TeleApps

HOW TO PROTECT AGAINST TODAY'S #1 SECURITY RISK: EMPLOYEES

How you can fulfil the needs of your modern workers
without compromising your organisation's security.

A whitepaper by Teleapps

Introduction

Today's workplaces are becoming increasingly complex and fluid – particularly when it comes to security management. The modern worker expects to be able to work from anywhere, on any device, and at any time. Office spaces are no longer centralised with singular technology and protected by a robust firewall. They're now wireless, with hot-desks, hybrid infrastructure (both cloud-based and on-premise), and all kinds of connectivity scenarios. Even the physical office space now abounds with IoT devices and wireless automation: all designed to help people work more comfortably and effectively. **11.2 billion IoT devices will be in smart buildings by 2021 and 34% of those IoT devices will be installed in commercial general office spaces.**

To attract and retain the best people, providing this compelling and engaging employee experience (EX) is essential. However, it's important to remember that just as demand for a positive EX is growing – so are security risks.

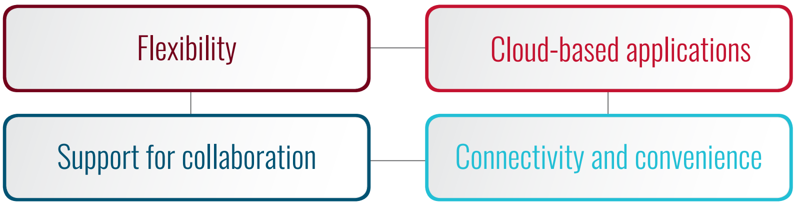
Unless your flexible, digital workplace is designed with security as top of mind, security issues can very easily occur – and can have a lasting impact on your business' overall safety. In fact, the biggest risk to an organisation's security is its people. According to a recent study by Aruba Networks, 74% of employees have inadvertently jeopardised company security in the past 12 months.

In this whitepaper, we explore the needs of the modern workers, outline the security risks, and explain how your business can stay protected.

> “74% of employees have inadvertently jeopardised company security in the past 12 months”

What do modern workers want?

To do their best work, the modern worker needs to be able to work productively from anywhere and at any time. **Key priorities include:**


Flexibility

Cloud-based applications

Support for collaboration

Connectivity and convenience

Flexibility

Today's workers want to be able to work from anywhere – at a time that suits them. According to a study from Intuit, freelancers will comprise 40% of the workforce by the year 2020. As a result, mobile devices are now ubiquitous, and organisations are charged with providing a seamless connection to enterprise applications as well as the internet.

Fixed office PCs and telephones are fast being replaced by laptops and smartphones with mobile unified communications and collaboration tools: all of which need to be secured, reliably, around the clock.

Cloud-based applications

To support this need for remote working, and enable greater productivity, employees expect their workplace tools and apps will be cloud-based. According to a recent study by Aruba, 43% of workers expect their workplace to have above-average use of cloud applications. This cloud migration extends across all layers of the technology stack, from core infrastructure to business apps. And as a result, the network must support and secure various models of public and private cloud connectivity at all levels.

Support for collaboration

Modern workers function well in teams. Workers today spend twice as much time collaborating than two decades ago, and today's workplaces are more team-based than ever before. To do their best work, 40% of employees expect their employer to provide digitally-connected conference rooms, and most expect to have reliable, up-to-date collaboration tools at their fingertips. If these tools aren't provided by the company itself, many workers simply take matters into their own hands – downloading and using their own (potentially unsecured) collaboration applications.

Connectivity and convenience

Today's worker expects that at least some element of the place in which they work will be improved or enhanced by technology. Whether it's a security pass that lets them into the office carpark, facial recognition on their device, or automated climate control in their office, 24% of employees say they expect their employer to provide smart building services . In seemingly endless ways, data-led tools are transforming the environments in which people work – whether at a hospital, a school, a factory or a traditional office.

> “The modern worker now uses an average of three devices.”

Modern IT teams are under pressure

To facilitate the flexibility and connectivity demanded by a modern workforce, many organisations are now operating with quite complex, hybrid IT infrastructure, which is increasingly difficult for IT teams to manage. According to a recent study :

- **43%** are providing cloud apps and storage
- **69%** have invested in digital technology in the past year
- **23%** provide customised mobile applications for the workplace

What are the security risks of supporting a modern workplace?

With the increasing digitisation of the workplace, security risks come from several areas:

Reliance on perimeter-based security

Until fairly recently, enterprise security teams could easily identify the perimeter they were protecting. IT operations would maintain tight control over computing and network resources, such as systems, apps and the data their employees could access and use. Today, a number of technology disruptions – mobile, BYOD, virtualisation, cloud, big data, and IoT – have rendered a perimeter-based security approach insufficient. Legacy security technologies were designed for yesterday's threats and environments, not today's highly sophisticated and targeted attacks.

Employees

The modern worker is the biggest risk to a company's security. According to a recent study:

- 74% of employees have inadvertently jeopardised company security in the past 12 months
- 30% of employees have connected to unsecure WI-FI networks, opening a door to potential hackers
- 25% of employees let others work from their company devices, creating an opportunity for data theft
- 18% stored passwords on shared work devices, circumventing company security protocols.

Hybrid IT complexity

Hybrid IT environments – despite delivering flexibility - can be complex and difficult to manage for IT teams and for the business as a whole. According to Right Scale's 2019 State of the Cloud Report, 81% of enterprises now operate multi-cloud strategies but 77% see security as a challenge.

The increasing prevalence of IoT devices in a workplace context has also enhanced this hybrid IT complexity. According to Aruba Networks, the use of IoT devices on wired and wireless networks is shifting IT's focus. Many organisations secure their wireless networks and devices, but may have neglected the wired ports in conference rooms, behind IP phones and in printer areas. Wired devices – like sensors, security cameras and medical devices – force IT to think about securing the millions of wired ports that could be open to security threats.

Dated infrastructure

Many enterprises are still operating with dated legacy infrastructure. However, the velocity, variety, and volume of users and devices connecting to networks is presenting complex new challenges. The traditional network can no longer cope with escalating demand. Traditional networks have become a mess of VLANs and ACLs because organisations have enforced policy and security on an infrastructure never designed to handle policy based on applications. Switch ports have static configurations and VLAN interfaces have hundreds, sometimes thousands of ACLs—leading to network designs that are fragile and that IT is afraid to touch.

Pressure to do more with less

IT budgets are also shrinking, which can also impact security. A recent article in Forbes Magazine suggests:

> ***"While management complexity grows, there is also an increased expectation for reduced IT spend due to a greater outsourcing of services. This tension between rising complexity and fewer resources increases risk because there will be a temptation to cut corners on security policies and testing to meet the demands of the digital business strategy. Security breaches and business-impacting service outages may result."***

5 ways to ensure watertight security

The smart digital workplace requires a network foundation that provides more than just traditional connectivity. It requires sophisticated policy and monitoring tools for a diverse environment of wired and wireless end-user and building IoT devices. To maintain watertight security, organisations need to:

Be strategic

Today, a perimeter-based approach to security is no longer sufficient. A fresh approach, whereby user and device risk is constantly assessed - with the help of advanced technology - is essential in dealing with the increasingly dangerous and fast-changing threat landscape.

"Security really needs to be the number one priority of the modern organisation," says Sreeni Raghavan, Principal Consultant at TeleApps. "To stay one step ahead, you need to make your organisation's security strategy a priority. This means investing in it, and ensuring it complements your organisation's wider digital strategy."

According to Raghavan, when it comes to developing your strategy, it's essential to consider how you will tackle several key elements:

- Admission/access control – ensure you have very strict systems for controlling the authentication of every device onto your corporate or guest network.
- End-point security – be sure to have a system that can secure you from malware, viruses and other similar threats.
- Interoperability – if you have a multi-vendor environment, design your architecture using products that have strong integration capabilities and are vendor agnostic – ensuring no barriers or gaps exist.
- Visibility – ensure you always have clear visibility over your infrastructure, as well as analytics capabilities, so you can correctly determine your performance at any time.
- Multi-factor authentication – protect your infrastructure and reduce the likelihood of user error by implementing this security precaution as a mandatory step.

Build secure collaborative and flexible workspaces

In today's modern workplace, collaboration is vital. Recent research suggests workers are now on twice as many teams and spend 80% of their time collaborating. Given this, it's important to ensure your people have consistent, proven tools to collaborate and work effectively, so they don't rely on their own, disparate solutions – which can put you at risk of shadow IT.

"Managing complex and disparate IT solutions, as a result of shadow IT, can be extremely difficult and therefore risky from a security point of view. In order to stop this from happening, technology investments need to be closely matched to users' needs, so they will be adopted business wide" says Raghavan.

Ensure that whatever collaboration solution you choose, and the policies and templates that you implement, are unified and can be centrally managed by your IT team or IT provider. Reflecting the fact that more people are now working remotely than ever before, it's also important that any strategy you develop is mobile-first.

Collaborative and flexible workspaces can also require a lot of IoT devices. As such, it's important to design policies to identify such devices, and only provide the required level of access. By creating an interoperable, vendor agnostic environment, you avoid the risk of there being any gaps created by a lack of compatibility.

Automate and improve security systems and processes

IT teams are being increasingly burdened by the huge workload associated with maintaining security – especially as the number of devices and applications increases.

You can streamline your approach by automating as many steps as possible. This could include, for instance:

- Automatically quarantining non-compliant users.
- Creating security policies that can identify and provide the right access to all types of devices without manual intervention.
- Automatically identifying unusual behaviours from devices, and instantly blocking access and alerting relevant team members.

According to Raghavan, enterprise security is something that needs to happen around the clock. As such, it's essential to invest in robust and automated systems that can protect the organisation at every step, and continually.

Enhance security training and awareness

Raghavan also suggests that when it comes to security, employees remain a major risk.

"People can be the number one risk to an organisation's security. Educating staff about the security risks, and necessary protocol may sound mundane, but it's essential," he says.

When it comes to maintaining security, it's vital that you ensure your people are aware of the risks of not following protocols. You can do this by conducting training and education programs on a regular basis – either online or face-to-face.

Ensure that procedures are being followed correctly, and educate users on the sensitivity of your company data and how to go about protecting it.

Continually improve

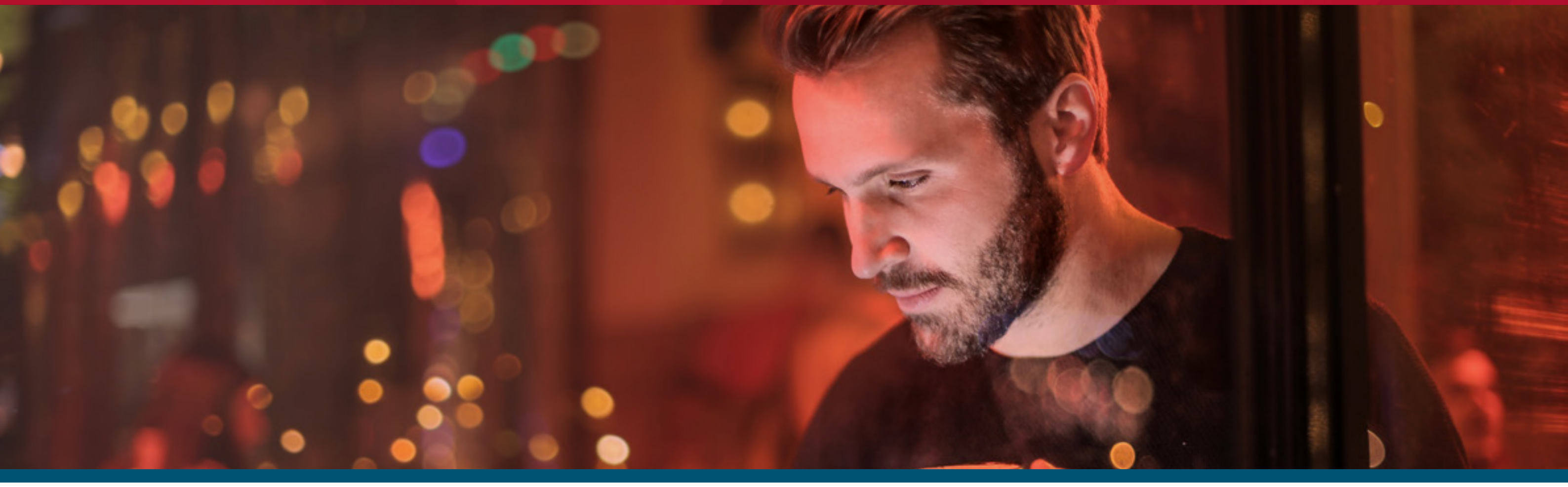
Workplace security is a moving target, and threats and risks are evolving and changing constantly. As such, you need to ensure you always keep your systems and processes up to date, and set goals to ensure continued transformation of the workplace and its underlying technologies.

"Security threats are ever changing and expanding, and as such, an organisation's security strategy needs to be too. Organisations need to continually improve and innovate in order to stay a step ahead," says Raghavan.

It's important to ensure your compliance policies are always revised and up to date, and that you're utilising the latest technology and tools when it comes to automation.

Performing regular audits, identifying vulnerabilities and ensuring security concerns are addressed regularly is also essential, as is having full visibility and analytics capabilities to provide a clear indication on which areas require improvement.

Utilising AI-capable systems, and machine learning, can also help you develop systems which learn and improve themselves over time – reducing the burden on your internal teams.



How TeleApps and Aruba Networks can help

TeleApps are considered to be among Australia's leading system integrators for collaboration and network environments. The organisation has a long-standing, strong technical background that has benefited hundreds of companies across Australia, since 2007. With over a decade of experience in unified communication, collaboration and customer experience, TeleApps brings a wealth of knowledge in providing collaborative, flexible and secured workspaces solutions.

TeleApps is also an Aruba Gold Partner and specialises in integrating Aruba's market-leading 360 secure fabric-based enterprise security framework to deliver the level of protection which modern workplaces need.

Together with Aruba, TeleApps can help you meet the needs of your modern workers by providing a solution which is:

Mobile-first

Users and things can connect to your network with the same policy and permissions regardless of how they connect (wired or wireless).

Secure

Protect your wired and wireless network with signed code, secure boot, and cryptographic hardware protection. Protect your user data and devices with strong encryption and per-user level policy.

Open

Your network can support multiple vendors so you can innovate at your pace and not be locked-in and limited by a single vendor's architecture.

Optimised

Automated systems – driven by machine learning - optimise your network performance and alert you of changes or highlight potential changes that require acceptance via on-premise and cloud-managed network operations.

Find out more

To find out more about how TeleApps and Aruba can help with your organisation's security, visit **teleapps.com.au/aruba360securefabric** or **call 1300 454 717** and request a free consultation.