The Internet of Things in Healthcare
Build a secure foundation to leverage IoT solutions and optimize the care pathway
The Internet of Things (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. IoT refers to the networking of physical objects such as embedded sensors, actuators and other devices that collect and transmit information about real-time activity, via a network. The data gathered from these devices can then be analyzed by the organization to:

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

### IoT scenarios in healthcare

IoT solutions for healthcare hold the promise to make medical organizations smarter and more successful at what they do. 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. Examples of healthcare IoT solutions include:

- **Connected medical devices**, such as MRI and CT scanners, which generate vast flows of data that network with computing infrastructures providing analysis and visualization.
- **Wearable medical devices and remote patient monitoring devices**, which offer safer and more effective healthcare through real-time patient monitoring of vital signs, post-procedure recovery, and adherence to treatment, both in hospital and remotely. With wearable sensors, doctors remotely track and respond to a patients’ health status in real time.
- **Video security cameras and electronic ID-enabled security doors**, which increase security and prevent threats and unauthorized entry and departure.
- **Medical asset tracking**, which uses Bluetooth Low Energy (BLE) tags to monitor location of medical devices, medicines and supplies.
- **Preventative maintenance solutions** for medical equipment, to reduce unplanned repair of essential medical tools, devices and systems.
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, healthcare organizations need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

Hospitals, clinics and care facilities need a cost-effective network infrastructure that meets security and privacy mandates while handling 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 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 medical systems such as 3D and color imaging require bandwidth reservations on a high performance network infrastructure to ensure service delivery and reliability.

- **Provide a secure environment against cyberattacks and data loss.** Since many networked devices can 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 growth of IoT in healthcare also brings an explosion of cyber security 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 cyber security.

**IoT compounds healthcare’s exposure to cyber crime**

- **The WannaCry ransomware attack in May, 2017,** infiltrated hospital networks across Europe and North America, stopping care and treatment for days at sixteen NHS hospitals in Britain.¹
- **St. Jude Medical,** a medical device manufacturer of pacemakers, defibrillators and other cardiac devices, was forced to patch its device software in Feb. 2017, after it was reported that implantable devices made by the company were vulnerable to potentially catastrophic hacks. Infiltrators could take advantage of the vulnerability to change configurations and cause cardiac devices to malfunction and alter pacing to dangerous rates, or deliver harmful shocks. The attacks, the report said, are within reach of relatively unskilled hackers.²
- **Johnson & Johnson** warned customers about a security vulnerability in one of its connected insulin pumps in 2016, which hackers could exploit to overdose diabetic patients with insulin.³

---

**The hacker exploit known as MedJack** allowed attackers to inject malware into medical devices, which then fanned out across the healthcare network infrastructure. The medical data stolen in these types of attacks was used in tax fraud or identity theft schemes, and was even used to track active drug prescriptions, enabling hackers to order medication online to sell on the dark web.⁴
Building a secure IoT network infrastructure for healthcare

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 healthcare 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 infrastructure 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 hospitals, clinics and medical care facilities 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 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 applications.
- 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.

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 healthcare operations with significant operational and management advantages.

- ALE enables multiple separate networks to operate on a single, common infrastructure, eliminating the need for additional CAPEX investment in multiple physical networks.

- The ALE Unified Access framework allows wired and wireless technologies to work together as a single, robust network, with a common set of network services, policy rules, 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 and wireless LAN 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. Network Management is also available “as-a-Service” with OmniVista Cirrus, ALE’s cloud-based network management solution.

Secure IoT networks and strategies are here today

ALE products and solutions build a secure network foundation to help hospitals, clinics and care facilities deploy IoT systems that can reveal the insights to optimize products and processes, save staff time, make workflows more efficient, and deliver improved patient 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 healthcare organizations unlock the full potential benefits of IoT by providing enhanced levels of network intelligence, automation and security.

A high performance network portfolio

ALE switches, access points and cloud applications 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 networking needs for healthcare organizations of all sizes. ALE also provides a selection of ruggedized switches, access points and routers for network deployments outdoors or in harsh environments where ambulances and emergency medical teams operate.
Connected Healthcare

At Alcatel-Lucent Enterprise we help you connect your patients, staff and healthcare ecosystem. Delivering technology that works, across and beyond your facilities. With global reach and local focus, we deliver specialized networking and communications for healthcare providers, to optimize the care pathway and enhance patient outcomes.

---

1 Hacked Cameras Were Behind Friday’s Massive Web Outage
2 St. Jude Patches Additional Cardiac Device
3 J&J warns diabetic patients: Insulin pump vulnerable to hacking
4 Medical Devices Are the Next Security Nightmare