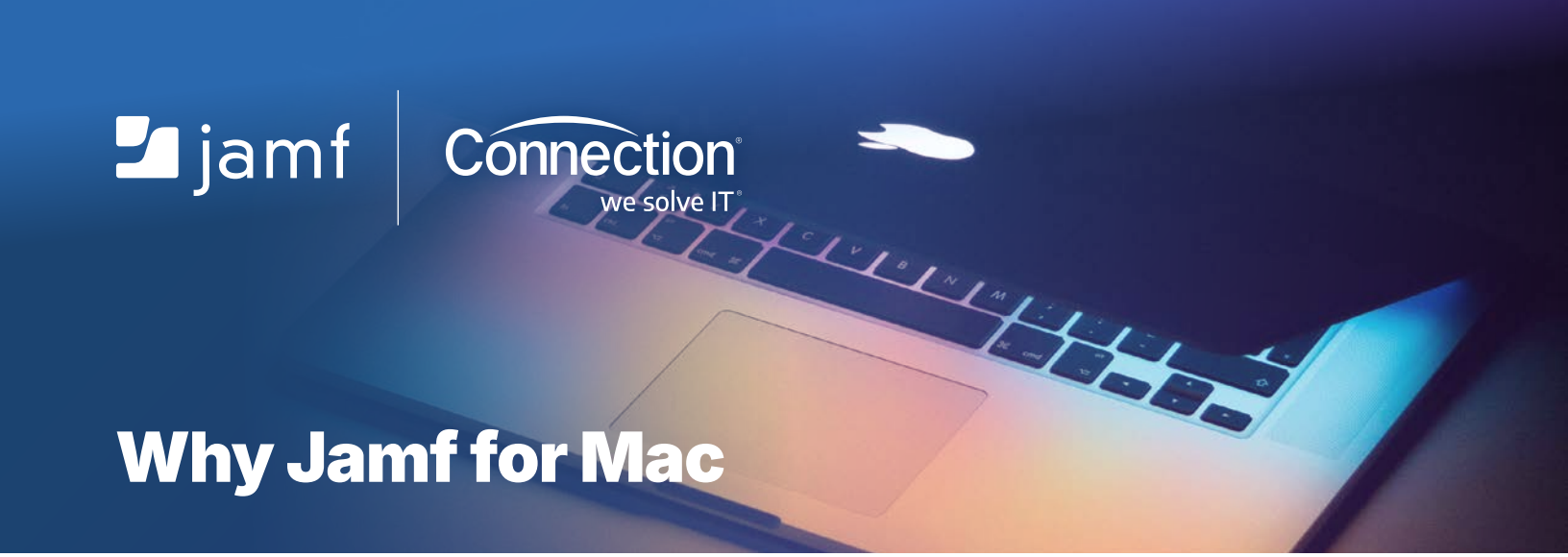

Why Jamf for Mac

Enterprise IT leaders are tasked with limiting device downtime and keeping end users productive and happy, while reducing risk exposure and mitigating any cyber threats.

As more employees choose Mac, IT teams are expected to deliver seamless experiences and enterprise-grade security—without compromise, within their given budget. That's where Jamf comes in.

IT Teams are spending an excessive amount of time on routine IT tasks.

The modern IT environment demands speed, but outdated workflows, disconnected tools, and lack of real-time data force teams to waste hours stitching together solutions. It's not scalable.

49%

of organizations say they have limited access to information at the right time [1]

Without visibility into devices, IT teams waste time piecing together data using makeshift solutions and manual API calls just to build basic reports. Lack of real-time data is an even bigger risk to keeping devices secure.

80%

of IT leaders say integration challenges slow down digital transformation initiatives [2]

Without clear documentation, native-built integrations, or the policy framework to support seamless integrations, IT teams are spending needless time getting their tools to work together smoothly.

36%

of Macs were found to have FileVault disabled [3]

55%

of Macs were found to have Firewall disabled [3]

IT Teams are spending too much time manually hardening and remediating devices for compliance baselines. Other vendors are offering templates for compliance that are not complete or do not reflect the compliance baselines in the macOS Security Compliance Project. This creates more work for IT Teams.

Each year increases risk exposure across Apple environments.

The increased popularity of Mac in the enterprise is a mixed blessing: hackers now believe that the difficulty of cracking Apple devices is worth the effort.

Lack of protection from Apple specific threats only increases risk exposure. Telemetry that lacks Mac-specific event data (i.e., Gatekeeper and XProtect) means you'll have limited visibility until threat actors trigger other security controls. Without threat hunting teams dedicated to Apple, most security vendors struggle to keep up.

The average cost of failing to comply with data protection regulations is $14.8M.[2]

Lack of extensive logging and audit trails results in poor audit readiness, but supporting integrations with SIEM providers offers additional visibility for a true security single pane of glass.

39% of organizations have at least one device with known vulnerabilities;[3] limited visibility into CVEs and lack of automated software patching workflows leaves you at risk to vulnerable software.

300

Jamf Threat Labs tracks over 300 malware families on macOS [3]

21

Jamf Threat Labs found 21 new malware families in 2023 alone [3]

$14.8M

The average cost of failing to comply with data protection regulations

of organizations have at least one device with known vulnerabilities [3]

So why Jamf for Mac?

Jamf increases productivity twice as much as our competitors[4] by seamlessly integrating into any IT stack. This reduces time spent on data collection, device downtime, tier one support and manual operations.

Our security solutions reduce risk exposure two-to-three times more than competitors by reducing Apple-specific threats, increasing response times, reducing unpatched vulnerabilities and increasing compliance readiness.

We achieve this through:

- Real-time threat monitoring across multiple vectors with threat hunting teams dedicated to Apple
- Comprehensive inventory, reporting, logging and audit capabilities
- Expansive pre-built IT and InfoSec integrations
- A robust policy framework offering automated, real-time execution and end-user Self Service
- Automated app sourcing, validation, repackaging and deployment

Our extensive support and services teams are legendary. We also offer Jamf Nation—the world's largest forum of Apple administrators—where members share their vast expertise with each other.

"The excellent technical support I am receiving from Julie [Technical Support Engineer] goes a long way in proving the validity of choosing Jamf for Mac management. I can confidently show my management team that Jamf is a reliable choice."

– IT Analyst at a government agency

Jamf increases productivity more than other solutions.

Jamf beats the competition with:

- Less device downtime
- Increased IT operational efficiency
- Less need for direct end-user support
- Better monitoring and visibility

Faster speed to production

Real-time access to comprehensive device information and automated workflows decreases the need for manual reporting, auditing and workflow management.

Here's how:

- **Automated onboarding workflows** that set configurations based on role, department, user, and location save IT time and get new employees up and running right away
- **Precise targeting** helps to automate troubleshooting, device hardening, software updates — saving end-user and IT time
- **Tier one support** extends troubleshooting beyond basic user functions and allows users a self-serve model for adding productivity apps

Jamf reduces more risk than others.

Jamf's robust policy framework covers device management frameworks, policy-based script execution and network controls. Our expert threat-hunting team uses well-trained behavior analytics to stop Apple-specific attacks.

With Jamf, IT leaders can:

- Block known and novel Apple-specific threats zero-day
- Respond faster to security risks with targeted, real-time execution for remediation
- Limit unpatched vulnerabilities with CVE reporting and automated software and app updates
- Reduce probability of data loss with secure connectivity built for Apple with dynamic risk assessment against an increased number of data points
- Automate device hardening by integrating into the macOS Security Compliance Project, eliminating the risk of human error and increasing audit readiness with detailed logging and audit trails

1. *"Automation: Trends, Challenges and Best Practices," IDC, 2023*
2. *"State of IT Report," third edition, Salesforce*
3. *"Jamf Security 360: Annual Trends Report 2024," Jamf, 2024*
4. *"Driving ROI: The Case for a Proven Apple Enterprise Management Solution," Jamf whitepaper, 2021*

Jamf is the right choice. But don't just take our word for it!

G2 reviews:

"Jamf Pro remains the pre-eminent Mobile Device Management for Apple Mac."

"Tons of support from vendors. Jamf is usually explicitly included in vendor documentation as it is the lead product for Apple MDM."

jamf

Connection
we solve IT

1.800.800.0014
www.connection.com/Jamf

C3779449-0626