PO SECURITY

Security without sacrifice: CommonLit uses PO Security to balance developer autonomy and SOC 2 compliance

CommonLit

About CommonLit

CommonLit is a nonprofit delivering high-quality literacy curriculum to millions of students and teachers worldwide.

Over the past decade, the CommonLit team has delivered on the belief that the right tools could transform teaching.

Today, they deliver an easy-to-use and affordable program for all thousands of schools to accelerate student learning.

Overview

Education is under attack. School districts across the U.S. are increasingly targeted by ransomware and data breaches—including a high-profile case involving leaked sensitive psychological notes about students in major districts.

As a result, many states have begun enforcing SOC 2-level expectations for vendors, even without formal mandates.

CommonLit needed to up their compliance posture—not only to demonstrate strong access controls and satisfy audit requirements, but to protect something even more fragile: trust in the classroom.

Challenge

With rising security demands and just nine engineers, the CommonLit team needed to secure access to their cloud environments without introducing complexity or slowing development.

Their solution had to preserve classroom trust and engineering velocity, with evolving compliance standards like SOC 2. Even a two-hour access delay is considered a deal-breaker for CommonLit's lean, high-performing team.

CommonLit

> We pay for top-tier engineers. Every hour they lose because of access bottlenecks is unacceptable. P0 lets them move fast without making compromises.
>
> Before P0, I would probably burn three and a half hours a quarter just taking screenshots for audit purposes."

Geoff Harcourt,
Chief Technology Officer,
CommonLit

Solution

When Indent—an access request platform built for IAM workflows—announced its end-of-life, the CommonLit team began searching for a replacement that could do just-in-time access management and integrate with Tailscale, their zero-config VPN used to securely connect services and users across their environment.

Most options were oversized and overpriced—built for legacy on-prem environments, bundling features they didn't need. What they wanted was a fast, clean, Slack-native tool for managing just-in-time access to AWS and GitHub—with auditability and ease of use.

That's when they found P0 Security.

P0 now governs access to CommonLit's most sensitive systems, enabling engineers to request time-bound access via Slack. During incidents, on-call engineers can temporarily add themselves to a GitHub "hotfix" team, push a critical change, and automatically have access revoked with every step logged for compliance.

By eliminating lingering permissions and manual user group cleanup, P0 also saves hours of audit prep time each quarter, reducing risk and effort for a small team with limited bandwidth.

Why It Matters

CommonLit competes with some of the largest textbook publishers in the country—but as a lean nonprofit, its superpower is speed.

That only works if the team can stay secure and compliant without adding friction. With Tailscale and P0, CommonLit built a modern, nimble access stack that protects student data, meets SOC 2 standards and keeps learning uninterrupted.

CommonLit

> If we go down for eight minutes in the middle of a 45-minute class, teachers may never trust us again. You lose the thread with students—and the whole experience can break down."

Geoff Harcourt,
Chief Technology Officer, CommonLit

Results

Incident response and operational resilience

- **Faster incident response:** On-call engineers can self-serve access during emergencies without waking teammates.
- **Minimized bottlenecks:** By distributing access approvals across the team, P0 reduces the risk of blocking work during critical incidents or PTO.
- **Small team, enterprise posture:** P0 gives a nine-person team the security rigor and operational agility to compete with the largest education providers.

Compliance and audit readiness

- **SOC 2 compliance, made tangible:** CommonLit can confidently demonstrate that no individual can change production without peer review.
- **Streamlined audits:** Groups remain empty by default, eliminating lingering access and significantly reducing quarterly audit prep time.
- **Automated, auditable workflows:** P0 integrates directly with CommonLit's compliance posture, helping the team meet strict customer and regulatory expectations with less manual overhead.

Developer velocity and productivity

- **Fast approvals:** Access requests during business hours are typically approved in under 10 minutes, keeping developers in flow.
- **Uninterrupted shipping:** Blocking engineers—even for two hours—is a nonstarter. P0 ensures developers stay productive and focused on delivering features.
- **Real-world educational impact:** With reduced friction, the team shipped a digital annotation tool that enhances student retention and gives teachers visibility into student thinking.