jamf

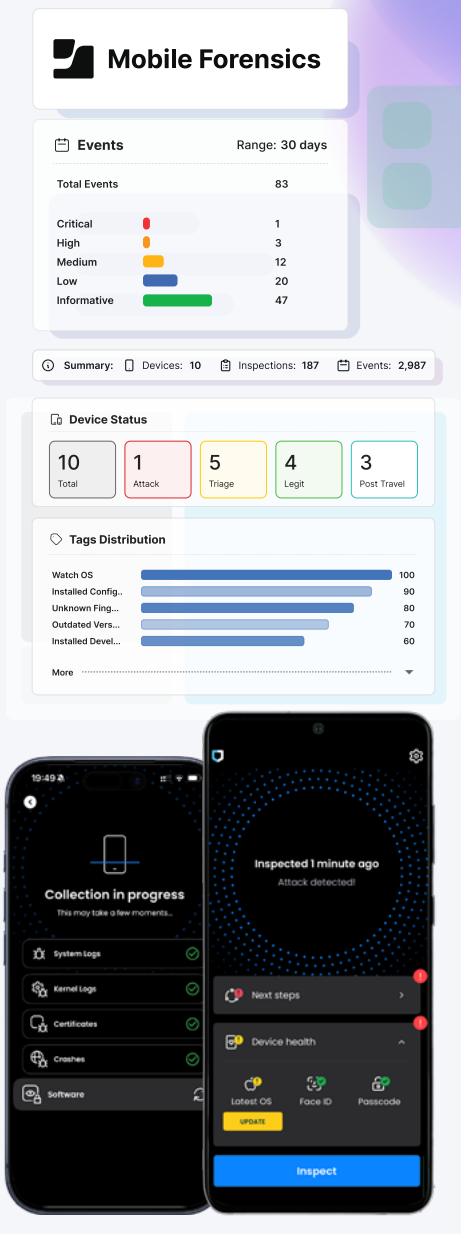


Jamf Mobile Forensics

Schützen Sie mobile Geräte vor hochentwickelten Cyberangriffen.

Benutzer mit hohem Risiko: Regierungsbeamte, Führungskräfte aus der Wirtschaft, Politiker und andere wichtige Personen **sind Gefahren ausgesetzt, die handlungsfähige Abwehrstrategien erfordern**. Angesichts von APTs, Söldner-Spyware und staatlichen Cyberattacken ist eine permanente Analyse der Geräteintegrität unerlässlich. Sicherheitsteams müssen Indicators of Compromise (IOCs) sichtbar machen, ohne die Arbeit der Benutzer zu unterbrechen oder den Datenschutz durch invasive Software oder die Offenlegung von personenbezogenen Daten zu gefährden.

Jamf Mobile Forensics ergänzt die Verteidigung gegen mobile Bedrohungen um eine entscheidende Ebene: Sie hilft Sicherheitsteams dabei, selbst jene Gefahren aufzuspüren und zu untersuchen, die herkömmlichen Tools verborgen bleiben.



Die wichtigsten Vorteile:

- Erkennen Sie gezielte Angriffe und Zero-Days, bevor sie in das Netzwerk eindringen
- Analysieren Sie tiefgreifende System-, Absturz-, Kernel- und Anwendungsprotokolle, ohne das Gerät zu rooten oder zu jailbreaken
- Vereinfachen Sie die forensische Analyse und reduzieren Sie die manuelle Recherche
- Schützen Sie die Privatsphäre und stärken Sie das Vertrauen in die Gerätesicherheit Ihrer Benutzer mit hohem Risiko

Exploitationskette bei Mobilgeräten

Wie die Exploitationskette bei Mobilgeräten von dem Erstzugriff bis zur Post-Exploitation verläuft:

Schädlicher Anhang / WebKit-Exploit → Erstzugriff → Codeausführung (Kompromittierung des WebContent-Prozesses) → Rechteausweitung → Tarnung / Evasion → Post-Exploitation-Aktivität (Datenerfassung, Mikrofon-/Kamerazugriff etc.) → C2-Kommunikation → Bereinigung / Anti-Forensik

Die Analyse von Bedrohungen und der Exploitationskette hilft Sicherheitsteams zu verstehen, was passiert ist und wie sie reagieren müssen. Jamf Mobile Forensics bietet Ihnen diese Transparenz.

Reduzieren Sie die forensische Analyse von Mobilgeräten von Wochen auf Minuten.

Digitale Forensik aus der Ferne und Reaktion auf Zwischenfälle

Reduzieren Sie Ausfallzeiten und halten Sie kritische Benutzer produktiv

- Proprietäre Verhaltensanalysen erkennen anomale Gerätezustände, Zero-Day-Exploits und IOCs für Pegasus, Predator sowie weitere Spyware
- Verhindern Sie eine langfristige Gefährdung durch die gezielte Untersuchung von Telemetriedaten auf Geräteebene
- Sofortige Analyse ermöglicht es Sicherheitsteams, die erforderlichen Schritte zu verstehen und sofort auf fortgeschrittene Angriffe zu reagieren

Proaktive Bedrohungssuche

Umwandlung komplexer Sicherheitsdaten in verwertbare Informationen

- Vereinfachen Sie Untersuchungsprozesse, indem Sie Ereigniszeiträume, Typen und Schweregrade in zentralen Vorfällen zusammenfassen
- Automatisieren Sie Ereigniszeiträume, um direkt zu prüfen, wie und wann ein Gerät kompromittiert wurde
- Erkennung unbekannter IOCs durch die Analyse von Dateien, Apps, Prozessen, Absturzprotokollen und mehr

Menschliche Expertise, unterstützt durch KI-basierte Analyse

Die KI-Analyse fungiert als forensischer Forschungsassistent

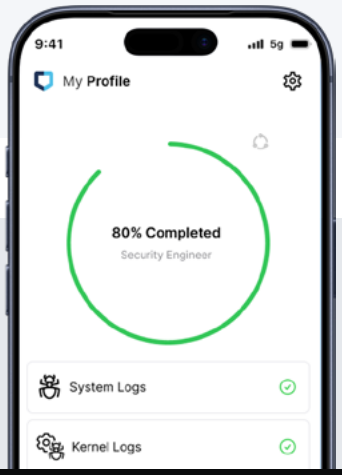
- Reduziert den manuellen Aufwand für die Analyse von Geräteabstürzen und Anomalien
- Fasst die Vorfälle zusammen und empfiehlt die nächsten Schritte zur Problemlösung
- Die KI-Analyse ist standardmäßig deaktiviert, so dass die Unternehmen die Kontrolle über die KI-Nutzung behalten

** Die KI-Analyse ist eine reine Cloud-Funktion.*

Forensik nach dem Prinzip „Privacy by Design“

Lückenloser Schutz für Benutzer – von der Privatsphäre bis zur Geräteintegrität

- Keine personenbezogenen Daten nötig. Für die Analyse ist kein Zugriff auf Kennwörter, Fotos, Videos, Nachrichten, Kontakte, Anruf- und Browserverläufe, Token für die Zwei-Faktor-Authentifizierung oder Anwendungsdaten erforderlich.
- Die DFIR-App führt in organisatorisch festgelegten Intervallen stille Scans durch und versorgt die Benutzer mit Informationen zur Gerätesicherheit



Jamf Mobile Forensics wird von **Jamf Threat Labs** unterstützt, unserem Team von Sicherheitsforschern, Analysten und Entwicklern, die Forschungsergebnisse zu mobiler Malware und Spyware veröffentlichen und die Jamf Mobile Forensics-Engines kontinuierlich weiterentwickeln.

jamf

www.jamf.com/de/

© 2026 Jamf, LLC. Alle Rechte vorbehalten.

Wenden Sie sich an Ihren Jamf Representative, wenn Sie weitere Informationen benötigen. Oder fordern Sie eine Testversion an.