IoT has the potential to transform healthcare by profoundly altering how hospitals, clinics and other care facilities gather and use data by bringing together the major technical and business trends of mobility, automation and data analytics to improve patient care delivery. The data gathered from these devices can then be analysed by the organisation to:

- Improve patient care, by offering new or enhanced care delivery and services that help differentiate a data-driven healthcare organisation
- Optimise processes, by developing new services, workflows and solutions that increase efficiency and reduce operating costs
- Learn more about patients' needs and preferences, enabling healthcare organisations to offer more personalised care and experiences
- Make hospital networks smarter, by proactively monitoring critical infrastructure and automating the deployment and management of the IT infrastructure

The growth of IoT in healthcare also brings an explosion of cybersecurity threats, as the proliferation of sensors and connected devices greatly expands the network attack surface. IoT for healthcare is especially susceptible because many IoT devices are manufactured without security in mind or built by companies that don't understand current security requirements. Consequently, IoT systems can potentially represent the weakest link in hospital, clinic and care facility cybersecurity.

Education

Educational institutions are no exception in the IoT anywhere world. A world in which technologies are being designed into every imaginable product. IoT brings numerous benefits to universities and schools by proving a new generation of smart things that can immensely enhance the learning experience and significantly improve campus safety and security. IoT devices, be it small like a light sensor or big as in smart boards, bring about major changes into how the school environments are managed and the way students learn. IoT devices:

- Create new ways for students to learn by supporting more personalised and dynamic learning experiences such as immersive digital textbooks and game-based learning
- Change how teachers deliver lessons and test achievement with smart audio-visual equipment, digital video recorders for lecture capture, and online testing
- Simplify operations for school administrators by proactively monitoring critical infrastructure and creating more efficient, cost-effective processes for HVAC, lighting and landscape management
- Provide a safer environment for students and teachers with digital surveillance cameras, smart door locks and connected school buses

In these reshaped schools and universities, admins can collect, store, and analyse huge data quantities about the environment and student performance. This will equip schools with the intelligence they need to improve processes for student success and enable them to identify the gaps to be filled.

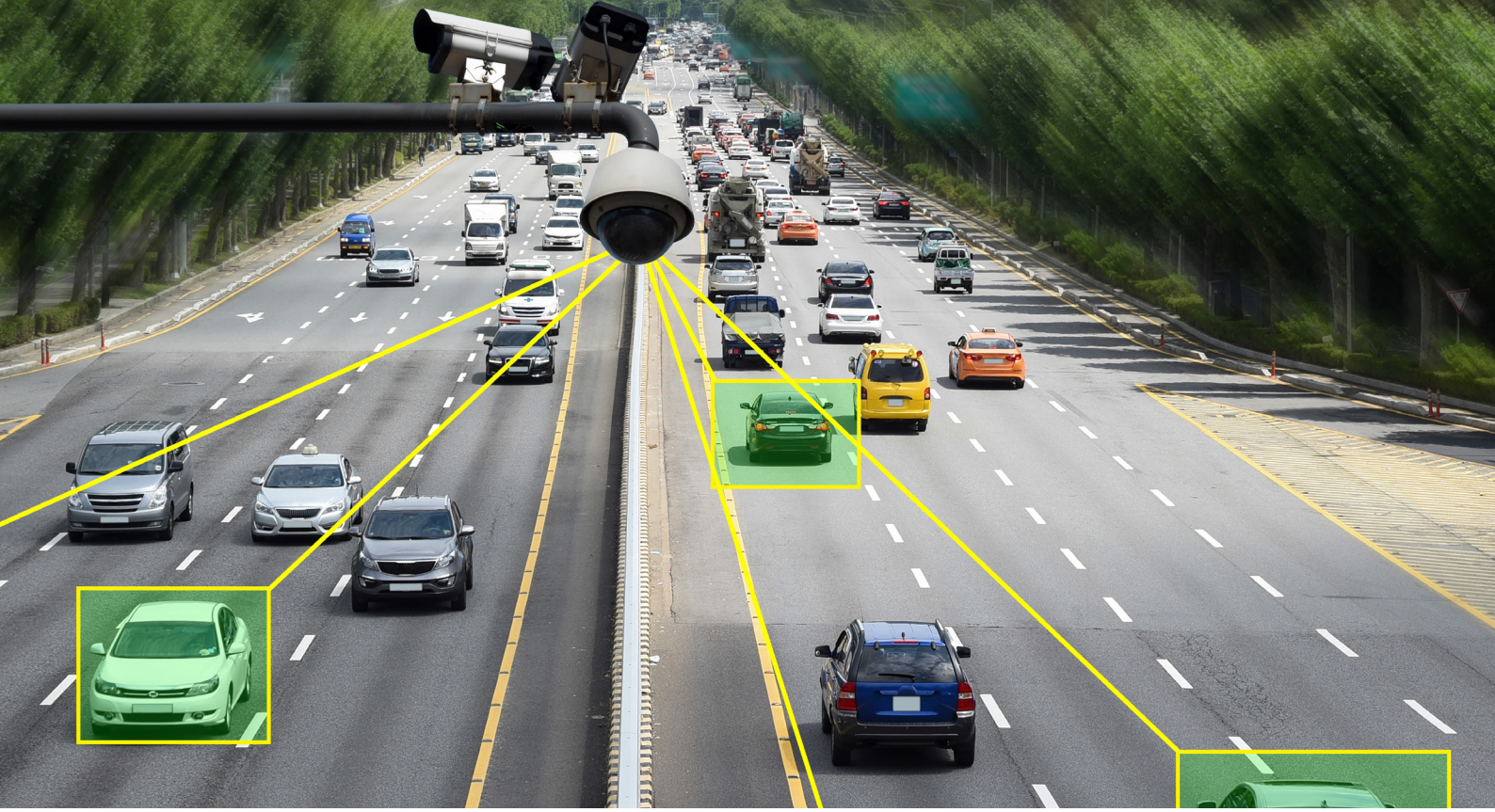
These transformative changes bring both opportunities and threats. It is imperative to employ a defence in depth strategy that furnishes secure connections to the IoT devices and prevents breaches that can target student data privacy and security of research or endanger data authenticity and integrity.

Government

Governments and municipalities are joining the IoT flow. Smart cities are presenting major business opportunity and new means to serve and protect citizens. In these connected cities, utility companies are pushing smart metres to create adaptable pricing systems and developers are rolling out sensors and automation components into new properties. Smart parking lots save citizens time and make them more efficient and smart waste bins call for action when they near the overflow. IoT helps municipalities and governments collect mobility information and data trends which provide critical analysis that are vital for city strategy formulation and long-term-planning. IoT brings:

- Better connected citizens and public entities to deliver high quality, secure and responsive services and resources that improve engagement and trust between governments and the public they serve by increasing liveability, workability and sustainability
- Increased transit safety by better understanding transportation system operations through sensor data that tracks everything from anomalies in light rail train speeds, roadway temperatures, and real-time location of mass transit buses
- Reduced congestion and energy use through Smart City technologies that leverage real-time data to improve how officials scale resources to meet demands; and provide the agility to react quickly to fast-changing traffic patterns, variations in water or power usage, or changes to air quality
- Improved operational performance and maintenance by proactively monitoring critical public infrastructure and creating more efficient processes to reduce operating costs and improve system capacity
- Improved public safety by responding faster and more effectively to emergencies

The bar for cybersecurity, however, must be set high, very high indeed. In the IoT cities where not all applications, sensors and devices are designed with security in mind, you need a smart and automated infrastructure that can put these devices in separate categories and stops them from talking to what they are not supposed to talk to. This containerisation will significantly improve the security and put the public sector entity on the right track to move toward a zero trust environment by creating multiple layers of protection in a defense-in-depth cyber strategy.



Transportation

The Internet of Things (IoT) is transforming the transport industry, by profoundly altering how systems gather data and information by bringing together automation and data analytics. Sensors, actuators and other devices can collect and transmit information about real-time activity in the network. That data can then be analysed by transportation authorities to better improve the traveler experience and safety, reduce congestion and energy used, while at the same time, optimising operational performance.

IoT is at the core of forces reshaping transportation to provide greater safety, more efficient travel, improved vehicle and aircraft maintenance and more strategic traffic management. Examples of transportation IoT application include:

- Efficiencies, to increase system capacity and enhance passenger safety and comfort while lowering costs and risks
- Dynamic roadside message signs, for intelligent transportation systems which display real-time road status, toll rates, lane closures and travel
- Autonomous vehicles, with the ability to sense their environment, predict behavior, communicate with other vehicles and their surroundings, and react instantaneously to real-life highway scenarios
- Video surveillance, to secure the movement of people and crowds, to automates and provide early detection of suspicious behaviour and abandoned luggage

Cyberattacks can impact daily operations for extended periods. Not only is service disrupted, but the exposure of highly sensitive data is also a huge risk when it comes to this sector. While some cybersecurity attacks are an attempt to earn money, other attempts are designed to cause chaos and disarray by shutting entire systems down. Disruptions of traffic lights, blocking access to important files and data, interrupting payroll services, and compromising ticket machines and fare gates are just some of them.

- In 2018, Bay & Bay Transportation became the victim of a massive ransomware attack that locked up the systems it uses to manage its 300-truck fleet
- In 2018, Hackers shut down 2,000 computers belonging to the Colorado Department of Transportation, disrupting operations for weeks. More recently, cybercriminals infiltrated three of 18 computer systems in New York's Metropolitan Transit Authority.
- The first half of 2020 revealed a staggering increase in ransomware incidents, with an overall 715% year-over-year increase
- In 2020, 9 million EasyJet customers' email addresses and travel details were stolen. Of those, 2,208 had their credit card information compromised. This cyberattack coupled with the blow from the global pandemic, resulted in the airline losing 45% of its share value and clocking its first annual loss ever in its 25-year existence.

Secure IoT networks and strategies are here today

ALE products and solutions build a secure network foundation to help organisations deploy IoT systems that can reveal the insights to optimise products and processes, make businesses smarter and more efficient and deliver improved customer experiences. ALE's IoT containment and layered security strategies reduce the risks and simplify the setup of IoT networks by easing device onboarding, providing more efficient operations and greatly increasing security. ALE helps organisations unlock the full potential benefits of IoT by providing enhanced levels of network intelligence, automation and security.

Want to learn more?

For more information about ALE's IoT solutions go to ALE IoT Security.

Alcatel·Lucent Enterprise