ALE | Where Everything Connects

The Internet of Things in the Enterprise

Build a secure foundation to leverage IoT business opportunities

Solution Brief
IoT in Business

Alcatel·Lucent
Enterprise

IoT Fundamentally Changes the Business Equation

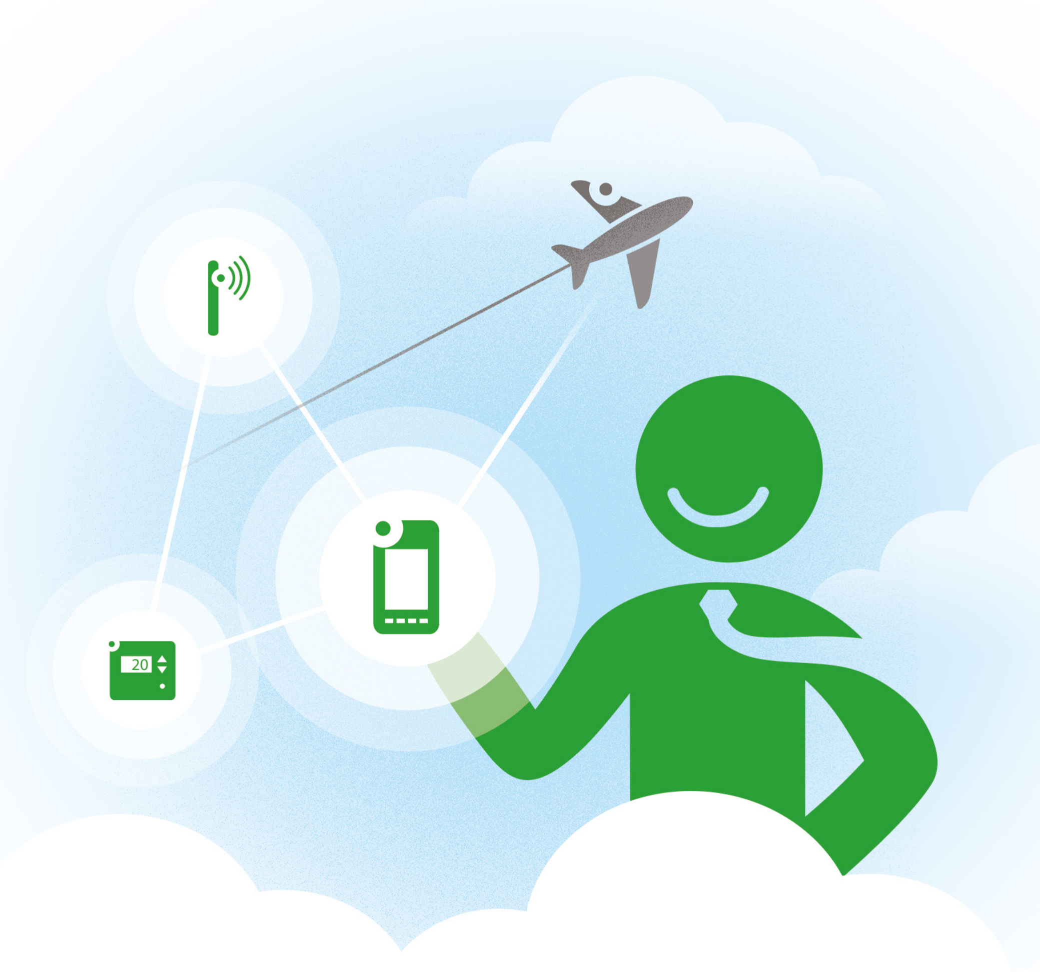
The Internet of Things (IoT) has the potential to transform business by profoundly altering how organizations gather data and information by bringing together the major technical and business trends of mobility, automation and data analytics. IoT refers to the networking of physical objects through the use of 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 analyzed by the organization to:

- **Optimize 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 personalized 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 scenarios in key industries

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

- **Healthcare –** The IoT has the potential to redefine how people, technology and devices interact and connect with each other in healthcare environments, helping promote better care, reduced costs and improved outcomes.
- **Education –** The IoT is changing both learning and teaching experiences in connected classrooms and improving how schools and campuses can monitor operations and safety for both primary and secondary education.
- **Hospitality –** IoT solutions provide opportunities for the hospitality industry to better serve customers, increase the efficiency of operations and provide differentiated services.
- **Government –** The IoT provides government agencies the opportunity to deliver higher-quality services, streamline processes, cut costs and find innovative ways to add new value for citizens.
- **Transportation –** The IoT is at the core of forces reshaping transportation to provide greater safety, more efficient travel, improved vehicle and aircraft maintenance, and strategic traffic management.



Challenges of IoT deployment

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

Organizations 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:

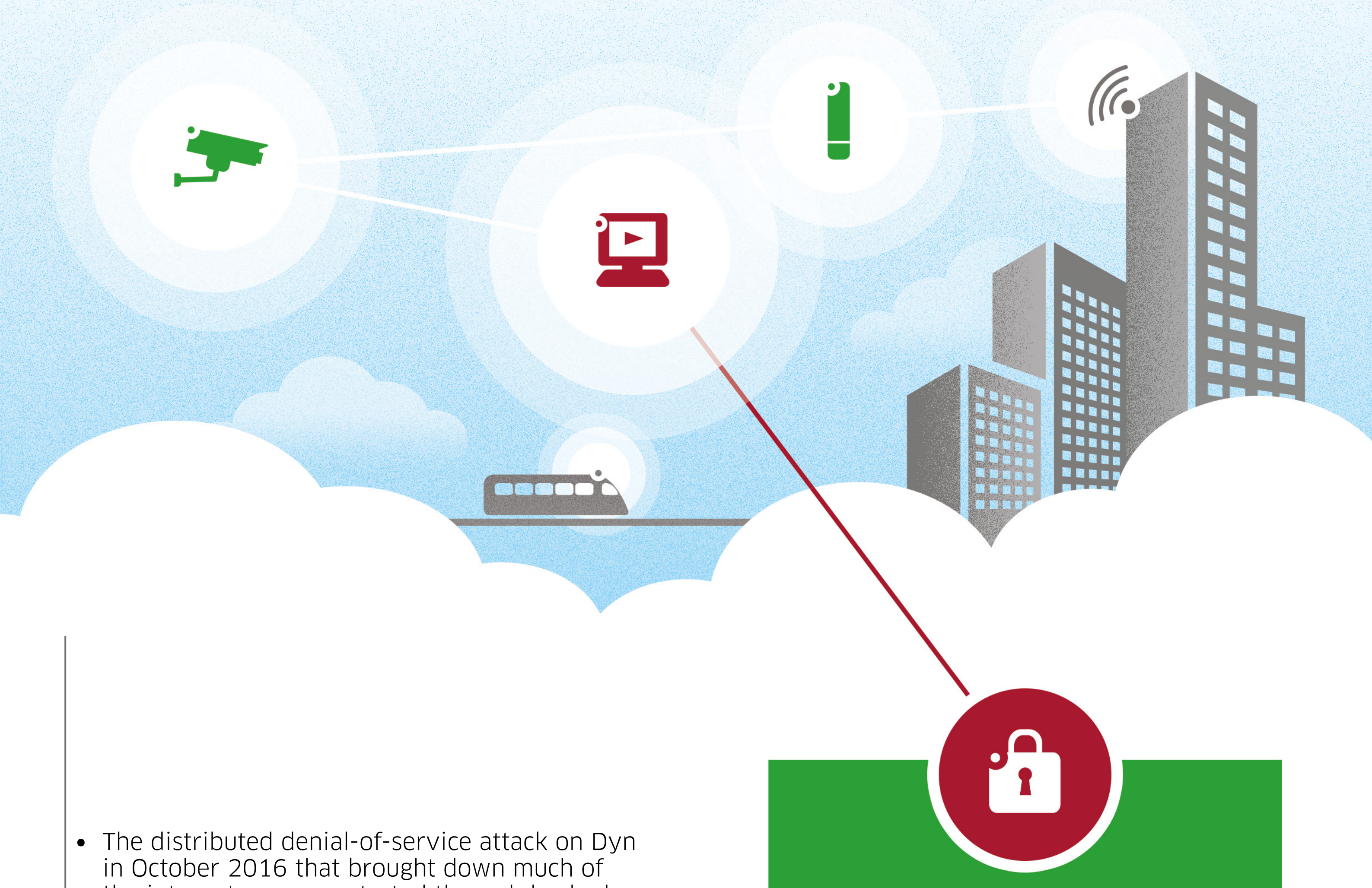
- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems can contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error-prone. Automated onboarding enables the network infrastructure to dynamically recognize 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 containment of the IoT networks themselves.

IT professionals are making plans for more IoT

IT professionals in a variety of industries are already planning for increased use of IoT solutions in the near future. According to the 451 Research survey 2017 Trends in the Internet of Things, 67 percent of responding IT professionals said their companies had either already deployed an IoT solution, or had an IoT system in pilot. Twenty-one percent of respondents said their companies planned to deploy IoT solutions within 12 months, with 11 percent claiming their companies' plans for implementing IoT were over a year away.

The IoT Compounds an Organization's Exposure to Cybercrime

With the growth of IoT also comes an explosion of cyber security 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 weak link in enterprise security.



- The distributed denial-of-service attack on Dyn in October 2016 that brought down much of the internet was perpetrated through hacked networked devices such as security cameras and digital video recorders.[1]
- Hackers attacked the network of San Francisco public transit system Muni in November 2016, rendering ticket machines and other computing infrastructure inoperable as part of a ransomware scheme.[2]

The electronic key system at Austria's Romantik Seehotel Jaegerwirt was hacked in January 2017, leaving guests locked out of their rooms and the hotel locked out of its own computer system, until the hotel paid the two Bitcoin ransom.[3]

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 organizations take advantage of the benefits and mitigate the risks of IoT deployment, Alcatel-Lucent Enterprise (ALE) provides a multi-level security strategy. ALE's strategy delivers protection at every layer of the infrastructure, from the individual user and device out to the network layer itself. It also provides an IoT containment strategy to simplify and secure device onboarding and deliver the right network resources to run the system properly and efficiently, all in a secure environment to safeguard organizations from cyberattack.

IoT containment

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

- Devices are placed in "virtual containers," using network virtualization techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network.
- In these virtual containers, QoS and security rules are applied.
- By segregating the network with virtual containers, if a breach does occur in one part of the virtual network, it does not affect other devices or applications in other virtual networks.
- When a new IoT device is connected, the network automatically recognizes 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 center that controls these devices.
- Because all users also have profiles within the ALE network, access to the IoT virtual containers can be limited to authorized individuals and groups.

In-depth security

In addition to IoT containment, ALE networking technologies provide layered security across multiple levels of the network.

- At the user level, profiles ensure users are authenticated and authorized 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 CodeGuardian™. 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 unauthorized activity and network intrusions.

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

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 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 management suite provides a single pane of glass to manage virtual environments, switches, access points and all other components of the network.

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 are able to address the networking needs for organizations of all sizes. ALE also provides a selection of ruggedized switches, access points and routers for network deployments outdoors or in harsh environments.

Secure IoT networks and strategies are here today

ALE products and solutions build a secure network foundation to help organizations deploy IoT systems that can reveal the insights to optimize 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 organizations 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](#).

We are ALE.

We make everything connect by delivering technology that works, for you. With our global reach, and local focus, we deliver networking and communications. On Premises. Hybrid. Cloud.

ALE | Where Everything Connects

[1] Hacked Cameras Were Behind Friday's Massive Web Outage

[2] Metro transport systems eyed after hack attack in San Francisco

[3] Hackers Use New Tactic at Austrian Hotel: Locking the Doors