



Stay Ahead of Student Bypass Attempts: Filter by Page Content, Not Just Domain

Most content filters can only block what they already know. That leaves two gaps that students actively exploit — and that put your district at risk. **Blocksi's Smart Proxy Detection** and **AI Context Filter** are built specifically to close them.

The Problem

Static blocklists and category databases can't keep up with the speed of the internet. Two gaps consistently emerge:

- **Harmful content on allowed domains** — a page on a permitted site can contain content that violates policy, but a traditional filter only sees the domain, not what's actually on the page.
- **New proxy and VPN bypass tools** — freshly created proxy sites can take up to two days to be categorized. During that window, students can use them freely.

These aren't edge cases. They're the two most common ways students get around school content filters today.

Smart Proxy Detection

Smart Proxy Detection identifies and blocks websites that exhibit proxy or VPN behavior — even before they've been officially categorized. It closes the gap between when a new proxy site is created and when it gets officially rated.

When enabled, it detects web-based VPNs, tunneling pages, and traffic-hiding or redirection behavior, and flags those sites as *Proxy Avoidance* — applying your existing blocking policy immediately. It operates as a simple toggle within the *Web Filter* in the **Blocksi Admin Dashboard**.

With vs. Without Smart Proxy Detection

Scenario	Without Smart Proxy Detection	With Smart Proxy Detection
Student visits new proxy site (created yesterday)	Not yet rated → accessible for up to 2 days	Proxy behavior detected → blocked immediately
Student uses VPN-based browser tool	May not be categorized yet → accessible	Traffic-hiding behavior flagged → blocked

AI Context Filter

Blocksi's AI Context Filter doesn't stop at what the traditional web filter decides. **It analyzes the actual content of every page** the traditional filter allows through — and **applies your filtering policy based on what's actually there.**

Key facts

- Processes approximately **500,000 classification requests per day**
- Runs via the **Blocksi Chrome Extension** on student devices
- Catches harmful content on **any page the traditional filter allows through** — including pages on permitted domains
- For previously visited URLs, filtering is **instant** — results returned in **milliseconds**
- Supports **Allow, Block, or Warn** actions per category

What It Catches That Traditional Filters Miss

Scenario	Traditional Filter 	Blocksi AI Context Filter 
Student visits newly registered harmful site	Not in database → loads	Content analyzed → blocked
Student accesses harmful page on allowed domain	Domain allowed → loads	Page content evaluated → blocked



Stronger Filtering, Less Maintenance

Together, Blocksi's **AI Context Filter** and **Smart Proxy Detection** go beyond what traditional domain-based filtering can see — evaluating page content in real time and blocking proxy bypass attempts **before they're even categorized.**

Neither feature requires manual updates or admin intervention to stay current — they work in the background within your existing Blocksi setup.

See It in Action

Book a demo with Blocksi

or contact our team at sales@blocksi.net