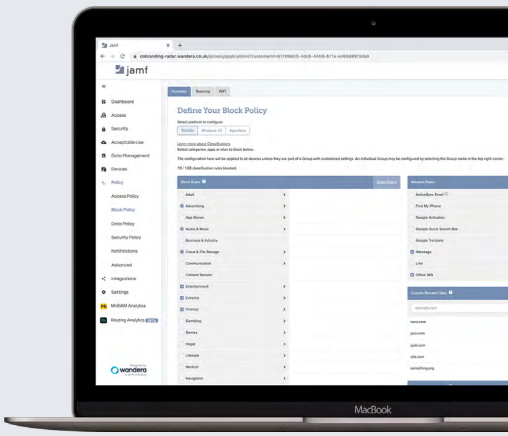
jamf

JAMF DATA POLICY

Enable remote work with confidence and help employees stay productive



Enforce acceptable use, eliminate shadow IT, prevent excessive data usage and educate end users on their data use across cellular, roaming, and Wi-Fi networks.

Enforce Acceptable Use Policies

Content filtering with Data Policy allows organizations to define which websites and apps can be accessed from company-owned mobile devices. Jamf ensures online behavior is compliant with acceptable use policies by providing real-time visibility into usage and category-based policy controls to automate enforcement

Monitor for Shadow IT

Organizations that operate in regulated industries or handle sensitive information are expected to stay compliant with various information security and industry policies. Jamf can prevent sensitive corporate data from being exposed—either through a browser or through the native mobile app—by blocking access to unsanctioned services.

Manage usage in real-time

Elevate your security posture by allowing only secure and trusted devices to access business applications. Threat Defense continuously monitors a broad set of telemetry and contextual inputs that can be used to prevent application access when an endpoint is compromised or at high risk. Adaptive access policies can be enforced natively through the Zero Trust Network Access solution or Jamf's management solution, Jamf Pro.

jamf

> "At Campari, we use Wandera Data Policy to control our mobile data usage. It is very simple to configure including the deployment of Wandera's app and traffic routing profile over-the-air to our mobile endpoints without the need for our end users to install anything. We've seen a strong ROI from using the product due to data cost savings and simple, integrated mobility management"
>
> - Campari

Features

Real-time Policy Control

Configure cap policies to be applied when data usage thresholds are reached. Customize alerts and notifications for users and admins.

Fully customizable

Apply policies to individual users, groups, or the organization as a whole. Tailor the predefined content filtering categories with customized allow and block lists.

Content filtering

Set intelligent rules to prevent inappropriate websites and apps from being accessed. Ensure that usage is compliant with HR, IT, and regulatory policies.

Network aware

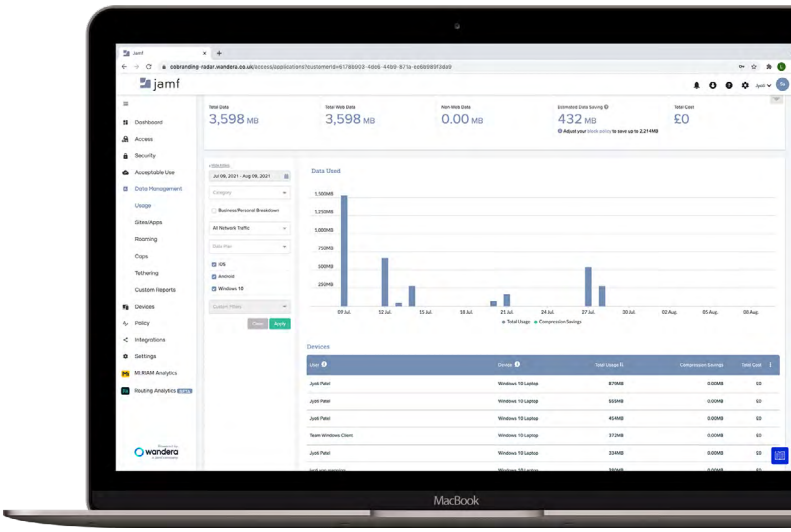
Create and enforce policies for different networks. Data Policy automatically detects the network to allow Wi-Fi users to have content filtering applied without data management.

Any mobile device, any ownership model

Data Policy supports mobile devices and laptops, allowing you to choose the device that's best for your business.

Real-time Insights

Monitor data usage without waiting for the bill using Jamf's real-time insights and usage analysis tools.



Jamf Data Policy works seamlessly with your existing IT services and technologies.

Deep integrations with Microsoft, Google, Cisco and more help you extend the value of your existing tech stack.

jamf

www.jamf.com

To learn more about how Data Policy can help enforce your acceptable usage policy please visit jamf.com

Feature Matrix

Jamf Threat Defense, Jamf Data Policy and Jamf Private Access

	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Core Components	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Jamf Security Cloud	✓	✓	✓
Endpoint App	✓	✓	✓
Admin Console	✓	✓	✓
Essential Integrations	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
MDM/UEM integrations for streamlined deployments	✓	✓	✓
Identity Provider integrations for end user activations	✓	✓	✓
SIEM/SOAR/EDR integrations for InfoSec workflows	✓	✓	✓
Public APIs and Data Export	✓	✓	✓
Common Settings	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Privacy & Anonymity Controls	✓	✓	✓
Customizable notifications for users and admins	✓	✓	✓
Context-aware policy (by user, group, device, network, etc.)	✓	✓	✓
Endpoint Security	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Device risk and vulnerability assessments	✓		
App intelligence	✓		
Mobile malware protection	✓		
Network Security	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Zero-day phishing protection	✓		
Malicious traffic blocks (spam, cryptojacking, etc.)	✓		
Risky hotspot protection	✓		
Data & Usage Policy	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Data caps & Usage limits by MB/GB		✓	
Content filtering for websites & native apps		✓	
Shadow IT discovery		✓	
Modern Remote Access and VPN Alternative	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
Fast, encrypted microtunnels			✓
Protected access to on-premises applications			✓
Protected access to cloud-hosted applications			✓
Conditional Access	Jamf Threat Defense	Jamf Data Policy	Jamf Private Access
via MDM	✓		
via MAM-WE (BYOD)	✓		
via IDP	✓		
via native Private Access	✓		✓