jamf

A Practical Guide to Mac Compliance

For IT teams managing growing Apple environments

Why does Mac compliance matter?

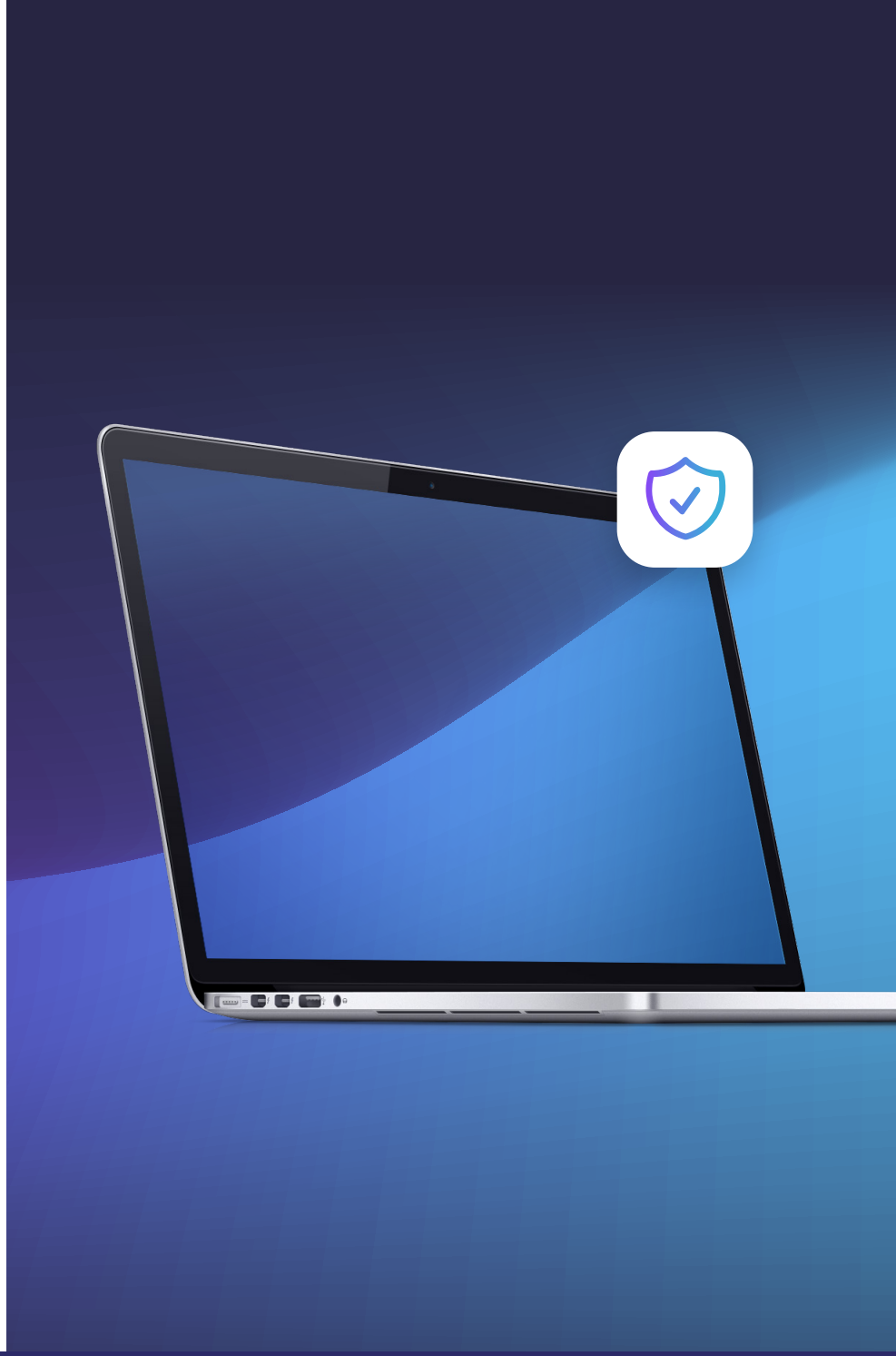
Growing organizations managing Mac and mobile devices must meet compliance requirements while keeping IT operations efficient and manageable. Compliance is not only about meeting legal or regulatory standards. It also plays a critical role in strengthening security, reducing risk and building trust, all without adding unnecessary complexity for already stretched IT teams.

Understanding why Mac compliance matters is the first step in building a secure and scalable environment.

At its core, compliance is guided by benchmarks. A compliance benchmark in IT security is a set of standards used to measure an organization's adherence to regulations and requirements and provides best practices for protecting sensitive data.

For example, CIS Controls and Benchmarks are widely adopted across industries as a foundational layer of security best practices. While not tied to any single regulation, they often serve as a baseline on which organizations build additional industry-specific or region-specific compliance measures, such as those required by GDPR or HIPAA.

Growing organizations rely on these benchmarks to reduce risk, protect data and avoid security gaps as their environments scale. In fact, failure to comply with relevant regulations can result in hefty fines, legal action and reputational damage. Regularly tracking and meeting these benchmarks helps companies stay secure and competitive in the digital world.



The art of maintaining Mac security for IT teams

Part of why IT admins love Apple is that the Mac has incredible built-in security features.

For lean IT teams responsible for both Mac and mobile devices, these built-in protections are most effective when managed centrally and enforced automatically.

Mac computers are, by their very nature, more stable and efficient than other devices. And with the right tools, IT can enforce powerful, flexible Apple-specific management and security measures without hampering Apple's excellent UI experience. When you combine a world-class MDM solution with Apple's Declarative Device Management (DDM) protocol, you can ensure that company data, employee data and networks are protected.

Regulatory compliance for Macs: What to consider

Many organizations must meet the same compliance requirements as larger enterprises, while operating with leaner IT teams and fewer resources.

As a result, compliance involves navigating multiple standards and requirements at once.add space here Your organization will probably have multiple compliance standards to meet. This will ensure corporate and employee data stays secure. You'll need to enforce these as well as industry and governmental benchmarks.

Just how many regulations are there?

Each industry and region has its own regulations and best practices, and some overlap. A small sample from around the world:

ISO **ISO 27701** certification ensures proper handling of PII (Personally Identifiable Information) in healthcare across the globe

DORA regulations address financial regulation in the EU

CIS benchmarks from the Center for Internet Security offer prescriptive configuration recommendations to keep organizations safe

NIS2 requirements ensure adherence to EU-wide legislation on cybersecurity

The German IT Security Acts 1.0 and 2.0 (das IT-Sicherheitsgesetz 1.0 und 2.0) regulate IT security with their own compliance requirements

Cyber Essentials+ defines minimum cyber security standards for all organizations in the UK

There are many complex regulations to track and enforce.

Once you identify which requirements apply to your organization and device environment, the next step is putting the right processes in place to support them.

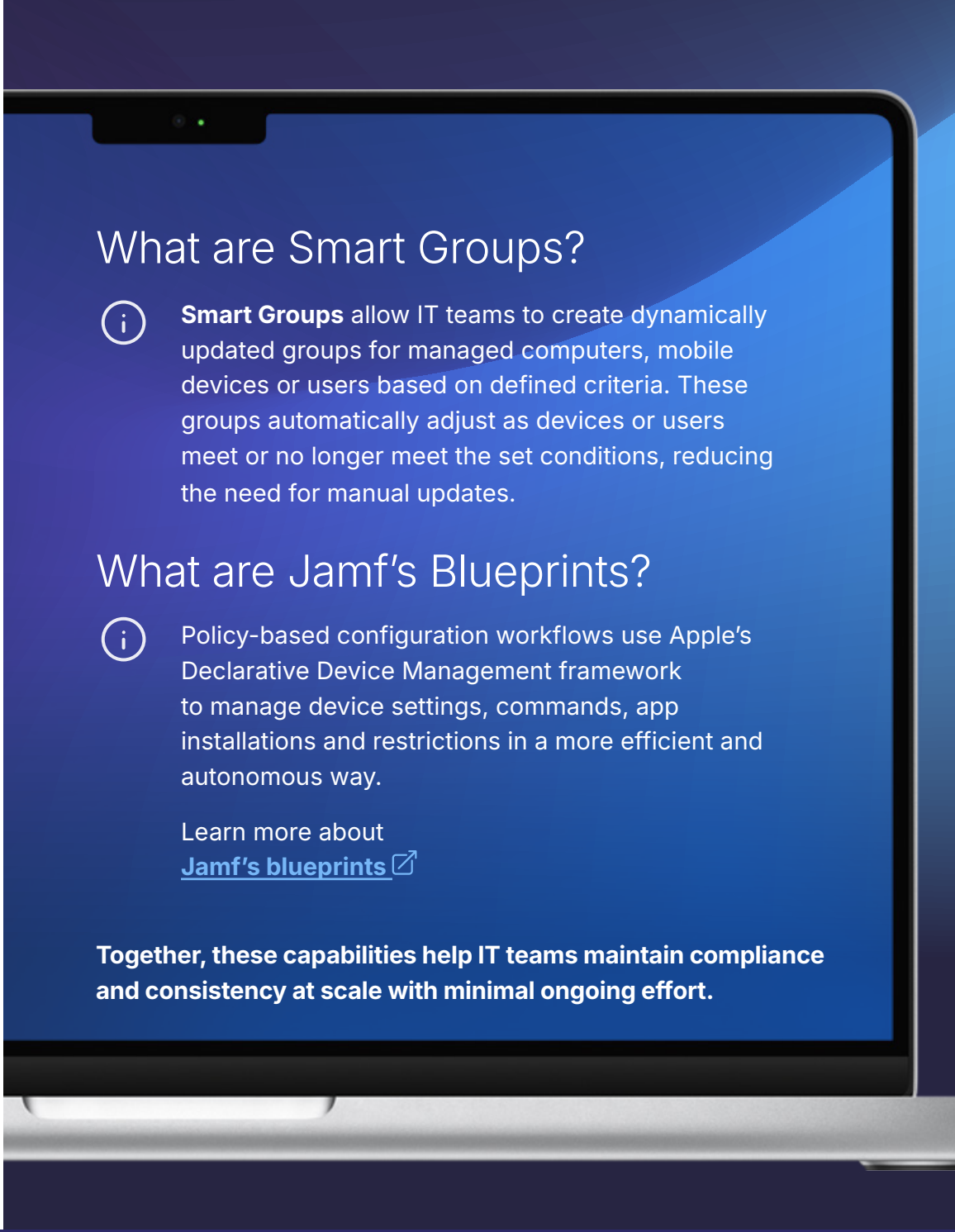
With a modern device management approach, IT teams can automate much of this work and continuously validate compliance across their fleet.

With device management in place, you can:

- **Apply consistent configuration and compliance policies**
- **Use dynamic groupings to assign settings and actions automatically**
- **Rely on automation to reduce manual effort and maintain compliance at the device level**

At this point, everything might seem under control. You could even step away for a moment.

Except...



...In compliance, change is constant.

As technology, business practices and regulations evolve, compliance requirements must evolve with them. The goal of compliance is to keep organizations secure and operating smoothly, even as environments change. Staying aligned with emerging security risks and regulatory expectations is an ongoing process.

This typically involves:

- **Regular compliance audits and reviews**
- **Timely operating system and security updates**
- **Ongoing monitoring for security threats**
- **Adapting to changes in regulations and policies**
- **Responding quickly to changes in user roles or access needs**

If this sounds demanding, that is because it often is.

This is where a structured compliance checklist becomes essential.

By following a clear, step-by-step approach, IT teams can streamline compliance efforts and stay aligned with evolving requirements.

A well-defined checklist helps ensure nothing is overlooked and that security controls, monitoring and enforcement are applied consistently.

Preparation phase

- **Create user accounts and profiles.**
- **Define organizational policies and permissions with decision-makers in your organization.**
- **Define outside compliance regulations based on which industry or governmental regulations your organization must follow.**
- **Ensure hardware and software compatibility with all tools you'll be using.**

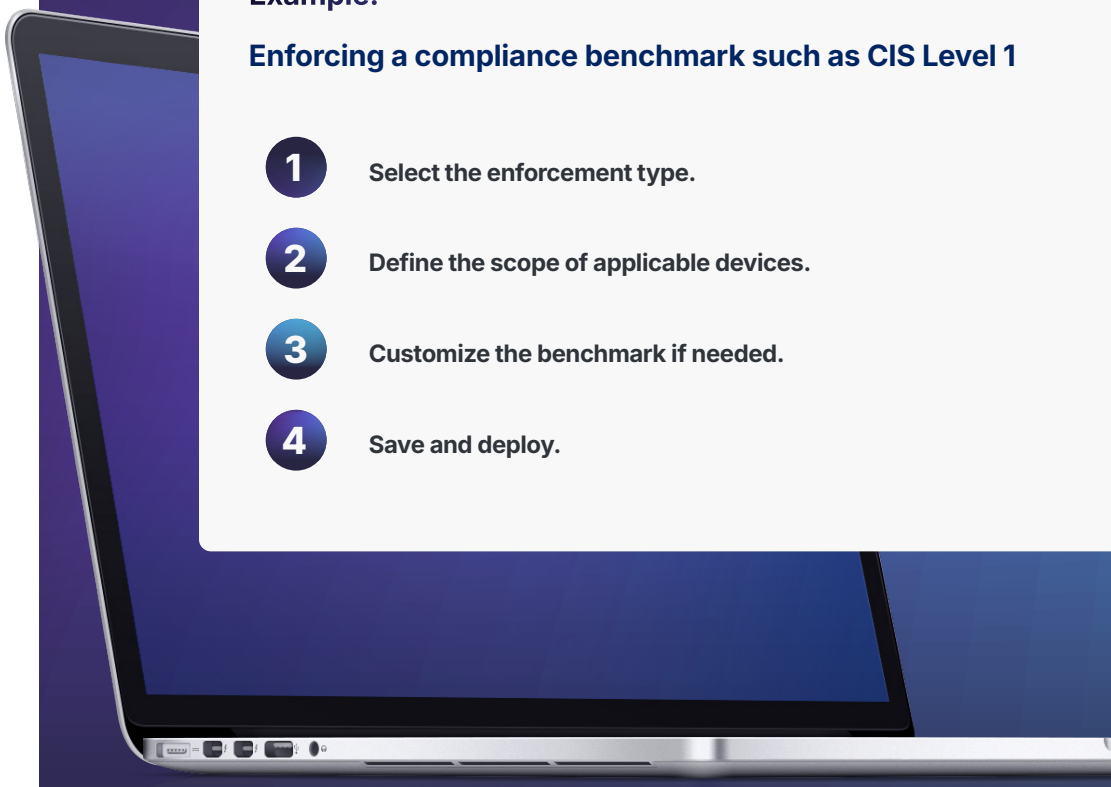
What are compliance benchmarks?

Compliance benchmarks allow IT teams to define, audit and enforce compliance in a structured and repeatable way.

The feature:

- ✓ **Reduces the time required to audit and enforce compliance across the device fleet**
- ✓ **Simplifies complex security standards and configuration requirements**
- ✓ **Helps improve overall device security posture**

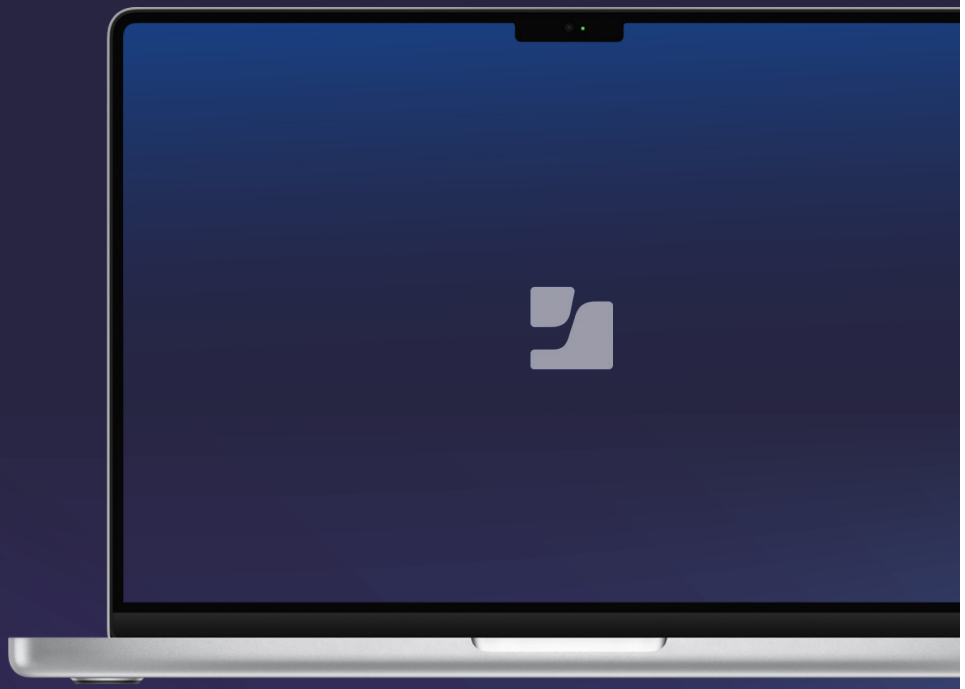
Compliance benchmarks automate the application and maintenance of security settings, helping ensure devices remain aligned with defined standards over time.



Example:

Enforcing a compliance benchmark such as CIS Level 1

1. **Select the enforcement type.**
2. **Define the scope of applicable devices.**
3. **Customize the benchmark if needed.**
4. **Save and deploy.**



Compliance benchmarks are based on the macOS Security Compliance Project (mSCP), a joint effort led by federal IT security teams from the National Institute of Standards and Technology (NIST), National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA) and Los Alamos National Laboratory (LANL).

Continued maintenance and monitoring

Compliance benchmarks provide visibility into the status of applied benchmarks and overall device compliance. More detailed views allow IT teams to review compliance at the individual rule level, such as password requirements, for closer inspection.

Watch a compliance benchmarks demo:

Setup and configuration

Use automated provisioning to ensure each device is configured correctly for its user and that applications and access settings remain up to date at the device level.

- ✓ **Use compliance benchmarks to simplify and speed up configuration by applying requirements based on common standards, such as CIS Level 1 or 2.**
- ✓ **Use predefined configuration templates or create your own to save time and improve consistency. This saves time and increases security with passcode policy settings, service configuration files settings and background task management.**
- ✓ **Install essential applications and updates using a combination of Self Service+ and Smart Groups, allowing users to access the tools they need while IT maintains control through automated assignment.**
- ✓ **Configure core security settings such as disk encryption, system protections and application controls.**

Testing

- ✓ **Verify functionality of apps and system features.**
- ✓ **Conduct security reviews and audits to confirm compliance.**
- ✓ **Consider rolling out these changes to a smaller group of employees first who can function as on-the-job testers.**

Start out strong

- ✓ **Provide clear instructions to users.**
- ✓ **Schedule an onboarding session for questions and troubleshooting.**
- ✓ **Ensure automated compliance updates are enabled so systems remain aligned as requirements evolve, reducing the effort required to stay on top of changing compliance protocols.**

What is Self Service+?

Self Service+ is an end-user portal for macOS. It allows users to access content and updates that have been preconfigured in Jamf Pro. In Self Service+ users can:

1. **View the security status of their devices.**
2. **Browse, search and install apps from the App Store and third parties, configuration profiles and books.**
3. **Perform identity-related tasks such as changing passwords.**

Best practices and future considerations

You can ensure that your device fleet remains securely configured and compliant with regulatory requirements and internal policies by using the right tools and processes.

With the right approach in place, compliance can be maintained with minimal ongoing effort. Security teams can also more easily generate and present compliance documentation and status when required for audits or reviews.

Stay informed on changing laws, regulations and compliance standards by following announcements from the regulation entities. While IT teams should always be aware of upcoming requirements, updates to compliance frameworks and benchmarks can help reduce the manual effort required to stay aligned.

The important thing to remember is this: the role of IT teams in maintaining and future-proofing compliance is essential.

Seeking out information such as this e-book to better understand the importance of this issue is a great start. You can also follow this checklist.

Perhaps the most important thing of all? Continuing to advocate for efficient and reliable compliance practices helps ensure your organization remains prepared for future changes.