ALE | Where Everything Connects

The Internet of Things for Government

Build a secure foundation to leverage IoT for improved public sector services, smarter infrastructure, and enhanced livability and safety

Solution Brief
IoT in Government

Alcatel·Lucent Enterprise

IoT fundamentally changes the government equation

The Internet of Things (IoT) has the potential to transform the public sector by profoundly altering how government entities 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 collect and transmit information about real-time activity within the network. The data gathered from these devices is then analyzed by public officials to:

- **Better connect 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 livability, workability and sustainability.
- **Increase 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.
- **Reduce congestion and energy use** through Smart City technologies that leverage real-time data to improve how officials scale resources to meet demands; and providing the agility to react quickly to fast-changing traffic patterns, variations in water or power usage, or changes to air quality.
- **Improve operational performance and maintenance** by proactively monitoring critical public infrastructure and creating more efficient processes to reduce operating costs and improve system capacity.
- **Improve public safety** by responding faster and more effectively to emergencies.

IoT scenarios in government

IoT solutions promise to make public sector organizations smarter and more successful. The IoT is at the core of forces reshaping government entities to provide better services, greater safety, efficient transit, smarter public infrastructures, and strategic traffic management. Examples of IoT scenarios in the public sector include:

- **More efficient, cost effective mass transit** that employs a network of sensors, digital cameras, and connected vehicles to increase system capacity and enhance passenger safety and comfort while lowering costs and risks.
- **Video surveillance solutions,** which feature high-resolution CCTV cameras to secure public transport and infrastructure, monitor movement of people and crowds, and expedite emergency responses. Intelligent video analysis software can automate early detection of suspicious behavior and abandoned packages.
- **Dynamic roadside signage** for Smart Roads and Highways, which displays real-time road status, toll rates, lane closures and travel times relayed automatically from sensors and cameras.
- **Smart energy solutions** that monitor power usage to create more resilient energy systems that reduce consumption and lower energy-related emissions to enhance municipal energy efficiency and sustainability.

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, government agencies need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

Public sector organizations need a cost-effective network infrastructure that securely handles vast flows of data, and is also simple to manage and operate. The infrastructure must:

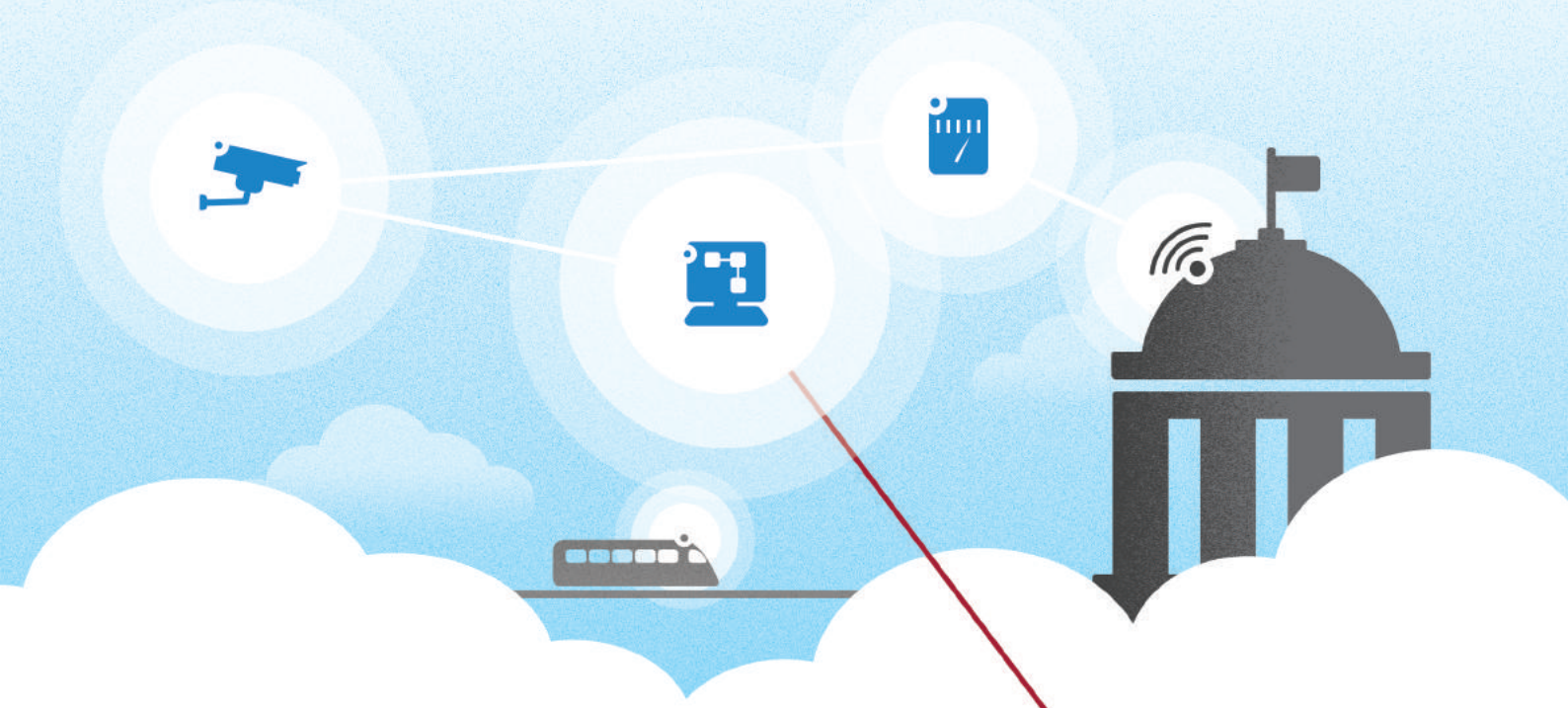
- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error-prone. Automated onboarding enables the network infrastructure to dynamically recognize devices 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 instance, 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.** There is a significant increase of potential attack vectors in government IoT systems due to the many networked devices and sensors within public sector networks, 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 organizations had either already deployed an IoT solution, or had an IoT system in pilot mode. Twenty-one percent of respondents said their organizations planned to deploy IoT solutions within 12 months, with 11 percent claiming their plans for implementing IoT were over a year away.

IoT compounds government's exposure to cyber crime

The growth of IoT in the public sector also brings an explosion of cyber security threats, as the proliferation of sensors and connected devices greatly expands points of entry for the network attack. 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 government network security.



- **The WannaCry ransomware attack in May, 2017, infiltrated governmental networks around the world,** encrypting data and paralyzing computers for days at the Ministry of Internal Affairs of the Russian Federation, the Romanian Ministry of Foreign Affairs, and four state governments in India.[1]
- In March, 2018, **Atlanta's municipal government was brought to its knees** when ransomware hackers exploited vulnerabilities in the city's Smart City network and encrypted government files, locked access to online services (including email), and blocked the city from processing court cases and warrants.[2]

The Sweden Transport Administration Trafikverket was hit with a distributed denial of service (DDoS) attack in 2017 that brought down the automated system that operates trains and also the organization's email and communication network, stranding rail passengers across the country without information about what had happened to the service.[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 to the network layer itself. It also provides an IoT containment strategy to simplify and secure device onboarding, delivering the right network resources to run the system properly and efficiently, all in a secure environment to safeguard governmental systems from cyberattack.

IoT containment

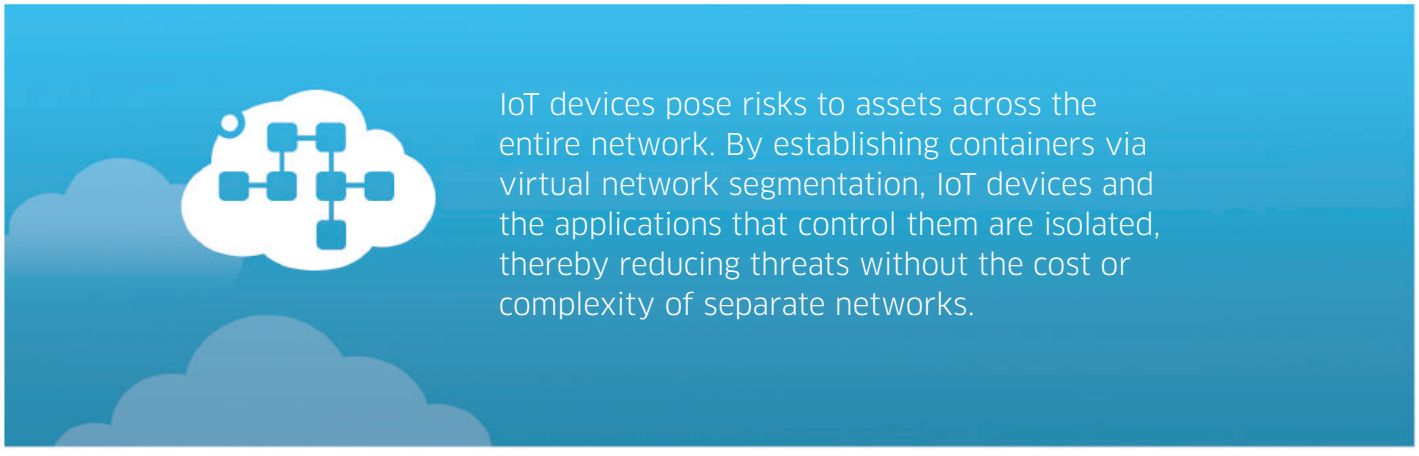
To enable IoT containment, all users, devices and applications within the ALE network are assigned profiles. These profiles, which define roles, access authorizations, QoS levels, and other policy information, are relayed to all switches and access points in the network.

- 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 establishes 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.



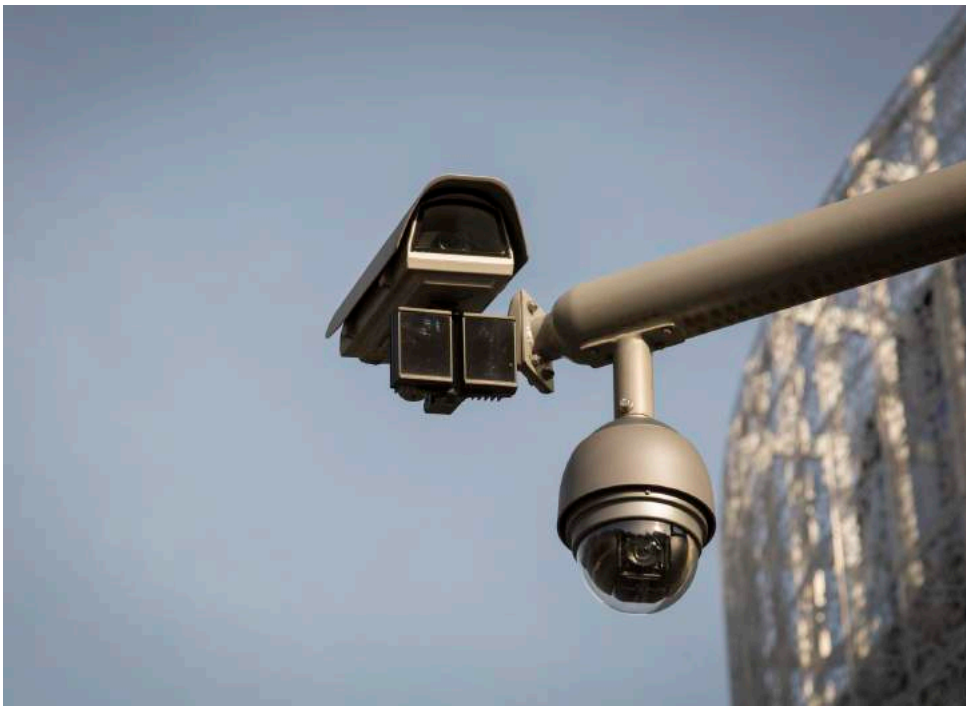
End-to-end operational and network management

ALE network solutions for education also provide significant operational and management advantages.

- **ALE enables multiple separate virtual networks to operate on a single infrastructure,** saving CAPEX investment in multiple physical networks.
- **The ALE 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 educational institutions of all sizes. ALE also provides a selection of ruggedized switches, access points and routers for network deployments outdoors or in harsh environments.



Secure government IoT networks and strategies are here today

ALE products and solutions build a secure network foundation to help public sector organizations deploy IoT systems that help better connect citizens to services, enable Smart City solutions, and improve operational efficiency of public infrastructure while decreasing costs and risk. ALE's IoT containment and layered security strategies simplify the setup of government IoT networks by easing device onboarding, providing more efficient operations and greatly increasing security. ALE helps public sector 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.

Connected Government

We help you connect your communities by delivering technology that works, for your organization and the public you serve With global reach and local focus, we deliver networking and communications built to provide mobility, security and safety for public sector organizations.

ALE | Where Everything Connects

[1] WannaCry Ransomware Attack
[2] A Cyberattack Hobbles Atlanta, and Security Experts Shudder
[3] DDoS Attack Halts Swedish Transport Systems