Beacon by Jamf Threat Labs · FAQ

This FAQ addresses some common data use and privacy questions that customers may have about the Beacon by Jamf Threat Labs service. This FAQ is for informational purposes only, is not legal advice, and will not become part of your contract with Jamf. Capitalized terms used, but not defined in this FAQ, are defined in the Jamf Software License and Services Agreement ("SLASA").

1. **What is Beacon by Jamf Threat Labs?**

   Beacon by Jamf Threat Labs is a managed threat hunting service that layers expert human analysis on top of your existing Jamf for Mac + Jamf Protect deployment. Jamf's Professional Services team sets it up; Jamf Threat Labs analysts deliver the ongoing service.

2. **What data does Beacon collect from my devices?**

   Beacon operates through Jamf Protect, which is already installed on your managed Mac fleet. Threat Labs analysts work with Telemetry Data. No additional agent is deployed on your Devices specifically for Beacon.

   The focus is security-relevant Telemetry Data. Jamf collects the minimum data needed to provide the Product Offerings, and customers decide what Customer Content, which may include Personal Data, flows into Jamf Pro (for example, whether Devices carry user-linked names or anonymous inventory identifiers).

   ↗ Jamf Privacy principles — Trust Center

3. **Does Beacon collect or access on-Device Personal Data of end users?**

   No. Beacon is scoped to security Telemetry Data at the operating system layer. Jamf Protect does not access email, documents, browser history or other content. The data Threat Labs analysts work is confined to the signals needed to identify adversary activity: process trees, binary hashes, network flows, and related indicators of compromise.

4. **Who at Jamf can see my organisation's threat data**?

   Access is limited to the Jamf Threat Labs team responsible for delivering the Beacon service and access is only for the purpose of providing you the Beacon service.

5. **Where is Beacon threat hunting data processed and stored?**

   Please see Jamf's sub-processor documentation available at:

   https://www.jamf.com/trust-center/legal/jamf-sub-processors/.

6. **Can I choose which region my data is stored in?**

   Beacon data storage follows your Jamf Cloud hosting region. Where more than one regional location is available, the default is the location geographically closest to your organisation; customers can also specify a preferred hosting location. Speak to your Jamf contact if you have specific data residency requirements before onboarding.

   ↗ Jamf Cloud Hosting Locations

7. **How is data encrypted at rest and in transit?**

   Jamf Cloud uses AES-256 bit encryption for data at rest and TLS 1.2 for data in transit between managed endpoints and Jamf servers. An external, third-party SSL certificate is used for the Jamf Pro web application. Databases are continuously replicated to a secondary server in a different data centre, providing both resilience and encrypted redundancy.

   ↗ Cloud security controls — Information Security

8. **What compliance certifications does Jamf hold that are relevant to Beacon?**

   Jamf maintains a broad compliance program and several certifications, demonstrating Jamf's commitment to information security and privacy. Please see Jamf's Information Security page for more information and to request copies of our certifications.

9. **Does Jamf comply with GDPR?**

   Jamf's approach to privacy and protecting Personal Data is founded on three principles — Compliance, Trust, and a culture of Privacy by Design — which means privacy considerations are built into product decisions, not added after the fact.

   ↗ Jamf's approach to Privacy by Design

   This approach helps Jamf comply with applicable Data Protection Laws, including GDPR. Jamf has built its Personal Data handling practices around GDPR principles and Jamf's DPA for Customers explains how Jamf meets its obligations under applicable Data Protection Laws. Jamf's DPA for Customers is incorporated into the SLASA. You can review Jamf's DPA and a DPA FAQ on the Trust Center.

   Jamf also publishes a Transfer Impact Assessment (TIA) as a resource to assist customers in performing their own assessments.

   ↗ https://www.jamf.com/trust-center/compliance/gdpr-compliance/

   ↗ https://www.jamf.com/trust-center/privacy/

10. **I'm in a regulated industry (healthcare, finance, government). Is Beacon appropriate for my environment?**

    Jamf's compliance portfolio — including SOC 2, ISO 27001/27701, StateRAMP (for US government), and Cyber Essentials (for UK public sector) supports customers with industry-specific regulations and compliance obligations. We encourage all customers to review our SOC 2 Type II report, ISO certificates, and other documents that are available via Jamf's Security Portal.

    We also encourage customers in highly regulated ares to review our agreements, including our DPA and Information Security Schedule, and other resources like our sub-processor documentation and Transfer Impact Assessment before deploying Beacon. These are all available on the Legal Trust Center.

    Note: For US federal/FedRAMP environments: Beacon is delivered through Google Cloud and is not currently FedRAMP-authorised. Customers with FedRAMP requirements should confirm scope with your Jamf account team before purchase.

    ↗ Request SOC 2 / ISO reports — security.jamf.com

11. **How long is threat hunting data retained?**

    Specific retention periods for Beacon telemetry are governed by your service agreement and Jamf's data retention policies. Jamf's general principle is to retain customer data only as long as necessary to deliver the service. Please see our Service Level Agreement and DPA (available on the Trust Center) for more information about retention and deletion.

12. **What happens to our Personal Data if we stop using Beacon?**

    If you stop using Beacon and other Jamf Product Offering and are no longer an active customer of Jamf, we will retain Personal Data retained for 90 days following termination of your agreement with Jamf, after which it will be returned to you or deleted in accordance with DPA.

    Additionally, Jamf's Privacy team handles Data Subject Access Requests (DSARs) and organisational deletion requests.

    To ask questions about Personal Data that may be processed by Jamf, iay be processed by Jamf, individuals may contact Jamf's Privacy team at privacy@jamf.com or submit a request via the Trust Center.

    ↗ Submit a Data Subject Access Request (DSAR)

13. How are Jamf's sub-processors assessed and managed?

Jamf conducts annual compliance reviews of all sub-processors and performs Transfer Impact Assessments in line with applicable Data Protection Laws. Before onboarding a new vendor, Jamf runs a security and compliance assessment, including review of the vendor's SOC 2, SOC 1, and/or ISO 27001 certifications. Material findings trigger a formal remediation tracking process.

As part of its diligence and onboarding, Jamf ensures it has the necessary data transfer mechanisms in place with each sub-processor.

↗ Vendor Management — Compliance Trust Center

14. How does Jamf protect the Beacon service infrastructure from compromise?

Jamf's engineering team follows a Secure Software Development Lifecycle (SSDLC) covering risk identification, system analysis, technical design, development, QA, and post-implementation review.

Additionally, Jamf's Information Security and Compliance teams deliver and maintain a comprehensive security program. Our various certifications show our commitment to security and privacy. We conduct third-party penetration testing annually on Jamf Pro Server and the Jamf Management Framework. We also pefrom automated dynamic and static security scans on builds to identify critical risk classes including XSS, CSRF, injection attacks, and authentication issues.

A dedicated Product Security team handles ongoing vulnerability discovery and customer-reported issues. Jamf also operates a public Vulnerability Disclosure Programme.

↗ Product security programme — Information Security

↗ Vulnerability Disclosure Programme

15. What is Jamf's approach to business continuity and availability for Beacon?

Jamf Cloud infrastructure is built on industry-leading platforms with real-time availability monitoring. Databases are continuously replicated to a secondary server in a different data centre. Built-in redundancies and disaster recovery plans are in place and tested periodically. Jamf's Service Level Agreement outlines specific uptime obligations.

↗ Jamf Cloud Status page — live availability

16. Who do I contact with further data privacy questions about Beacon?

For privacy-specific questions, contact Jamf's Privacy Office directly:

- **Email:**
  privacy@jamf.com

- **Post:**

  Privacy Office, JAMF Software LLC, 100 Washington Avenue South, Suite 900, Minneapolis, MN 55401

For Beacon commercial and deployment questions, contact your Jamf account representative or Professional Services contact.

Last Updated: 2026-07-09