Servium

aruba
a Hewlett Packard Enterprise company

4 STEPS TO PREPARE YOUR NETWORK FOR THE FUTURE OF WORK

Insight Guide

Building your digital workplace with Aruba

+44 (0)303 334 3000 | www.servium.com | hello@servium.com

4 STEPS TO PREPARE YOUR NETWORK FOR THE FUTURE OF WORK

Traditional working environments are evolving and at a pace that's hard to keep up with. The tide of mobile devices and the dawn of the Internet of Things (IoT) have heralded the arrival of the digital workplace - an interconnected world where the network ties together more endpoints than ever. These connections are often referred to as edges, and are categorised into operational technology edges, IoT edges, and information technology edges. Together they form the intelligent edge where analysing the data collected by these technologies reveals valuable insights, new innovations foster greater creativity, and people are brought closer together through improved collaboration.

By 2020 it is forecast that there will be more than **3 billion smartphones**[1] and **20.8 billion IoT devices on the planet**[2]. This staggering statistic paints a world of digitally-influenced businesses full of extraordinary possibilities where a smarter digital workplace presents a serious competitive advantage.

Mobile devices are already deeply entrenched in our personal lives and IoT technology is going that way too. Google Home and Amazon's Alexa organise our busy schedules, smart heating warms up our homes before we return, and high-tech security transmits video footage of the postman straight to our smartphones. Like many modern technology trends, things that pervade our personal lives very quickly trickle down into our professional lives too. The digital workplace started with smartphones connecting with the corporate network, but now tablets, watches and a host of other devices want to connect too. Some devices are more familiar IT, others are emerging operational technologies like the pumps and valves built into industrial systems.

The result is that enterprise networks are increasingly bearing the weight of a broad spectrum of devices that are connecting through a mix of wired and wireless networks. And there's a good chance you'll find many of them already connected to yours.

So, what's not to love about the prospect of the digital workplace?

20.8 billion

IoT devices and nearly 3 billion smartphones will be in existence by 2020

Putting digital workplace into perspective

Whilst the opportunities for mobile and IoT are becoming more impressive by the day, there's a startling reality that businesses need to come to terms with.

Permitting (either consciously or sub-consciously) such a variety of mobile and IoT devices network privileges without ensuring that you have the proper protection measures in place will make your network vulnerable. There's an alarming number of IoT breaches affecting companies right now where commodity-grade devices open the backdoor for hackers to easily slip through the security cracks. Security isn't the only headache either - slow network performance and increased downtime are both likely if you don't get to grips with the reality and could instead result in the Internet of Troubles. Charting a path to a fully-functioning and healthy digital workplace that capitalises on all the opportunities takes careful planning.

Here's our 4 step guide to preparing your network for the digital workplace – we offer up the top insights you'll need to know and why you'll want to transform using Aruba.

1 Realise the digital workplace demands a different kind of network

Fundamentally, traditional networks are built on a design that assumes static connections to devices in fixed locations. Similarly, networks have grown on a plan and approve operational model focused on price versus performance rather than flexibility and speed. The convergence of mobile, IoT and cloud is creating critical incompatibilities. Modern networks need to be optimised for roaming devices, alien 'things' and be ready to adapt in real-time. In this world, the network needs to be totally reliable, highly secure and most of all smart.

2 It all starts with good Wi-Fi

Much of what underpins the digital workplace inevitably relies on Wi-Fi. The quality of the service is critical and demands high-performance and dependable connectivity. The digital workplace is mobile-first, and many networks struggle to cope with the volume and velocity of connected devices, both from staff and guests, whose PCs, smartphones and tablets need to get online, and then freely move around your premises without interruption.

Good Wi-Fi depends on good coverage

Wi-Fi service often breaks down when too many devices attempt to connect with the same access point (AP), even when they may be at the edge of its transmission range. Overpopulated APs are common in office hotspots where loyal devices seek the first AP they connected with regardless of where it is located. Having too many devices trying to connect with the same AP simultaneously erodes bandwidth and slows down performance for everyone.

The best way to ensure that devices remain connected is by using intelligent APs. Aruba's line-up is built for the modern network, harnessing industrial-grade componentry that creates stronger signals for devices to latch onto. Likewise, on-board intelligence analyses network traffic flows and automatically coerces individual devices to connect to the best available AP. This ensures that users always have continuous access to reliable Wi-Fi. Additionally, bandwidth-intensive applications like video conferencing may need to be given priority. Aruba APs recognise this and can throttle traffic accordingly and even shift devices to a less-trafficked AP to avoid lagging and dropped calls. The best part is, for up to 128 APs all this functionality is ready straight out-of-the-box and will largely self-manage after an initial configuration of the first AP, which then acts as the master, with all further APs cloning its behaviour. This dramatically minimises the need for IT teams to step in and undertake repetitive configurations to grow the network. For larger deployments a network access controller performs this role and achieves all the same capabilities.

Importantly, even if you don't think you're ready to fully embrace the future of the digital workplace, great Wi-Fi is essential for here and now.

3 Tackle the new security paradigm

There's a trend in the origin of security breaches. Where once security posture focused on protecting staff and data from external threats, now more attention is being given to insider risks as well. As digital workplaces mature and the role of mobile and IoT devices on the network increases, the attack surface is widening, and potential vulnerabilities are growing with it. And with many IoT devices functioning without a built-in firewall or the ability to be patched, there are more open doors into your network.

In fact, according to Gemalto, **58% of UK businesses can't detect an IoT security breach[3]**. It's therefore not surprising when hackers take advantage of network frailties, using this new breed of devices as a gateway to acquire company information.

58% of UK businesses can't detect an IoT security breach

Get context-aware with Aruba ClearPass

The lack of awareness surrounding mobile and IoT devices largely comes down to IT teams not being able to detect how many, or what types of device are connected to their network. And you can't control what you can't see. As alarming as it sounds, the inundation of private devices and IoT technology means a legion of unidentified technology connecting to your network without being properly traced or secured. Furthermore, when you've got so many devices attached to your network, it's easy to overlook the seemingly

aruba
a Hewlett Packard Enterprise company

> When you've got so many devices attached to your network, a lightbulb may seem like the least threatening object.

innocuous appliances like lightbulbs, thermostats, tags, and sensors. But hackers are banking on this. These devices are often the best targets, low on security and easily modified. It's entirely possible and increasingly common for their behaviour to be altered to obtain access to systems and data, unbeknownst to IT staff. At first this may seem unbelievable but look no further than the criminals who hacked a smart fish tank to steal data from a US casino[4]. By subtly changing the behaviour of an inconspicuous device over time, and using protocols normally reserved for streaming audio or video, cybercriminals sent business critical data to a server in Finland.

Trying to combat this with conventional network access control using VLANs and ACLs at the network edge is both challenging and resource-intensive, and implies that you already understand what devices are connecting with your network, which is often not the case. With a workplace that is constantly changing, old-school network actions are simply too rigid and too slow.

The answer is in building a context-aware network. A network that understands contextual clues surrounding the devices connecting with it and can make decisions about how they should be treated to improve the security of your digital workplace. This intelligence informs the creation of context-based security policies that then allow the quarantine or restriction of a devices's network privileges based on its type, ownership, location, identity, operating system, or even applications running on it.

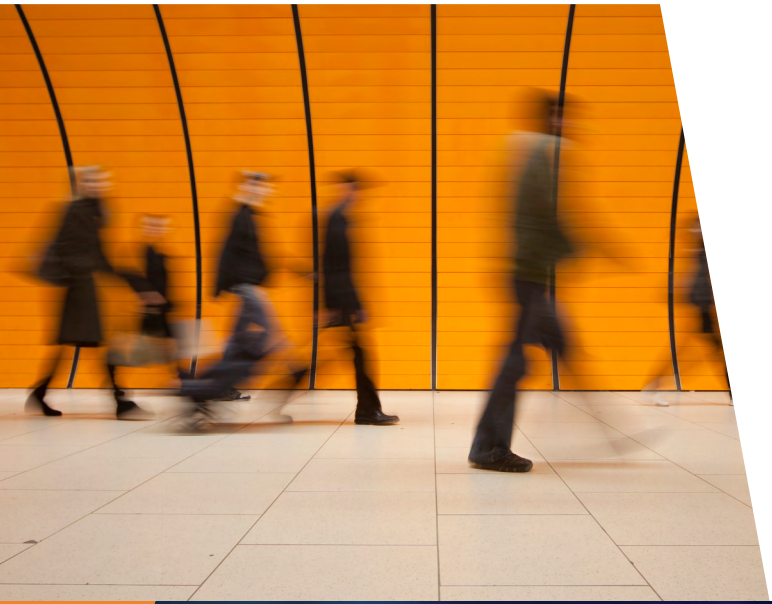
Being policy-driven, the security measures in a context-aware network are much easier to automate, creating scalable and powerful defences, and ensuring protection is always the top priority. Aruba has helped pioneer the context-aware network and has developed a family of technologies that deliver the visibility, insights, and controls necessary to achieve it.

Rich device insight

Aruba's ClearPass Device Insight provides the deepest understanding of your network, firstly by discovering new and existing devices – whether wired or wirelessly connected, then classifying them by type and finally through monitoring their activity. Even minor changes to device behaviour is detected instantly so that a threat is never missed. And if a hacker does target your network by disguising their IP address as a familiar device, ClearPass will instantly detect the behaviour change, quarantine it, and alert your IT team to investigate the issue.

Automating security policies

And it doesn't stop there. Aruba ClearPass Onboard enables you to create autonomous policies specific to your organisation to further enhance your network security. ClearPass Onboard dynamically aligns the policies to the classification of devices and other important attributes which then determine network access privileges. Functioning as an extra line of defence for your network, ClearPass Onboard can limit the types of operating systems that can join the network, mitigating the risks of unsupported software, which could potentially contain harmful code. For IoT devices, ClearPass Onboard ensures that their network access is driven by necessity, minimising the chances of devices becoming hostile.



Out of 57% of companies who have deployed IoT initiatives, 84% of them have already experienced security breaches.[5]

Zero-touch guest management

As guests enter your offices they bring their own devices and expect to get online. It's important to offer them frictionless access to your network as part of the visitor experience, but not at the expense of security. Using Aruba, guest policies can be configured beyond simply "just internet access" to enable access to printers, presentation screens and other helpful guest services. Likewise, creating guest Wi-Fi logins can tie up precious IT resource on a low-value task. Aruba ClearPass Guest automates the process of visitor access to ensure simple and fast connectivity by directing guest devices to a branded portal, determining their access permissions and providing a secure Wi-Fi connection separate to enterprise traffic. Additionally, future visits no longer require new credentials, as Aruba uses MAC caching to identify returning devices.

4 Start imagining and start innovating

Now that your Wi-Fi is ultra-reliable and super-secure, everything you need to go one step further and offer deeper engagement and richer services in your digital workplace is within reach. You're poised to shape new experiences for both staff and customers and in doing so, you'll make your organisation faster, smarter, and more fun. The foundations are set, ready for you to innovate across technology, real estate and culture, and unlock huge benefits along the way.

Get better insight into your workplace

A smart digital workplace is so much more than just a collection of internet-connected things, it's about having a network infrastructure which constantly learns and delivers valuable insights to create a more dynamic and efficient working environment. Using Aruba Net Insight machine-learning turns your whole network into a sensor, continuously tracking and monitoring ways to improve performance and deliver the best user experience possible whilst also freeing up the time of IT staff.

Capture exciting new opportunities

Start to harness the power of beacons and tags whether that's in wayfinding to help fellow co-workers locate each other and scout-out available workspaces, or the close integration of apps that support everything from catering to safety.

Optimise your physical environment

Net Insight also provides real-time insight into the function of your physical workspace. Everything from detecting meeting room occupancy to avoiding double-bookings, even tracking how people move around your premises and identifying popular areas to ensure real estate is not lit, heated or cooled unnecessarily - Net Insight helps you see and control it all.

Enable personal preferences

With Aruba's Smart Digital Workplace, you can embed IoT sensors into private workspaces for individual workers in order to activate everything from room lighting to temperature, therefore creating a comfortable working environment that suits everyone.

And these are just some of the ideas you might want to explore. Aruba is an open platform and ready to connect with an entire ecosystem of specialist technologies that could help you push the boundaries of what's possible.

References

1 Statista, Number of mobile phone users worldwide from 2015 to 2020.
2 Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017.
3 Gemalto, Almost half of companies still can't detect IoT device breaches, reveals Gemalto study, 2019.
4 Forbes.com, Criminals Hacked A Fish Tank To Steal Data From A Casino, July 2017.
5 Kevin Ashton, Making sense of IoT, 2017.
6 In-BuildingTech.com, December 2018.

PREPARING FOR THE DIGITAL WORKPLACE

There is so much talk about the digital workplace right now and the extraordinary possibilities it presents. Amazing stories like McDonalds reinventing its head office and capitalising on the power of a smart building app[6] are only possible with sound network foundations to manage the flood of mobile and IoT devices and by enabling them to enrich the experience of staff and customers.

Aruba helps you tackle these intensive demands – providing non-stop, high-capacity Wi-Fi, discovering and interrogating devices connecting with your wired and wireless network, and putting security front and centre with context-aware protections automated through powerful policies.

START YOUR TRANSFORMATION TODAY

To discuss your journey to the digital workplace, or get a taste of Aruba first-hand with a free trial of ClearPass, get in touch at **www.servium.com** or by calling **+44 (0)303 334 3000**.

Servium | aruba a Hewlett Packard Enterprise company