Optional Internal Services

Service	Description	Encryption Algorithm	Region	Type of Customer Data	Key Controls
Jamf Cloud Distribution Service (JCDS)	JCDS is one of the cloud distribution points supported by Jamf Pro that can be used to host packages, in-house apps, and in-house books.	AES - 256 TLS 1.2+	us-east-1	Customer uploaded files for distribution to their end points	Access Controls SDLC Encryption
Icon Service	Icon Service manages icons and allows them to persist in Amazon S3 to reduce overhead and create a better end-user experience.	AES-256 TLS 1.2+	us-east-1 us-east-2	Caching service for customer icons through the Self-Service application	Access Controls SDLC Encryption
SOUP	Soup is a service built to enable more seamless deployment of Jamf Protect & Connect from directly within	AES-256	us-east-1	Customer data (stored in DynamoDB) • Customer's Jamf Protect instance URL • Salesforce Account ID • Password to customer's Jamf Protect instance	Access Controls SDLC Encryption

	Jamf Pro. It handles connection to Protect to sync plans over to Pro for simple, more automated deployment. As part of automating deployment, Protect & Connect package artifacts are uploaded to Soup.			(encrypted - using AWS' KMS)	
Remote Assist	Remote Assist allows admins to initiate a remote desktop session directly from within the browser, regardless of where your users are working.	AES-256 TLS 1.2	us-east-1	• Tenant ID • Device Id • Session Id • Session Start • Session End • Session Status • Session Type • User Viewer Id • Admin Comment	Access Controls SDLC Encryption CSA Token
App Catalog	App Catalog streamlines app management and makes it easy to empower users to update anytime a new patch is available by notifying users that they need to update before continuing to use an affected app.	TLS 1.2+	us-east-1	App Installers Service: • N/A Global Patch Feed: • N/A Title Editor: • Username/Email • Customer ID from Salesforce • Auto-Generated random subdomain • Custom Application/patch data	Access Controls SDLC App Installers: • CSA token or proper AWS IAM role required to fetch data maintained by Jamf Global Patch Feed:

					• Public endpoints to fetch data maintained by Jamf Title Editor: • Public endpoint (random subdomain in url) to fetch data added by customer
Cloud Connector	Cloud Connector connects a cloud-hosted Jamf Pro instance with Microsoft Intune. The Cloud Connector automates many of the steps needed to configure the macOS Intune integration, including creating the Jamf Pro application in Microsoft Intune.	TLS 1.2+	us-east-1	Azure Tenant ID and Jamf Pro instance URL	Access Controls SDLC