Securing macOS in the modern work era

Global enterprises have entered a new era of modern work, one where individuals need to make well-informed decisions on the fly, using the tools they know and love best. Fueling this trend is the millennial generation, which makes up a growing percentage of today's enterprise workforce. These workers want to be able to choose the best tools without their mobile experience or privacy being compromised, and they are flooding the enterprise with their preferred devices and apps. The popularity of Apple among millennials has led to a surge of iOS and, more recently, macOS devices in the enterprise. In fact, in Q4 2017 Mac shipments were up 7.3%

MobileIron

401 East Middlefield Road
Mountain View, CA 94043
globalsales@mobileiron.com
www.mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006

year-on-year, which substantially outperformed the PC market as a whole, which grew by just 0.7%.[1]

Not long ago, Mac laptops and desktops in the enterprise were primarily used by niche users, such as graphic designers and video producers. With so few Mac workstations to manage, many IT organizations left these endpoints either unsecured or secured with a point solution separate from a unified endpoint management (UEM) infrastructure. While point solutions are an attractive option in the short term, they don't provide a long-term strategy or a layered security model needed to scale with growing, enterprise-wide Mac deployments. As a result, managing Macs with point solutions can put these endpoints at risk and create security gaps across the enterprise as a whole.

What's needed is a strategic approach to UEM that simplifies and reduces the cost of IT operations, supports a mix of operating systems including iOS, macOS, Android, and Windows 10, and gives users a seamless, secure, and productive experience in today's modern work environment. It requires a complete UEM platform like MobileIron, which allows users to securely tap into mobile and cloud innovation so they can make swift, well-informed decisions that trigger meaningful actions at the right moment. There is no point solution that can do all of that.

[1] https://9to5mac.com/2018/01/12/mac-market-share-2017/

Why UEM is the ideal solution for macOS security

The time has come for a more mature approach to managing Macs in the enterprise. This is especially true for organizations that have a UEM solution currently deployed, yet continue to manage macOS with a separate point product. By rolling all of these devices under the UEM umbrella, IT organizations can manage them with a higher standard of security as well as optimize two key management areas:

Improve operational efficiency. Through UEM, IT admins can easily deploy device and network settings, apps, certificates, and configurations to Mac devices from a central console. By continuing to manage Mac deployments with point solutions, IT must repeat these tasks multiple times using different management tools with no visibility between them.

Enable strong and complete compliance management. With a common platform, only a single set of rules needs to be defined. Once this set of rules is approved by the corporate security officer, it can be applied to all endpoints to ensure compliance — which greatly simplifies the process and makes IT's job much easier. However, with point systems IT must define different rules in different systems to meet corporate security and compliance guidelines. Since each system operates differently, there might be gaps in meeting compliance regulations. For instance, when regulations change, policies may become out of date without IT knowing. It can also be challenging to produce complete audit reports without a uniform way to view them across each point solution.

Choose MobileIron to securely manage Mac deployments

MobileIron offers a layered security and access model for macOS, which improves operational efficiency and simplifies compliance by making it easy to manage all enterprise endpoints regardless of form factor or OS. The MobileIron macOS agent helps enroll users into the UEM solution and also helps with script execution for tasks that are outside the scope of the MDM protocol. It can also be pushed like any other application to already registered devices and does not impact existing management to provide endpoints a "script execution" capability.

Stronger security
With more granular visibility and control, organizations can meet compliance regulations and protect data on any corporate- or employee-owned Mac desktop as well other multi-OS devices. With MobileIron, organizations can leverage device encryption and data loss prevention settings as well as enforce conditional access to cloud services like Office 365 and Salesforce.com.

Easier management
IT benefits from more efficient, low-touch management that enables admins to configure any device over the air and provide secure access to business apps, email, Wi-Fi, VPN, and other productivity apps and content repositories such as SharePoint and Box. Now managing Macs with MobileIron is just as easy as managing iOS or any other type of device because there's no learning curve, manual intervention, or admin training required.

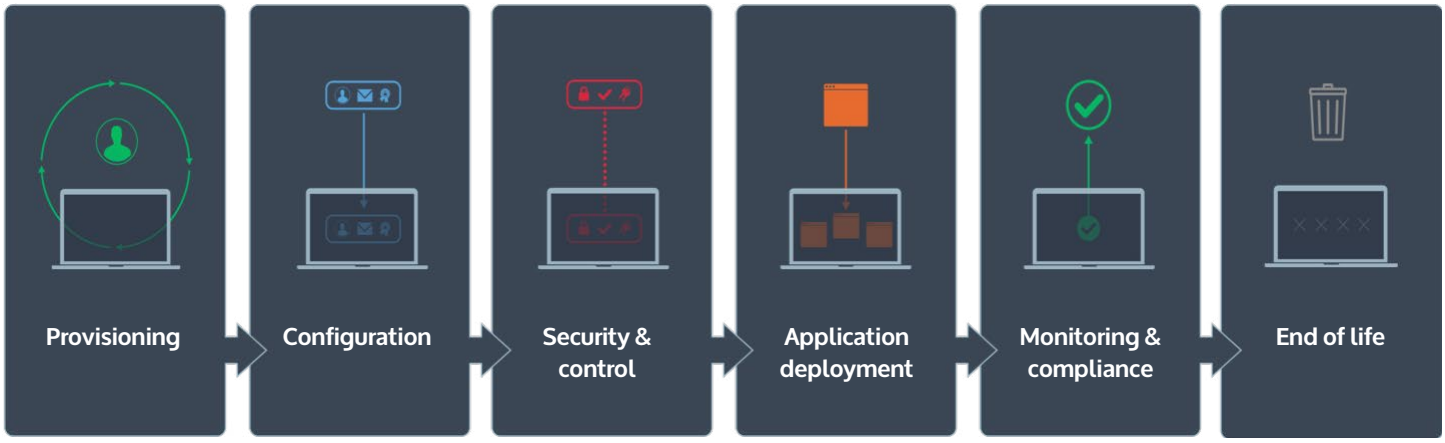
IT can also drive business productivity with a mobile application security framework that allows admins to distribute, protect, and manage apps at scale. Employee privacy is also protected through the separation of business and personal apps and data on employee-owned desktops. Just as important, IT can manage the entire device lifecycle with the ability to securely deploy, manage, and retire devices when employees leave the company or replace their desktops.

Better user experience

MobileIron helps IT accelerate productivity by getting users up and running in minutes on any device. Even remote and contract workers can quickly access business apps and content on a fully provisioned Mac desktop wherever they work. And, with easily accessible troubleshooting and self-service options, MobileIron helps users resolve problems on their own, which in turn reduces calls to the help desk. In addition, users get the same intuitive MobileIron experience across all of their devices, from smartphones to tablets to desktops. Employees don't have to navigate between multiple management interfaces on different devices. By enrolling enterprise devices in MobileIron, users enjoy a seamless experience across all of them.

MobileIron secures Macs across the entire device management lifecycle

MobileIron provides a full desktop management solution for Macs across every step of the device management lifecycle. If organizations are already using MobileIron to secure and manage iOS, Android, or Windows 10 devices, they can easily extend these capabilities to Mac workstations.



Provisioning
MobileIron supports the Apple Device Enrollment Program (DEP), which makes it easy for organizations to provision and set up new corporate-owned devices, including Macs. As mentioned previously, the MobileIron macOS agent provides more granular controls that go beyond security features supported through MDM protocol, but also serves as a point of enrollment.

Configuration
IT admins can access MobileIron's easy-to-use console to configure all modern endpoints with settings, certificates, Wi-Fi, VPN, and more. The macOS agent allows admins to run complex scripts that they might have used with legacy systems or point solutions to support niche use cases.

Security and control
Securing Macs with MobileIron is no different than securing other devices. Organizations can protect data in cloud services like Office 365 and Salesforce by blocking non-compliant devices through MobileIron Access. MobileIron also protects data as it leaves a Mac by securing connectivity through MobileIron Tunnel, which provides a per-app VPN and eliminates the need for a separate third-party VPN. IT admins can also deploy and update standard antivirus and anti-malware apps on every Mac through the MobileIron console.

Application deployment
MobileIron supports a full range of app distribution and lifecycle capabilities on macOS devices, including the Apple Volume Purchase Program (VPP). Apps from the Mac App Store as well as in-house apps can all be organized in Apps@Work and pushed to each Mac device. Different apps can be made available in Apps@Work to different users depending on corporate policy. End users can simply download and install the relevant apps by selecting them in Apps@Work. Through the MobileIron console, admins can set policies that restrict which apps employees can download to their devices and prevent any apps from performing malicious actions.

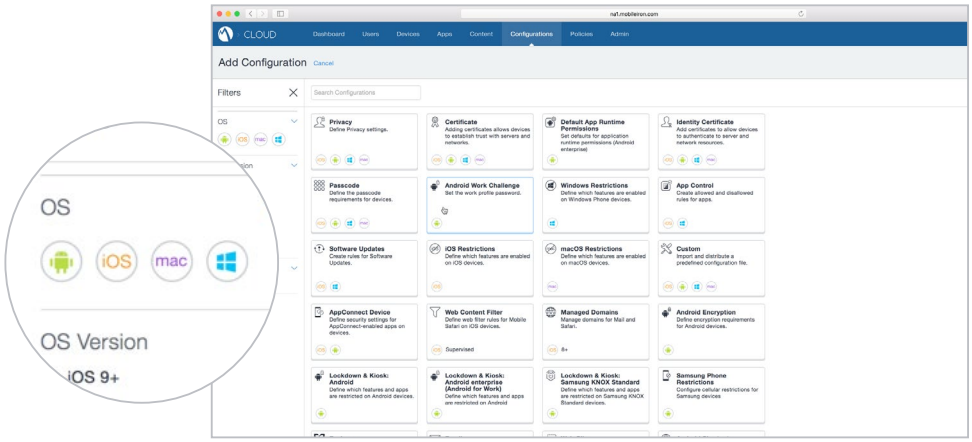
Monitoring and compliance
Ensuring that all devices, including Macs, are in compliance requires admins to have visibility into the compliance status of every device. With MobileIron, IT can establish and enforce a consistent mobile device and desktop security framework using an intuitive policy engine. Non-compliant devices can be quickly identified and denied access to corporate resources if needed. Granular policy settings and compliance configurations also allow IT to adapt and update security policies as business requirements and regulations such as GDPR, PCI DSS, and HIPAA evolve.

End of life
When a Mac is ready for retirement, or if an employee leaves the company, IT can remotely wipe all of the corporate apps, data, and configurations and restore the Mac to its factory settings. In the case of an employee-owned Mac, IT can simply wipe corporate apps and data while leaving the user's personal apps and content intact on the device.

Modern work requires a modern security model

The enterprise landscape has changed dramatically with the influx of millennials — and their preferred devices — into the workforce. As a result, Macs that were once limited to mostly niche usage are now rapidly expanding their enterprise footprint. These devices require the same level of security and oversight that organizations apply to all of their other devices. Otherwise, the risk of leaving Macs either unmanaged or secured by point products creates security gaps that can leave the enterprise open to cyberattacks and compliance violations.

The good news is, MobileIron makes it easy to secure Macs the same way all other devices in the enterprise are managed. No integrations, additional training, or learning curves are involved. The time has come for a modern approach to Mac management that is seamless for end users, improves operational efficiency, and simplifies IT operations across the entire device lifecycle. MobileIron makes it all possible.



MobileIron Cloud makes it easy to secure Mac desktops together with other multi-OS endpoints.

For more information

To learn how MobileIron provides modern endpoint security for macOS, visit us here.