How EverOps Helped a Popular Tech Startup Track Nearly $20M in Devices and Modernized Device Security Operations

The Client

A popular remote-first tech startup that relies on over 5,000 Technical Support Agents around the world to power both customer-facing and internal support operations. These agents use Chromebooks purchased by their staffing agencies and expensed back to the company, creating device sprawl and visibility gaps in infrastructure and security systems.

The Challenge

Prior to working with EverOps, the client lacked any system to register or verify these externally managed devices. As a result:

- Thousands of unverified Chromebooks accessed sensitive systems without oversight.
- The company suffered significant financial losses due to fraudulent device reimbursement claims.
- The security team had no reliable inventory or trust model to apply compliance policies.
- Onboarding remained slow and error-prone in a division with extremely high turnover.

EverOps was asked to take ownership of a loosely defined Problem/Proposed Solution (P/PS) doc and build a robust system that would enable visibility and control across these thousands of distributed assets.

The Solution

EverOps designed, proposed, built, and delivered a full end-to-end asset registration platform that became a critical pillar of the client's Device Procurement Program.

The solution included:

- **A Full-Stack Web Portal** – Built using React, this tool enabled Technical Support Agents to register Chromebooks before receiving credentials.
- **Design Leadership** – The EverOps engineer took the initiative to learn Figma, build out UI/UX designs, and gain cross-functional stakeholder signoff.
- **GraphQL API Rewrite** – A complete overhaul of the asset tracking backend in Go-lang, which enabled policy enforcement, device inventory, and security telemetry.
- **Modern Infrastructure** – The team worked across AWS-hosted infrastructure to enable scalable and observable operations while ensuring compatibility with identity and access tools.

- **Process & Testing Uplift** – EverOps introduced unit testing, CI/CD best practices, and long-term maintainability patterns, many of which were adopted by the client's own engineering team.

Despite initially being scoped as an isolated backend project, EverOps integrated deeply into the existing internal system, rewriting large parts of the platform and ultimately becoming the second-largest contributor to the codebase.

The Business Outcome

As a result of the partnership, the tech company achieved:

- **Full Visibility Into $20M+ in Devices** – A once-opaque fleet of Chromebooks is now centrally tracked and trusted.
- **Improved Security Posture** – Every agent device is now registered before access is granted, enabling consistent policy enforcement.
- **Faster Onboarding at Scale** – The new system supports rapid provisioning in a division with 5,000+ agents and frequent turnover.
- **Technical Upskilling and Process Improvement** – The client adopted new engineering patterns and test methodologies introduced by EverOps.
- **Elimination of Fraud Risk** – The platform reduced the likelihood of false expense claims by requiring real-time device validation.

In conclusion, EverOps delivered far more than just software. They enabled cultural change, improved security and engineering quality, and helped a fast-scaling company regain control over one of its most vulnerable operational surfaces.