jamf

Protect mobile endpoints against modern healthcare threats.

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

The frontline of care has rapidly expanded beyond the facility walls. So have the risks to sensitive healthcare and patient data.

Healthcare mobility has surged. Whether it is for facility, telehealth or in-the-field use, mobile devices offer apps that help to drive and streamline outcomes. They access a vast amount of protected health information (PHI), making them a perfect target for cyber attackers. And it's sometimes harder for mobile users to spot attacks, which makes additional protections critical.

According to IBM, the healthcare industry experiences the most costly data breaches, which has increased by 58% since 2020. An average incident costs nearly $11 million. Healthcare continues to see an increase in ransomware attacks, and is the top targeted sector. Mobile devices increase risk; the Department of Health & Human Services in the US has created a mobile device security checklist healthcare organizations to follow.

Enter Jamf Mobile Security

A purpose-built mobile security solution that defends against mobile attacks, enforces acceptable use or data capping policies and provides clear visibility into device compliance, as well as providing real-time conditional access for any app. Protect devices used for clinical workflow, telehealth and more – whether personally or company-owned – to ensure that business resources and sensitive patient health information (PHI) data remains safe.

Solve the unique challenge of securing mobile devices in healthcare.

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

Mobile endpoint security

Ongoing monitoring for endpoint security checkpoints to ensure mobile devices meet your required security baseline. Mobile fleet auditing to prove compliance with healthcare industry standards like HIPAA and GDPR.

Phishing protection

Advanced machine learning to block known and novel phishing attacks, cryptojacking and risky or malicious domains before devices are impacted. Key for providers using cellular devices, regardless of ownership.

Web content filtering

Category-based content filtering to enforce acceptable use policies. This prevents patients and providers from viewing prohibited or risky content. Valuable for shareduse patient tech— especially in pediatrics.

Jailbreak detection

Advanced scanning to determine if a mobile device has been rooted or modified, whether by end users or by malicious actors. This is especially important for devices accessing PHI or PII.

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 reporting & risk monitoring

Monitor for side-loaded apps, suspicious developer profiles, malicious code patterns, risky dynamic behavior and dangerous permissions. View and report on per device app usage across the entire mobile fleet.

Public Wi-Fi security

Prevent attackers from intercepting internet traffic that can put sensitive business, financial, or PHI at risk. Important for guest networks used by patients and families within inpatient facilities.

Network threat stream

Gain a new level of visibility: stream security data from iPhone, iPad and Android devices to Jamf, or directly to your SIEM.

Data capping and cellular usage

Prevent doctors, clinicians, or patients from using excessive amounts of data to control costs and prevent unexpected overages with data caps. View granular cell usage reports to understand which apps are consuming data and where devices are connecting from by country or region.

Risk signaling

Comprehensive mobile security data informs each device's individual risk score, which informs zero-trust access decisions. Block access to clinical apps and systems if a device is compromised.

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 healthcare organization.

Continuous conditional access

Jamf uses risk-aware access policies and per-app connections, delivering zero trust access to the work apps and data that employees need to be productive on their mobile device.

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 09/2024.

Request a trial to learn more about securing mobile endpoints in your healthcare organization.

Or contact your preferred reseller.