Devicie

Mission Possible

A how-to guide to making device security work for your employees, organisation and bottom line.

You can!

The future of end-user device management is a place where security meets productivity.

Device security reinvented, for a better future

Contents

1. Executive summary

Organisations perform their best when their security works *with* their employees, not *against* them.

When it comes to end-user device security and management, there are three big competing interests:

1. Employees wanting to work seamlessly and productively, wherever they are, on their device of choice
2. IT and security teams wanting to keep data and systems secure
3. Business leaders wanting to achieve organisational goals while making a profit.

Research shows that users increasingly need flexible technology solutions – including an ever-increasing swathe of business applications and the ability to work remotely from multiple devices. It makes employees happier and more productive. However, these same solutions – when not managed well – increase security risk. While prioritising security may deliver compliance and data protection benefits, this approach often hampers employee productivity.

Striking a balance between security and user experience has been a classic no-win situation. A 'best efforts' approach might be well-intentioned, but only heightens the security and productivity compromises the solution aims to resolve.

The rise of the hyper distributed workforce has exacerbated these issues. Cyber criminals are increasingly seeking to exploit the situation and research suggests end-user devices are their favourite target.

The truth is traditional organisational IT systems have not been designed for employees working remotely over the internet, with multiple applications, devices and operating systems.

In very recent times, ground-breaking technology innovations have changed what is possible, transforming the 'impossible choice' between security and productivity into an opportunity to achieve both. However, many within the IT and security industry, busy dealing with current challenges, have not yet recognised that this is one battle that should now be over.

Cloud-native solutions that are agentless and automated are changing the game for end-user device security and management. Every organisation can now rapidly achieve a Standard Operating Environment (SOE) that is flexible, empowering and secure.

As organisations continue to embrace cloud technologies and solutions, there is a golden opportunity to reinvent device security. The future of end-user device management is one where security meets productivity. It is a place where uncompromising security is an enabler of productivity, business success and an enriching user experience.

It's time to end the debate about 'security versus productivity' once and for all and make room for both to coexist for everyone's benefit.

2. The evolving threat landscape

Attackers seeking the path of least resistance are actively targeting organisations that haven't fully considered how their employees access infrastructure, assets and information over the internet.

The working-from-home revolution has posed multiple challenges for IT teams attempting to strike a balance between security and productivity.

Bring-your-own-device (BYOD) is as much an opportunity as a challenge, enabling flexibility, but also increasing the threats associated with insufficiently managed devices.

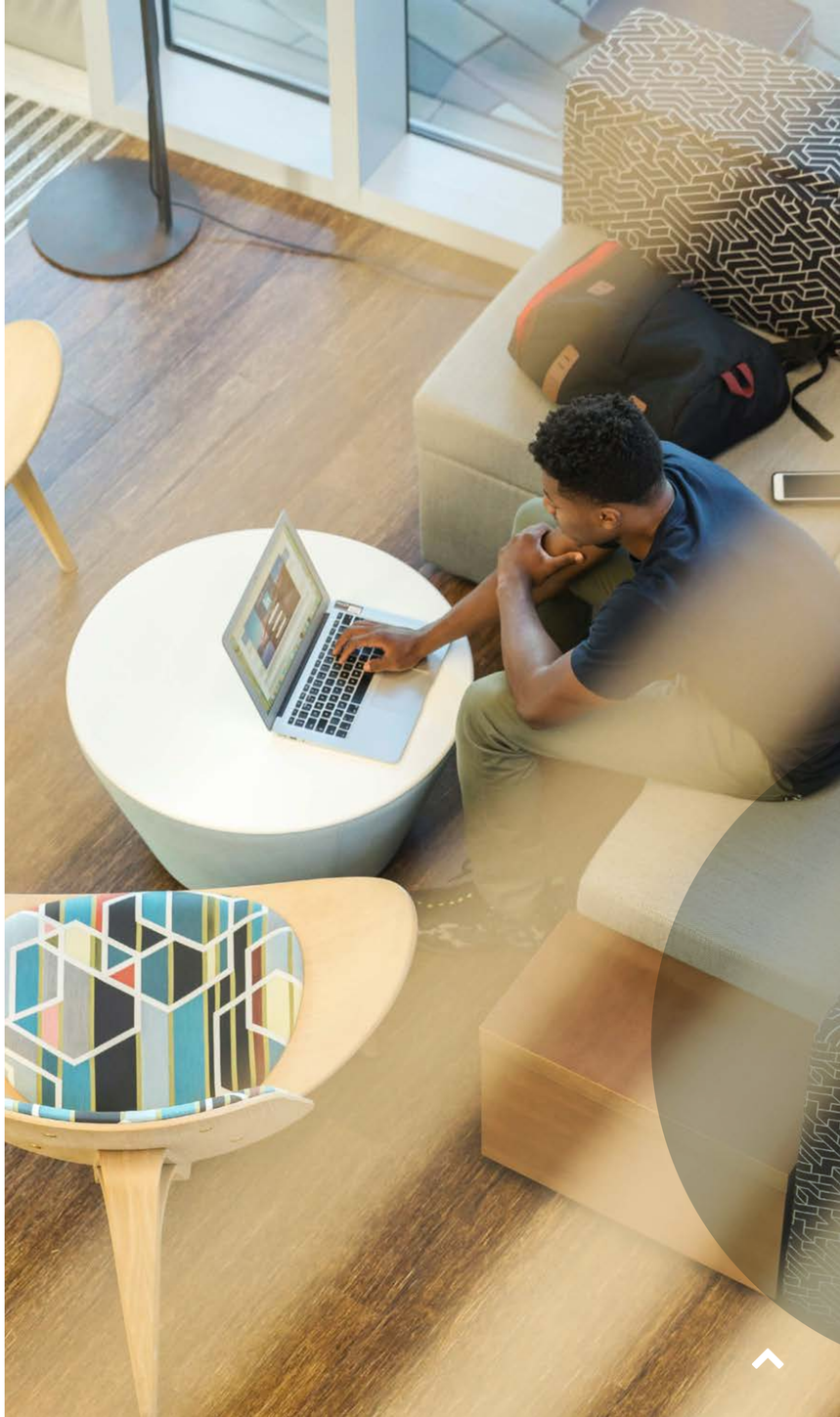
Employee devices are now a significant and increasing cyberattack vector and IT teams are shifting their attention to securing this risk.

According to the Australian Cyber Security Centre's (ACSC) 2021 annual threat report, a cybercrime is now reported every eight minutes in Australia, with criminals and spies taking advantage of large numbers of people working from home during COVID-19 lockdowns.

The Ponemon Institute's *2020 Cost of Insider Threats: Global Report* found that 62 per cent of insider incidents came from negligent employees or contractors, with an average cost of around US$307,111 per incident.

While security awareness training is an important consideration for organisations, no one should rely on employees to be 100% perfect with regards to their IT or cybersecurity behaviours. Negligence can be reduced with education and awareness, however, providing a secure workspace is an important safety net.

The cloud is synonymous with digital transformation, but the rush to move there has not delivered optimal outcomes for many organisations. In their hurry, many have forgotten to refactor their systems to cloud-native, meaning that inherent on-premises security foundations have been lost in the transition.



Think about the number of times IT had to use remote access via the internet just to get their employees up and running, or the couriers used to ship laptops to and from remote employees because they required rebuilding following compromises. Staying ahead of attackers while enabling employees to be productive is a constant battle, and one that cannot be won if we approach it the same old way.

Datapoints highlighting the evolving threat landscape:

- **Attack vectors:** Desktop and laptops are the most 'at-risk' vector for security threats or breaches, followed by smartphones and tablets.[1]
- **Ransomware:** In a survey of 582 security professionals, 50% say their organisation is prepared to repel a ransomware attack.[2]
- **Cybercrime increase:** U.N. warns cybercrime up 600% during COVID-19 pandemic.[3]
- **Unpatched vulnerabilities:** 60% of breaches in 2019 involved unpatched vulnerabilities.[4]
- **Endpoint protection:** 75% of companies infected with ransomware were running up-to-date endpoint protection.[5]
- **Updates:** Only 21.1% of updates are made available immediately; 48.5% of updates aren't managed at all.[6]
- **Patching delays:** It takes an average of 97 days to apply, test and deploy a patch.[7]
- **IT resources:** 63% of IT professionals say resources drained by device management could be used on other strategic IT projects.[8]
- **Mobile security:** 74% of global enterprise IT leaders report experiencing a data breach due to a mobile security issue.[9]

1 AT&T Cybersecurity Report – Vol 8
2 Mark Woolward CTO and CISO Varmour, (IN)SECURE Magazine
3 Izumi Nakamitsu – UN Security Council
4 Costs and consequences of gaps in vulnerability response – Ponemon Institute
5 Sophos
6 Verizon Mobile Security Index 2021
7 Ponemon Institute The Third Annual Study on the State of Endpoint Security Risk
8 IDC Transforming Device Lifecycle Management with Device as a Service
9 IDG – quoted from CPO Magazine, September 21

3. Our new remote workplace

When COVID-19 spread across the globe in 2020, many organisations were forced to accelerate their digital transformation to ensure business continuity.

IT teams and consultants raced to get employees up and running in their homes, with their suite of collaboration, communication and productivity applications.

Despite some risks and challenges, the remote work model has brought many benefits and is not a short-term trend. Many organisations have seen increased productivity and employee satisfaction afforded by more flexibility, not to mention waving goodbye to peak-hour commuting. In the space of a year, a remote workplace has become essential for almost every organisation.

Organisations now know that enabling their teams to work securely from anywhere, on multiple devices is not an optional benefit.

The 2021 Australian Productivity Commission Working from Home Research Paper found that even as stay-at-home orders eased in early 2021, the number of people working from home remained at almost 40%. To put this into context, just 8% of people regularly worked some time from home before the pandemic.

Organisations everywhere must embrace the remote workplace, empowering their employees in a way that balances security with productivity. Protecting sensitive data and securing end-user devices and applications is just as important as providing a positive user device experience and efficiently managing this new frontier.

4. End-user device management challenges

One of the biggest challenges of end-user device management is striking the elusive balance between the needs of end users, IT and security, all while enabling a productive workplace.

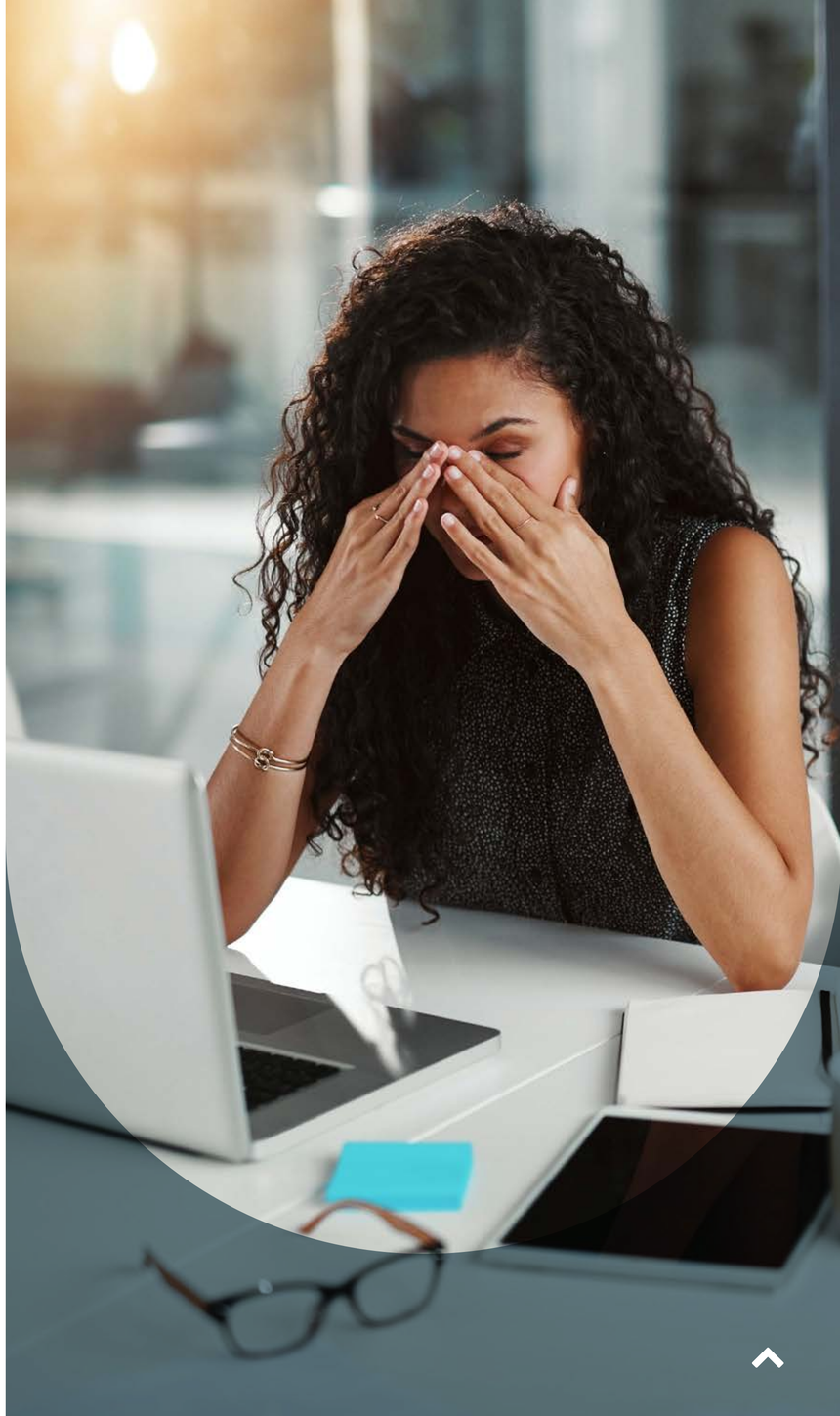
For many years, IT and security teams, as well as employees, have been forced to accept a compromised digital environment, either to keep the business secure or to keep the business running.

Despite good intentions, it has been proven time and time again that a ‘best efforts’ approach to end-user device management doesn’t achieve optimal (or even desired) outcomes.

When security gets in the way of productivity, employees create their own workarounds, inadvertently increasing the attack surface and creating visibility gaps for IT teams.

A 2021 study from HP revealed that employee buy-in to security is far from perfect. Thirty per cent of remote workers under the age of 24 said they circumvent or ignore certain corporate security policies when they get in the way of getting work done. While the young cohort is most likely to buck the system, 67% of IT leaders say they get “weekly” complaints about restrictive policies and 48% of all workers feel that these measures are a waste of time.

The reality is that most IT management systems – whether traditional, hybrid or even modern – do not meet the needs of organisations and their employees in a hyper distributed workforce.

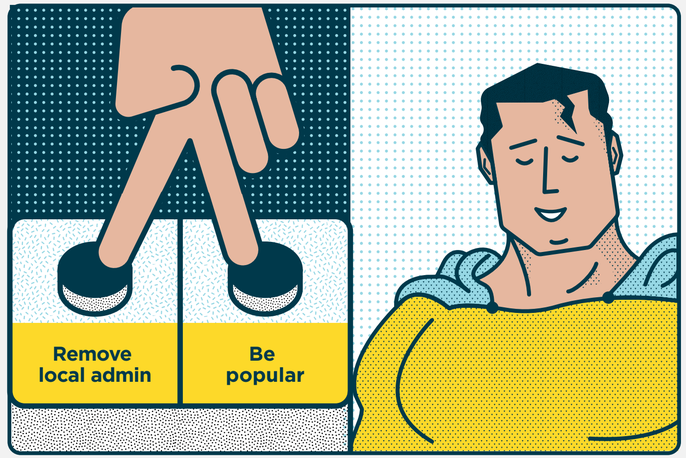


In the modern world the challenges of end-user device enablement, security and management are many.

Devicie has identified a view of the **top 10 end-user device management challenges** facing organisations today:

1. Employees suffering from unproductive devices rather than waiting for an IT resource to fix problems
2. Increasing cybersecurity attacks on end-users
3. Lack of visibility and control over remote devices accessing the corporate environment
4. Increasing need for and shortage of specialist IT and security skills
5. Skilled IT teams wasting time performing manual, repetitive and mundane tasks
6. Increasing number and types of devices, operating systems and applications
7. The cost and effort of moving to an agentless model
8. Neglecting basic security hygiene because it is too time-consuming and difficult to do well
9. Security compromises made to keep the business running
10. Increasing overheads for infrastructure, personnel and consulting to keep the modern workspace operating

The daily struggle



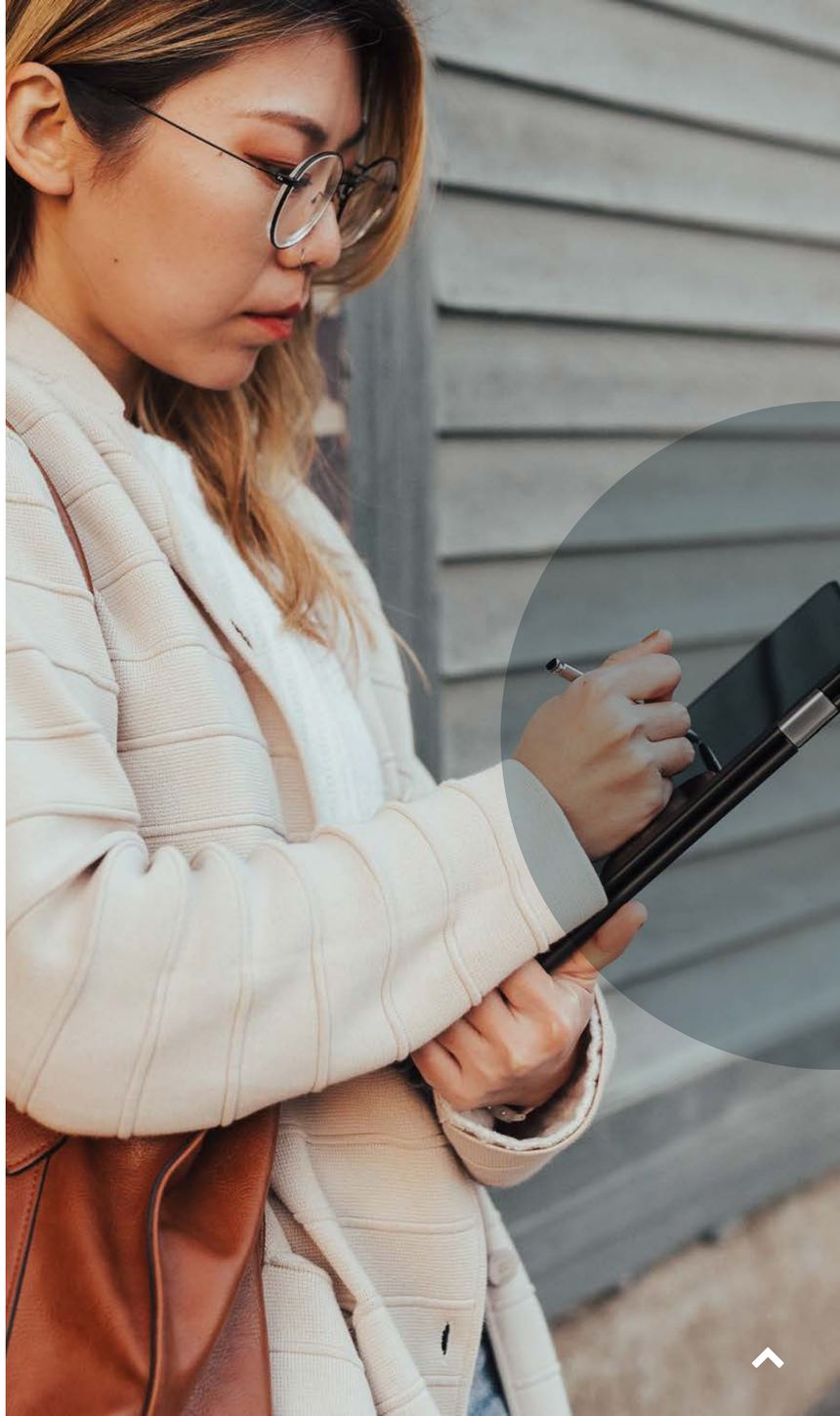
The reality is that most IT management systems – whether traditional, hybrid or even modern – do not meet the needs of organisations and their employees in a hyper distributed workforce.

This is not a new problem. In 2017 IDC published a solution brief called *Transforming Device Lifecycle Management with Device as a Service*, surveying 300 IT decision makers across EMEA. In the survey, 63% of IT professionals said resources drained by device management could be used on other strategic IT projects, and that 50% said they spent too much time procuring and managing devices.

There has been some progress towards this, with Managed Service Providers (MSPs) and Value-Added Resellers (VARs) managing hardware programs. and Mobile Application Management (MAM), Mobile Device Management (MDM) and even Unified Endpoint Management (UEM) solutions, improving elements of desktop and mobile device management.

There has also been a rise in asset management systems helping organisations to have better visibility of what devices are on their network.

However, none of these approaches or solutions – even combined with services - appropriately meet the end-user security challenges, nor can they be purchased and consumed by an organisation (at least not without building their own internal device management team, or hiring one externally). Every solution requires significant ongoing maintenance and teams to manage them, making it out of reach for most organisations to do well.



5. The future of end-user device security and management

The future of device security and management relies on creating an IT environment that supports distributed workforces to be productive and secure on their device of choice, delivered by and managed from the cloud.

According to Gartner Inc. by 2024, more than half of organisations will consolidate to a unified console for endpoint management and security tasks. This represents a significant increase from fewer than 5% in 2020.

The desired destination is a place where uncompromising security meets a positive end-user experience, where compliance is seamless and ongoing, and organisations set their employees up for success.

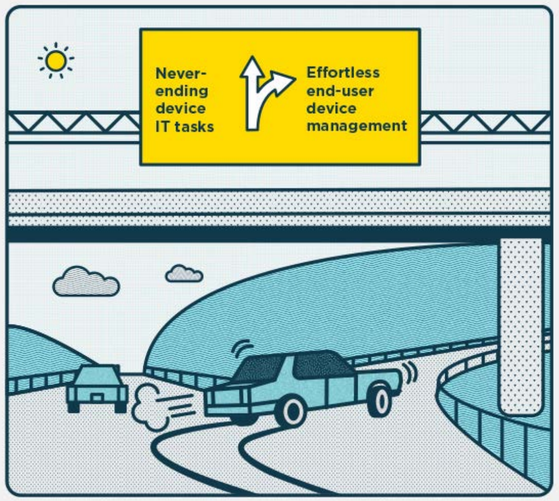
However, although the challenges of remote work and increasing cybercrime have accelerated the need for organisations to get there quickly, this has not proved an easy journey.

The good news is that getting there no longer requires an army of skilled experts, infrastructure overheads, or big IT projects. The only thing it requires is a growth mindset that embraces moving quickly to a modern workplace.

This is the future state that organisations of every size can and should aspire to, if they want a modern workplace that maximises security and productivity alongside a positive user experience.

What should the future of end-user device management look like for organisations of every size?

- Employees can work wherever they like, on their device of choice
- Devices and operating systems are always up to date and configured to maximise productivity
- Employees can self-service for new device onboarding and device rebuilds, via the internet
- IT and security teams have 100% actionable visibility and control over the fleet
- Automated deployment of ongoing layered security, in line with best-of-breed security controls
- Automated patching and updating of devices and operating systems
- Automated application packaging, deployment and management
- Automated security drift identification and remediation
- An audit trail of everything, with a central console for fast and easy reporting



Go there!

People who want to achieve an optimal future state for their organisation's end-user device security and management should understand two things:

1. Every organisation needs an SOE
2. Most organisations do not and should not need to build or manage their own SOE (or pay someone else to do it for them)

6. The solution is SOE as a service

Creating an IT environment that effectively deploys, manages and secures employee devices, operating systems and applications requires the configuration and automation of many complex tasks, controls and policies. This requires a highly specialised hybrid skillset, including expertise in security, application management and SOE infrastructure design and deployment.

Historically, SOE upgrades – whether do-it-yourself (DIY), or with consultants – have been associated with time-consuming projects that exhaust costs and require specialised skills that are hard to come by. Anyone who has ever been involved in a major IT upgrade will know there are always setbacks, workarounds and delays. Then, at the end of the project, the internal IT team is again tasked with taking on the ongoing management of these systems, when time permits.

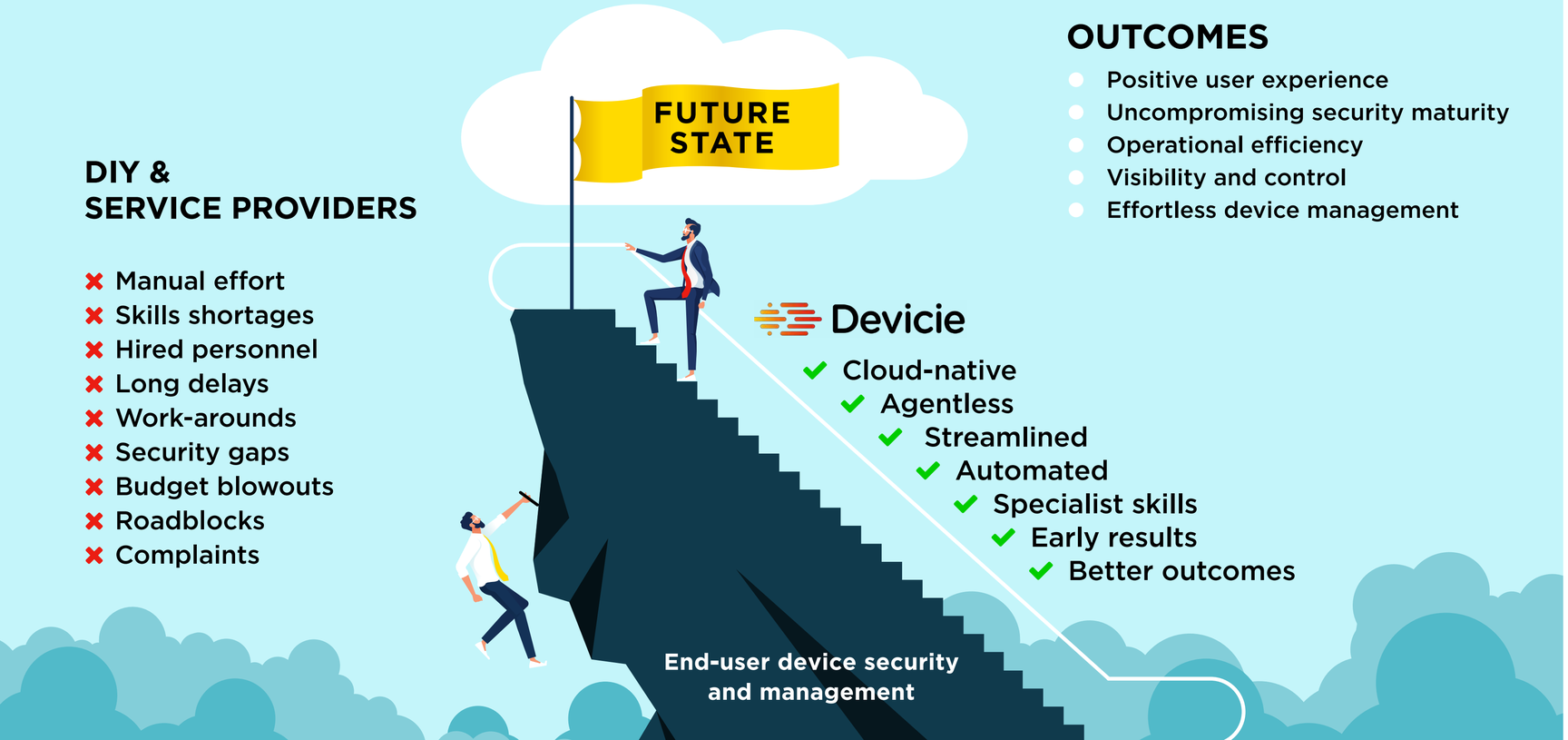
Thankfully, there is no longer any reason for people to build or own their own device security and management solutions. With maturing cloud technologies, agentless device management – coupled with automation – it doesn't make sense to initiate a 9-18 month project which may or may not be successful. Building and managing a corporate SOE will not make any business more competitive. In fact, the opposite is now true for most organisations.

The real opportunity is to leverage best-of-breed technologies that are expertly managed to provide a high performance SOE as a service. In this approach, organisations subscribe to the solution, rather than own it. There are tremendous benefits to be had:

- Organisations pay a monthly fee for a service, so they don't have to build anything. It is available in a matter of hours and can be rolled out to the organisation straight away. Unlike most bespoke SOE projects, IT won't have to maintain or upgrade it as the business and technology evolves. This is a huge win that will save significant time and money.
- Organisations achieve ongoing IT and security maturity that can be trusted and proven via a central dashboard. This complex, yet generic, part of the business can be optimally managed by experts, whose sole focus is to provide secure and productive infrastructure to support a modern workplace.
- By adopting SOE as a service, organisations can focus their technology experts on improving products and services internally, and on more strategic IT and security issues, while minimising corporate technology costs.

7. How Devicie takes organisations to the future state

Devicie champions the cloud-managed SOE route to deliver organisations with a modern workplace as a service for end-user devices.



What is Devicie?

Devicie is a cloud-native platform that automates end-user device security and management to enable people to do their best work safely and productively.

From Windows and macOS to iOS and Android, Devicie ensures all employee devices are secure, compliant and optimised in a way that liberates IT teams from manual configuration.

Devicie removes the time, effort and cost for organisations to manage a complex project to transition to the future state.

Devicie believes end users shouldn't have to be technology or security experts to operate their digital workspace effectively.

The Devicie Difference

automation where it makes sense

Harnessing the power of automation, Devicie manages the modern workplace as a service, assuring uncompromising device security and compliance with operational efficiency and a fantastic end-user experience. By automating the rollout and management of a customised IT environment for employees, Devicie liberates IT teams from mundane device management tasks, so they can focus on more strategic projects.

INTUNE AS A SERVICE

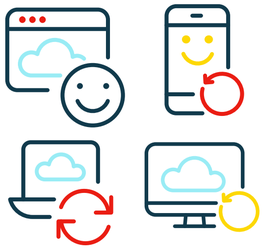
Devicie is a co-pilot for Microsoft Intune, automating the deployment of a production-ready Intune environment and integrating with Active Azure Directory (AAD).

SOE AS A SERVICE

Devicie automates the rollout and ongoing management of the organisation's SOE.

SECURITY CONFIGURATION AS A SERVICE

Devicie automates the rollout of security configurations and controls in line with best practice frameworks, including CIS, ASD Essential Eight, PCI DSS and ISO 27001.



PATCH MANAGEMENT AS A SERVICE

Devicie deploys scheduled patching and maintenance across the employee device fleet, including automated testing with a trial group of users in each organisation before staggered deployment across the fleet to minimise end-user disruption.

APP MANAGEMENT AS A SERVICE

Devicie automatically deploys and manages all end-user applications, ensuring they are approved and current on every end-user device.

COMPLIANCE AS A SERVICE

Devicie's dashboard provides IT teams with 100% visibility and control over the entire end-user device fleet, making compliance easier to achieve and report.

8. Challenge accepted, mission solved

Every organisation can solve their security versus productivity dilemma on end-user devices as part of their digital transformation to the future state.

As organisations continue to embrace the cloud, there is a golden opportunity to reinvent the way they deliver end-user device security and management. They have a chance to leverage cloud-native technology solutions that afford positive outcomes for IT teams, employees and the bottom line, so everyone can win.

The time has come to make end-user device security and management agentless and automated, so that secure and compliant devices not only become the norm, but an empowering part of the way organisations work.

Security as a business enabler

Best practice security means uncompromising security that is always on.

Best practice security recognises the importance of human nature, and provides solutions that work for people, not against them.

Security controls in line with recognised frameworks should become business as usual for every organisation.

Devicie automates best practice security, including CIS, ASD Essential Eight, PCI DSS and ISO27001. The Devicie platform continually verifies the security posture of all end-user devices, detecting any potential security exposures, and then auto-heals and reapplies security settings while maintaining an audit trail.

Devicie also facilitates the adoption of zero trust principles to make it achievable to most organisations, allowing them to modernise their applications while still supporting legacy safely.

Devicie

Device security reinvented, for a better future.

Devicie automates an uncompromising level of end-user device security for organisations and does this in a way that provides a radically better enablement and management experience for end users and IT teams. We have solved the security versus productivity dilemma for end-user devices, with a cloud-native solution that delivers a modern workplace as a service across end-user Windows, macOS, iOS and Android devices, wherever they are located.

If you're interested in finding out more about how to take your organisation to the future state, we'd love to chat or give you a demo.

askus@devicie.com

LinkedIn

devicie.com