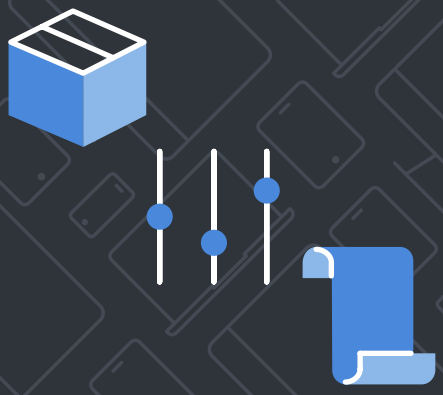
Jamf Partner Enablement Guide: Jamf Threat Defense and Data Policy



Secure your remote access and protect against the broadest range of cyber threats and content risks.

With Jamf Threat Defense and Jamf Data Policy, your customers can protect against zero-day security threats on the device and in the network.

Why combine Jamf Threat Defense and Data Policy?

Mobile security is a growing concern that your customers are trying to address. If you do not offer guidance on this subject, a different technology partner will. Jamf Threat Defense and Jamf Data Policy include both an on-device endpoint application and real-time, in-network protection. When combined, your customers benefit from an enterprise solution that protects your devices, data and users, all while preserving the legendary Apple user experience.

Why might a customer want this?

- Organizations want to provide flexibility and freedom to their users but need to balance that with their security posture. They need dynamic tools that can deliver the right experience at the right time, which Jamf Threat Defense and Data Policy can offer.
- Organizations strive to provide a mobile experience that keeps end users productive. They can achieve this by enforcing acceptable use policies that prevent users from accessing inappropriate content.
- Data overage and roaming costs can be considerable, especially at the enterprise level. Having an accurate understanding of data usage allows organizations to become more efficient and effective.

What problems will it solve?

Jamf Threat Defense is a solution that monitors for configuration vulnerabilities, network compromises, app risks and content threats. It assigns risk assessments and provides a range of policy enforcement actions for response. Jamf Data Policy provides deep insights into mobile data — both the content being accessed and how data is being used. Below, we've outlined features you can leverage from utilizing them together.

Jamf Threat Defense

- Manage endpoint risk by identifying device configuration vulnerabilities.
- Stop risky apps — including malware and data leaks — with zero-day threat detection and support for app vetting workflows.
- Prevent man-in-the-middle attacks from intercepting and tampering with network connections.
- Block advanced network-based attacks, like zero-day phishing and malware command and control communication.

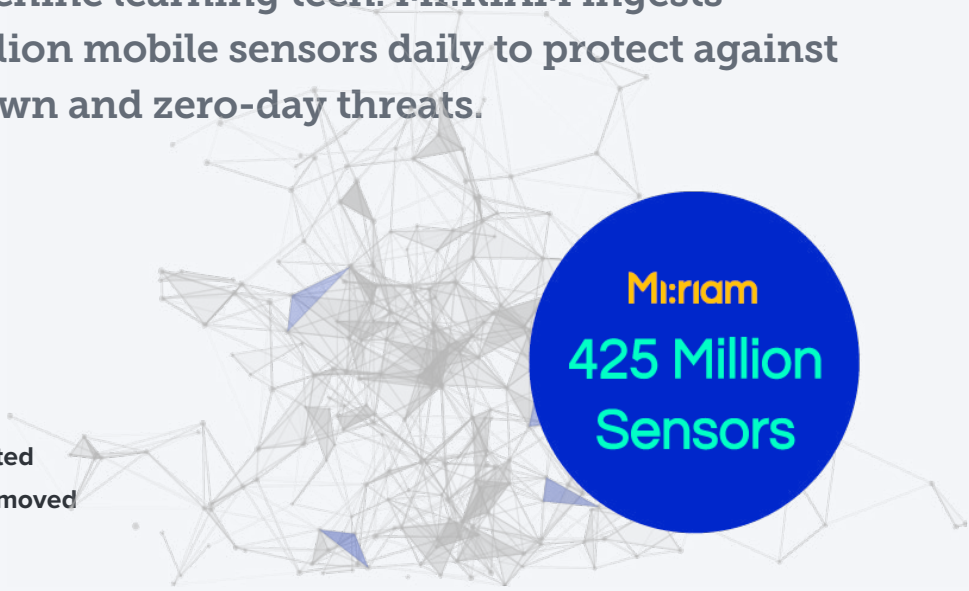
Jamf Data Policy

- Generate reports with detailed analysis of mobile data usage.
- Enforce corporate acceptable use policies by filtering content.
- Control costs by setting caps, alerts and blocks to prevent data overage charges.
- Ensure productivity by limiting access to non-work apps during business hours.
- Engage with protected workers by providing notifications with real-time insights into usage.

The backbone of our security is a threat intelligence engine called MI:RIAM, based on AI machine learning tech. MI:RIAM ingests information from 425 million mobile sensors daily to protect against the broadest range of known and zero-day threats.

- Advanced threat intelligence engine
- Unique zero-day phishing protections
- Track record of newsworthy discoveries
- Dynamic content classification
- Dedicated threat research team

Wandera is the only vendor to have detected malicious apps that were subsequently removed from the App Store.



Jamf Threat Defense and Data Policy key personas

To get the most out of positioning Jamf Threat Defense and Data Policy, it's important to understand the priorities and level of influence different members of an organization may have.

Jamf has identified key personas for you to focus on when positioning these solutions to help ensure your conversations are meaningful and lead to opportunities.

Decision Maker

Sets priorities for organization

Cares more about the value than the tech

Wants to know the ROI

WIll be the one to give final approval

Common titles:

- CISCO / CTO
- CISCO / CSO
- Security / InfoSec / Cloud / IT VP or Director

Catalyst

Your Jamf 'champion"

Heavily networked and well respected in the company

Has accesss to and influence over Decision Makers

Creates/allocates budget for the project

Common titles:

- Security Engineer
- Network Security
- Application Engineer
- InfoSec Analyst
- Engineer
- Mac Engineer
- SysAdmin
- Endpoint Security

Influencer

Has authority or alignment with authority

Has respect of Catalyst and Decision Maker

May be a supporter, neutral or opposed

End User Computing

Common titles:

- Security Manager
- InfoSec Manager
- IT Manager
- Endpoint Security Manager
- Security Architect

Outsiders

People outside the org who can influence or inform

Partners, resellers, Apple

References, user communities, trade groups, publications

Analysts – Gartner, IDC, Forrester Research

Partners, resellers and Apple can be great entry points into security conversations

Security organization overview

CSO or CISO
Leader responsible for InfoSec, corporate security or both.

Security operations
Monitors and analyses the security procedures of an organization.

Security architect
Builds and oversees the implementation of network and computer security for an organization.

Identity and access management
Ensures the appropriate level of access to the organization's technical resources.

Governance, risk management and compliance
Treats information as a business asset and protects it with processes, controls and metrics.

Understands risk and prioritizes responses to manage vulnerabilities. Measures adherence to policies and standards.

Security PMO
Sets, maintains and ensures security standards for specific projects.

Discovery questions

- What does your mobile device environment look like? Do you have a mixed fleet of device models?
- How are your employees using mobile devices to access corporate applications?
- How do you monitor for malicious or compromised apps today?
- Do you have corporate-owned devices? How many?
- How do you manage data plan allowances for your end users? Do you experience bill shock due to users exceeding their data plan allowances?
- How do you manage data costs and prevent overages?
- Do your users always notify corporate when they are about to "roam" outside of the region covered by your calling plan?

Benefits to you as a Partner

Our new suite of products complements Jamf's Mac leadership and end-user focus with unique iOS capabilities.

From a single provider, you're able to sell an Apple-first iOS enterprise solution that connects, manages and protects customers devices, data and users, all while preserving the legendary Apple user experience with same-day Apple operating support.

- Unlock additional solution selling opportunities within the Apple ecosystem
- Offer truly unique value to the Apple platform as part of Jamf's Apple Enterprise Management ecosystem
- Increase overall margin opportunity on Apple ecosystem sales
- Expand your network into new key business personas to sell to
- Provide a timely solution to the many security vulnerabilities and threats in the market today