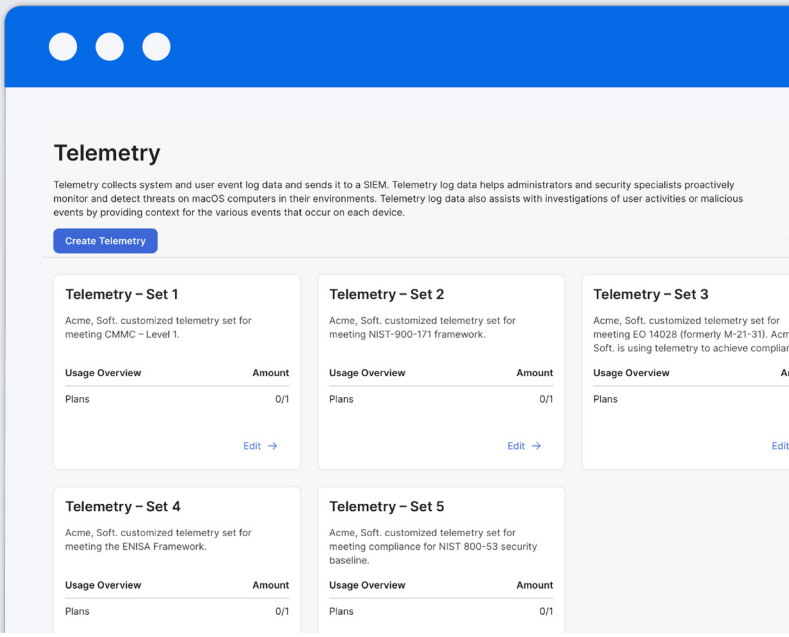
jamf

Mac **Endpoint-Telemetrie**

Wichtige Infos zu Ihren Macs
von unseren Apple Experten.



Mit der zunehmenden Nutzung von Macs am Arbeitsplatz steigt auch das Interesse und die Aufmerksamkeit bei den Cyberkriminellen.

Um die gleichen Standards in Bezug auf Compliance, Sicherheit und Betrieb zu erfüllen wie andere Plattformen, benötigen Macs spezifische Sichtbarkeits- und Schutzmaßnahmen.

Speziell entwickelte Endpoint-Telemetrie für Mac von Jamf

Diese Telemetrie basiert auf der Endpoint Security API von Apple und wurde von unserer Apple-Expertise von über 20 Jahren kuratiert. Sie ermöglicht eine detaillierte Überprüfung der macOS-Aktivitäten. Und sie liefert korrelierte, vollständig nachvollziehbare Erkenntnisse, die in die Lösungen einfließen, mit denen die Sicherheitsteams täglich arbeiten.

Wichtige Vorteile:

- Einhaltung komplexer gesetzlicher Rahmenbedingungen und Sicherheitsgrundlagen
- Beschleunigte Reaktion auf Vorfälle durch Rekonstruktion detaillierter zeitlicher Abfolgen der Angriffe
- Suche nach fortschrittlichen macOS-Bedrohungen, Verkürzung der Reaktionszeiten und Verbesserung der Widerstandsfähigkeit
- Nahtlose Integration in SIEM-Integrationen, die mit führenden Sicherheitsanbietern entwickelt wurden

Nutzen Sie die Daten aus den Vorfällen.

Endpoint-Telemetrie der nächsten Generation

Speziell entwickelt für moderne Compliance-, Sicherheits- und IT-Anforderungen

- **Zuverlässige Telemetriedaten**, die direkt von Apples macOS Endpoint Security API stammen
- **Nahtlose Integration** in die macOS Sicherheitsarchitektur sorgt für manipulationssichere Daten mit hoher Integrität
- **Schlankes Design**, das das Nutzererlebnis bewahrt und gleichzeitig eine detaillierte Sichtbarkeit über die kritischen Endpoint-Aktivitäten bietet

Unvergleichliche macOS Sichtbarkeit

Sie erhalten tiefere Einblicke in Ihre Mac Flotte als je zuvor

- **Sie können alle Aktivitäten** überprüfen: Prozessausführung, Authentifizierung, privilegierte Aktionen, Nutzerzugriff und -erhebungen, Persistenz, integrierte Sicherheitsereignisse und **mehr**
- **Das auf macOS fokussierte Datenmodell** liefert spezifische Daten für Compliance-Audits, Bedrohungserkennung und Nachforschungen auf Apple Geräten
- **Maßgeschneiderte Informationen:** Unser auf macOS fokussiertes Datenmodell liefert spezifische Daten für Compliance-Audits, Bedrohungserkennung und Nachforschungen auf Apple Geräten

Beschleunigte Nachforschungen

Von Apple Experten entwickelte Telemetrie für macOS-Bedrohungen

- **Rekonstruktion der zeitlichen Abfolge von Vorfällen** mit nachvollziehbaren Prozessdaten und umfassender Korrelation der Telemetrie
- **Erkennung von Angreifern** anhand von Informationen zu Anomalien, seltenen Ereignissen und bevorzugten macOS-Angriffstechniken wie „living-off-the-land“
- **Schnelle Sicherheitsentscheidungen** mit granularen, kontextbezogenen Telemetriedaten, die eine schnelle Nachforschung und Reaktion ermöglichen

Mühelose Integration

Einführung innerhalb von Minuten, nicht Wochen

- **Holen Sie mehr** aus Ihren SIEM-Lösungen heraus mit Plug-and-Play-Support für Splunk, Microsoft Sentinel, Elastic, Google Security Operations und weitere SIEMs
- **Reduzieren Sie die Belastung Ihres Teams** mit Parsern, die speziell für macOS-Bedrohungsszenarien entwickelt wurden und die Telemetriedaten an das Datenmodell Ihres SIEMs anpassen
- **Sicherstellung einer nahtlosen Implementierung** mit umfassender Dokumentation für Sicherheits- und IT-Teams

Durch Jamf erhalten Sie vollständige Transparenz über Ihre Mac Endpoints.

Die Mac Endpoint-Telemetrie wird von Jamf Threat Labs unterstützt: einem Team aus erfahrenen Bedrohungsforschern, Cybersicherheitsexperten und Datenwissenschaftlern, das die Zukunft der Sicherheitsbedrohungen erforscht.

jamf

www.jamf.com/de/

Wenden Sie sich an Ihren Jamf Representative, wenn Sie weitere Informationen benötigen. **Testversion anfordern.**

Oder wenden Sie sich an Ihren bevorzugten Partner.