jamf

WHITE PAPER

Filling the Gap: macOS Security

Native privacy and security, but no operating system is perfect.

The need for security extends across every operating system and macOS is no exception. Apple has invested heavily to provide native privacy and security features, but the value of attacking the Mac platform increases as its enterprise market share increases, making it a more desirable target for Malware, breaches, and vulnerability discovery. More than ever, companies allow their employees to use macOS through employee-choice programs. In doing so, they realized that just like any other platform, additional security and visibility are needed.

Several security vendors offer additional solutions to protect Mac, but many of these solutions use a security model specific to the vendor and their Windows product instead of working with modern frameworks that macOS provides. This makes it difficult to keep up with an ever-changing operating system. Instead, best practice is to extend the existing macOS security model, fill in the gaps, and add the macOS-specific value that security teams need to operate effectively to keep their organization safe from threats.

And while Apple operating systems protect both the user and their privacy, ease of use and productivity have always been top priorities. The Apple experience is heavily focused on the user rather than the business in which they operate. The same can be said for many of the security and privacy features in macOS.

In our white paper, we provide an overview of the current state of macOS security and provide guidance on how Apple's security baseline can be enhanced in an efficient, effective and user-friendly manner.

You'll learn:

- Details of available built-in macOS security features
- How Jamf enhances these features in the enterprise
- How Jamf extends threat detection beyond signatures and built-in features
- Additional ways to extend Apple's security model for advanced enterprise security

Applications on macOS

Apple has put a great deal of effort into designing security features to protect the user and the third-party applications they run. In this section, we will introduce several of these features and talk about ways in which they can be strategically enhanced and extended. For more insight into Apple security features, visit Apple's comprehensive platform security guide at: **support.apple.com/guide/security**.

Verify trust with Gatekeeper.

Apple's preferred and most trusted path for installing third-party applications is through the App Store. Doing so allows Apple to review and screen programs that do not meet their standards for privacy, security or user experience. However, Apple also limits the capabilities of applications in the App Store and many business-critical applications are not well-suited for this type of distribution.

Where distribution from the App Store is not an option, Apple allows macOS developers to distribute their applications directly via hosted downloads and other traditional distribution methods. To support these "ad hoc" distributions, Apple has introduced other checks into the operating system to reduce the risk of the widespread distribution of software across macOS devices. Gatekeeper is the name of the feature at the center of Apple's verification checks. What began in macOS as an option to allow programs to run depending on their risk appetite has evolved into an expanded and strict set of requirements and mitigations. The basic acceptance levels to allow apps downloaded from the "App Store" or "App Store and identified developers" still exist, but the option to run problematic or risky code continues to be marginalized.

Note that these checks only apply to applications downloaded from the internet. Apple tracks these applications by attaching additional metadata to the downloaded file, known as the quarantine attribute. When a program is executed, Gatekeeper performs a series of checks such as verifying the quarantine attribute to determine if it can execute.
One of these most basic checks is whether or not the application is signed by a legitimate developer or was distributed by the App Store, depending on the previously discussed setting.

If the application is signed by a developer, the certificate is checked against a revoked signature database to ensure that the signer has not been associated with malware in the past. This way, Apple can quickly revoke a certificate and stop widespread distribution of malware. Starting with macOS Catalina, passing the Gatekeeper verification also requires that the application be notarized by Apple. For an application to pass the

check, it must be uploaded to Apple for analysis. Upon successful analysis, notarization data is associated with the application to note that it has passed this additional level of inspection.

The ultimate trust lies with the user.

In the name of usability, macOS allows the end user in many situations to “Override” Gatekeeper. A user can simply right-click the application and select “open” or “open with”. Instead of flatly refusing to launch the application, a new prompt will simply warn the user that they are launching an unknown or potentially malicious application, but Gatekeeper will allow them to do so. It is important to note that malware that XProtect has definitively identified cannot be authorized to run by a user.

Once the application has been executed for the first time, the quarantine component gets updated so that the Gatekeeper actions are not repeated the next time the application is opened.

Block threats with XProtect and MRT.

The Gatekeeper suite of technologies also includes Apple’s signature-based detection mechanisms, known as XProtect and Malware Removal Tool (MRT). Together they are capable of scanning files on the operating system, looking for traits within files that are associated with known malware. XProtect is triggered upon application launch, while MRT periodically scans the file system.

XProtect operates using a binary signature scanning engine called Yara. Yara supports flexible and powerful binary signature definitions and an efficient execution engine. To verify an application, XProtect scans each executable download on initial execution and after subsequent updates. If any matching signatures are detected the program will not be allowed to run. The known bad signature file is provided via independent updates to macOS from Apple. Apple defines and delivers these signatures as they see fit, separate from the Yara execution engine itself. Just like Gatekeeper, this scan is only performed when an application holds the proper quarantine extended attribute which is updated after the first successful execution of the application.

MRT, on the other hand, is executed on a scheduled basis rather than at program runtime and scans the file system for specific file names and artifacts associated with past malware and removes them if discovered. This feature is largely intended to find and remediate known threats that may be already executing across the macOS population.

Extend Gatekeeper to the enterprise.

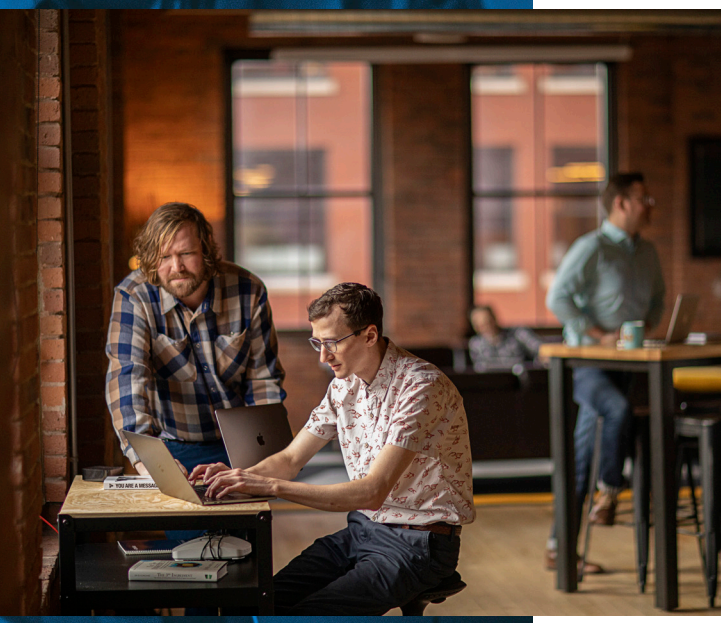
Gatekeeper effectively operates as it is intended. It blocks untrusted applications from launching and it notifies the user when it identifies an application as suspicious or malicious. IT and security administrators need to have visibility into attempts to run untrusted software on a corporate asset. More importantly, they need to be aware that a user decided to right-click and launch an application, effectively bypassing a business security control. To address these enterprise needs, Jamf Protect — an endpoint security solution purpose-built for Mac — monitors for indications of Gatekeeper actions and reports the results to a central location so that IT and security teams can accurately assess their risks and make informed decisions.

Beyond providing visibility into Gatekeeper activity, Jamf Protect also allows enterprises to take ownership of the developer trust model by registering additional signing information as untrusted in the enterprise environment. Using Apple’s latest Endpoint Security API, Jamf Protect will proactively deny execution of any application on the enterprise-specific block list. This can be defined on a per-application level (application ID) or on a per-vendor level (developer team ID).

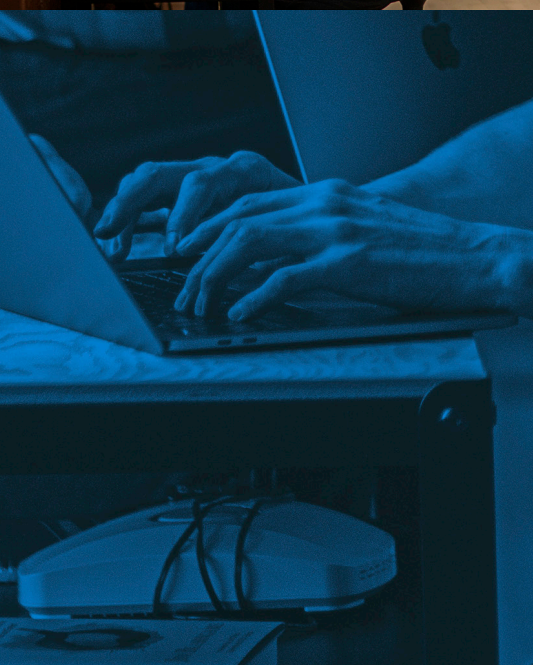
Furthermore, macOS does not provide signatures or blocking for a variety of Grayware (potentially unwanted or unsanctioned software) which includes many adware and crypto-miner applications that partake in undesired and potentially invasive behavior. Often, these programs are legitimately signed by an Apple developer and the

user agrees at install time to allow their information to be collected or resources to be used — usually without realizing it. Therefore, in many cases, Apple does not interfere with the operation of these applications.

However, the risk calculation is simply different in the enterprise and a more strict and targeted approach may be desired. Therefore, Jamf Protect enforces its own set of managed Yara rules, binary signatures, and untrusted developer certificates that are used to scan processes upon execution regardless of whether or not the quarantine extended attribute is present. This ensures that as new signatures are added, and the enterprise updates its security posture, existing applications are rescanned at next execution, not just the first time.



Jamf curates this feed of known Mac-targeted malware based on Jamf's extensive research into macOS-targeted threats as well as third-party Mac threat data. For organizations that want even more granular control of the software running in their environment, they can extend the list of applications blocked by Jamf Protect with their own list of binary hashes, TeamIDs, etc. When an application executes that matches the behavior or signature of known malware on macOS 10.15 (Catalina) or later, Jamf Protect will prevent the execution of that process, quarantine the offending file, and register an alert that malware was prevented. This operation happens outside of Gatekeeper/XProtect actions and is designed to be a superset of their functionality. Jamf Protect will identify known malware without regard to the quarantine bit to identify potentially unsafe binaries and maintains a much broader set of malware knowledge.



Extend the App Store trust model with Self Service.

In certain situations, it may be appropriate to dictate the programs that your users can install by leveraging a self-service app store pre-populated with IT-approved resources.

Jamf Self Service allows for secure and instant resource access by empowering IT to create its own enterprise app catalog where users can install apps, update configurations and troubleshoot common issues on their own — without requiring an IT help ticket.

Control and monitor application behaviors.

Limit and acknowledge application behaviors with privacy controls.

System privacy controls were introduced in macOS Mojave. These controls require users (or enterprises) to allow per-application access to specific actions and folders. Once applications have been granted access to specific actions, they won't be asked when the action takes place from the same application in the future. This feature ensures that applications are explicitly allowed to access potentially sensitive parts of the OS (webcam, mic, keystrokes, downloads) and causes users to slow down and acknowledge that they are granting applications access to private data.

Go beyond controls to audit and analyze application behaviors.

While privacy controls limit what applications are authorized to do, users will make mistakes and authorizations will be abused. We've already covered how Jamf Protect provides visibility into the actions of built-in Apple security features and traditional malware/adware prevention capabilities to keep enterprises informed and protected. But at Jamf, we believe that an endpoint protection solution should not stop there. Jamf Protect also delivers auditing and monitoring capabilities traditionally reserved for Endpoint Detection and Response (EDR) products — but with an Apple-first approach and eye on the standards of privacy and security that macOS users expect.

Detection engineering with Jamf Protect

At the core of the Jamf Protect agent is a lightweight, user-mode sensor (without an accompanying text) that leverages one of Apple's own logic execution engines, GameplayKit. Although using a game engine to analyze security events is non-traditional, it allows Jamf to remain closely integrated with the Apple ecosystem and analyze data on the device until necessary to collect or report. Game engines are also designed to handle a massive number of events as they occur in real time, making them perfect for analyzing activities as they take place on the device. Contrast this design to the many security solutions that are focused first on the Windows platform and then ported to macOS as an afterthought — or those that require that all of the data be collected and analyzed in the cloud.

An additional benefit of GameplayKit is that, like Yara, it separates the execution engine from the detection definitions, allowing detections to be updated and expanded without the update to the core agent. The detection definitions are also native to Apple, using NSPredicate, a powerful logic query mechanism that supports typical query syntax along with regular expressions. Jamf Protect's data model has been specifically architected to take advantage of the rich features of NSPredicate, including its ability to call native functions and chain data models together. This unlocks capabilities that are messy or computationally expensive to implement in other, more traditional ways. For example, using Jamf Protect's data model and NSPredicate we can:

- Alert if a file is self-deleted, a common technique for covering one's tracks. This seemingly simple use case involves analyzing both the file that is deleted and the process of doing the deletion without an expensive join operation or hardcoded detection.
- Alert if an unsigned or suspiciously signed binary persisted as a launch daemon. This involves parsing a configuration file, extracting an embedded binary path from the contents and using metadata about that binary file in the analysis.
- Alert if a Microsoft Office application created an unexpected child to identify Office Macro exploitation. This example highlights the ability to understand child/parent relationships and to uncover exploitation of application features.
- Alert if other "live-off-the-land" activities are being used in ways that are indicative of attacks. This class of activity requires access to

child/parent and process group relationships, command line parameters, etc., in order to uncover abuses of otherwise innocuous activities (curl, ssh, python, etc.)

- Track USB usage across the enterprise and report metadata about files that are being written to removable media.

To make it easy to understand the impact of these types of detections, Jamf Protect maps identified attacks to the MITRE ATT&CK™ framework, if applicable. Coverage today includes use cases from across the framework, including detection of techniques in the following categories:

- Persistence
- Initial Access
- Command and Control
- Defense Evasion
- Discovery
- Privilege Escalation
- Credential Access

Simple Unified Log collection and reporting

Most security analysts and IT administrators have strong needs for endpoint logs as part of a compliance audit or when looking to close gaps in other security controls. When macOS moved from syslog files to Unified Logging it became harder to collect, inventory and inspect this information across the enterprise. The macOS Console.app provides great access and visibility into the Unified Log infrastructure on a local Mac, but it does not allow an organization to easily centralize that data.

With Jamf Protect, client logs can be streamed to a system of record as soon as they are written to the Unified Log. To ensure that only targeted data is collected, Jamf Protect admins utilize the same predicate filter language (NSPredicate) from the built in `log stream` command line utility. With that, building systems of records for Mac log data becomes a simple configuration instead of a tedious collection on a machine-by-machine basis. Examples include log-in and log-off, SSH, AirDrop and authorization events. If data is logged to the Unified Log, Jamf Protect can collect it.

Align with Apple's standards.

Day-of-release support

To interface with macOS and gather the data necessary for security decisions, Jamf Protect leverages native Apple technologies. These technologies include emerging frameworks such as Apple's Endpoint Security API and the OpenBSM Audit framework prior. By using these mechanisms, Jamf Protect minimizes its device impact and does not run afoul of changes in macOS introduced in patches or major OS releases. Patching early and often is the most commonly recommended security protocol. Security tools that strongly adhere to day-of-release support are core to complying with that protocol and a critical component in a comprehensive defense-in-depth security strategy.

User experience as a feature

While Jamf Protect continuously monitors application and user activity for potential threats, it purposely does not scan for dormant or Microsoft Windows-related malware. Scanning files simply residing on the file system for a large variety of malware signatures is often a primary contributor to a bad user experience. This approach aligns with Gatekeeper/XProtect in that threats are identified at the time of potential execution so that the user experience and user productivity are minimally impacted.

Privacy

Jamf Protect analyzes data on the device and only collects pertinent information when configured to do so, typically when a potentially malicious or high-interest activity is detected in real time. This balances enterprise needs with user privacy as less user data is taken from the device and stored in the cloud. If any malicious activity is identified, the identified activity and associated data are passed to the Jamf Protect cloud console or configured Security Information and Event Management (SIEM) systems. Any specifically requested data beyond that is also pushed to Jamf Protect or the SIEM. By filtering out all unnecessary data, a security analyst that is tasked with monitoring and investigating incidents is presented with a high-quality collection of applicable data.

Other extensions to the Apple security model

Best practice: hardening macOS

While Apple delivers and supports some of the most secure and reliable operating systems available, it is common to ask what additional steps can be taken to make macOS an even better fit for your corporate environment.

The best first step is to start leveraging Apple's mobile device management (MDM) framework for automated management at scale. Not only will MDM help you better protect your organization, but it will also take much of the burden of managing and securing your fleet off of IT.

Introduced with OS X 10.7 ("Lion"), the MDM framework unlocks an incredible number of workflows to tailor device functionality to the organization's specific needs. Configuration profiles and management commands are the two most common ways to leverage an MDM to ensure teams are secure, wherever they are working.

Take security with MDM to another level by combining it with the power of Apple Business Manager, a free solution from Apple for businesses that helps automate hardware procurement, management and more.

Start with Apple...

Over the years Apple has built a reputation as a security-first company and it shows in macOS. Native functionality like FileVault 2 encryption, two-factor authentication, remote lock/wipe functionality and the ability to enforce passcode standards are available with every new Mac added to an organization's environment.

Modern management platforms — like Jamf Pro — leverage MDM to take these features a step further and help customize the implementation, enforcement and reporting on valuable security tools like encryption.

...Enhance with Jamf.

While MDM provides a great cornerstone for any organization, many wonder what else they can do to further enhance their security posture and fortify employee privacy. That's where Jamf comes in.

It's no secret that at a certain scale, device management becomes a big drain on team resources. More people means more hardware, and more hardware means more IT overhead.

At least, that was true before fleet management platforms like Jamf Pro.

With patented technology like Smart Groups to help organize corporate devices and automatically execute management functions, IT teams can spend less time in the weeds of device management and have more free time for other day-to-day IT tasks. Smart Groups will keep a watchful eye over device inventories, adding and removing devices from a pre-defined group in real time as device status changes.

Modern identity management on macOS

At the core of modern security is identity — secure and customized access for end users. Legacy IT relies on local directory services to act as a centralized record of employee information, such as name and department. As security and deployment needs evolve, businesses must adopt a new approach to identity and access management as part of their enterprise strategy. With a complete cloud-based identity stack, businesses unify identity across hardware and software to unlock functionality, advanced workflows and ultimately transform business.

Building on information from directory services, cloud-based single sign-on (SSO) ensures end users enter secure credentials to access company resources.

Jamf Connect extends these common forms of identity management.

Jamf Connect unifies identity across all company apps and the user's Mac, with seamless authentication workflows. End users leverage a single cloud identity to easily and quickly gain access to resources they need to be productive.

With Jamf Connect, organizations have:

- Streamlined provisioning and authentication out of the box for full support of remote and on-site employees
- Automated syncing of user identities and device credentials
- IT with full identity management capabilities across their services and devices
- A Zero Trust Network Access (ZTNA) solution to replace legacy VPNs (virtual private networks) and meets the needs of the modern, hybrid enterprise

Respond and remediate threats on Mac

Jamf Pro provides dashboards that help keep organizations appraised of the state of their Mac devices and flags hardware that needs attention. Through patented Smart Group functionality, IT admins can target devices that need to be updated or patched to improve their security posture. This is all done remotely and can be automated, so IT never needs to physically touch the device.

When pairing Jamf Protect with Jamf Pro, threat remediation is taken one step further. Leveraging this Smart Group technology, all MDM and Jamf Pro commands can be orchestrated in response to an activity-based alert from Jamf Protect. This includes automated network isolation, failed conditional access, user notifications or any number of other targeted forms of remediation and response. Together with Jamf Pro and Jamf Connect, attacks on a user or device can result in credential suspension, access changes and a variety of other remediations around identity.

Security beyond device management

Read our report on the state of Apple security in the enterprise, which surveyed 1,500 IT and InfoSec professionals. It includes current device usage and approaches, challenges to device security and the future state of endpoint security.

Trusted Access

Trusted Access is Jamf's solution to security beyond management. Trusted Access is a unique workflow that brings together device management, user identity and endpoint security to help organizations create a work experience that users love and a secure workplace that organizations trust.

By using Jamf Protect with Jamf Pro and leveraging Jamf Connect admins can ensure only trusted users are accessing corporate applications on trusted and compliant devices. If there is an issue with an infected device, it can be remediated quickly and brought back into service with Jamf Pro.

Trusted Access with Jamf dramatically increases the security of your modern workplace while streamlining work for your users — regardless of where work happens.

Manage and secure Apple for unprecedented benefits.

With the right tools in place, IT and Information Security teams can confidently roll out a Mac initiative, verify and authenticate identity and access, and fully empower users with the resources and access they need — all with the boxes checked for security and privacy.

Take advantage of Jamf enterprise solutions today and enjoy the visibility and remediation that your modern organization needs.

Get Started

Or contact your preferred reseller to take Jamf for a free test drive.

jamf

www.jamf.com