Addigy

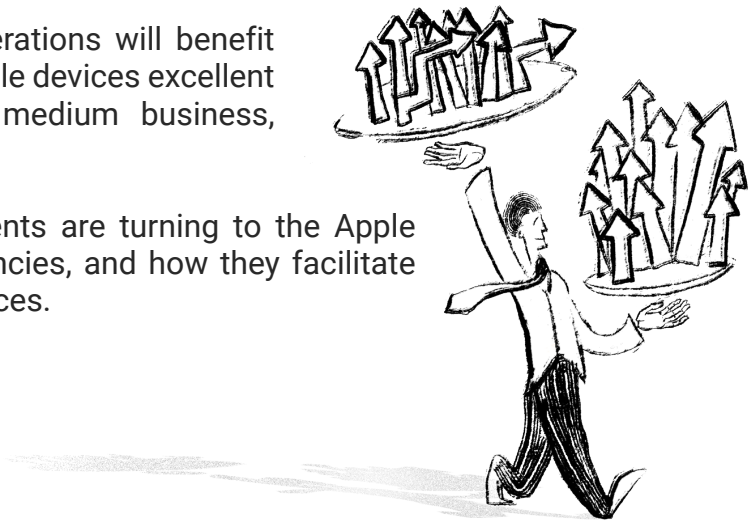
How Apple Devices Enable and Secure the Modern Workforce

WHITE PAPER

Apple devices aren't just beautifully designed – they're practical tools that enable teams to work quickly and efficiently in an enterprise environment.

Even better, organizations' IT and security operations will benefit from the built-in security features that make Apple devices excellent in any environment – enterprise, small or medium business, education, or nonprofit.

This white paper will outline why IT departments are turning to the Apple ecosystem for security and operational efficiencies, and how they facilitate end users to be more productive on secure devices.



WHY APPLE DEVICES ARE THE CHOICE OF THE MODERN WORKFORCE.

Apple device use is on the rise at major corporations. Technology giants like IBM are increasingly turning to Mac computers for employees who want them.[1] And this movement isn't new anymore. As early as 2014, a study by Gartner indicated that PC sales were declining — 87 percent of devices shipped back 2015 were mobile phones and tablets.[2]

As trends move toward mobile devices and an increasingly remote workforce, it follows that companies are choosing the brand that builds devices optimized for mobile use.

Many IT admins now use a mobile device management solution (MDM) for the Apple devices in their environments, which can help generate operational efficiencies for the IT department with responding to help desk tickets from end users on Apple devices. Excellent Apple MDM solutions are designed to be straightforward for brand acolytes and non-Mac users to alike.

HOW IT SAVES TIME WHILE PROVIDING TOP-LEVEL SUPPORT.

While there are plenty of formulas online that can help you estimate just how much labor your team or company wastes each month due to downtime, there's no need to go that far down the rabbit hole when it comes to support for Apple devices.

Apple products are famously low-maintenance, and an MDM makes software updates and application installations efficient, saving your team and the business valuable time. Mac and iOS devices that are connected on a cloud-based IT system are easy to update and built to facilitate frictionless remote management, in the event that an end user does need support.

Whether an employee is trying to access a new application license through Apps & Books or sharing a file to the network storage, with an MDM, IT admins are enabled to access end-user machines to assess any concerns and help end users get back to work quickly.

Help desks can be cumbersome and clunky, but with an Apple MDM solution, it's simple to communicate with end users, wherever they're located. Even better, these programs provide excellent portals for self-service, empowering end users to answer questions and access solutions without waiting for a response from the help desk.

[1] https://www.computerworld.com/article/3452847/ibm-mac-users-are-happier-and-more-productive.html

[2] https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm

MANAGED DEVICES GIVE VISIBILITY, A KEY COMPONENT TO A SECURE NETWORK.

Apple puts security first and gives IT a roster of features to help make the most of their safety-first devices. With an MDM capability, IT admins can manage Apple devices in a straightforward way, granting access to every machine in their environment. With that visibility, IT admins have the first step complete in minimizing security risks.

Apple mobile device management programs keep everyone operating on a secure network by giving the IT team a clear picture of what devices are on the network, whether they're encrypted, and if there are any security risks that can be eliminated by something as simple as a software update. But you must know what devices (and threats) are in your environment in order to address them.

Forrester's report on the economic impact of Apple devices in enterprise quoted an endpoint services director who described an all-to-familiar scenario:

> **"People were jury-rigging their Mac workstations. There was literally no support for Mac from IT. It was a choose-your-own adventure, self-support type thing."** [3]

Think about the situation this person is describing: there's no oversight, no way to monitor the security of these devices, and no way to locate critical software updates. As the saying goes, you don't know what you don't know. And for your company, that means that unsupported Mac devices may pose a security risk.

If organizations welcome Apple devices without providing IT support, the potential cost of not securing those devices can be limitless. If there is a security breach or malicious activity, there is risk of losing revenue, productivity, and reputation. Especially if the Mac computer and iOS devices have come through a BYOD or CYOD policy, a common adoption in modern organizations, there may not just be a gap in end user support – there's likely a missing hole in network security or encryption, and the business could be missing out on the access needed to backup or reproduce troves of user data.

The good news: Mac computers and iOS devices are easy to manage when you have the right tools and a plan in place to ensure your users' data and applications are secured.

[3] https://tools.totaleconomicimpact.com/go/apple/TEI/

EMBRACE THE SHIFT.

While startups and modern workforces have embraced the Apple ecosystem, many organizations are actively updating hardware and policies to reflect the choices and working style of its end users.

If you're in an environment that primarily supports Windows PC users, your team may not be familiar with the language of the Apple ecosystem. As an example, an admin managing settings in the Windows world would use a tool like Group Policy where with Apple devices you would be using Configuration Profiles. It's important that your team knows how to talk to Mac and iOS device users about their products, programs, and problems while being able to translate for other team members what this means for the business. Mac and iOS users deserve the same knowledgeable, white glove support as the rest of network users enjoy.

An Apple mobile device manager will empower your team to provide excellent support to the Mac and iOS devices on your network, whether or not your IT team members prefer a macOS at home. With the help of an MDM, organizations of any size don't have to cross their fingers and hope they're not overlooking a place where they could be better handling the diversity of devices in their environment.

By choosing IT tools that support the Apple ecosystem and that are built to maximize the features and applications of Apple devices, you'll see the efficiencies grow your IT support team's capacity and enjoy the benefits of having happy Apple users who know where to look for resources and how to help themselves.

ABOUT ADDIGY

Trusted by more than 3,000 global organizations, Addigy provides cloud-based Apple device management solutions for IT teams in enterprise, education, and MSP environments. Our multi-tenant SaaS offerings are changing the way administrators support their end users, helping people get the most out of their Apple products every day. We believe good ideas are made great through community and collaboration, and strive to live that charter in all that we create and do.