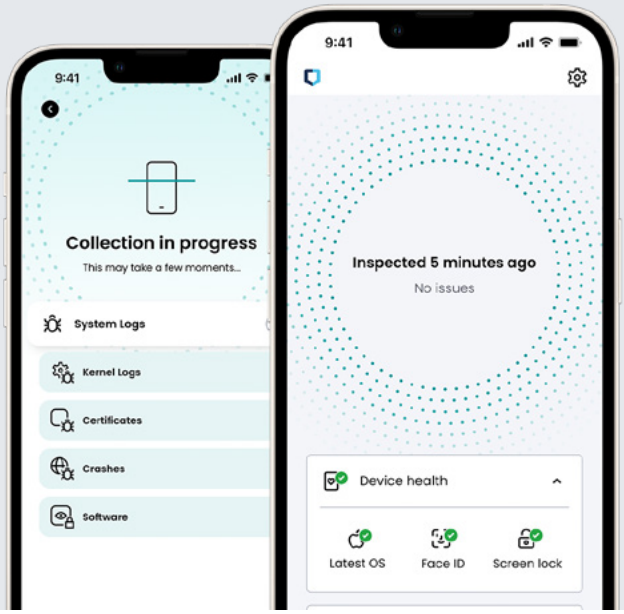
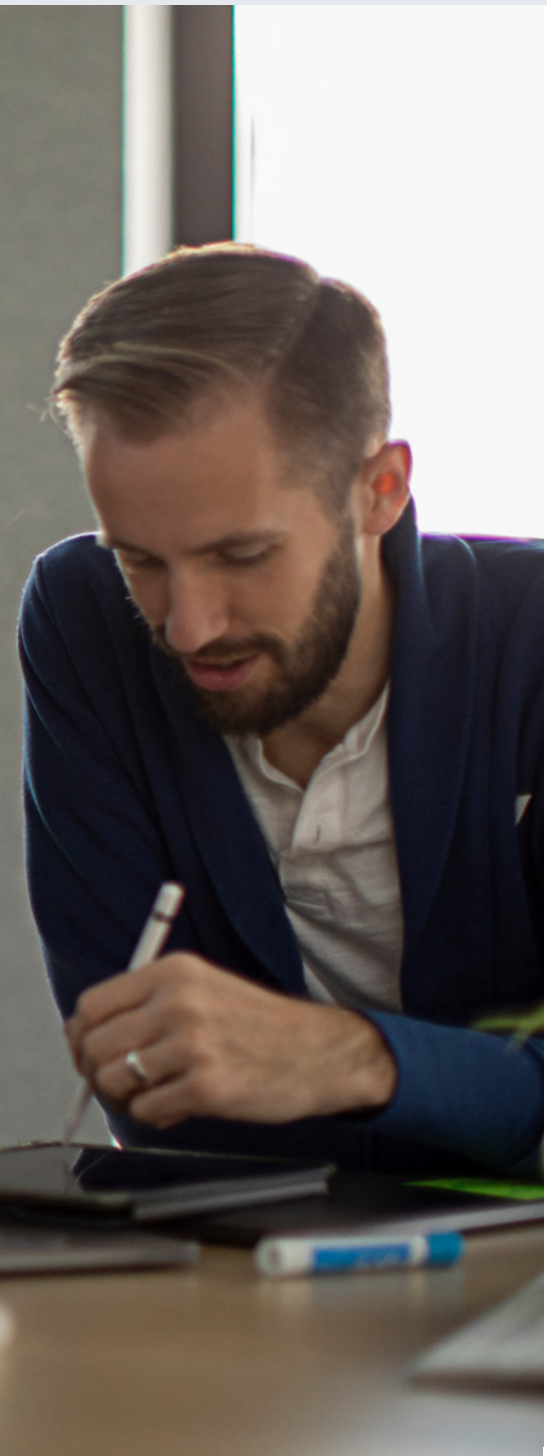
jamf

Jamf Executive Threat Protection

Mobile Angriffe sind endlich sichtbar.





Mobile Geräte werden den ganzen Tag über für verschiedene berufliche und private Aufgaben genutzt, zumal sich Remote- und Hybridarbeit in vielen Unternehmen als Norm etabliert hat. Mit Apps können Sie alles, von E-Mails bis hin zu Besprechungen, mit einem Fingertipp in Ihrer Handfläche erledigen. Smartphones enthalten oft berufliche und persönliche Daten und sind ständig mit dem Internet verbunden, was sie zu einem idealen Ziel für Hacker*innen macht.

Die gefährlichsten Zero-Click- und Zero-Day-Exploits greifen aus der Ferne auf alles auf einem Gerät zu - von Geschäftsapps und Anfragen zur Multi-Faktor-Authentifizierung (MFA) bis hin zu Fotos und Notizen. Einige Exploits können sogar die Kamera und das Mikrofon unbemerkt aktivieren. Es ist wichtig, über Tools zu verfügen, die erkennen, wann ein Gerät gefährdet ist, damit Sie Maßnahmen zur Beseitigung der Bedrohung ergreifen können.

Jamf Executive Threat Protection

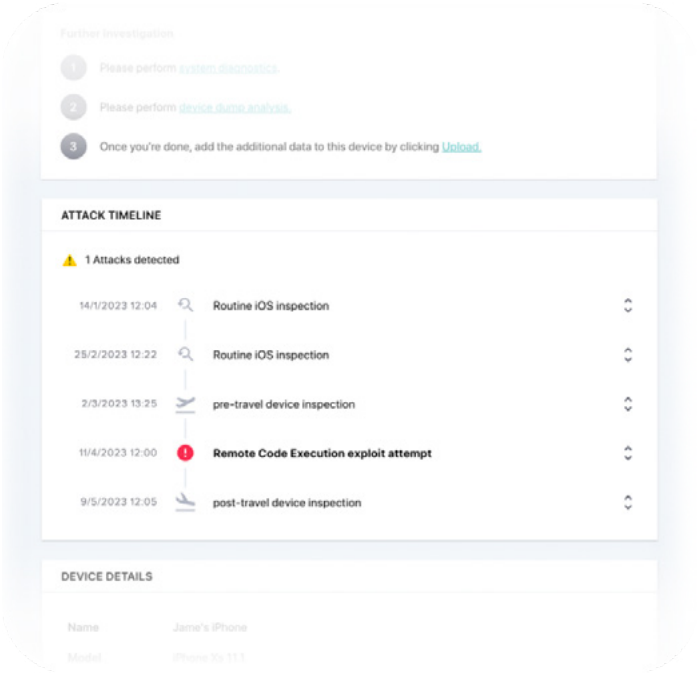
Jamf Executive Threat Protection ist eine fortschrittliche Erkennungs- und Reaktionslösung, die Unternehmen eine ausgefeilte Remote-Methode an die Hand gibt, mit der sie wissen, was auf ihren mobilen Geräten passiert ist, und die ihnen die Möglichkeit gibt, auf fortschrittliche Angriffe zu reagieren.

Tiefe Sammlung

Verschaffen Sie sich mit der umfassenden Telemetrie mobiler Endgeräte von jedem Ort aus einen umfassenden Überblick über Ihre mobile Flotte und reduzieren Sie die manuelle Untersuchungszeit von Wochen auf Minuten. Erfassen Sie über MDM hinaus Systemprotokolle, um umfassende Untersuchungen zu unterstützen.

Erkennen und zerstören Sie ausgeklügelte mobile Angriffe.

Jamf Executive Threat Protection geht über die Verwaltung und Sicherheit hinaus und bietet mehr Transparenz bei Angriffen, die auf Ihre wichtigsten Benutzer*innen abzielen.



Schneller erkennen

Selbst die raffiniertesten Angriffe hinterlassen eine Datenspur, aber man muss wissen, worauf man achten muss. Jamf führt tiefgreifende Analysen zur Identifizierung von Kompromissindikatoren (Indicators of Compromise, IOC) durch und präsentiert diese fortschrittlichen Erkennungen direkt den Sicherheitsteams. Wo ausgeklügelte Zero-Day-Angriffe sonst im Verborgenen bleiben würden, bringt Jamf Executive Threat Protection Licht ins Dunkel.

Selbstbewusst nachbessern

Erstellt automatisch eine Zeitleiste mit verdächtigen Ereignissen, aus der hervorgeht, wann und wie ein Gerät kompromittiert wurde. Integrierte Reaktionstools ermöglichen es den Sicherheitsteams, fortschrittliche anhaltende Bedrohungen (Advanced Persistent Threats, APT) zu zerstören und die Sicherheit der Benutzer*innen zu gewährleisten, während die fortlaufende Überwachung sicherstellt, dass die Bedrohung beseitigt wird.

Verschaffen Sie sich einen erweiterten Überblick über Ihre mobile Flotte mit ausgefeilten Analysen und kuratierten Erkenntnissen der Forscher*innen von Jamf Threat Labs. Beginnen Sie noch heute.

jamf

www.jamf.com/de

Erfahren Sie mehr auf **jamf.com/de**