Managed Methods

A Content Filter

BUYER'S GUIDE

Managed Methods

TABLE OF CONTENTS

INTRODUCTION

In today's digital age, ensuring a safe and protected online learning environment is paramount to K-12 education. Web filtering solutions, which block access to unauthorized websites and applications, are key to this process. With an effective content filter tool, your district can:

Block malicious websites and safeguard against malware, ransomware, phishing scams, and more.

Protect students from inappropriate content or risk factors that could harm their well-being, mental health, and physical safety.

Simplify compliance and satisfy federal and state data regulations.

Boost student and teacher productivity with a distraction-free learning environment.

Choosing the right solution isn't always easy. Fortunately, we're here to help. In this guide, we'll walk you through the five criteria you should consider when looking for a web filtering tool — plus, how to make the switch as seamless as possible.

BREADTH OF COVERAGE

Students are crafty when it comes to evading content filters. Unfortunately, many legacy solutions only filter direct web traffic — i.e., visiting a website directly through its URL. They don't block users from accessing content through referral links or search engines, which means kids may still expose themselves to harmful websites.

The good news is that newer, more advanced solutions do cover a much wider range of traffic. Content Filter by ManagedMethods, for example, blocks embedded traffic such as YouTube videos within Google Docs. This is increasingly important given 90% of school districts operate in the cloud using either Google Workspace, Microsoft 365, or a combination of the two.1

Moreover, school districts don't always have the time to configure filters manually from scratch. Out-of-the-box functionality ensures they're well-protected from dangerous websites, including those they may otherwise not have considered. Content Filter provides pre-built blocklists, covering over 300,000 websites, that you can customize according to your district's needs.

USER EXPERIENCE (UX)

UX is a pivotal aspect of any security tool, web filters included. Ideally, your solution should be user-friendly enough for both administrators — e.g., whoever is responsible for managing the filter — and your end users, which includes both students and staff. In other words, you want it to seamlessly integrate into the IT environment without causing any disruptions.

For administrators, look for a tool that provides a straightforward and intuitive interface where they can manage policies and make changes to blocklists with ease. Depending on your needs, consider prioritizing cloud-based or browser-based solutions that don't require physical installation or manual maintenance.

Take Content Filter, for example. As a browser-level filter, it natively integrates into the Google Admin console, so there's no need to configure your OUs in another system. Plus, you get automatic enrollment and updates so you're always protected against the latest threats.

The result? Virtually zero impact on your end user's browsing experience. That means students are free to focus on their studies without interruption while Content Filter works in the background.

CUSTOMIZATION

No two school districts are exactly alike. Why should your web filter be any different?

The right solution will be highly customizable, allowing you to configure it to your district's unique needs. For example, if you're looking for extra protection, you may require a solution that offers multiple filtering techniques for more granular control, such as:

URL filtering:

Block specific pages on websites, such as those that contain games or inappropriate content.w

Category filtering:

Filter sites or pages that fall under a particular category, such as adult content, shopping, social media, and more.

Keyword filtering:

Customize policies to account for certain keywords or phrases, filtering all related content. For extra control, you can block specific YouTube channels and videos, or analyze keywords associated with a video using its link.

Not all policies apply to all users. You may want certain websites blocked for students, but accessible to teachers. With Content Filter by ManagedMethods, you can easily apply policies across the entire domain or by organizational unit — no need to copy updates manually from one OU to another.

SAFETY MONITORING AND REPORTING

Back in the day, web filters did little more than the bare minimum: blocking inappropriate content. But now, with school districts more online than ever before and hackers always at their heels, it's time for them to evolve.

How? Two ways:

Safety Monitoring:

Content Filter uses sophisticated artificial intelligence (AI), called Signals, as well as keyword and regex filters to detect risks that could endanger students. It scans user activity, keywords, and content for signs of self-harm, suicide, sexually explicit media, cyberbullying, and toxicity directly in the Chrome browser.

Data Loss Prevention (DLP):

The solution's DLP capabilities can be configured to monitor user behavior for actions that violate your predefined data security policies as well. Using keyword and regex configurations, it identifies potential incidents, such as students sharing personal data or attaching sensitive information to an email.

Together, these features bridge the gap between cybersecurity and safety. And, with comprehensive reporting tools, you'll know exactly which user accounts are associated with policy violations.

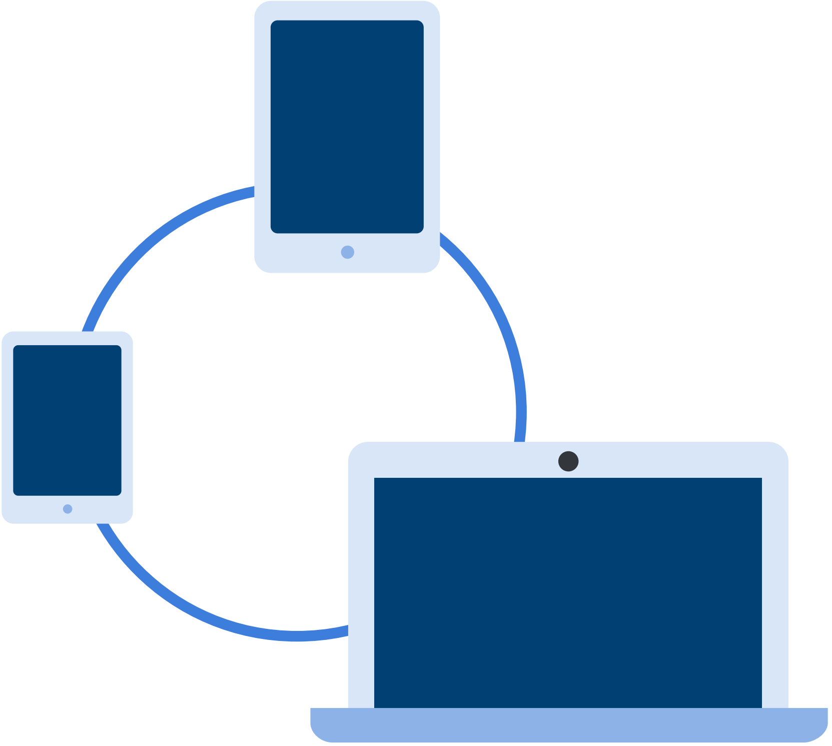
Pull reports based on timeframes, individual users or organizational units, or even specific URLs and keywords. Most importantly, you gain all the insight you need to step into action and protect your students from potential danger and help improve digital citizenship training.

DEVICE MANAGEMENT

Bring-Your-Own-Device (BYOD) and 1:1 policies are increasingly more common in K-12. However, with each additional endpoint, your attack surface grows even further. Consequently, you need to keep watch over the devices you're offering students.

The right solution will make it easy to see a device's last-known location. For instance, browser-based filtering and Google Admin integration can help your administrators keep tabs on devices and how many users are logging into them. They provide insight into the computer's most recent IP address, when users last accessed it, and which version of Chrome is currently running on it.

Using Content Filter on Chromebooks means that you can flag the device as lost or stolen and remotely identify, lock, and (hopefully) recover it. But, if you can't, you can also block anyone who may be using it from accessing the Chrome browser.



SWITCHING PROVIDERS

If you've come to the conclusion that it may be time to consider switching to a new solution, you may be dreading the inevitable transition. So, how can you make it as easy and seamless as possible?

For starters, consider the type of filter you're deploying. Hardware-based tools have to be installed on each individual device, which is both time-consuming and painstaking. Worse yet, you'll have to manually update them over time.

Cloud-based solutions like Content Filter make implementation fast and frictionless. In fact, because it's a browser-level platform and native to Google Admin, it installs within minutes. Plus, it comes pre-loaded with everything you need to hit the ground running — blocklists, allowlists, policies, safety signals, and more.

CONTENT FILTER BY MANAGEDMETHODS

Whether it be blocking malicious websites or detecting signs of self-harm, today's K-12 school districts deserve more from their web filtering providers. The landscape is changing, and it's time for vendors to answer the call with innovative, scalable, and user-friendly solutions.

In this guide, we've discussed five essential criteria you should consider when choosing your next web filtering tool. Luckily, you don't have to search high and low for a vendor that supplies them — you can find them all at ManagedMethods.

With Content Filter, you gain the advantage of an AI-powered, browser-level solution that can keep your students safe from a number of cyber threats — all without sacrificing user experience. And, as a highly customizable tool, you can tailor it to match your changing needs and deliver an engaging, distraction-free learning environment.

Ready to make the switch?

Give Content Filter a spin and request your free demo today.

Managed
Methods

ManagedMethods is on a mission to make online learning safer and more secure for education.

From the browser to the cloud, ManagedMethods makes Google Workspace, Microsoft 365, and browser cybersecurity, student safety, and compliance easy for K-12 school districts—no proxy, no agent, and no special training needed.