![jamf logo]

Jamf enhances endpoint telemetry for Mac to support investigations, analysis, and high compliance requirements

December 15, 2022

Jamf Protect now includes powerful telemetry data and offline mode for non-cloud workflows

MINNEAPOLIS, Dec. 15, 2022 (GLOBE NEWSWIRE) -- Today, Jamf (NASDAQ: JAMF), the standard in managing and securing Apple at work, rolled out new updates to Jamf Protect to address requirements outlined in the new Executive Order 14028, Improving the Nation's Cybersecurity. These updates make Jamf Protect a more powerful macOS security solution for organizations with high compliance requirements, such as government agencies.

"At Jamf, our mission is to bridge the gap between what Apple provides and what the enterprise requires. Today, we're excited to announce these updates to Jamf Protect, which empower security teams with the rich audit telemetry they require, while adhering to the strictest data handling requirements for organizations with high compliance needs," said Michael Covington, Vice President of Portfolio Strategy, Jamf.

Key enhancements to Jamf Protect announced today include:

Endpoint telemetry for compliance with auditing standards
Jamf Protect now collects critical data necessary for incident investigation to meet the most stringent logging and auditing standards, including those outlined in the new Executive Order 14028 (EO M-21-31). This added capability gives organizations the tools required to capture required endpoint telemetry and stream that data to customer-owned data repositories and SIEMs. This capability, previously included in Jamf's Compliance Reporter, is now available to all Jamf Protect endpoint security customers.

Robust security telemetry for threat hunting
Rich telemetry, including system data, threat detection logs, and network traffic details, empowers security admins to monitor and threat hunt on macOS computers in their environments. Threat hunters will be able to analyze macOS activity logs in near real-time using a single endpoint agent.

Endpoint telemetry with offline mode
Jamf Protect's new offline deployment mode is for customers with high compliance requirements. This deployment model for streaming telemetry data provides an option for organizations that must meet the strictest standards of data collection for internal auditing and require non-cloud-based services.

With these updates, Jamf Protect provides the essential building blocks required to achieve the highest standard of macOS security, all in one platform, including:

- Best-of-breed malware protection
- Integrated network threat prevention and content filtering
- Endpoint telemetry that enables investigations, analysis, and proactive threat hunting
- Integrated compliance reporting
- Offline mode to support non-cloud workflows

Jamf Protect uses native Apple frameworks to deliver a robust endpoint security solution while maintaining the great Apple experience users desire. To learn more about Jamf Protect, visit: www.jamf.com/products/jamf-protect.

About Jamf
Jamf's purpose is to simplify work by helping organizations manage and secure an Apple experience that end users love and organizations trust. Jamf is the only company in the world that provides a complete management and security solution for an Apple-first environment that is enterprise secure, consumer simple and protects personal privacy. To learn more, visit www.jamf.com.

Media Contact:
Liarna La Porta | media@jamf.com

Investor Contact:
Jennifer Gaumond | ir@jamf.com