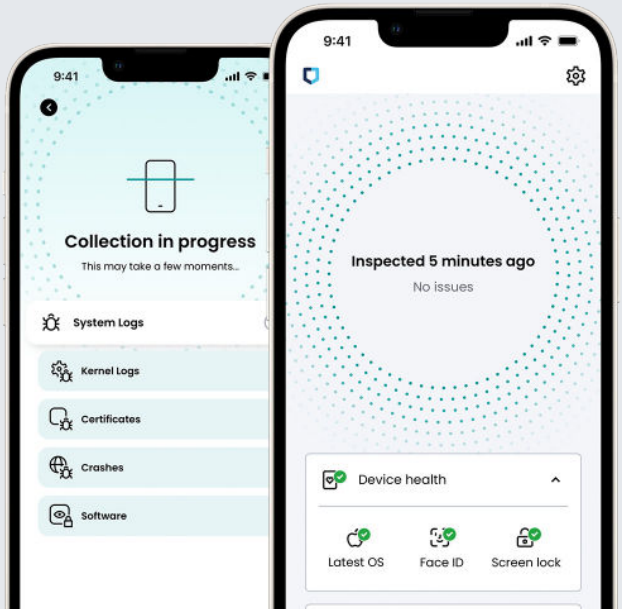
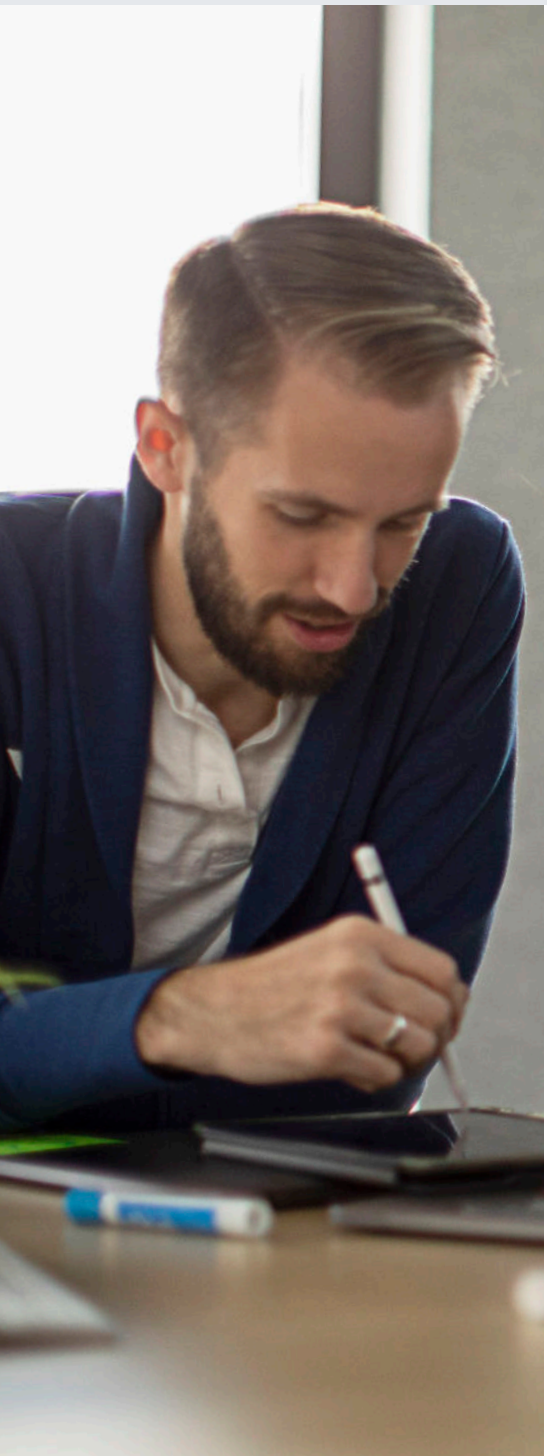
jamf

Jamf Executive Threat Protection

Mobile attacks are finally visible.





Mobile devices are used for various work and personal tasks throughout the day, especially as remote and hybrid work has established themselves as the norm for many organizations. Apps put everything from emails to meetings one tap away in the palm of your hand. Smartphones often contain work and personal data and are always connected to the internet, which makes them an ideal target for hackers.

Attacks come in a variety of forms, with the most dangerous zero-click, zero-day exploits remotely accessing everything on a device — from business applications and multi-factor authentication (MFA) requests to photos and notes. Some exploits can even silently activate the camera and microphone. It's important to have the tools to understand the moment a device is compromised so you can take action to remediate the threat.

jamf | PROTECT

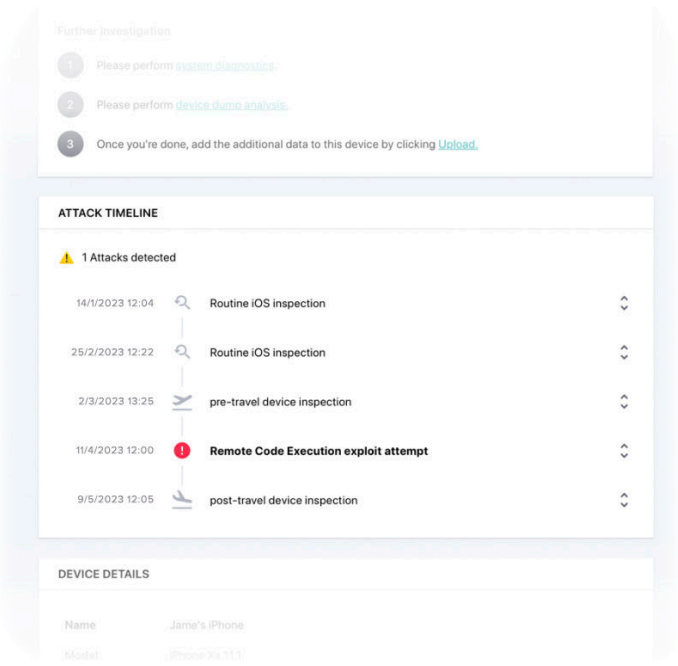
Jamf Executive Threat Protection is an advanced detection and response solution that gives organizations a sophisticated, remote method to know what has happened on their mobile devices and the tools to respond to advanced attacks.

Deep collection

Gain extended visibility into your mobile fleet from anywhere with rich mobile endpoint telemetry and reduce manual investigation time from weeks to minutes. Go beyond MDM to collect system logs to support comprehensive investigations.

Detect and destroy sophisticated mobile attacks.

Jamf Executive Threat Protection goes beyond management and security to extend visibility into attacks that target your most important users.



Detect faster

Even the most sophisticated attacks leave a data trail, but you need to know what to look for. Jamf performs deep analysis to identify indicators of compromise (IOC) and straightforwardly presents these advanced detections to security teams. Where sophisticated zero-day attacks would otherwise remain hidden, Jamf Executive Threat Protection shines a spotlight.

Remediate confidently

Automatically construct a timeline of suspicious events that shows when and how a device was compromised. Built-in response tools allow security teams to destroy advanced persistent threats (APT) and keep users safe while ongoing monitoring assures that the threat is eliminated.

Gain extended visibility into your mobile fleet with sophisticated analysis and curated insights from Jamf Threat Labs researchers. Get started today.

jamf

www.jamf.com

Learn more on jamf.com

IMAGETEXT IT SPECIALISTS