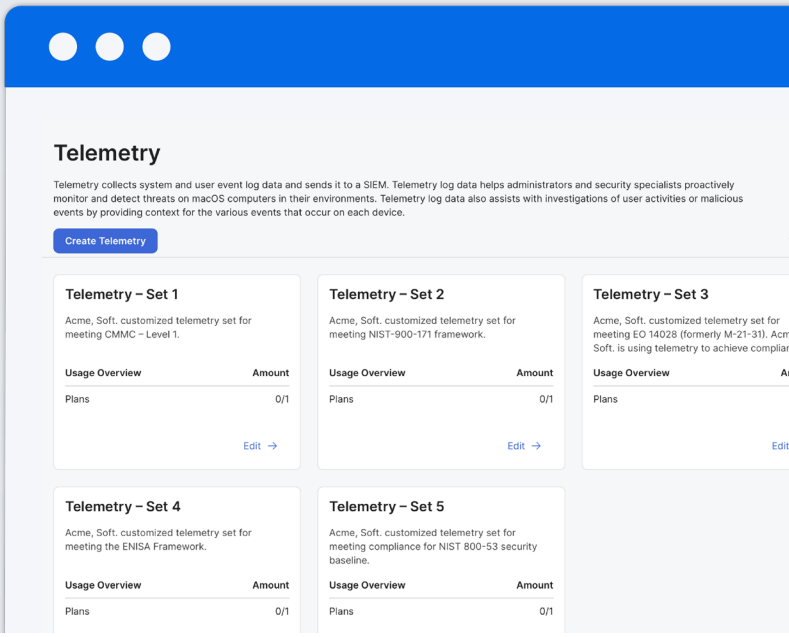
jamf

Mac **Endpoint Telemetry**

Actionable insights into your Macs by the Apple experts.



As Mac use has grown in the workplace, so has the interest and attention of bad actors.

To meet the same compliance, security and operational standards as other platforms, Macs require tailored visibility and defenses.

Endpoint Telemetry purpose-built for Mac, from Jamf

Powered by Apple's Endpoint Security API and curated by Jamf's 20+ years of Apple expertise, this telemetry enables in-depth auditing of macOS activity. It delivers correlated, fully traceable insights–streamed to the solutions security teams use daily.

Key Benefits:

- Achieve compliance with complex regulatory frameworks and security baselines
- Accelerate incident response by reconstructing detailed attack timelines
- Hunt for advanced macOS threats, reduce dwell time and enhance resilience
- Seamless adoption with SIEM integrations built with leading security vendors

Turn event data into action.

Next-generation endpoint telemetry

Purpose-built for modern compliance, security and IT needs

- **High-fidelity telemetry** sourced directly from Apple's macOS Endpoint Security API
- **Seamless integration** with macOS security architecture delivers tamper-resistant, high-integrity data
- **Lightweight by design**, preserving user experience while offering granular visibility into critical endpoint activity

Unparalleled macOS visibility

Gain deeper insight into your Mac fleet than ever before

- **Audit every angle** for activity like process execution, authentication, privileged actions, user access and elevations, persistence, built-in security events and **more**
- **macOS-focused data model** delivers insights tailored to compliance auditing, threat detection, and investigations on Apple devices
- **Tailored insights:** our macOS-focused data model delivers insights tailored to compliance auditing, threat detection and investigations on Apple devices

Accelerated investigations

Telemetry built by Apple experts for macOS threats

- **Reconstruct incident timelines** with traceable process heritage and comprehensive telemetry correlation
- **Detect attackers** using insights into anomalies, rare events and favored macOS attack techniques like living-off-the-land
- **Fast-track security decisions** with granular, contextualized telemetry that empowers rapid investigation and response

Effortless integrations

Adoption in minutes, not weeks

- **Gain more** from your SIEM solutions with plug-and-play support for Splunk, Microsoft Sentinel, Elastic, Google Security Operations and other SIEMs
- **Reduce team burden** with purpose-built parsers designed with macOS threat scenarios in mind, aligning telemetry to your SIEM's data model
- **Ensure seamless implementation** with extensive documentation for Security and IT teams

Gain complete visibility into your Mac endpoints with Jamf.

Mac endpoint telemetry is backed by Jamf Threat Labs: a team of experienced threat researchers, cybersecurity experts and data scientists that investigate the future of Apple security threats.

jamf

www.jamf.com

© 2025 Jamf, LLC. All rights reserved.

To learn more, reach out to your Jamf Representative.

Request a trial.

Or contact your preferred reseller.