The Internet of Things for the Hospitality Industry

Build a secure foundation to leverage IoT business opportunities

Solution Brief
IoT in Hospitality

Alcatel·Lucent Enterprise

IoT fundamentally changes the hospitality business equation

The Internet of Things (IoT) has the potential to transform the hospitality industry by profoundly altering how hotels, resorts, cruise ships, casinos, restaurants and other leisure service businesses gather data, interface with users and automate processes. 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 activities in an environment. When IoT is combined with technologies such as user mobility and data analytics, it brings a new paradigm in hospitality. IoT enables organizations to:

- **Improve guest experiences** by offering new amenities, services and a unique digital experience to differentiate from the competition.
- **Optimize processes** by reducing operating costs, increasing productivity and developing new services.
- **Learn more about guest 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.

IoT scenarios in the hospitality industry

IoT solutions promise to make businesses in the hospitality industry smarter and more successful at what they do. Here are examples of how IoT solutions provide opportunities for the hospitality industry to better serve customers, increase the efficiency of operations and provide differentiated services:

- **Smart devices that turn ordinary mirrors into personal interactive information stations** to enable guests to manage hotel room functions, ambiance and entertainment. With a simple touch, guests can connect with hotel services and access information, including local news, weather and traffic.
- **Autonomous indoor delivery robots** that automate hotel room service. Employing sensors, artificial intelligence and machine learning, the robots are able to operate elevators and navigate crowds while handling tasks such as room deliveries quickly, safely and reliably.
- **Through use of connected thermostats,** hotels can adjust guest room temperatures at check-in and checkout to eliminate the cost of cooling or heating vacant rooms. Linking thermostats with other sensors, air conditioning turns off automatically when a guest opens a window or balcony door; automated window coverings close during afternoon sunshine to reduce temperature swings.
- **Preventative maintenance IoT systems** identify appliance or equipment issues before they become costly problems. In guest rooms, sensors can monitor HVAC systems and automatically notify maintenance when units are beginning to fail.

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, hotels, resorts and other hospitality businesses need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

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

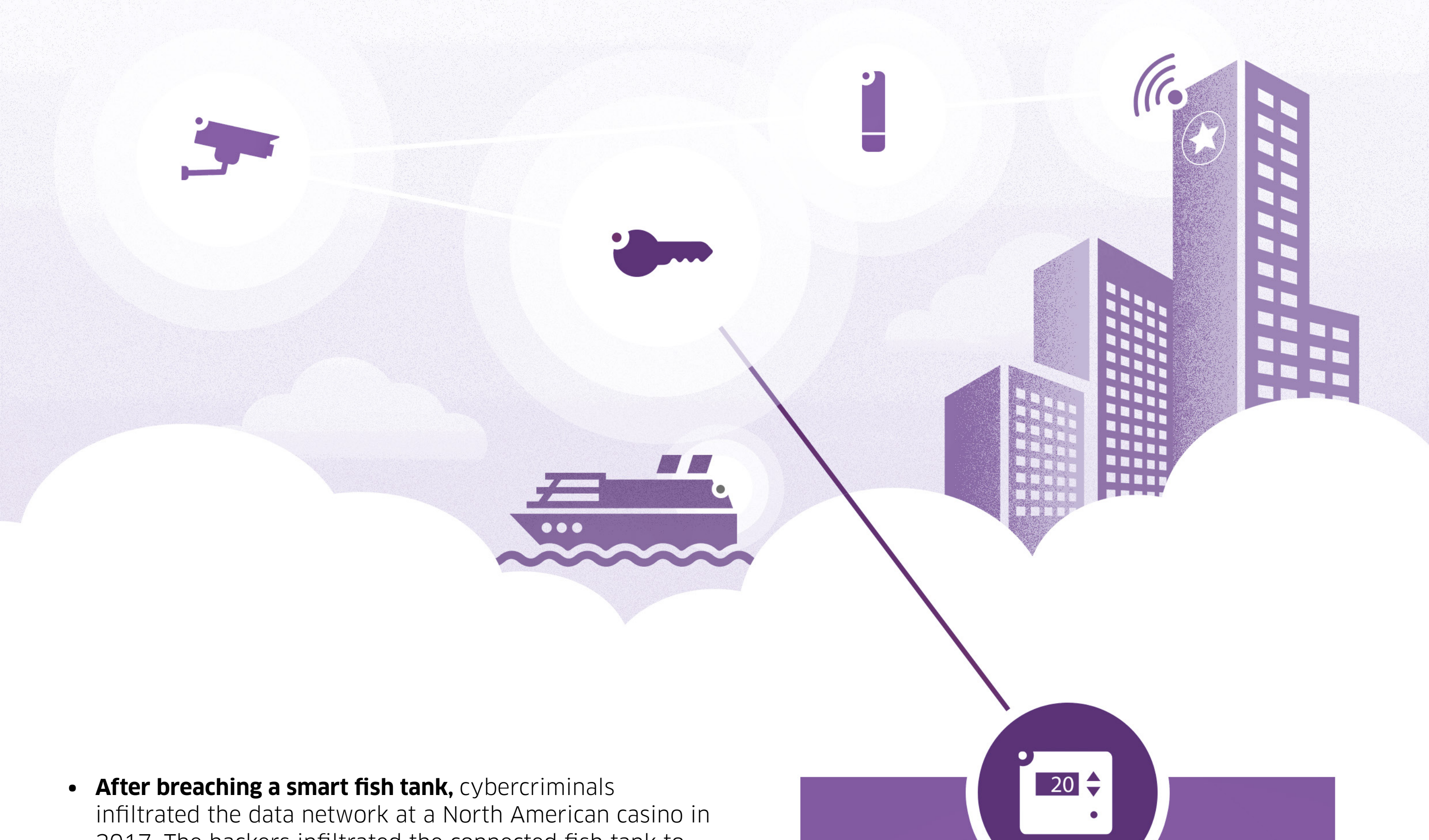
- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems can contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error-prone. Automated onboarding enables the network infrastructure to dynamically recognize 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, Smart TV's (IPTV) require proper bandwidth reservations on a high-performance network infrastructure to ensure service delivery quaility.
- **Provide a secure environment against cyberattacks 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 cyber crime

The growth of IoT in the hospitality industry also brings an explosion of cyber security threats, as the proliferation of sensors and connected devices greatly expands 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 network security for hospitality businesses.



- **After breaching a smart fish tank,** cybercriminals infiltrated the data network at a North American casino in 2017. The hackers infiltrated the connected fish tank to get into the casino's network, which they scanned to find vulnerabilities elsewhere. The hackers began relaying data to a device in Finland before the threat was discovered and stopped.[1]
- **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 Bitcoin ransom.[2]
- **The CIA has tools for hacking IoT devices,** such as Samsung SmartTVs, Wikileaks revealed in 2017. Operatives are able to hack into smart devices to remotely record conversations in hotel or conference rooms.[3]

As part of Def Con 24, penetration test experts Pen Test Partners demonstrated how easy it was to hack into a smart thermostat and create fully functioning ransomware that could lock a user out until they paid up.[4]

Building a secure IoT network infrastructure for hospitality

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 hotels, casinos, resorts and other hospitality businesses take advantage of the benefits and mitigate the risks of IoT deployments, 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 hospitality businesses 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 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 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.

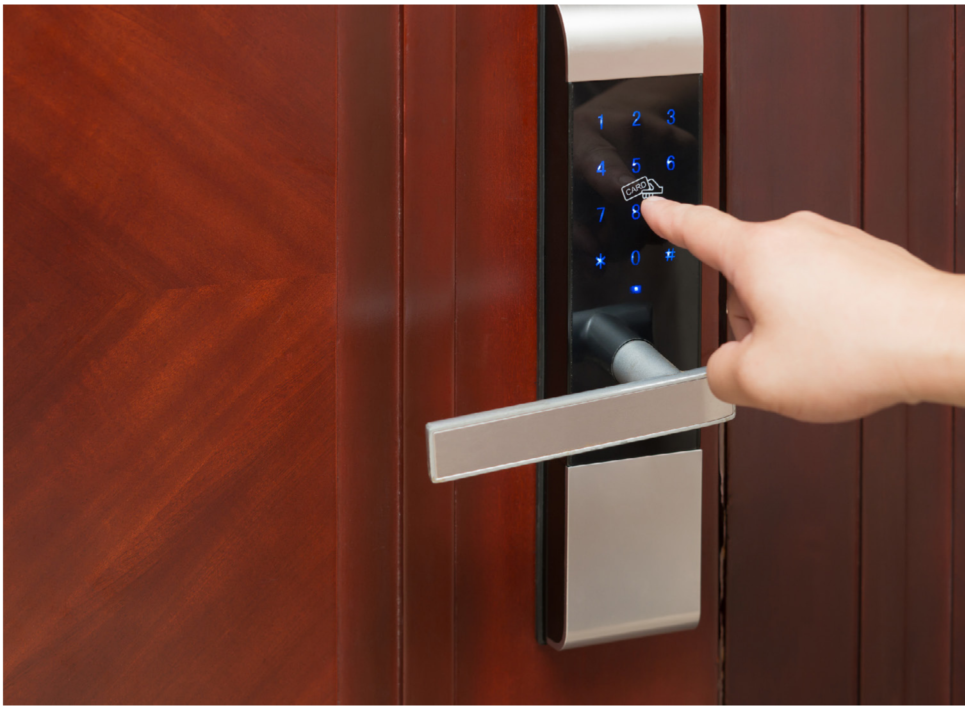
End-to-end operational and network management

ALE network solutions also provide significant operational and management advantages to hotels, resorts, casinos and other hospitality operations.

- ALE enables multiple separate virtual networks to operate on a single, common infrastructure, eliminating need for CAPEX investment in multiple physical infrastructures.
- 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 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 of hospitality 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 for the hospitality industry are here today

ALE products and solutions build a secure network foundation to help hospitality organizations deploy IoT systems to deliver unique guest experiences, optimize processes, increase the efficiency of staff and offer new services. 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 hospitality operations 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 Hospitality

Where guests connect to personalized and memorable experiences. Where staff connect to deliver efficient, responsive services. Where your ecosystem connects to improve revenue, safety and guest engagement.

[1] A smart fish tank left a casino vulnerable to hackers

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

[3] If the CIA can compromise our gadgets, can't others do the same?

[4] Thermostat Ransomware: a lesson in IoT security

www.al-enterprise.com The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2020 ALE International, ALE USA Inc. All rights reserved in all countries. 00303780 (October 2020)