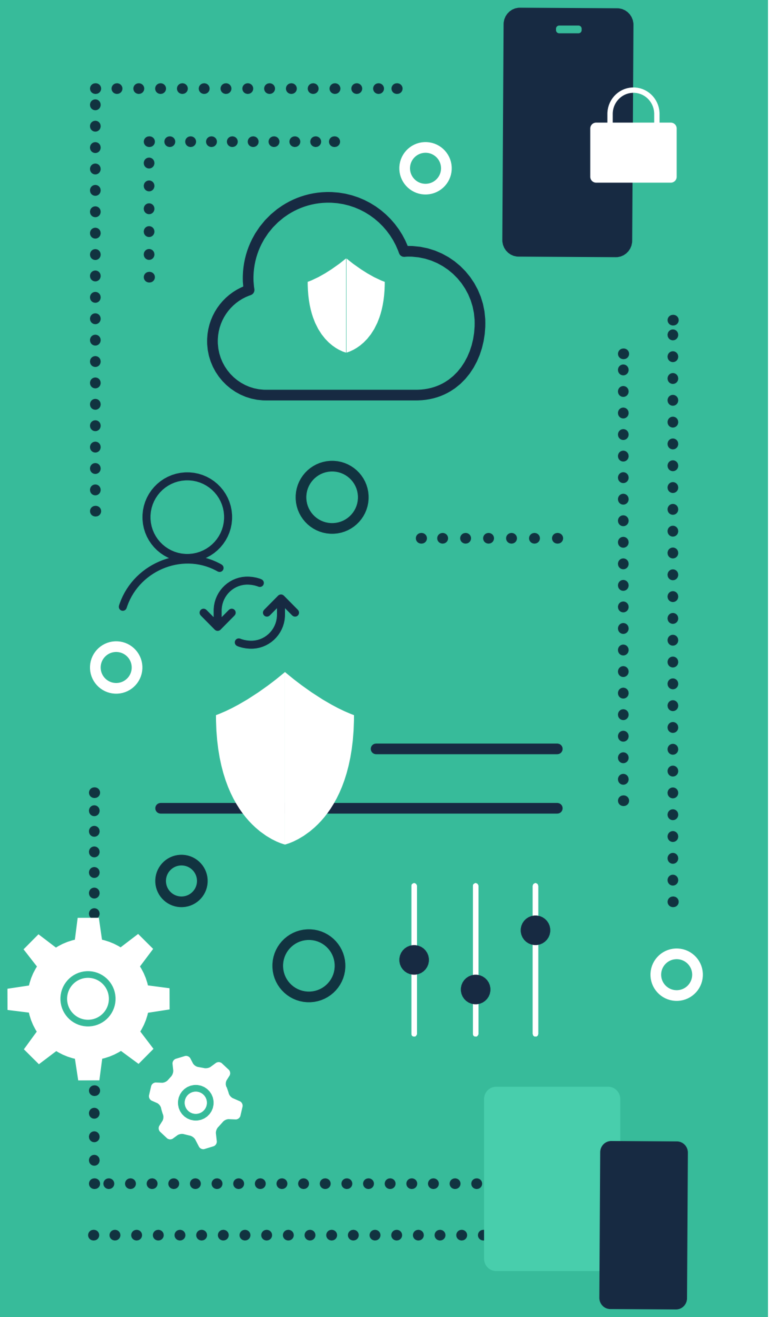


jamf

Mac Endpoint Protection

for Beginners

Native security isn't the end(point)

There's no doubt about it, Mac is the most secure out-of-box device on the market. What has been a decades-long truth still holds today. As organizations consider the makeup of their fleet, security solutions to protect data, devices and users are critical.

Complacency can lead to detrimental or high-cost breaches. With an endpoint protection solution that is made for Mac, IT and security teams can not only protect against known threats but also continue to adapt and anticipate future security needs of your organization.

Whether you are an enterprise with an Apple fleet or small business managing a handful of Mac devices, Jamf extends endpoint protection beyond what Apple provides as native functionality to work together to protect your macOS devices, organization's data and end users.

IN THIS GUIDE, WE'LL DISCUSS THE FOLLOWING:

- Mac endpoint protection entails
- Why endpoint protection designed for multiple operating systems is insufficient for Mac

ENDPOINT PROTECTION ON MAC:

Extend the security advantage native to Apple and prepare for the unknown.

As Mac continues to increase within enterprises, small business, schools and healthcare organizations, ensuring devices and data are used for legitimate purposes, correctly and by authorized users, is of increasing importance — enter Mac endpoint protection.

To accomplish this, many moving parts — identity management, patching, antivirus (AV), configuration, endpoint detection and response — work together to support your IT and security team's needs.

Learn more about managing corporate resources, data and users with our Identity Management for Beginners e-book.

IDENTITY AND ACCESS MANAGEMENT

Security measures implemented through identity management affect both end users and IT throughout the employee lifecycle, regardless of the on-site or remote work states. Zero Trust Network Access (ZTNA) solutions, virtual private networks (VPNs) and SaaS applications connect employees to enterprise resources all provide opportunities to harden your endpoint protection.

In an increasingly mobile workforce, with employees working from different locations on different devices, organizations need to be able to manage and secure those devices and their company information without the challenges of binding to on-premises Active Directory. Jamf Connect supports users from their first day of work through their last. A user can unbox their Mac, power it on and access all of their corporate applications after signing on with a single set of cloud-identity credentials. With Jamf Connect, organizations can monitor identity and access with minimal impact to end-user experience and enjoy consistent prioritization of device and data security.

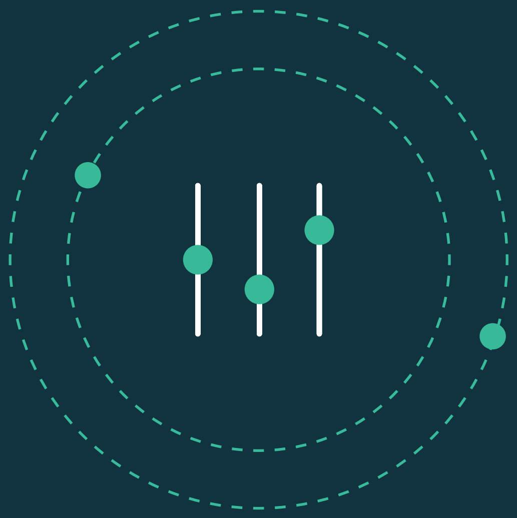
APP MANAGEMENT

Automated app management simplifies work and supports efficient, secured users.

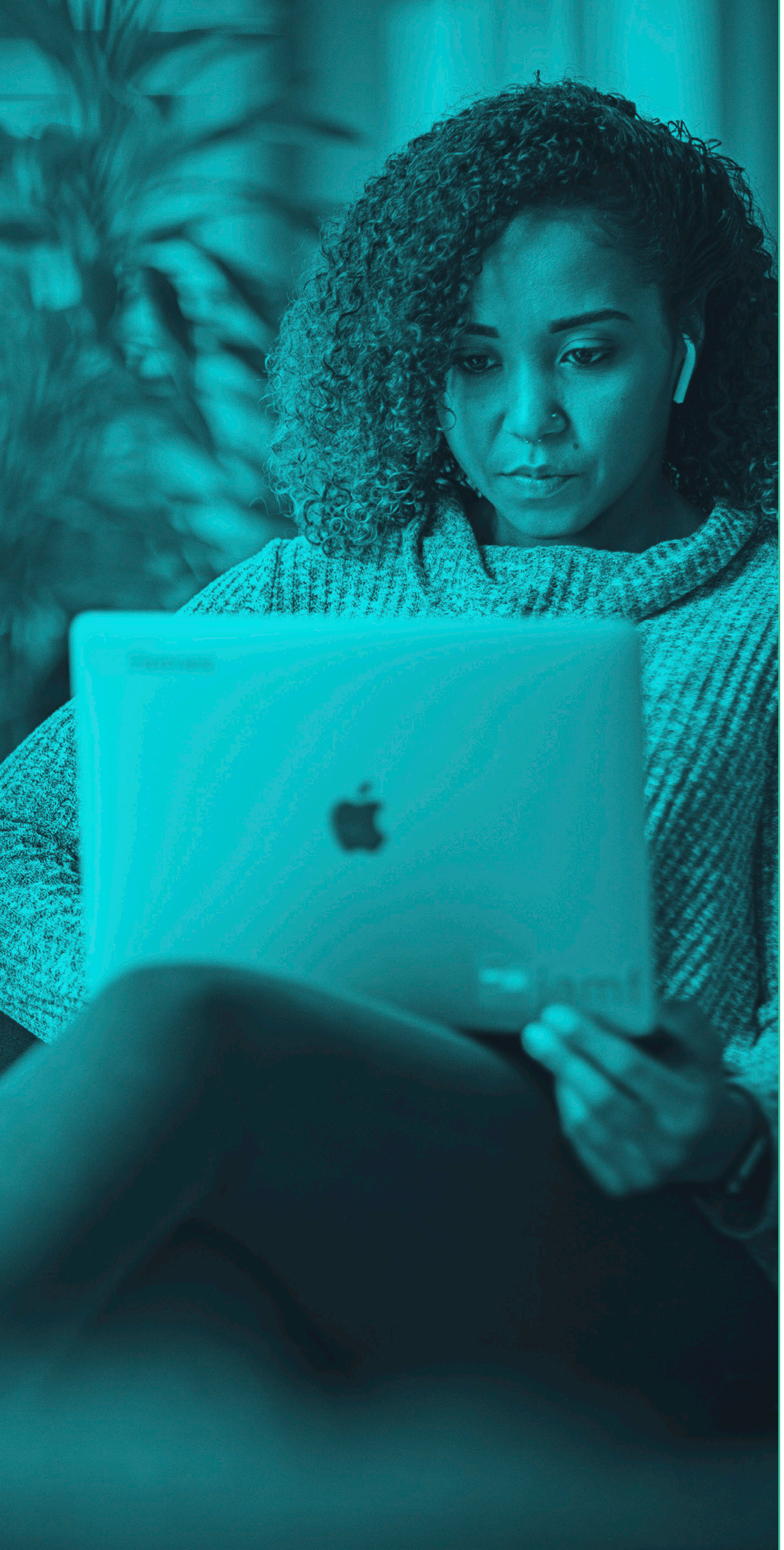
By ensuring users are getting the right apps through secured means, like Jamf Self Service or the Mac App Store:

- Apps can be deployed to the correct users and devices
- Custom titles and apps are available for users to get when they need them
- IT can push updates and set requirements that secure the organization and users

Integrate Jamf Pro with Apple Business Manager to assign and manage licenses of your organization's applications and software. Additionally, Jamf Pro can assist with patching and software updates. This also ensures you can update and manage any possible vulnerable software versions and maintain visibility of the status for your entire Mac fleet. Security patching should be done frequently and easily to ensure that any known app vulnerabilities are mitigated. With Jamf, streamline the work required to maintain or update applications on macOS and provide additional visibility for compliance and compatibility while delivering a quality end-user experience. This also means running the latest version of macOS as it's released to avoid gaps in security because of upgrade delays.



Security and management tools should not be the reason to postpone OS updates or upgrades. With Jamf, you are not held back by the solution, rather you're supported on new macOS versions the day they are released with no delay. Upgrade your devices on your schedule not ours.



ANTIVIRUS (AV)

AV may feel like a new need for Mac, but there is a new reality. Greater attention is being placed on Mac and macOS as its footprint in the enterprise expands.

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 adds sophisticated AV capabilities to prevent and quarantine Mac malware and goes far beyond what Windows-focused solutions are able to provide on macOS.

Organizations shouldn’t wait until malware, adware or other unwanted software issues arise. They need to implement AV that effectively identifies and remediates Mac-specific attacks without spending precious resources looking for threats to Windows on a Mac. Effective, efficient and comprehensive Mac AV capabilities are essential to both security and device experience. At the same time, any AV solution that interferes with your end user’s ability to be productive will only lead to annoyance for everyone involved. Jamf Protect is designed to protect macOS from malware without changing the experience end users expect from Mac.

Mac AV is no longer a nice to have, it’s a need to have. Not only do you need AV, you need built-for-Mac AV without the limitations that come from AV designed for cross-system usage.

CONFIGURATION

The out-of-box security standing for Mac is great — it's the best there is — but with the modern and ever-evolving threats in the cybersecurity landscape, it's not enough. You need to evaluate and evolve your security posture to protect your devices and data. And if hardening your security is easy, why aren't you doing it?

There is a substantial existing body of knowledge available and scripts already exist to do this within the security community.

With Jamf, it's easy to implement and execute on these and monitor for any users that attempt to modify these standards. Jamf removes the obstacles that have perhaps been holding you back from setting up a baseline security across your devices.

FileVault, enabling firewall and password requirements, setting screen saver and lock requirements all come into play for positioning your security requirements and benchmarks.

Don't know where to start? The Center for Information Security provides industry benchmarks and Jamf is CIS certified. So with Jamf, you're already on your way and we have resources to help you.

Learn more about CIS security benchmarks and Jamf with our macOS Security Checklist.

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. Instead, they attempt to force Windows models on Mac devices. With Jamf Protect's focus on Mac and macOS, Jamf minimizes false positives while maximizing the detection rates on Mac.

When pairing Jamf Protect with Jamf Pro, you are granted minimally intrusive remediation capabilities that go far beyond your average EDR capabilities. With Jamf, IT and security teams can set up a seamless incident response plan that allows your teams to work together.

JAMF IS ENDPOINT SECURITY.

Mac endpoint protection with Jamf Protect supports endpoint compliance, addresses anti-virus needs by preventing macOS malware, controls and secures Mac applications within the organization, and detects and remediates Mac-specific threats with minimal impact to the end-user experience.

And when paired with Jamf Pro, Jamf unlocks extensive automation, investigation and remediation capabilities to mitigate endpoint security risks, both large and small.

Request a free trial >

or contact your preferred Apple reseller when you're ready to harden your security.

Learn more about Jamf's endpoint protection capabilities.