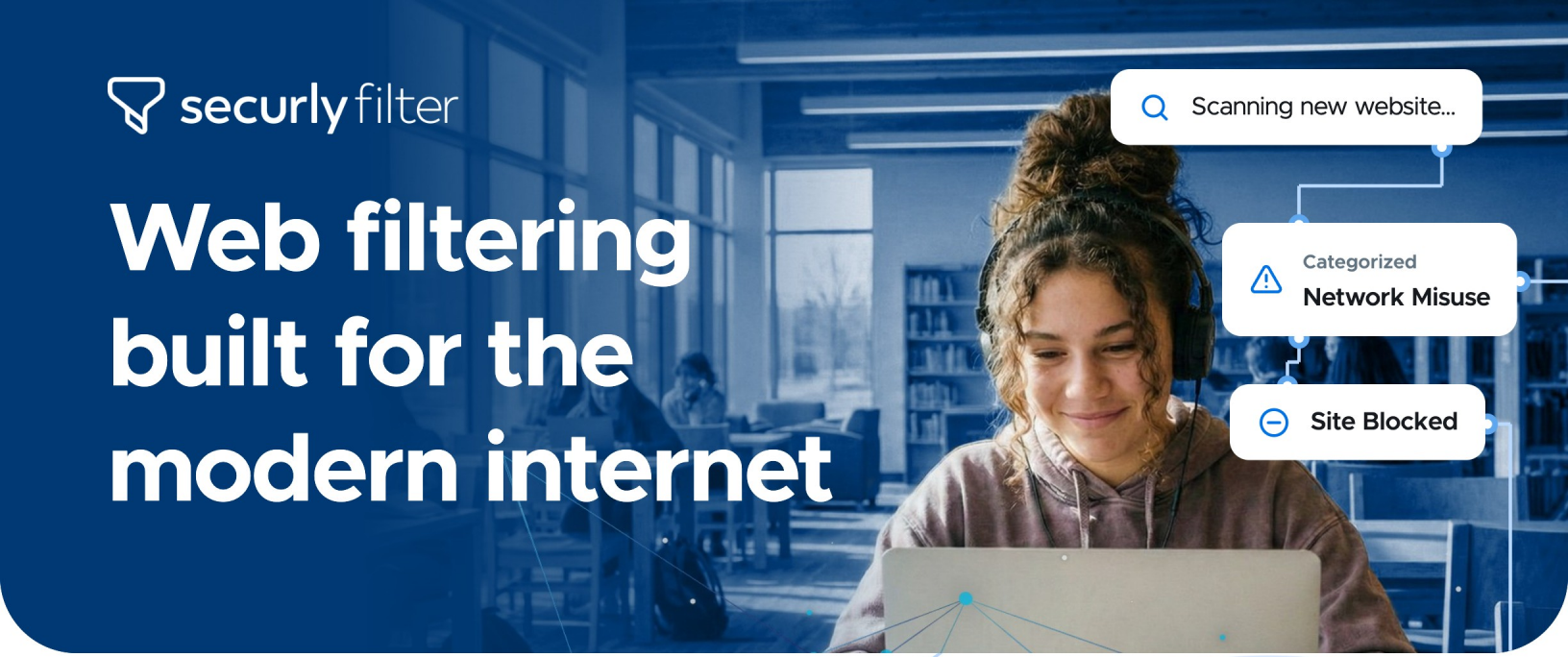
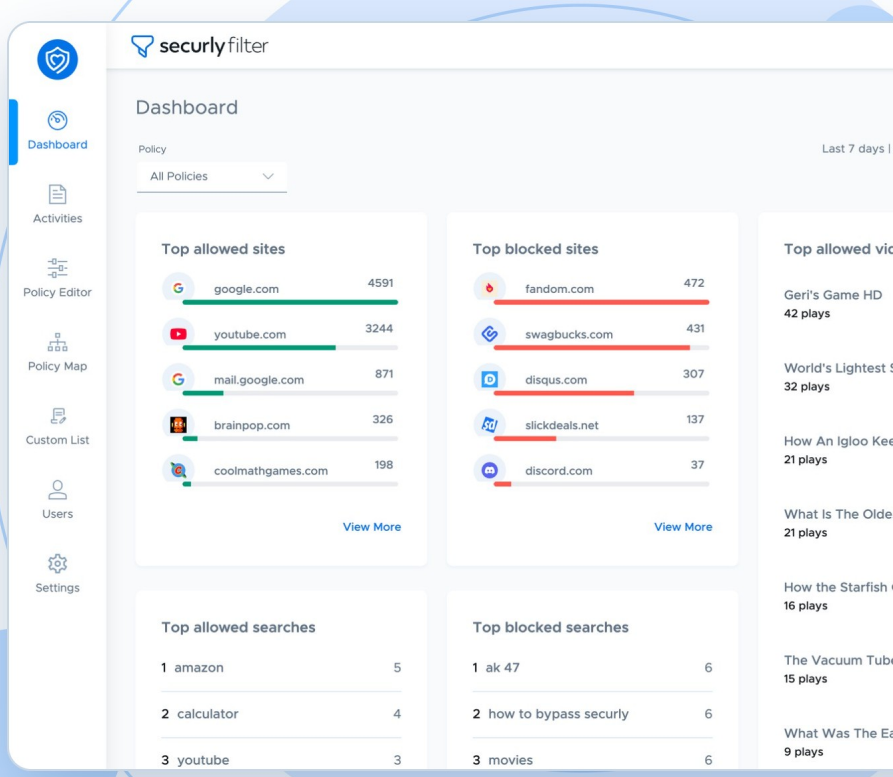
securly filter

Web filtering built for the modern internet



With Securly Filter, you can...

- **Filter any device, anywhere**
- **Get user-level reporting on iPads** without requiring students to log in
- **Apply custom policies** to off-network and BYOD devices
- **Scale without bandwidth limits** or on-site hardware
- **Give parents control** of school devices when they go home
- **Make your district proxy-proof** with real-time site classification and proxy detection powered by AI



20% of US K-12 internet traffic is filtered by Securly

8.6 M+ students are protected by Securly Filter

"Securly's site categorization has been so effective that ***we have not received a single request to unblock a site this school year. This is unprecendented"***

Cory Ulrich, System and Database Administrator
Elgin School District U-46, Illinois

Automatically block proxies the moment they appear

For as long as schools have filtered the internet, students have found ways to get to their favorite non-educational sites. What started as simple proxy sites has evolved into an ecosystem of professional proxy technologies that are purpose-built to defeat your content filter. Securly Filter uniquely approaches these problems with three next-generation engineering solutions that keep students off proxy sites 24/7.

PageScan

PageScan uses finely tuned AI to read a new page's text, metadata, images, and structure in real time, even when proxy sites try to disguise themselves as educational ones. When PageScan finds a new proxy site, it is blocked for all 8.6 million students that use Securly Filter immediately.

Proxy Unmasker

Proxy Unmasker is a tool purpose-built for sites that try to disguise themselves. It uses techniques learned from the thousands of proxy sites its seen to unlock and identify proxy sites.

Domain Families

Domain Families groups sites that share the same code together. When one site in a family is identified, the rest are blocked with it.

How Securly Filter works

1 Traffic is captured

Securly Filter captures web traffic from on-campus users through our **browser extension** or **SmartPAC** for managed devices, and **SmartDNS** for BYOD or other unmanaged devices.

It also captures traffic from your managed devices that go off campus.

2 Filter applies policy

filter

Detects the user and applies the appropriate policy

3 The request is resolved

- **Allowed**
  The page is served as normal
- **Encrypted sites**
  Selectively decrypted, then allowed or blocked
- **Blocked**
  A block page is shown, with an optional alert to admins
- **AI chat sites**
  Optionally, redirect AI chat sites to Securly AI Chat for added control

Securly is commited to student data privacy and security

Certified and audited

iKeepSafe certifies Securly for FERPA, COPPA, CSPA, and relevant state data privacy laws. An independent audit backs Securly's SOC 2 Type 2 certification.

Protected and never sold

Student data is encrypted with AES-256 at rest and TLS in transit. Securly does not sell, rent, or trade student data, and student AI usage data is never used to train AI models.

Powerful core filtering technology

PageScan: Analyzes webpage text, structure, and metadata in real time using AI to automatically categorize and block inappropriate or newly created websites.

AI-Powered Proxy Detection: Scans site traffic patterns and metadata to identify and block web proxies and circumvention tools before students can bypass school filters.

Live activity feed: See a real-time visual audit trail of student browsing that includes visited sites, exact search queries, and video thumbnails.

Custom Groups: Group students and map specific filtering policies flexibly without having to modify directory structures in Google Workspace or Microsoft Azure.

Custom Lists: Build a collection of resources once and apply it across multiple policies. When you update a list, every policy associated with it updates automatically.

Extension-based filtering: Provides lightweight, browser-level policy enforcement across Chrome and Edge devices both on and off campus.

SmartPAC: Our patented technology that lets you get agentless, user-level filtering and reporting for iOS devices without requiring young students to sign in.

SmartDNS: Delivers network-level filtering and selective proxying for unmanaged devices, guest networks, and BYOD environments without requiring installed agents.

Image Blurring: Automatically detect and blur sexually explicit images on normally allowed pages, like image search results. Customize the detection threshold and blur strength.

GuestDNS: Applies secure filtering to guest Wi-Fi networks to prevent misuse while isolating guest traffic from core district networks.

Delegated administration: Grant policy editing and site-unblocking privileges for specific organizational units to designated teachers or staff members.

Scheduled & Shared Reporting: Generates automated, downloadable reports detailing browsing trends, blocked traffic, and user activity across specific organizational units.

Features designed for K-12

Granular YouTube controls: Get detailed oversight over YouTube access by allowing or restricting content by channel, category, or specific videos, even without Google Admin.

Time-based policies: Schedule dynamic filtering policies that automatically adjust access permissions according to the time of day, such as after school hours.

Selective SSL decryption: Inspects encrypted web traffic selectively to uphold student data privacy while maintaining visibility over unmanaged and BYOD devices.

Take-Home Policies: Establish filtering configurations that activate specifically when school-managed devices leave the district network.

Included with Securly Filter

Securly AI Transparency

See how students really use AI tools, and keep that use within your district policy.

Securly Reveal

Know how much screen time students are getting, and which apps are actually used

Securly Home

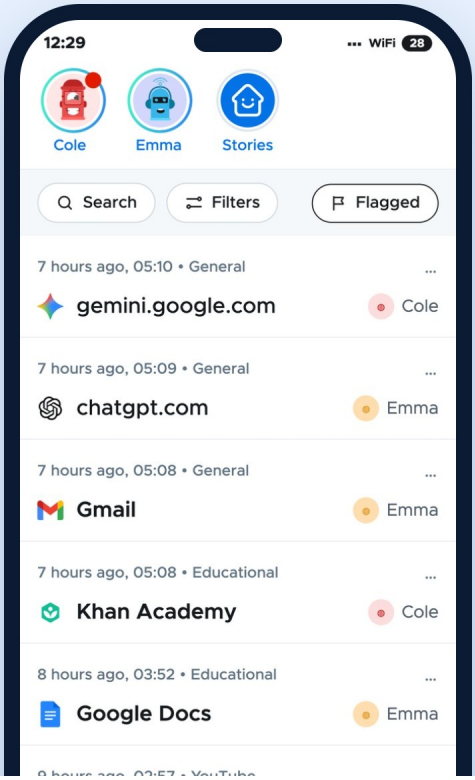
Promote family engagement and customize parents' control over devices when they goes home

Give parents control when devices go home

securlyhome

Customizable control and visibility for families

- Parents can allow or block specific sites and content categories on the school device at home.
- A live activity feed and optional alerts flag searches and activity related to self-harm or bullying.
- Parents can pause the internet instantly or schedule offline hours for dinner or bedtime.
- Give parents access to their child's AI conversations from their school-owned device, including deflected prompts.
- Whether you want to show only at-home, educational, or all activity, you choose what data parents can see.



Works with the rest of Securly safetyOS™

securlyclassroom

Easy-to-use classroom management software that lets teachers see student screens during class, push resources, and teach without digital distractions.

With Securly Filter: Put an end to unblock requests. Teachers can temporarily override Filter restrictions for their students, during an active class session.

securlyaware

Scan student online activity for signs of self-harm, bullying, and violence, and give school staff the tools they need to follow up on alerts and help proactively.

With Securly Filter: Safety alerts come with more context, so you can see what happened before and after a students' flagged activity.

Make security simple with cloud-based web filtering designed for schools

We'll show you how Filter handles new proxy sites, take-home devices, and student AI use, and answer questions about your district's setup.

Book a demo at securly.com/filter-demo or scan the code.

securly sales@securly.com 1-855-SECURLY www.securly.com
© 2026 Securly. All rights reserved.