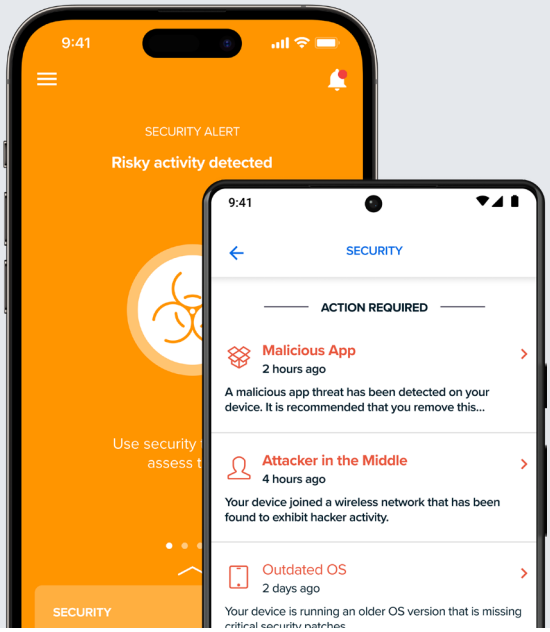
jamf | PROTECT

Protect mobile endpoints against modern threats.

Prevent cyber attacks, maintain endpoint compliance and identify and respond to active threats.



The modern workforce has adapted exceptionally well to hybrid and remote work environments.

As a result of this increased flexibility, more and more work is done on mobile devices. These devices store a vast amount of work and personal data and are always connected to the internet, making them a perfect target for cyber attackers. The mobile experience often makes it more difficult for users to spot suspicious attacks, so additional protections are critical to keeping users and work information safe.

Enter Jamf Protect

Jamf Protect is a purpose-built mobile threat defense solution that defends against mobile attacks, enforces acceptable use or data capping policies and provides clear visibility into device compliance. Protect all mobile devices used at work, whether personally or company-owned, to ensure that work resources remain safe.

Solve the unique challenge of securing mobile devices

Jamf Protect combines layers of security to protect users, endpoints and the network with the following capabilities:

Mobile endpoint security
Ongoing monitoring for various endpoint security checkpoints to ensure mobile devices meet your required security baseline.

Phishing protection
Advanced machine learning to block known and novel phishing attacks, crypto jacking and risky or malicious domains in real time before devices are impacted.

Web content filtering
Category-based content filtering to enforce acceptable use policies, which prevent users from accessing prohibited or risky content.

Jailbreak detection
Advanced scanning to determine if a mobile device has been rooted or modified, whether by end users or by malicious actors.

OS vulnerability reporting
Easily report on operating system vulnerabilities detected on macOS, iOS and iPadOS. Devices running a vulnerable operating system are flagged with an elevated risk status.

Application risk monitoring
Monitor for side-loaded apps, suspicious developer profiles, malicious code patterns, risky dynamic behavior and dangerous permissions.

Public Wi-Fi security
Prevent attackers from intercepting internet traffic that can put sensitive company information at risk.

Network Threat Stream
Gain a new level of visibility by streaming a variety of security data from iPhone, iPad and Android devices to Jamf or directly to your SIEM.

Data capping and reporting
Manage cellular data consumption on mobile devices. Prevent users from using excessive amounts of data domestically or while roaming to control costs and prevent unexpected overages.

Risk signaling
Comprehensive mobile security data informs each device's individual risk score, which can be used to inform zero trust access decisions with **Jamf Connect** and other Zero Trust Network Access (ZTNA) solutions.

Simple deployment
The Jamf Trust app can be deployed and configured through **Jamf Pro** — or any modern mobile device management (MDM) solution — making comprehensive mobile endpoint security accessible to any organization.

Jamf Protect is backed by Jamf Threat Labs: a team of experienced threat researchers, cybersecurity experts and data scientists that investigate the future of security threats to continuously build up the security capabilities of Jamf products.

jamf

www.jamf.com

Updated 06/2023.

Request a trial to learn more about securing mobile endpoints with Jamf Protect.

Or contact your preferred reseller.