USERAUTHGUARD

BLOG PRODUCT

Why Schools Are Switching from Securly to AuthGuard

Stef Verleysen | April 25, 2026

> Discover why K-12 districts are adding AuthGuard alongside or instead of Securly for device lifecycle management, inventory tracking, repair workflows, and 1:1 assignment capabilities that go beyond content filtering.

Securly has earned a strong reputation in K-12 technology circles, and for good reason. Its content filtering and student safety monitoring tools have helped thousands of schools meet CIPA compliance requirements and keep students safe online. But as 1:1 Chromebook programs have matured, many IT directors are discovering that filtering and monitoring are only part of the device management puzzle, and the missing pieces are costing them time, money, and sanity.

Over the past two years, a growing number of districts have added UserAuthGuard to their technology stack, and in some cases replaced Securly entirely, because they need capabilities that a filtering-first platform was never designed to provide. This article examines where Securly excels, where it falls short for IT operations, and why the **securly vs authguard** comparison often leads districts to a clear conclusion about what their device program actually needs.

Where Securly Excels

Before diving into the comparison, it is important to acknowledge what Securly does well. Any honest **securly vs authguard** evaluation starts with recognizing Securly's strengths:

- **Cloud-based content filtering:** Securly's DNS-based filtering works across networks and off-campus, providing consistent web filtering regardless of where a student uses their Chromebook. It is one of the most widely deployed K-12 filtering solutions in the country.
- **Student safety monitoring:** Securly's AI-driven safety alerts scan student activity for signs of self-harm, bullying, and other concerning behavior. For districts with limited counseling resources, these alerts can be genuinely valuable.

- **Parent engagement:** Securly's parent portal gives families visibility into their child's online activity and the ability to set home-use restrictions, extending the school's safety net beyond campus hours.
- **CIPA compliance:** For schools receiving **E-Rate funding**, Securly provides straightforward CIPA compliance documentation and reporting.

These are meaningful capabilities, and many districts will continue to use Securly for exactly these purposes. The question is not whether Securly is a good filtering tool. It is. The question is whether filtering alone constitutes a complete device management strategy. **CoSN's research on K-12 IT operations** consistently shows that device lifecycle management, not content filtering, is the top operational cost driver for school technology programs.

The Gap: What Securly Was Never Built to Do

Securly was designed as a student safety and content filtering platform. It was not designed to manage the operational side of a 1:1 device program. When IT directors evaluate the full scope of what it takes to run a successful Chromebook fleet, they consistently identify gaps in these areas:

Device Lifecycle Management

A Chromebook's lifecycle extends far beyond its time in a student's hands. Devices need to be procured, received, enrolled, tagged, assigned, monitored, repaired, reassigned, and eventually retired or recycled. Securly does not track where a device is in this lifecycle. It cannot tell you which devices are in the repair depot, which are in the spare pool, or which are approaching end of life.

UserAuthGuard tracks every device from the moment it enters your inventory to the moment it is decommissioned. Every transition, whether it is an assignment change, a repair event, or a status update, is recorded with timestamps and audit trails. This complete lifecycle visibility is what separates device management from device monitoring.

Inventory Tracking and Asset Management

When your superintendent asks how many working Chromebooks you have available for a new program, can you answer in under 60 seconds? With Securly, the answer is almost certainly no, because Securly does not maintain an operational inventory. It knows which devices are enrolled in your Google domain and what students are browsing, but it does not track spare pools, repair parts, accessories, or device condition.

UserAuthGuard's **inventory management** gives you a real-time count of every device and accessory in your ecosystem, broken down by status, location, model, and condition. You know exactly what you have, where it is, and whether it is available for deployment.

Repair Workflows

Broken Chromebooks are an inevitable part of any 1:1 program. What matters is how quickly and efficiently you can get them back into students' hands. Securly offers no repair tracking capability. When a student reports a cracked screen, your IT team needs a separate system to log the repair, track parts, manage the queue, and notify the student when the device is ready.

UserAuthGuard provides end-to-end repair workflow management, from intake to diagnosis to parts ordering to completion. Devices move through configurable service stages with clear ownership at every step. Your techs see their full queue, your principals see repair metrics for their building, and your students know when to expect their device back.

1:1 Device Assignment

Knowing which student is assigned to which device is foundational to any accountability program. Securly can tell you who last logged into a device, but it does not maintain formal assignment records. There is no concept of device check-out, no condition documentation at handoff, and no assignment history.

UserAuthGuard's **1:1 device assignment** system maintains a complete record of every device-to-student relationship, including check-out dates, condition at handoff, and digital acknowledgments. When a device goes missing, you know exactly who had it, when they received it, and what condition it was in.

What Schools Discover They Actually Need

The shift from Securly to UserAuthGuard (or adding UserAuthGuard alongside Securly) typically happens when an IT director steps back and evaluates the full scope of their device management responsibilities. Here is what that self-assessment usually reveals:

Beyond Filtering: The Complete Device Management Picture

Content filtering addresses one dimension of device management: controlling what students access online. But IT directors are responsible for much more:

- **Asset accountability:** Knowing where every device is and who is responsible for it at all times.
- **Operational efficiency:** Minimizing the time between a device breaking and a student having a working replacement.

- **Financial stewardship:** Tracking the total cost of ownership across procurement, repair, replacement, and retirement.
- **Compliance reporting:** Demonstrating to the school board, auditors, and grant agencies that publicly funded devices are tracked and accounted for.
- **Staff productivity:** Giving technicians, teachers, and administrators the tools they need without drowning them in manual processes.

Securly addresses the first bullet point only partially (through monitoring, not assignment tracking) and does not address the remaining four at all. This is not a criticism of Securly; it is simply not what the product was built to do.

Feature Comparison: Device Management Capabilities

When districts conduct a formal **securly vs authguard** comparison focused on device management, here is what they typically find:

Device Assignment and Tracking

- **Securly:** Tracks last login and browsing activity per device. No formal assignment system. No check-in/check-out workflow. No condition documentation.
- **UserAuthGuard:** Full 1:1 assignment with timestamped records, digital acknowledgments, condition photos, bulk assignment via CSV, and complete assignment history for every device.

Inventory Management

- **Securly:** Lists enrolled devices visible through Google integration. No spare pool tracking, no accessory management, no custom status fields.
- **UserAuthGuard:** Comprehensive inventory with device status tracking (deployed, spare, repair, retired), accessory management, parts inventory, warranty tracking, and real-time fleet health dashboards.

Repair and Maintenance

- **Securly:** No repair tracking capability. Districts need a separate system for repair workflows.
- **UserAuthGuard:** Configurable repair queue with service workflows, parts tracking, loaner device management, repair cost tracking, and technician workload balancing.

Reporting and Compliance

- **Securly:** Strong reporting on web activity, safety alerts, and filtering effectiveness. Limited reporting on device fleet operations.
- **UserAuthGuard:** Comprehensive operational reporting including device utilization, loss rates, repair turnaround, cost analysis, and board-ready compliance reports.

Google Workspace Integration

- **Securly:** Integrates with Google for user authentication and basic device identification.
- **UserAuthGuard:** Deep bi-directional sync with Google Admin console including OU management, device enrollment data, policy compliance monitoring, and automated OU placement based on device assignment.

Pricing Considerations

Cost is always a factor in K-12 technology decisions. When comparing **securly vs authguard** pricing, districts should consider the total cost of their device management ecosystem, not just the sticker price of individual tools. The **CoSN Total Cost of Ownership framework for K-12 technology** provides a structured way to compare platforms beyond subscription price alone.

Securly's pricing is typically per-device per-year for its filtering and safety features. If you add Securly's device management add-ons (which are more limited than purpose-built platforms), the per-device cost increases accordingly.

UserAuthGuard is priced specifically for device lifecycle management and often costs less than adding device management add-ons to a filtering platform. More importantly, districts should calculate the cost of not having proper device management: lost devices that are never recovered, extended repair turnaround times that require larger spare pools, and staff hours spent on manual tracking and spreadsheet maintenance.

Many districts find that the combination of UserAuthGuard's device management plus a dedicated filtering solution (whether Securly or an alternative) costs about the same as Securly's premium tiers, while providing significantly deeper capabilities in both areas. Check the **detailed Securly comparison page** for current pricing breakdowns.

The Migration Path: Moving from Securly to UserAuthGuard

For districts that decide to add UserAuthGuard to their stack, the migration is straightforward because UserAuthGuard and Securly operate in largely non-overlapping domains. Here is what a typical transition looks like:

Phase 1: Parallel Deployment (Weeks 1 through 2)

1. Deploy UserAuthGuard and connect it to your Google Workspace domain.
2. Import your existing device inventory from Google Admin and any spreadsheets you are currently using for tracking.
3. Configure your organizational structure (schools, grade levels, device groups).
4. Keep Securly running unchanged during this phase.

Phase 2: Assignment and Inventory Setup (Weeks 3 through 4)

1. Map existing device-to-student assignments in UserAuthGuard, either through bulk import or SIS integration.
2. Set up your repair queue and service workflows.
3. Configure automated monitoring and alerting rules.
4. Train IT staff on the new workflows.

Phase 3: Operational Cutover (Weeks 5 through 6)

1. Begin using UserAuthGuard as your primary device management and assignment platform.
2. Retire any spreadsheets or manual tracking processes that UserAuthGuard replaces.
3. If keeping Securly for filtering, no changes needed on that side.
4. If replacing Securly entirely, evaluate alternative filtering options that focus specifically on content filtering and CIPA compliance.

The entire process typically takes four to six weeks with minimal disruption because you are adding new capabilities rather than replacing existing ones.

When Schools Use Both Tools Together

Many districts choose to run UserAuthGuard and Securly side by side, and this is a perfectly valid approach. In these deployments, each tool does what it does best:

- **Securly handles:** Content filtering, student safety monitoring, parent portal for web activity, and CIPA compliance documentation.

- **UserAuthGuard handles:** Device assignment and accountability, inventory management, repair workflows, compliance reporting for device fleet operations, and Google Workspace integration for device lifecycle management.

This dual-platform approach gives districts best-in-class capabilities in both safety monitoring and device management without forcing compromises in either area. The platforms do not conflict because they serve different operational needs.

When Districts Replace Securly Entirely

Some districts choose to move away from Securly completely when they adopt UserAuthGuard. This usually happens when:

- The district is already using a different content filtering solution (GoGuardian, Lightspeed, Linewize, or their firewall's built-in filtering).
- The district's primary pain point is device management, not filtering, and they want to consolidate their technology spend.
- UserAuthGuard's **keyword alert capabilities** address the district's student safety monitoring needs without requiring a separate platform.
- Budget constraints make it difficult to justify two per-device subscriptions when one addresses the district's most pressing needs.

Real-World Switching Scenarios

Here are three common scenarios we see when districts evaluate **securly vs authguard**:

Scenario 1: The Growing District

A district with 5,000 Chromebooks started with Securly three years ago for filtering and safety. As the fleet grew, the IT team realized they were spending 20+ hours per week on spreadsheet-based device tracking. They added UserAuthGuard for device management while keeping Securly for filtering. Result: the combined cost was only marginally higher than Securly alone, but the IT team recovered over 15 hours per week in manual tracking time.

Scenario 2: The Budget-Conscious District

A rural district with 2,000 devices was paying for Securly's premium tier, which included some basic device management features. When they compared Securly's device management capabilities against UserAuthGuard's, they found UserAuthGuard offered significantly more depth

for a similar price. They switched to a lower-cost filtering solution plus UserAuthGuard, reducing their total spend by 18% while gaining much stronger device management capabilities.

Scenario 3: The Post-Audit District

After a state audit revealed that a suburban district could not account for 340 Chromebooks purchased with federal grant funding, the IT director needed a device management solution immediately. Securly could confirm the devices had been enrolled but could not provide assignment histories, condition records, or chain-of-custody documentation. The district deployed UserAuthGuard within two weeks and recovered 280 of the 340 devices through automated tracking and parent notifications within the first month.

Making the Right Choice for Your District

The **securly vs authguard** decision is not really about choosing one over the other. It is about understanding what your device program needs and selecting the tools that address those needs most effectively. **Futuresource Consulting's K-12 market research** notes that districts with mature 1:1 programs increasingly separate content filtering tools from device lifecycle management platforms, using best-in-class solutions for each function.

If your primary challenge is content filtering and student safety, Securly is a strong choice. If your primary challenge is device management, inventory tracking, repair workflows, and operational accountability, UserAuthGuard is purpose-built for exactly those problems. And if you need both, the two platforms work well together.

Ask yourself these questions:

- Can I tell you exactly how many working Chromebooks are available in our spare pool right now?
- Do I have a complete assignment history for every device in our fleet?
- Can I show the school board our device loss rate, average repair turnaround, and total cost of ownership?
- Do my technicians have a structured repair queue, or are they working from sticky notes and email?

If you answered no to any of these questions, you have a device management gap that content filtering cannot fill.

See UserAuthGuard in Action

The best way to understand what UserAuthGuard can do for your district is to see it working with your own data and workflows. Our team will walk you through the platform, answer your questions, and help you evaluate whether UserAuthGuard is the right fit, whether alongside Securly or as a standalone solution.

Schedule a personalized demo and see how UserAuthGuard can close the device management gaps in your 1:1 program.