

Product Guide

dataJAR
a Jamf company



dataJAR Defend

Your internet security guard

What is it?

In a world where Apple is no longer in the minority, the threat landscape is changing. Despite Apple building the very best in device security, its rapid growth and adoption in the enterprise makes Apple an increasingly-appealing target for determined attackers.

Using unrivalled technology focusing purely on Apple, our mission is to protect endpoints from being compromised through mobile threat detection and zero-day phishing prevention.

Once enabled, dataJAR Defend will work in the background to aggregate and analyse all known threat detection layers, enabling ironclad device security with minimal end-user impact. This intelligent integration between Mac and mobile endpoints and the datajar.mobi platform means we can understand when 'bad stuff' happens, such as attacks that successfully execute on organisation devices and act on it.

Combined with our data analytics systems and expert research analysis, we process thousands of device remediations each day keeping your organisation's Macs and mobiles secure and healthy.

Service highlights:

- Automatic threat detection and remediation
- Simple deployment and integration to datajar.mobi
- Managed alerting
- Same-day support for Mac and mobile operating system updates
- Safeguard online privacy with encryption and protection against personal data phishing
- Ensure regulatory compliance with advanced privacy features
- Advanced machine learning and threat intelligence engine to identify and prevent novel threats
- Block zero-day threats like phishing and malicious domains in real time, before your devices are impacted
- USB device restriction for Mac
- USB device restriction for Mac
- Modern cloud infrastructure - no hardware to manage
- Protection from any network
- Protect mobiles against cryptojacking, phishing, data leaks, malware, sideloading, dangerous certificates, MITM and jailbreak

How does it work?

Designed to work alongside Apple's built-in security framework, dataJAR Defend is as lightweight as possible.

Once enabled within datajar.mobi, a small agent will be deployed to your managed Macs and mobiles. This will require no user-intervention and the process takes place in the background without affecting the user experience.

Using the latest capabilities provided by Apple in macOS and iOS, we can filter all network traffic using DNS over HTTPS. Additionally, and specifically on Mac, we use our own security agent called Warden which is there to ensure your device is kept running, secure and threat free. It will proactively monitor, initiate scans and watch for any suspicious quarantined files. If it detects a threat, it will forcibly initiate communication with the datajar.mobi cloud and immediately alert our service desk of the issue as well as remediating the threat.

Our dataJAR Defend service is managed by our technical team in its entirety. We do this to ensure we maintain complete control of the data and technology stack, providing you with the knowledge and confidence your managed devices and data are secure.

This is an annual subscription that can be purchased as a datajar.mobi add-on.

What version of dataJAR Defend is right for you?

	dataJAR Defend for Mac	dataJAR Defend Enhanced for Mac	dataJAR Defend for Mobile	dataJAR Defend Enhanced for Mobile
On device threat detection and remediation	●	●	●	●
Same day support for major OS updates	●	●	●	●
Managed automated alerting	●	●	●	●
Scheduled file system scanning	●	●		
Automatic definitions updates	●	●	●	●
Zero day network phishing attack prevention		●	●	●
Advanced network threat intelligence engine		●	●	●
Content filtering		●		●
Safe Search management		●		●
UEM integration		●	●	●
USB device restriction		●		

Who is dataJAR Defend for?

Organisations that do not currently have any security product, or have a security product that is delaying their adoption of the latest version of Apple's operating systems. Also, any organisation that has datajar.mobi and requires the following:

- Additional protection and filtering of organisational devices
- Additional web protection of devices outside the network perimeter

Requirements:

- **dataJAR Defend requirements:** <https://support.datajar.co.uk/hc/en-us/articles/360005452798>

FAQs

Q: How do I install dataJAR Defend?

A: Our team will enable the service automatically for you.

Q: How do I see the status of dataJAR Defend?

A: The risk status can be seen within the dataJAR Portal.

Q: How does dataJAR Defend stack up against other solutions?

A: We have a tight partnership with leading security vendors as well as our own development team - the result makes it a true game-changer in securing the Apple platform.

Q: Does dataJAR Defend provide on-access scanning?

A: No. With all the other security frameworks already in place, automatic detection and remediation offer best all-round device performance and security.

Related products:

- **datajar.mobi for macOS** - Licensing
- **datajar.mobi for iOS** - Licensing

Ready to find out more about dataJAR?
We would love to hear from you.

Chat with our experts