Securing Web Use for K-12 Schools

The internet presents huge educational opportunities coupled with very serious risks to student safety.

On the positive side, the web offers cost-effective access to essential educational resources, programs and information. It enables collaborative learning and serves as the ultimate research tool. Web-enabled assistive technologies and IEP platforms offer teachers the ability to personalize curricula and materials for students with diverse learning styles and educational needs.

For administrators, web and SaaS applications help optimize school management, streamline documentation of performance and regulatory compliance, and facilitate ongoing communication with parents, staff, students and oversight bodies.

On the flip side, of course, are the risks posed by the web to students, teachers, school district leaders, school administrators, technology officers and IT staff. These range from students' exposure to inappropriate content to cyberattacks that can – and do – shut down schools, cost hundreds of thousands of dollars to remediate, breach sensitive data, and expose schools to regulatory penalties and legal risk.

How Ericom Zero Trust Security Solutions Protect K-12 Schools

Ericom Zero Trust Web Security leverages cloud-based remote browser isolation (RBI) to airgap user devices from the internet. It provides granular access and security controls to protect users from malicious or inappropriate content, while protecting school apps, networks and data from cyberattack.

ericom security by cradlepoint

Ericom Zero Trust Security for Schools at a Glance

- Role-based internet filtering for students, faculty, and staff
- Blocks access to blocklisted sites and noncompliant content on unblocked sites
- Restricts use of Generative AI sites
- Prevents phishing, ransomware and breaches of sensitive data
- Clientless Zero Trust Network Access (ZTNA) simplifies and secures access from unmanaged devices
- Eliminates over-blocking of websites typical of many traditional security solutions
- Applies CDR to prevent attacks via weaponized downloaded files
- Assists with CIPA compliance
- Transparent to users

Protection of apps from breach

Ericom WAI secures schools' private and web applications and SaaS solutions to secure them from hackers and unauthorized access. Isolating apps in the cloud protects them from threat actors probing for vulnerabilities and ensures that only authorized users have access.

Secure virtual meetings

As the only RBI-based solution that secures virtual meetings like Zoom, Google Meet and Teams, Ericom Virtual Meeting Isolation (VMI) enables schools to ensure that no sensitive data is exposed during virtual meetings and that hackers cannot penetrate via meeting apps.

Flexible, role-base web filtering

Within the cloud, Ericom Web Security applies easy-to manage identity-based policy controls to granularly restrict access by user identity or role, as well as by site category or individual URL, in compliance with acceptable use guidelines. Sites and downloads may be fully blocked to comply with regulations, blocked for specific categories of users, or selectively filtered for non-compliant content.

Social media sites, for example, include useful information as well as content that's inappropriate or might be used for cyber-bullying. Ericom granular domain controls allow secure access to acceptable material while filtering out inappropriate content. Similarly, Generative AI sites can be blocked or their use restricted to reduce AI misuse for schoolwork.

Protection from phishing and web-delivered threats

Ericom Web Security executes all sites – including sites opened from email links – in cloud-based virtual browsers that are airgapped from user devices. Only safe rendering data is streamed to users' browsers, where users enjoy an excellent experience and interact just as they would with native web content.

No active content – even zero-day exploits that detection-based solutions fail to stop – reaches user devices, so school networks remain safe from malware, ransomware and breach. Untrusted sites can be opened in read-only mode to prevent users from entering credentials and content disarm and reconstruct (CDR) is applied in the cloud to documents prior to download to eliminate weaponized content.

Prevention of data loss and PII exposure

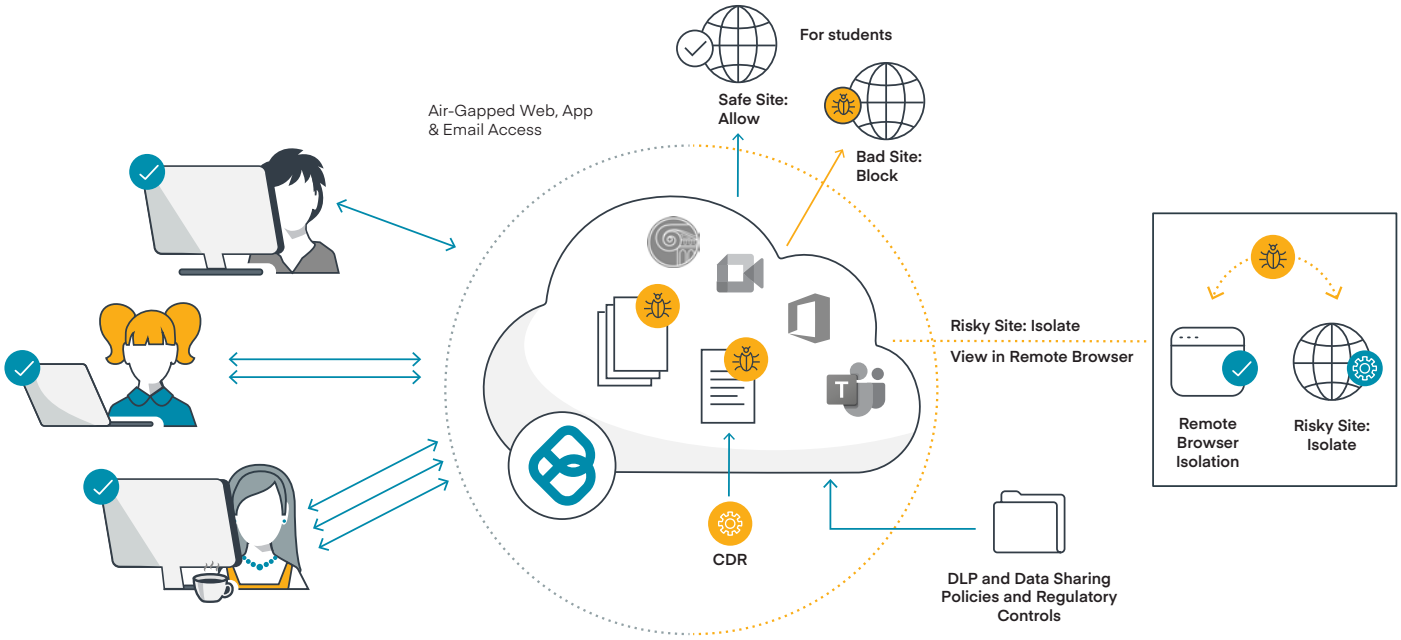
Advanced clip-boarding and data sharing controls prevent data exfiltration from private, web and SaaS apps. Data loss prevention (DLP) is applied in the cloud to block exposure of sensitive personal information.

Secure access from any device and any location

Ericom Clientless Web Application Isolation (WAI) enables schools to filter web content when students log on remotely via school networks. It also protects sensitive student data and apps from breach via unmanaged, potentially compromised personal devices used by students, teachers and administrators.

The Bottom Line

Ericom Security Solutions for K-12 schools protect students from harmful content and support compliance. They prevent exposure of sensitive data and safeguard schools from web-originated cyberattacks. The solutions are transparent to users, easy to integrate with existing infrastructure and simple to manage and use.



Discover how Ericom solutions for K-12 schools can protect your students from exposure to harmful content and your sensitive data from cyberattacks.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service.