White Paper

Ten ‘Must-Have’ Features of a Cloud Filtering Solution

A guide for school administrators and IT leaders

Here are 10 indispensable features you should look for when you are evaluating cloud filtering solutions for your schools.

As K-12 technology continues to evolve, the number of cloud filtering solutions available to schools is growing. But not all products offer the same experience for users. How can K-12 leaders compare the many options that exist?

Obviously, the needs of each school system will vary—and what works well for one school or district might not be the best choice for another. But some features of a K-12 cloud-based web filter are so important that they should be considered indispensable for all schools.

Here are 10 such features that you should look for when you are evaluating cloud filtering solutions for your agency, district or school:

✓ A cloud filtering solution that provides cross-platform intelligence and the same user experience regardless of device, browser, or location.

✓ Granular, policy-based control over social media sites and popular domains.

✓ Transparent user authentication to ensure age-appropriate policy management—and users don’t have to navigate a login screen.

✓ Reliable SSL inspection and controls across *all* devices and web browsers.

✓ Suspicious application management and visibility, so IT administrators can control and block apps that students use to circumvent school web filters.

✓ Real-time monitoring, contextual analysis and alerting to proactively prevent bullying, self-harm, and other harmful behaviors.

✓ Real-time visibility, analytics and comprehensive reporting

✓ Dynamic whitelisting and LMS integration.

✓ Flexible and scalable deployment options.

✓ Highly responsive service and support.

In the remainder of this white paper, we will explore each of these features in more detail—and we’ll explain why it should be considered a critical element of any K-12 cloud filtering solution.

A cloud filtering solution that provides cross-platform intelligence and the same user experience regardless of device, browser, or location.

As Chromebooks have surpassed iPads, MacBooks, and Windows devices as the top-selling mobile technologies in schools, a growing number of school cloud-based web filters have emerged that are designed specifically for the Chrome web browser.

Most of these solutions rely on client apps or Chrome extensions for their functionality. But managing a solution that relies on an app or extension installed on each client device can be challenging.

Whenever the service provider upgrades its software with new functionality, for instance, these changes must be pushed out to each client machine.

What's more, a solution designed specifically for Chrome limits the options available to users. What if a student forgets his Chromebook at home and wants to access the network from an iPhone instead? What if school or district leaders decide to go in a different direction when it's time to refresh devices? "Bring your own device" (BYOD) programs and mixed device learning environments along with IoT and guest networks become problematic when schools take a Chrome only approach to web filtering.

A cloud filtering solution that provides cross-platform intelligence solves these challenges by providing real-time visibility and control of web traffic from *any* device and web browser. In addition, a cross-platform solution allows administrators to apply the same filtering policies that govern students' in-school web use when they take a school-issued device home with them. As a result, students have the same Internet experience—and administrators have the same level of visibility and control regardless of what device students are using or where they're connecting from.

Granular, policy-based control over social media sites and popular domains.

An effective school cloud-based filter should not only provide the same functionality across all browsers, device types, and user locations; it should also enable K-12 leaders to apply very fine-tuned control over the types of content that students can access.

For instance, administrators should be able to set different policies for various student groups, so the Internet access a first grader receives can be more restrictive than that of an eighth grader. Administrators should also be able to set different policies for various times of day, so schools can have one set of rules for classroom use and a separate, less restrictive set of rules for after-school access.

In addition, K-12 leaders should be able to give students access to specific content *within* a website, even if the site is encrypted. For instance, students should be able to watch certain educational videos on YouTube or Vimeo—or read certain educationally appropriate material on social media sites—while still being restricted from inappropriate videos or content on those sites.

Transparent user authentication to ensure age-appropriate policy management—and users don't have to navigate a login screen.

To apply granular, policy-based controls over students' Internet use, administrators need to be able to identify and authenticate each network user. This process should be seamless and transparent, happening automatically in the background when students try to access the network. If students are confronted with a login screen and must enter their password whenever they try to log on, they might not remember their network credentials—resulting in more work for IT support staff.

Often, cloud filtering solutions built around Chrome cannot seamlessly identify users trying to log on with another browser or device type. If the software doesn't recognize a network user, then the user typically receives "guest" privileges under a default web policy. This means a teacher or another adult in the building would be treated the same as a third grader. Not only would they lose the ability to have a customized, age-appropriate Internet experience—but administrators would not be able to tie their network use back to a specific user identity.

Reliable SSL inspection and controls across all devices and web browsers.

Applying granular control over students' Internet use also requires a cloud filtering solution that can decrypt and inspect Secure Sockets Layer (SSL) web traffic across all devices and browsers, not just Chrome.

SSL encryption has become the standard protocol for establishing a secure link between a server and a web browser, and nearly all social media sites and web search engines now use it. If cloud filtering and monitoring tools can't decrypt SSL traffic, they can only see the top-level domain of a requested website, and not the full URL string of either the requested page or the content that is returned.

Without cross-platform SSL intelligence, K-12 leaders don't have granular domain and sub-domain control of YouTube, Vimeo, Facebook, Google and other popular domains, forcing them to over-block access to valuable online educational content. They must either block or allow access to the top-level domain—meaning they would have to let students access all of YouTube, for example, or else block YouTube videos altogether. In contrast, granular domain and sub-domain controls enable the educational use of popular domains while blocking misuse, ensuring student safety and policy compliance.

SSL decryption can create significant challenges if not designed well and can negatively impact the learning experience. Therefore, when evaluating a cloud filtering solution ensure the solution offers a superior design that can decode, inspect, filter, and log the full URL string for SSL-encrypted traffic to and from any website across all platforms and browsers —resulting in real-time visibility and control over *all* web traffic, including BYOD, IoT and guest networks.

Application management and visibility, so administrators can control and block Apps that students use to circumvent school web filters.

Students often try to use web-based or native applications that violate their school or district's Internet Use policy. For instance, they might use Spotify to stream music, Skype to message their friends, BitTorrent for peer-to-peer file sharing, or tunneling Apps such as UltraSurf, Tor or Psiphon to circumvent the web filter. An effective cloud filtering solution should be able to recognize the unique signatures of these applications and block or deter students' use of these tools.

ContentKeeper, for example, can identify a variety of tunneling applications that students might download. When the system identifies an App like UltraSurf or Tor, it can notify the user that his or her network privileges will be suspended unless the App is shutdown.

Real-time monitoring, analytics and alerting to proactively prevent bullying, self-harm, and other harmful behavior.

Keeping students safe while they're online is important, but keeping them safe offline is critical, too. Growing up can be hard for students both socially and emotionally, and adolescents face a number of threats to their well-being—from thoughts of suicide, to experimentation with drugs or alcohol, to bullying, sexual assault, or even gun violence.

A cloud filtering solution that can recognize certain warning signs and alert administrators in real time allows K-12 leaders to create a safer environment for their students. For instance, ContentKeeper's behavioral intent alerting technology monitors students' web searches for indicators of potentially harmful behavior, and if a match is found, the system alerts a designated administrator. What's more, comprehensive analytics evaluate the *context* of the student's web search, to determine urgency and if immediate follow-up action is required.

Comprehensive, enterprise-class reporting and analytics that identify and detail specific users and subdomains.

Effectively managing digital and virtual learning requires administrators to know what students are doing online and which sites they are trying to access. To remain CIPA compliant and enforce Acceptable Use Policies, K-12 leaders need comprehensive insight into students' Internet use, with real-time visibility, intelligent dashboards, in-depth analytics and forensic-level reporting that can identify which users have accessed inappropriate, malicious or non-policy compliant content on the web.

Ideally, this reporting should be centralized as well as comprehensive. Administrators should be able to view this information from a single, centralized source, so they don't have to waste time tracking down the information they need to investigate an incident. Therefore, the ideal cloud filtering solution should offer "single pane of glass" management and seamless reporting for *all* web users across all devices, whether they are on or off campus.

Try it for yourself! Email **sales@microshare-inc.com** to set up a free demo.

Dynamic whitelisting and LMS integration.

If a teacher finds a useful instructional video on a resource such as Vimeo or YouTube, he or she can request that the specific link to the video be unblocked. This adds work for the IT administrators charged with making the change, and it can sometimes take days for such a request to be fulfilled. By that time, the teacher might have moved on to another topic in class.

A dynamic video whitelisting feature solves this problem by empowering teachers to give students instant access to videos and other resources that are hosted on blocked websites. For instance, ContentKeeper integrates with leading learning management systems such as Canvas, Schoology, and others. This integration allows teachers to post a link to a video from a blocked website on their class LMS page—and then students can access the video directly and seamlessly from within the LMS. Teachers don't have to wait for IT staff to allow access to the link, instruction can continue uninterrupted—and everyone benefits.

Flexible and Scalable Deployment Options

An ideal cloud filtering solution should offer multiple cloud, hybrid and on-premises deployment options to meet individual agency, district or school requirements. It should also provide a seamless deployment approach without interrupting operations and scale on demand.

Highly responsive service and support.

A cloud filtering solution should just work. But even so, there might be times when users have questions. When this is the case, users should be able to call customer support and get a timely, friendly, and accurate response. ContentKeeper is known for its superior customer service. Network Engineers have extensive experience in supporting K-12 networks.

The Bottom Line

As you are evaluating cloud-based web filters for use in your schools, pay attention to these 10 key features that matter. ContentKeeper excels in all 10, making them the leading cloud filtering provider in the market.