jamf

WHITE PAPER

Apple Native Security

Proof that less (layers) is more (secure)

Enterprise information security is a never-ending battle against constantly evolving threats. Attackers are increasingly sophisticated and their attack vectors are always changing. The threat landscape is expanding, with new devices joining corporate networks every day. One solution to this security challenge is to embrace the Apple platform and take advantage of the native Apple security frameworks. For a modern, mobile workforce, this allows for good device security without compromising on the user experience.

THE FOUR PILLARS OF MOBILE SECURITY

Securing a mobile computer—whether a laptop, smart phone, or tablet—requires careful attention to four key areas:

1. Data at rest—Securing data on a device
2. Data in transit—Securing data as it moves over a network connection to the device
3. Application security—Installing trustworthy software from a safe source
4. Patching—Keeping software up to date to avoid vulnerabilities

To implement good security reliably throughout an organization, three additional capabilities are crucial:

- Device management—Deployment, application distribution, security policy enforcement
- Reporting—Inventory of all devices and their configuration
- Auditing & remediating—Audit for compliance to security standards and tools to remediate as needed

DON'T ADD LAYERS IF YOU DON'T HAVE TO

Complexity in a system makes securing that system more difficult. Each layer of complexity introduces new points of failure, vulnerabilities to exploit, and potential conflicts. In the IT domain, complexity takes the shape of additional sof tware layers. The IT security software industry offers many solutions for the four pillars of device security, but at the cost of complexity. All else being equal, a computer system with native security controls is easier to manage and inherently more secure. By integrating the security framework with the operating system layer, updates are painless and complexity is minimized.

APPLE'S NATIVE SECURITY LEADS THE WAY

Apple is best known for leading the industry in design and intuitive functionality. Less well known is their implementation of native security frameworks for iOS and OS X. In the past few years, Apple significantly raised the bar with Mac, iPad, and iPhone. Today, no other platform

Complexity in a system makes securing that system more difficult.

in the desktop or mobile ecosystem offers a comparable combination of ease-of-use, privacy controls, and solid IT security.

HOW APPLE CEMENTS THE FOUR PILLARS

Apple's OS X (Mac) and iOS (iPhone, iPad) operating systems include native security controls for each of the four pillars above:

1. **Data at rest**—The iPhone and iPad features hardware-based encryption for data at rest that is enabled by default. For Mac, the FileVault whole disk encryption system (a native feature in OS X) protects data with virtually no impact to system performance or battery life.
2. **Data in transit**—Apple devices can connect via VPN (Virtual Private Network) to secure data in transit. No additional software is required to take advantage of this security feature, and once configured it is transparent to the user.
3. **Application security**—One of Apple's best contributions to the IT security field is their App Store ecosystem. Apple reviews all software submitted to the App Store to weed out malware. Each software package is cryptographically signed to prevent any tampering with the files. OS X and iOS are configured to reject any software that lacks a signature. IT staff can sign their own software packages to take advantage of this application security layer.

4. **Patching**—Since the dawn of computing, all software includes some number of defects or bugs. Some of these defects can be used by malicious attackers to gain access or steal information. The best practice for IT security is to keep all software up to date to eliminate vulnerabilities as they're discovered. Apple makes this easy with native software patching utilities built-in to the OS. IT staff can host an Apple Software Update Server on the corporate network to speed up patching.

NATIVE SECURITY, MANAGED

Apple's native security controls are designed for ease-of-use and, once configured, require minimal interaction from users. This is ideal for the individual or small business. For larger organizations, remote management tools are essential to configure, deploy, and audit security configurations. The Jamf Pro from Jamf is built for the Apple platform and integrates with all native Apple security controls. It features a full suite of deployment and configuration tools, dynamic inventory collection, and auditing & remediation capabilities.

Conclusion

Implementing good security practices does not have to be a complex, burdensome process. Over the past decade, Apple built a rich ecosystem of devices, software, and services that offer the best user experience for personal computing. At the same time, the native security controls included with Apple operating systems provide a truly enterprise-grade security framework. When paired with an Applefocused management tool like the Jamf Pro, the Apple ecosystem represents the best experience for end-users and IT security staff alike.

To learn more about how Jamf Pro can make an impact on your Mac and iOS management, visit **jamf.com/products/Jamf-Pro**.