WHITE PAPER

IoT AND THE SMART DIGITAL WORKPLACE: OPPORTUNITIES AND CHALLENGES

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

The Internet of Things (IoT) can be defined as a universe of devices, software, and systems that interact directly with the physical environment while communicating with each other and the IT infrastructure. IoT is one of the foundational drivers for the emergence of the Smart Digital Workplace. Workplaces equipped with a growing range of IoT sensors and other IoT devices will be able to offer enhanced, interactive experiences to their occupants, visitors, managers and operators. In addition to new IoT components, the capability and maturity of IoT security frameworks, combined with new forms of cloud-based platforms, will incorporate traditionally-segmented systems like Building Management Systems (BMS) and access control into the overall IoT environment.

THE PHENOMENAL GROWTH OF IoT DEVICES AND DATA

IoT continues to experience phenomenal growth. Gartner forecasts 10 billion business (non-consumer) endpoints in offices and other workplaces worldwide by 2021, with a CAGR of 30.7%.[1] This represents a three-fold increase over today's level of about 3 billion devices. The total becomes even greater when considering the number of "hybrid" devices that might emerge – for example, devices such as personal PCs and printers associated with home or remote offices. Other estimates range as high as 30 billion devices. Memoori Research forecasts that Smart Building devices will represent about 30% of all Smart City devices – the largest segment of non-industrial IoT, with a CAGR of about 20% for office-related devices.[2]

At some point, overall IoT device and traffic growth rates will slow down, given the law of large numbers, but it's Aruba's view that this increase in the number of opportunities and the number of facilities that do not yet feature IoT will drive new demand for edge infrastructure over the upcoming years.

> "Gartner forecasts 10 billion business (non-consumer) endpoints in offices and other workplaces worldwide by 2021, with a CAGR of 30.7%."

A COMPLEX SET OF INTERCONNECTED DEVICES AND SYSTEMS

IoT devices in the Smart Digital Workplace fall into the following broad categories:

- **Environmental** – Includes "smart" lighting, HVAC, fixtures like automatic shades, furniture and similar systems, many of them connected to a Building Management System (BMS)
- **Security** – Includes physical access control, video surveillance cameras and recording/processing equipment, fire control, and other systems associated with safety and protection
- **Mobile** – Includes users' smart devices, dedicated mobile devices, mobile PoS and many others
- **Application-focused** – Includes Bluetooth beacons, room occupancy sensors, digital signage, AV, collaboration and other devices and systems focused on end user services
- **Other** – The ever-decreasing cost of increasingly-capable IoT devices ensures that more types of devices, in categories other than the above, will continue to be connected to the network

For many of the systems being brought into the IoT universe of interconnectivity, openness and data sharing already exist, but often the systems and devices are running on their own unmanaged networks. A good example is the typical Physical Access Control System (PACS) that locks doors or environmental systems. These systems generate large volumes of data and require sophisticated controls, but enterprise networks traditionally could not, or would not, support them. IT managers had little interest, because the stakeholders of these systems and associated data were specialized groups like Security Management or Corporate Real Estate.

Today, this landscape is changing. The desire to improve experiences and cybersecurity initiatives being driven by executive management, IT, Corporate real estate, HR, and other business functions is one of the drivers of IoT deployment and integration in the enterprise.

[1] "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017," Gartner, 2017. www.gartner.com
[2] "The Internet of Things in Smart Commercial Buildings: 2018-2022," Memoori Research, 2018. www.memoori.com

> Many of the systems being brought into the IoT universe of interconnectivity, openness and data sharing already exist, but often the systems and devices are running on their own unmanaged networks.

SECURITY IS VITAL TO IoT – AND THE NETWORK IS VITAL FOR SECURITY

Even in its short history, IoT continues to be a top identified security challenge by corporate executives. The concern with IoT security at high levels of government and enterprise management has helped to drive considerable research, fund the creation of startup companies, and provide lucrative business opportunities to security products and expert consultants.

Recently, the US Government's National Institute of Standards (NIST) began an effort to develop security standards specific to IoT. The NIST Interim Status Report, NISTIR8200, quotes the President's Commission on Enhancing National Cybersecurity's conclusion on IoT cybersecurity risk:[3]

> "*The IoT facilitates linking an incredible range of devices and products to each other and the world. Although this connectivity has the potential to revolutionize most industries and many facets of everyday life, the possible harm that malicious actors could cause by exploiting these technologies to gain access to parts of our critical infrastructure, given the current state of cybersecurity, is immense.*"

A recent international study conducted by Aruba supports the conclusions identified by NIST, revealing that security remains a key concern with 84% of organizations surveyed reporting an IoT-related security breach.

> Security remains a key concern with 84% of organizations surveyed reporting an IoT-related security breach.

Some examples of security risks associated with IoT are:

- **Vulnerable firmware** – This was highlighted by a recent global denial of service (DDoS) attack that harnessed flawed security camera firmware to build a "botnet" that then launched a massive Distributed Denial of Service (DDoS) attack on major websites. IoT device manufacturers often think of security last and utilize off-the-shelf firmware that has not been thoroughly tested. Some firmware is of questionable origin, and may have been compromised by hackers or state-sponsored organizations prior to installing in a particular device.
- **Physical accessibility** – IoT devices in the Smart Digital Workplace are often mounted in an open environment, which can lead to unauthorized network access and connection of malicious devices. For example, a security camera mounted outdoors with an Ethernet connection can be a vulnerable point for a bad actor to tap into the entire enterprise network or control the building management network, unless suitably protected.
- **Compromising malfunction** – This refers to an IoT device or system that malfunctions in a manner that causes wider damage. For example, a broken or misconfigured sensor may cause a flood of data to be sent erroneously over the network, may fail to send data, or send impersonated data.
- **Insufficient authorization, authentication, and access control** – IoT systems may not interact with enterprise systems designed to protect access, authentication, and authorization. For example, a decoupled database of valid users for a particular IoT device or system may expose the system to risk when a user leaves his or her job. IoT management software may not provide granular levels of authorization sufficient to prevent accidental or malicious misconfiguration.
- **Weak data security** – IoT devices and systems may collect or store Personally Identifiable Information (PII) and other sensitive data, which causes issues in many cases. Regulated environments like Financial Services and Healthcare generate even greater risks when data is collected or stored. Smartphones in the workplace environment are a common source of information leakage via photographs, recordings, emails, and other media.

[3] "Interagency Report on Status of Standardization for the Internet of Things (IoT)," Draft NISTIR 8200, US National Institute of Standards and Technology (NIST), February 2018.

How can the enterprise best protect against IoT security concerns? Aruba strongly believes that the best combination of techniques is to correctly implement as much security as is available at the point of entry into the network, along with active monitoring once a device has been admitted to the network. Specifically, the network should check for device authenticity and vulnerabilities via profiling, analytics, continuous monitoring and other means. Such a network must have an overall security fabric built into the core.

Traditional enterprise networks are not well-equipped to deal with IoT's security needs. The networks' physical configuration and software capabilities were intended for "enterprise classic" environments: data centers and offices with trusted and enterprise managed client and server computers primarily connected via unsecured Ethernet connections. This design restriction limits the network's ability to manage a large number of disparate devices with individual security needs and behaviors.

IoT GENERATES NEW DEMANDS AT THE EDGE

Enterprise networks face significant opportunities and challenges with the rise of IoT. As IoT continues to grow and assimilate into the workplace, the connections and traffic associated with this new infrastructure will need to be connected to the enterprise network in order to enable new services and experiences and supersede old, isolated systems.

Each new IoT device connected to the network requires the network to grant sufficient bandwidth, security protection, and appropriate access to other resources on the network. IoT devices may be wired, wireless or both, in any given system. The network must be capable of providing a common service and security fabric across all the devices. In the Smart Digital Workplace, the network itself becomes a key part of the IoT architecture and infrastructure, serving not only to connect other devices but also as its own constellation of sensors and source of data.

A unified wired and wireless network with sufficient reliability, scalability, flexibility and security to support an IoT environment requires an architecture and product suite that is intelligent, open, insightful, and autonomous – designed to support a heterogeneous environment without traditional borders or the limits of traditional traffic patterns.

At the connectivity layer, this requires coordinated management, support for multiple radio access networks (RANs), flexible connectivity, high capacity and reliability and security across the wired and wireless fabric. At higher levels, the network must provide open APIs, intelligent data analysis, machine learning, policy-based management, and coordinated orchestration for new services.

As more sensors are deployed and more data is generated, secure compute resources at the edge may become a necessity to process high volumes of data, such as video, before forwarding insights to their final destination.

A security-centric network built with a mobile-first approach can serve as a catalyst for broader IoT buildouts. The optimal network for IoT allows each device to be categorized and "fingerprinted" by network behavior, and specifically authorized to connect. Machine-learning software on the network then monitors for anomalous behavior, autonomously adjusting device access entitlements when such behavior is detected. Aruba's 360 Secure Fabric provides these mechanisms and controls, so that an enterprise can deploy IoT with fewer security concerns.

In summary, all stakeholders and end users can benefit from an organized approach to IoT, with a set of goals, business case, metrics, strategy, and roadmap. This type of approach can help to ensure a successful IoT implementation. The process should begin sooner rather than later, because IoT tends to grow organically, often in the realm of "shadow IT," unless there is cooperation among groups toward common goals and objectives.

THE NETWORK IS CRITICAL FOR ENTERPRISE IoT AND EXPERIENCES

The rapid growth of IoT in the enterprise, with all its opportunities and challenges, creates a new mandate for IT and other stakeholders to re-examine and update the enterprise network platform. Aruba's Mobile First Architecture and range of products are specifically designed to support the growing needs of IoT in the enterprise.

Aruba's Smart Digital Workplace initiative is focused on the concept of Experiences. The rich data and powerful control capabilities provided by IoT can enrich experiences for all stakeholders.

For example:

- **Office workers and other end users** can utilize smartphone apps and sensors to help guide them on the floorplan, find other users, locate common facilities like printers, and escape or report safety in an emergency situation. IoT-based climate and lighting control, along with smart furniture, can increase the comfort and wellness of the workplace.
- **Real Estate managers** can utilize IoT-enhanced and interconnected BMSs and sensors to optimize energy consumption, detect malfunctions, remotely monitor conditions, improve physical security, and provide better services to their clients.
- **IT specialists** can utilize IoT to monitor equipment, detect data leakage vectors and other security breaches and drive new applications that enhance productivity for their business clients. An IoT-friendly network approach, such as Aruba's Mobile First Architecture, can greatly simplify the task of managing IoT components as well as serve as a giant sensor to provide unique data of its own.
- **Business managers** can derive new and useful conclusions about workplace productivity, real estate costs, space utilization, remote work, and other metrics in their organizations. This can reduce real estate costs and improve worker metrics such as retention and employee satisfaction.

Aruba's Smart Digital Workplace partnership initiative continues to build a best-of-breed ecosystem with partners such as CBRE, Herman Miller, Deloitte and others to help enterprises implement IoT and other components needed for the future of work.

To learn more about Aruba and their Smart Digital Workplace solutions, and how to unlock its potential, go to www.arubanetworks.com/solutions/digital-workplace/.

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM