Addigy

Minimizing Risk Through Proactive Apple Device Management: Addigy

Written by Drew Robb, Security for TechRepublic

In this Executive Brief by Preetham Gurram, Vice President of Product, Addigy, learn how to proactively manage Apple devices.

Enterprise IT teams are struggling to cope with three major forces of change: the evolving regulatory environment, a globally dispersed workforce, and the diversification of device types. The current regulatory landscape is marked with the emergence of data protection regulations such as the EU's General Data Protection Regulation and other data sovereignty laws that have recently been enacted in places such as California and New Zealand, which dictate that information must remain within a country, state, or region. The goal is to ensure the privacy of the data of individuals. Violations can result in hefty fines. Since being passed in 2016, **GDPR fines have soared beyond 4 billion euros.**

But there are other regulations and frameworks that also influence data movement and device management. These include PCI DSS, CISS, NIST and CMMC. While they may not be new, they are being enforced more strictly than in the past. CIS and NIST, for example, are introducing requirements that go beyond the dictates of the GDPR. The CMMC certification program rolled out by the U.S. Department of Defense, too, poses a big challenge for any organizations doing business with the DoD and related U.S. federal agencies as it holds GDPR rules to an even higher standard.

Geographic and device diversity add complexity

The global and remote nature of many modern enterprises places even further and more severe challenges on the regulatory front. In a working environment increasingly defined by remote work, most companies are operating at an expanded geographic scale. In some cases, workers are spread across an entire nation. For many other organizations, the daily reality is a globally dispersed workforce.

Adding to the regulatory and geographic dispersal of the workforce is the ongoing trend toward device diversification. Corporate networks increasingly encompass a multitude of different device types. The notion of a Windows-only workforce has become thoroughly outmoded in recent years as an increased number of Apple devices enter corporate networks: MacBooks, tablets, smartphones and watches. Each of these drivers of change puts pressure on enterprise IT leaders to take device management standards to the next level of control and security.

The need for Apple device management

As device diversification continues and more Apple devices enter corporate environments, IT leaders face added management complexity. In addition, employees often use corporate devices for personal computing needs, and vice versa worsens the situation. This poses risk in terms of cybersecurity, data privacy and overall device management.

Frequent system updates to Apple devices are especially difficult to manage, particularly on a global scale. Apple's operating model, too, can create problems due to the company's hands-off and sometimes inflexible attitude. The onus is on IT leaders to oversee viable strategies for the efficient management of Apple devices.

The latest major change is Apple's introduction of Declarative Device Management. This new device management standard is built around the concept of shifting device management from centralized servers onto the devices themselves. This change of operating basis from Apple is upending traditional device management practices.

Adopting an effective Apple Mobile Device Management solution, therefore, is more mission-critical than ever. A robust Apple MDM solution allows IT to manage Apple users safely and capably to the same standard as all other devices within the network. It allows IT to seamlessly manage any Apple devices remotely while improving the overall end-user experience.

IT leaders, then, are responsible for vetting existing MDM solutions and looking for the qualities that separate the leaders from the laggards. The best way to categorize potential Apple MDM vendor solutions is based on whether they take a reactive or proactive approach.

Reactive vs. proactive Apple management

Addigy recently conducted a survey of 250 IT leaders to better understand the state of MDM across mixed computing environments. Among Apple MDM users, the frequency of Apple updates came up as a significant challenge. Reactive MDM solutions are stuck with time-consuming update rollout processes that fail to keep pace dependably with update frequency. The consequences include greater potential for cybersecurity breaches and user disgruntlement.

Unresponsive support is another indicator of a reactive approach to Apple MDM. Support must be fully engaged, not perfunctory. When IT calls these vendors, they experience lengthy delays, endless voice prompt options and lack of actual hands-on support.

Perhaps the biggest "tell" for a reactive Apple MDM solution is complacency and outdatedness. Unfortunately, some established vendors are content to profit from their existing users rather than evolving with the marketplace to address the changing landscape. Thus, they don't invest in continuous upgrades to their products.

This manifests in ways such as a lack of attention to changing regulations and standards, and failure to keep pace with Apple's platform development timeline. The constantly shifting regulatory landscape demands that vendors become nimble in updating their tools to ensure they can track and follow all relevant standards.

IT leaders, therefore, need to not only familiarize themselves with the evolving regulatory landscape, but they also need to evaluate vendors from the perspective of regulatory compliance. It may be time to take a closer look at whether an existing device management provider supports clearly articulated compliance to the latest standards.

Further, those using reactive MDM solutions can expect prolonged delays in dealing with sudden changes such as DDM. Apple's new standard for device management as Apple will soon require "passwordless" management and device attestation – steps that require following its DDM framework. DDM, therefore, is certain to introduce volatility into the Apple device management landscape. Platforms that are historically inflexible or overly reliant on traditional device management approaches will struggle to adapt. As a result, internal IT teams may find their device management provider failing to effectively manage devices under the DDM framework. They may also be unable to support MacOS Sonoma, Apple's new operating system (which is expected to be released later this year). Sonoma will formally roll out DDM and that could spell real trouble for many businesses if their vendor is unprepared.

Proactive Device Management

Addigy's "Mobile Device Management Benchmark 2023" report reveals a marked correlation between the use of proactive Apple MDM solutions and overall feelings of security, visibility, and maintainability. IT staff consistently list the three biggest challenges they face when it comes to managing Apple devices as dealing with the frequency of updates, addressing security threats, and being responsive to user-level issues. Enterprises that partner with a proactive vendor enjoy much higher levels of confidence across all these factors.

A proactive Apple MDM solution can be defined as one that doesn't wait for Apple updates to roll out before devising solutions. Such vendors stay ahead of the game. They develop solutions to preemptively mitigate issues associated with updates, leading to a more seamless user experience. A continuous iteration philosophy imbues their solutions with deep familiarity with the security and compliance landscape, and users can expect a steady stream of software refinements based on changes in security frameworks.

Another way to separate proactive from reactive solutions is to evaluate vendors based on their level of expertise with Apple operating systems and devices. Only those that truly understand the Apple landscape will be capable of developing tailored solutions for enterprise IT environments.

Additionally, proactive Apple MDM vendors treat customers as partners, pushing beyond the traditional vendor relationship. They are responsive in that they are always available to walk IT through solutions to problems as they arise. They are receptive and committed to personalizing the user and IT management experience. They take product suggestions seriously as demonstrated by putting them into play in the evolution of their products. And they won't try to rope customers into long contracts or upsell add-on features that should have been packaged in their solutions in the first place.

Read the Report

Addigy's "Mobile Device Management Benchmark 2023" can be downloaded here. It details:

- The three key issues faced by those managing Apple device fleets.
- How to efficiently manage Apple updates.
- How to implement Apple DDM in the enterprise.
- The degree of adoption of cybersecurity insurance and the factors inhibiting companies from obtaining it or qualifying for it.
- How MDM weaknesses often lead to cyber-insurance violations and denial of policies.
- How ill-prepared many organizations are in dealing with cross-border compliance and data sovereignty challenges.

The talent vacuum of available Apple admins places additional strain on managing Apple devices. It serves to underscore the need for an industry-leading device management solution. Addigy is dedicated to elevating the Apple IT ecosystem for organizations of all sizes. Its best-in-class solution empowers enterprise IT teams and MSPs to securely manage their Mac and iOS devices easier, faster, and better than ever before. It is the only cloud-based multi-tenant Apple MDM solution designed for scalability. As such, Addigy can provide Apple fleets of any size with rapid device and software deployment, comprehensive monitoring, remediation, security protection and compliance, automated system updates, and simplified migration.

Addigy is your proactive partner in meeting the evolving needs of Apple MDM.

For more information on how you can partner with Addigy and take your Apple device management to the next level of readiness, get in touch with us via email at sales@addigy.com or please visit **addigy.com/contact-us/.**

Proactivity in practice: Apple's 1st RSR update

Addigy was unique in the Apple MDM space in getting ahead of Apple's first Rapid Security Response update to address undisclosed vulnerabilities in its macOS, iOS, and iPadOS systems. Classified at the highest level of security, an RSR typically addresses an active exploit that exists today, allowing IT to quickly close the vulnerability. Addigy made it easy to quickly push these upgrades to all Apple devices anywhere on the network. In addition, the company provided installation and troubleshooting tips related to the update and improving system protection.

The Addigy MDM Watchdog Utility, for example, can help rectify any issues experienced. This self-healing mechanism proactively monitors if the MDM services on any device have become unresponsive which would block the device from updating appropriately. It ensures that an entire fleet of devices can be 100% up to date with the latest security from Apple.