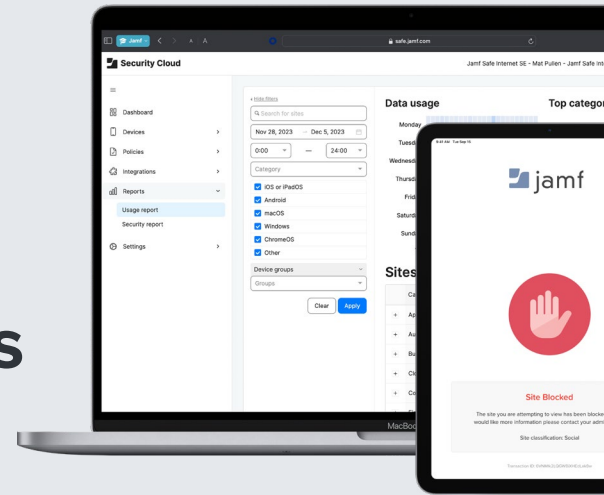




JAMF SAFE INTERNET

Safe, private connections everywhere you need access



Powered by Jamf's network threat protection engine, Jamf Safe Internet is designed to help protect networks from malicious content and attacks.

Education has seen a rapid growth in cyber-related crime over recent years presenting a growing need for digital safety to eliminate cyberattacks and prevent staff and students from accessing unsafe content through phishing attacks or compromised websites.

Jamf Safe Internet is a purpose-built, education security solution that protects against network threats and blocks inappropriate content, everywhere you need to access the internet, whether working on campus or elsewhere.

Cyber security that's always on

Protecting networks from cyber attacks is essential in education to maintain continuity of learning, protect staff and student data and eliminate other potential risks that come with cyber attacks.

Jamf Safe Internet, utilizing machine learning tools to identify and remediate against Phishing, Malware, Cryptojacking and other forms of cyber attacks, keeps institutions and their networks secure.



Easy-to-build Reporting

Security professionals know that threat management doesn't stop with protective tooling; you want to report on and understand the effects of your work. Never miss a beat with device usage statistics available the moment a device is deployed.

Content Filtering Database

Comprehensive content filtering optimized and integrated with MDM for simple, powerful user protection. Using lightweight, performant domain name system (DNS) technology, Jamf Safe Internet allows admins to create and customize the content filter results that fit their specific institution and course needs, without invading privacy.

Education optimized

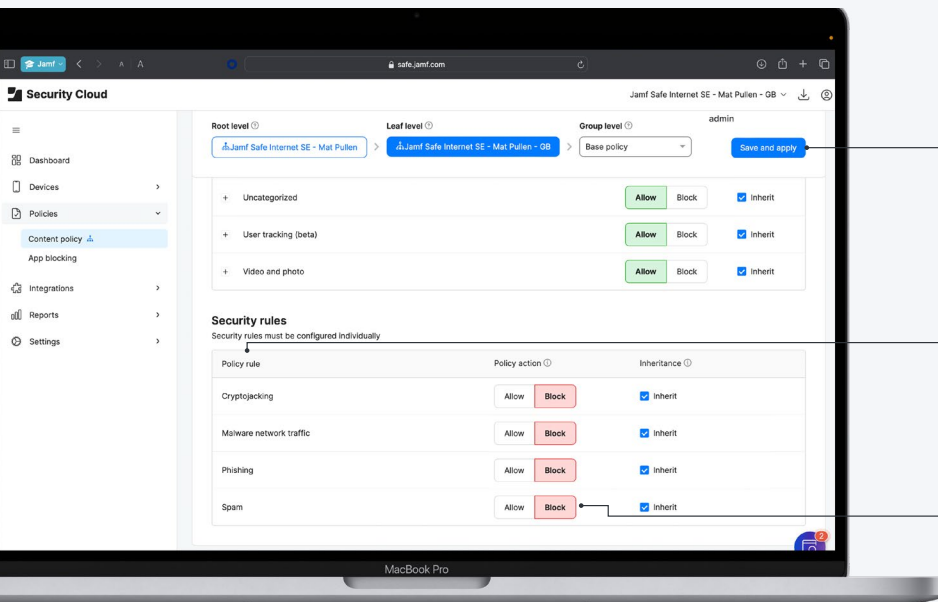
A brand new console, with workflows specifically for the education user, designed from the ground up, with seamless Jamf integration to make deployment and on-going syncing simple and intuitive from the platform you're comfortable with. Jamf Safe Internet integrates with **Jamf Pro** as well as **Chromebook** and **Windows devices**, right out of the box.

On-Device Content Filtering (ODCF)

Ensure end-users cannot bypass domain-based rules by visiting sites via IP addresses. ODCF first inspects traffic in a restrictive sandbox and strips away sensitive data when it leaves, meaning a powerful and still privacy-preserving experience for Apple device users.

Security scoping made simple

Scope and add security rules right to your policies with a simple click.



Simple, Save and Apply updates to your policies

Wide set of block categories to protect users and devices

Simple click-to-toggle Allow/Block functionality

See how [Jamf Safe Internet](#) works with your MDM platform to ensure security and digital safety remain core to the educational experience.



www.jamf.com

© 2002–2022 Jamf, LLC. All rights reserved.

To learn more about how Jamf Safe internet protects students and users, please visit [jamf.com](#)