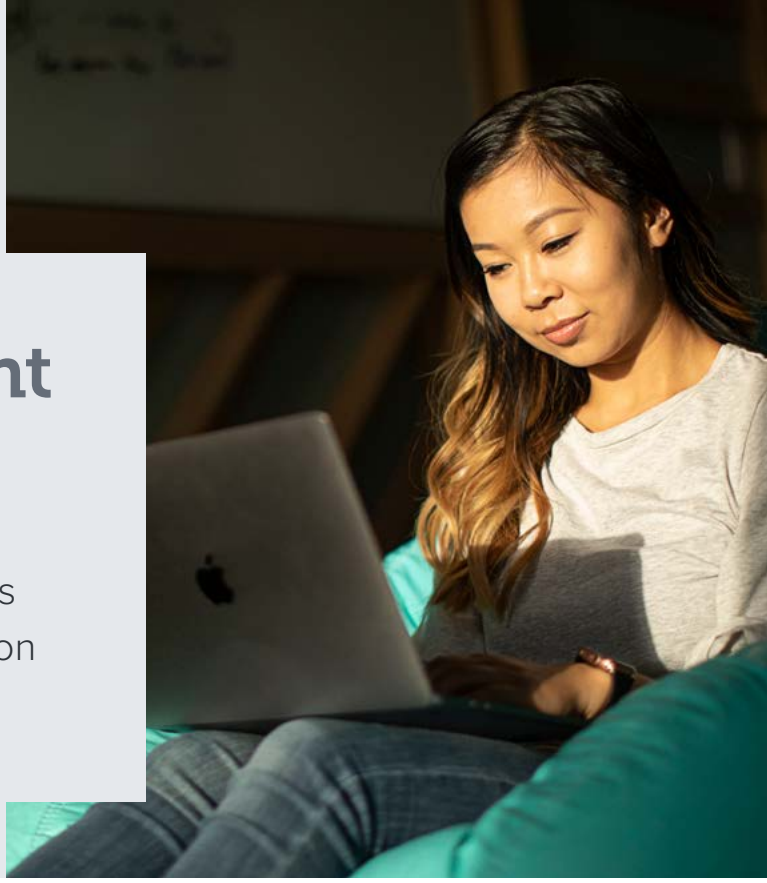
jamf

Jamf Protect Endpoint Security Capabilities

As Mac adoption in the enterprise continues to rise, attackers are increasing their focus on building more attacks that target macOS.



jamf PROTECT

Endpoint Security

- AV
- Behavioral Detections
- Data Control
- Custom and Automatic Remediation

Security Operations

- Custom Analytics
- macOS Security Visibility
- Threat Hunting
- CIS Benchmarking
- Unified Log Forwarding
- SIEM Integration
- Device Isolation
- Device Lockdown
- File Retrieval
- User Isolation
- User Lockdown

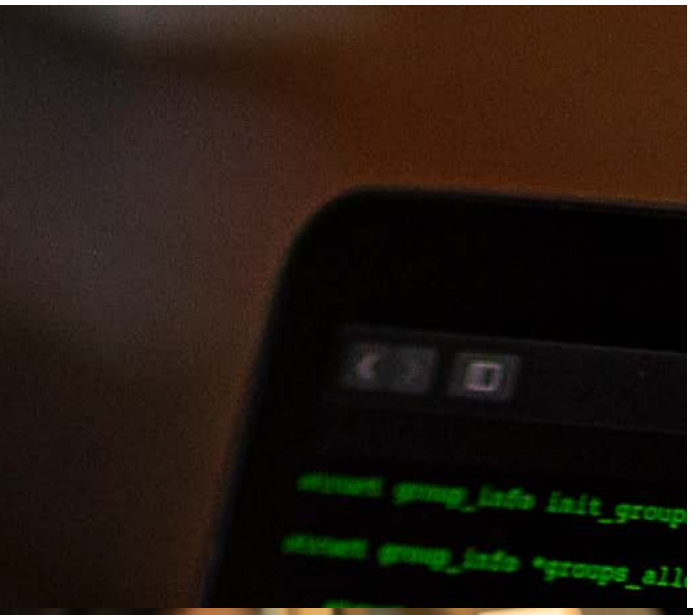
Information Technology

- File Integrity Monitoring
- Application Control
- Compliance Monitoring
- Standardized Remediation
- Application Inventory
- macOS Redeployment

Jamf Protect

with Jamf Pro

with Jamf Connect



While the macOS platform has its roots in the Unix world, macOS is a unique Operating System (OS) with specific inner workings for files, processes and networks. As a result, attacks targeting macOS rarely resemble attacks against Windows or other platforms. However, most security vendors focus on building out detection, prevention and remediation capabilities for Windows first and then attempt to port the Windows-based models of their tool to Mac.

Because one-size-fits-all security tooling on the market today isn't designed for the Mac, organizations may be missing attacks on their Mac infrastructure and must add a Mac-specific security solution into their existing security stack.

Jamf Protect is endpoint security built for Mac. Maintain Mac endpoint compliance, address anti-virus needs by preventing macOS malware, control Mac applications within the organization, detect and remediate Mac-specific threats with minimal impact to the device and the end-user experience. And when paired with Jamf Pro and/or Jamf Connect, Jamf Protect unlocks extensive automation, investigation and remediation capabilities to mitigate endpoint security risks, both large and small.

Jamf builds on Apple's core security approach for macOS and amplifies it with same-day support for Apple OS upgrades for greater prevention, stronger control, broader visibility and remediation that adapts to your environment. Unlike one-size-fits-all security solutions, which often have gaps of days or weeks between when Apple ships a new version of macOS and when they are prepared to support it, Jamf works seamlessly with the latest version of macOS the day it is available without disruption to end users or delays in security coverage.

Mac focused Anti-Virus

Anti-Virus (AV) is a basic requirement for most organizational devices to provide baseline security. Apple includes a basic AV mechanism in macOS with XProtect, Gatekeeper and MRT. However, these tools are updated sporadically and organizations lack visibility into their actions. Jamf Protect provides sophisticated AV capabilities to prevent and quarantine Mac malware that leverages the functionality present in macOS and is far greater than what Windows-focused solutions are provide.

- **AV:** Prevent known Mac malware from executing on organizational devices
- **Visibility:** Have organizational visibility of built-in prevention activity by XProtect, Gatekeeper and MRT
- **Malware insight:** Prevent common malware from executing by taking advantage of Jamf's extensive knowledge of macOS malware through research and third-party feeds
- **Quarantine:** When malware is identified, automatically remove it from the user's environment and quarantine it for analysis
- **User experience:** Jamf Pro ensures that users are aware of corrective actions taken when Jamf Protect identifies a threat to avoid future risky behavior by the user
- **File capture:** Retrieve file samples through Jamf Pro when a threat is identified

Mac focused detection and response

Traditional endpoint detection and response (EDR) tools have existed for Mac for quite some time, but most are not built to effectively detect attacks that specifically target Mac. Rather, they attempt to force Windows models on Mac devices. With Jamf Protect's sole focus on Mac, Jamf minimizes false positives and maximizes the detection rates on Mac. Together with Jamf Pro, Jamf Protect provides minimally intrusive remediation capabilities that go far beyond your average EDR response capabilities.

- **Behavioral analytics:** Detect unknown malware and advanced threats through a broad collection of on-device behavioral analytics
- **Broad alert coverage**: Jamf Protect maps alerts to Mitre ATT&CK framework, including initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration and impact categories
- **Notifications:** Mac security alerts you in real time via the Jamf Protect console, email notifications or your SIEM
- **Alert context:** Get full insight into why a security alert was raised, removing guesswork for your analysts
- **Minimize false positives:** Tune any detections to minimize false positives in your environment
- **Custom detections:** Create custom detections to minimize risks unique to your organization

Security incident response

When an attack is detected, the clock on isolating the threat, removing the threat, and getting the device or user into a trusted state starts ticking. The longer an attacker has a foothold the more likely they are to move laterally to other devices, steal data, damage data, or damage the organization. While automatic incident response that goes unnoticed by the end user is usually the goal of any Security team, many situations require manual decision making and even manual intervention.

- **Quarantine:** Malware prevented from execution is quarantined to minimize subsequent damage and allow for further analysis
- **User notification:** The user is always informed of any prevention actions to minimize future risky behavior
- **Automate recovery:** Automatically trigger Jamf Pro corrective actions during incidents, minimizing dwell time
- **File retrieval:** With Jamf Pro, retrieve any file necessary for an investigation from a device when malicious activity is flagged

- **Data Collection:** Collect forensic data and standard device context data from a device with Jamf Pro when a threat is identified
- **Device/User isolation:** Automatically restrict device access to network resources with Jamf Pro or restrict user access to resources with Jamf Connect when malicious activity is identified
- **Device/User lockdown:** When a threat leaves a device in untrusted hands, automatically lock down the device with Jamf Pro or the user with Jamf Connect
- **Redeploy macOS:** Restore an untrusted device to a trusted state by remotely redeploying macOS and applications to the device via Jamf Pro
- **User Guidance:** Provide guidance and redirect users to training materials with Jamf Pro when suspicious activity is detected

Application control to minimize risk

Organizations need to ensure that users do not install applications that introduce risk to the environment or data. While Jamf Pro allows organizations to define a library of vetted applications to end users, security organizations often need to go further. With Jamf Protect, you can control:

- **Unwanted apps:** Prevent unwanted applications from executing on organizational devices
- **Prevent known threats:** Prevent known vulnerable versions of apps from executing
- **Unwanted developers:** Prevent applications from untrusted developers from executing

Monitoring activity for compliance and threat hunting

Mature security teams thrive off identifying malicious activity and cross-referencing data collected from multiple security tools. On the other hand, IT teams often share the responsibility to collect data required for compliance audits. In either case, a consistent flow of the right data from devices to central systems of record is necessary.

- **Activity visibility:** Collect file, process and authentication activity on Mac with minimal impact on the end-user experience
- **Device logs:** Forwards device log data (from the unified log in macOS) for off-device analysis
- **Data aggregation:** Centralize collected data in a SIEM or other system of record for cross-referencing or long term storage

Data control

As users and their devices become more mobile and dispersed, securing data is even more central to organizational success, and a greater focus on how data flows and ways that information may be leaving is essential.

- **Monitor USB device usage:** Capture USB device usage to ensure only approved devices are used
- **Control USB device usage:** Limit any device's ability to access USB storage devices with Jamf Pro
- **Monitor USB data activity:** Maintain visibility of file movement onto USB storage devices
- **Monitor Screenshot activity:** Identify any screenshots captured on devices by unapproved applications

Maintaining baseline security

Enabling basic OS hardening settings on devices has been standard practice as long as computer security has been considered. Modern security benchmarks were developed for various operating systems that are commonly shared by the industry. Deploying and maintaining these settings is now an issue of the past.

- **Monitor benchmarks:** Monitor device adherence to common security baseline configurations Jamf Pro deployed to your devices
- **Identify benchmark drift:** Quickly identify devices drifting from benchmarks
- **Reset benchmarks:** Reset security baselines on devices when necessary with Jamf Pro
- **File integrity monitoring:** Monitor changes to critical files

A better end-user experience

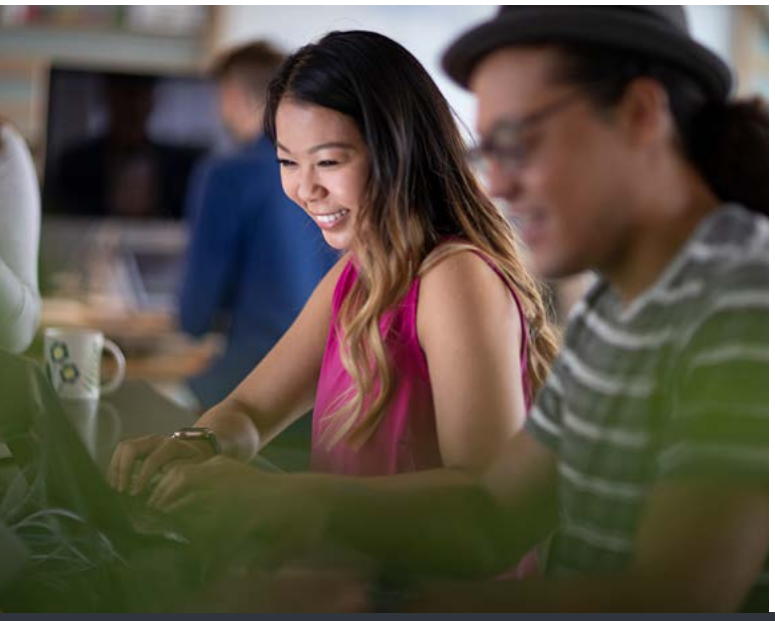
Mac users expect a smooth, stable and productive experience on their devices. Jamf Protect keeps the user in mind — minimizing impact while maintaining user privacy.

- **Native security frameworks:** Support the Endpoint Security Framework (ESF) for minimal end-user impact
- **No Kernel Extensions (Kext) required:** Jamf applications run in user mode to maximize stability and have no kernel mode components. System Extensions are leveraged when appropriate
- **Same-day support:** Jamf products support new macOS versions as they are released with no delay. Security and management tools should not be the reason to postpone OS updates or upgrades
- **Real-time prevention and detection:** Detect and prevent malicious activity in real time. Minimize device impact by not continuously scanning the system for dormant threats
- **Built for Mac:** Jamf is only for Apple. Jamf Protect identifies Mac attacks on Mac devices, not Windows threats that lie dormant on Mac

Ecosystem integration

Few organizations run only one security tool in their environment. It is critical that various tools integrate well, either technically or in processes, to maximize the efficiency of those responsible for device security.

- **SIEM:** Data and alerts can be pushed into your own SIEM
- **Azure Sentinel:** Ingest data and alerts from Jamf Protect directly into your Azure Sentinel instance
- **Custom data buckets:** Raw data and alerts can be pushed into your own AWS S3 bucket
- **General third-party support:** Data and alerts can be pushed into your SOARs and other systems directly from endpoints via JSON http endpoints
- **Role Based Access Control:** On a per-user basis, manage what resources each user of the Jamf Protect console can read, modify or be prevented from getting access to. Easily assign custom defined roles to users via the Jamf Protect console or by syncing group membership from Azure Active Directory



Jamf provides industry-leading security solutions for your Mac estate with extremely-high threat prevention and detection rates. Our solution is clean, intuitive, compatible with native Apple functionality and is highly effective at managing endpoint risks for our customers.

Unprecedented visibility. Industry-leading remediation capabilities. 100% Mac.

jamf

www.jamf.com

© 2002-2021 Jamf, LLC. All rights reserved.

To learn more about how Jamf helps you better protect your Mac endpoints and users, contact us.