Kollective

WHITE PAPER

Distributed Devices

How Today's IT Leaders Are Taking Their Businesses To The Edge

Released: September 17, 2019

Across the globe, IT teams are increasingly incorporating the Internet of Things (IoT) into workplace operations. According to telecommunications company, Ericsson, we can expect 18 billion IoT devices by 2022. The integration of IoT devices into the workplace will open up access to important data and insights, improve workplace safety, and increase efficiency and productivity through automation.

Many large companies are encouraging the rapid adoption of IoT networks to drive business transformation. However, every new IoT device deployed in the workplace introduces numerous network challenges for CIOs and IT managers. Microsoft recently launched its IoT Signals Report looking into the trends, challenges and benefits surrounding enterprise IoT. Alongside personal items, this interconnected web is set to expand into the corporate world, with the appearance of wearable technology, voice assistants and even smart fridges in the workplace. For every new smart device introduced, IT departments are faced with yet another piece of hardware to update, manage and secure across their networks. At the same time, the rise of edge computing means more processes will be managed at the device level, rather than in the cloud. This opens up even more complex network and security challenges for enterprise IT teams.

Drawing upon research, this report explores key considerations that IT professionals should consider when incorporating IoT devices into their business ecosystems, and enabling these IoT networks to scale effectively and securely.

METHODOLOGY

This report incorporates research carried out with over 270 IT decision makers across the US and the UK. Commissioned by Kollective and conducted by independent research agency, Censuswide, all data was collected from a combination of online and phone surveys. Survey respondents were then broken down by company size and industry sector.

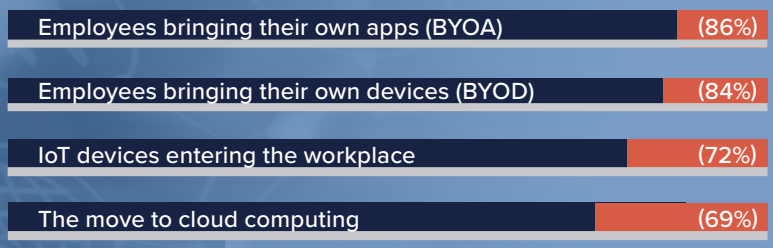
THE STATE OF ENTERPRISE IOT

There is a clear demand for the enterprise adoption of IoT devices, with 88% of IT decision makers believing IoT devices will make their workplaces more efficient. Maximizing productivity is a key focus for businesses. IoT devices can make the process of everything from collecting data to managing stock or automating processes quicker, more accurate and more effective. Head of Azure IoT at Microsoft, Sam George, stated that IoT is having a beneficial impact on the planet, before reducing energy, natural resources and improving sustainability."

There are also genuine challenges to overcome before industry-wide adoption can be achieved starting with overcoming concerns about who will regularly manage, monitor, update and test these IoT devices to make them more efficient for users and businesses. Microsoft research shows many companies struggle to get IoT adoption off the ground in the first place, with 30% of IoT projects failing in the proof-of-concept stage. Following the move towards Bring Your Own Device (BYOD) policies, enterprise IT teams are already struggling to keep on top of an increasingly diverse list of employee devices. As these emerging technologies begin to shape how people work, it's clear from our research IT leaders will need to ensure that measures are in place to make this process as reliable, effective and secure as possible.

While distributing these updates present a challenge, the issue of testing them should also be considered. 90% of businesses say IT teams should test all updates before they are installed, including those for IoT devices. With the number of IoT devices in the workplace growing exponentially, the IT resources required to maintain these devices will also increase dramatically. Already, over half of IT teams (61%) believe it will be impossible to keep all IoT devices up-to-date all the time. As businesses become increasingly IoT-centric, it is clear that there are some considerable challenges to overcome.

WHAT ARE THE CURRENT AND FUTURE SECURITY RISKS?



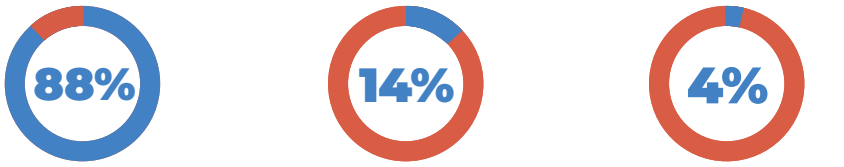
ROADBLOCKS TO LARGE-SCALE IOT NETWORK ADOPTION

Only 5% of businesses claim there is nothing standing in the way of enterprise-wide IoT adoption. For the rest, there is work to do in preparation for building large-scale IoT networks and overcoming adoption barriers, starting with security. The growing use of IoT in business increases the attack surface of an organization. Over half (55%) of IT leaders agree, considering security risks to be the number one roadblock for IoT adoption in the enterprise. Additionally, 72% of IT teams see the IoT as a security risk to their company. These concerns are overshadowing the potential business benefits of IoT, limiting the likelihood that IT teams will deploy them at scale, and slowing the overall adoption of IoT networks. This could lead to companies being left behind as their competitors potentially race towards better products or faster digital transformation.

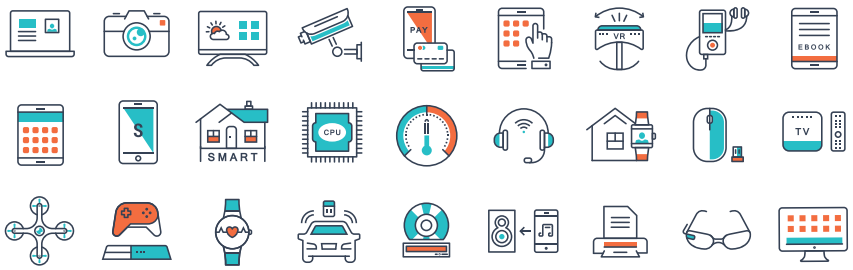
Another roadblock for IT organizations is the lack of centralized operating systems for the Internet of Things. While businesses might be able to guarantee that all of their mobile devices and computers run a single operating system, such as Windows 10, and thereby simplify the updating and orchestration process, when it comes to the IoT, no clear front-runners have been settled on by the industry. While big players like Microsoft and Google have put forward their own OS, many devices still run bespoke, customized or open source operating systems without the regular security update mechanisms associated with big-name brands.

The deluge of new internet-enabled devices entering the workplace presents many potential network challenges for IT teams. For every new device introduced into the workplace, a CIO must consider exactly how these devices impact the wider IT and security ecosystem. Each internet-enabled device will also require regular updates and patches to meet compliance protocols and guarantee that the organization is protected against potential cyberattacks.

WHOSE RESPONSIBILITY IS IT TO UPDATE IOT DEVICES?



Business demand is driving more IoT use cases that will require enterprises to build large-scale networks with sufficient infrastructure to distribute thousands, tens of thousands, and eventually millions of updates across their networks on a more frequent basis. For those organizations with global distributed offices and outdated network infrastructures this represents a near impossible task.



72% of IT teams see the IoT as a security risk to their company

IOT BARRIERS: A REGULATED APPROACH

Almost a third of IT leaders (31%) believe that a lack of clear rules for use is a considerable barrier to the adoption of the IoT. However, despite regulations being introduced in both the US and the UK, IT decision makers still do not have a clear understanding of what these regulations mean for their companies. IoT devices can represent a weak point in a network's security and leave it vulnerable to an attack. Recognizing this, many governments have already introduced laws that encourage manufacturers to build more secure devices, enforce the use of more complex passwords for the devices by end-users and require businesses to remove or destroy data which may open them up to risk.

OPERATING SYSTEM PREFERENCES:

56%
Would like to run all of their IoT devices on Windows IoT Core (Microsoft)

13%
Would like to run all of their IoT devices on a Google OS

14%
IT leaders would rather not run all their IoT devices on a single OS

Do Businesses Understand Current IOT Regulations?

IOT Cybersecurity Improvement Act (USA)	California SB-327 (USA)	GDPR	The EU Cybersecurity Act	The Code of Practice for Consumer IoT Security (UK)
31% of US IT professionals do not fully understand this act.	**36%** of US IT professionals do not fully understand this regulation.	**26%** of US IT professionals don't fully understand GDPR.	**34%** of UK IT professionals do not fully understand this regulation.	**32%** of US IT professionals do not fully understand this act.
12% of US IT professionals are not aware of this.	**26%** of US IT professionals have never heard of this regulation.	**13%** of UK IT professionals don't fully understand GDPR.	**14%** of UK IT professionals are not even aware of this regulation.	**25%** of US IT professionals do not fully understand this act.

REACHING THE EDGE

While more regulation and safer IoT environments provide a more seamless and secure experience for businesses, this does not solve the larger problem of keeping hundreds and even thousands of devices up to date. In fact, over a quarter (29%) of IT decision makers state that difficulty controlling and updating devices at scale is set to be another major roadblock to IoT adoption. Over half (52%) of IT leaders state that ensuring full security across all edge devices is a key concern. Also listed in these challenges is identifying and deploying the edge device technologies. Over a third (38%) list this as a concern and another 38% agree that handling the volume of data generated at the edge will be an issue for the company.

Already IT teams are struggling to keep all non-IoT devices on their networks up-to-date, with many opting to use a software-defined network to help manage the load.

EDGE COMPUTING CHALLENGES

52% State that ensuring full security across all edge devices is a key concern.

38% See identifying and deploying the edge device technologies as a challenge.

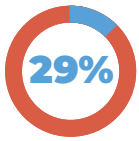
38% Agree that handling the volume of data generated at the edge is an issue.

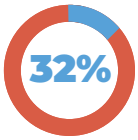
36% Believe that a key issue is fitting edge components into your existing architecture.

36% Agree that overcoming latency issues when communicating from cloud to edge is cause for concern.

THE IOT AND EDGE NETWORKS:

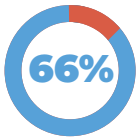
IT teams agree that an inability to reach devices at the edge of their networks is a barrier to IoT adoption.





IoT departments are still forming their edge computing strategy.

IT teams consider edge computing a risk to the company's security.

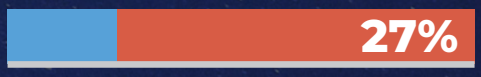


A SOFTWARE-DEFINED SOLUTION

Despite the advantages of enterprise IoT, there are numerous network concerns to overcome to keep networks safe and avoid potential attacks. For businesses choosing not to update all of the devices on a regular basis, the outcome could be disastrous, affecting employees, customers and the business as a whole. When asked what technology solutions would help overcome these potential risks, *almost half (47%) of IoT leaders stated that investment in software infrastructure could resolve these issues.* 27% specifically believe Software-Defined Enteprise Content Delivery Networks (SD ECDN) could provide a solution to these concerns. Kollective has been on the frontier with SD-ECDN while delivering large, high-quality video files to the network edge. The Kollective platform has recently added additional solutions to deliver important software updates and patches to desktops and mobile devices across corporate networks. This same peer-to-peer technology platform is well-suited to eventually extend into the universal delivery of edge updates across any type of device, including IoT.

WHAT TECHNOLOGY SOLUTIONS DO IOT LEADERS BELIEVE WILL SOLVE THE IOT CHALLENGE?

Investment in Software Infastructure



Peer-To-Peer Networking

More Computing at the Edge

THE USE CASES FOR A SOFTWARE-DEFINED ECDN

- Decreases the bandwidth load on an organization's network.
- Allows thousands of devices to be kept up-to-date without putting a strain on their own networks.
- Delivers content efficiently across a complex distributed enterprise
- More effective than legacy hardware-based WAN optimisation solutions to resolve edge computing concerns.

The use of an SD ECDN reduces many of the fears that IT managers have around timings and workload when it comes to distributing updates to many devices. Without putting a strain on their networks, an SD ECDN can help large organizations keep thousands – or even hundreds of thousands – of IoT devices up-to-date. An SD-ECDN could be the first step in a future-proofing an enterprise network as it would offer an efficient, modern solution for building large-scale IoT networks while addressing many of the current roadblocks to the adoption. The result is a future-proof enterprise, equipped with a system that can monitor and distribute continual updates at high speeds, all around the globe. SD ECDNs offer an efficient, modern solution to the IoT's update, regulation and security concerns.

For more information on the future of enterprise technology,

or to learn how a software-defined solution can help your business distribute updates at scale, visit:

kollective.com