CISO Guide: Who Still Has Access to My SaaS?

Why visibility is the foundation of SaaS security—and the risks that hide in plain sight.

It's one of the simplest, most important security questions a CISO can ask: Who still has access? But in most SaaS environments, that question is surprisingly difficult to answer. With hundreds of apps, dozens of integrations, and new users added daily, visibility into who has access to what—right now—is rarely complete.

This guide explores why access drift happens, how shadow integrations and dormant roles quietly create risk, and what it takes to answer this question with confidence.

1. Too Many Doors, Not Enough Locks: Why Access Drift Happens

When employees join a company, they get access. When they switch roles, they usually keep access. **When they leave, access is often removed from core systems... but not from connected tools, integrations, or legacy accounts.**

And with SaaS, access is fragmented across:

- The identity provider (e.g. Google, Microsoft)
- The app itself (e.g. Salesforce, Canva, Notion)
- API tokens and integrations
- Admin roles assigned months—or years—ago
- Service accounts no one remembers owning

Over time, this creates "access drift"—a slow buildup of roles, permissions, and connected apps that no one is actively managing.

2. The Risks of Untracked Access

Access that no one sees is access no one secures. When you don't know who still has access, these risks emerge:

- **Orphaned Accounts:** Users who've left the company but still have valid tokens or logins
- **Overprivileged Roles:** Employees with admin access long after they need it
- **Dormant Logins:** Accounts that haven't been used in months but can still authenticate
- **Shadow Integrations:** Apps connected to your core systems that no one approved or monitors
- **Shared Credentials:** Logins passed between users with no clear ownership or audit trail

These aren't rare edge cases. They're the norm in SaaS-heavy environments.
And they're exactly where attackers look.

3. When You Can’t See Access, You Pay for It—Twice

Poor SaaS access visibility creates measurable business risks:

- **Security Incidents:** Unmonitored access points become attack vectors. When breaches occur through dormant admin accounts or shadow integrations, the impact extends beyond immediate security costs to include business disruption, customer trust erosion, and regulatory scrutiny.
- **Operational Inefficiency:** Security teams spend hours manually auditing access across multiple admin panels. What should be a 10-minute compliance check becomes a multi-day investigation involving IT, HR, and application owners.
- **Audit Failures:** External auditors expect clear answers about access controls. Gaps in visibility lead to audit findings, remediation costs, and potential compliance violations that can impact business partnerships and market access.
- **License Waste:** Organizations often maintain expensive licenses for users who no longer need access, leading to unnecessary software spending that can reach thousands of dollars monthly for enterprise tools.

4. When “Who Has Access?” Becomes an Incident Response Question

In the middle of a breach investigation, one of the first things you'll be asked is:
Who had access to this system? When was it last reviewed? Who approved that level of access—and when?
If the answer is unclear, or if you need hours (or days) to find out, it's already too late.
More importantly: **if you can't answer that question today, it means you may already have access risks inside your environment, and just don't know it yet.**

5. Why This Question Is Getting Harder to Answer

SaaS sprawl and decentralized adoption are making access management harder every month:

- Teams are connecting tools without IT oversight
- Vendors and contractors are granted access for short-term projects and never removed
- MFA may be turned off on secondary tools
- OAuth tokens remain active long after the user or app is gone
- Admin roles are created and never reviewed

And yet, every one of these points becomes your responsibility in the event of a breach or compliance review. The challenge isn't just technical—it's organizational. **As SaaS adoption accelerates, the traditional IT-controlled access model breaks down, leaving security teams to manage risks they can't fully see.**

6. How FrontierZero Helps You Answer This In Minutes

FrontierZero gives you real-time, app-level visibility into who has access, where, when, and what they can do.

Challenge Area	FrontierZero Capabilities
Unclear access across apps	Unified view of all users, apps, roles, and integrations
Orphaned accounts	Flags inactive users and unowned accounts with active tokens
Shadow integrations	Surfaces unapproved tools connected to critical systems
Overprivileged access	Identifies risky roles and unused admin rights
No visibility between audits	Continuous monitoring and reporting, not point-in-time snapshots

You don't need to dig through multiple admin panels or trust an outdated spreadsheet. FrontierZero brings it all together—automatically.

Unlike traditional identity management tools that focus on provisioning, FrontierZero specializes in the ongoing visibility challenge that SaaS environments create. We understand that in today's distributed access model, the question isn't just "who should have access?" but "**who actually has access right now**?"

7. Compliance and Governance Considerations

Access visibility is not just a security feature — it's a compliance enabler.
Across frameworks like SOC 2, ISO 27001, NCA, and industry-specific regulations, access reviews and audit trails are mandatory. But they're often treated as static snapshots instead of real-time processes.
Without continuous visibility into who has access to what, when that access was last used, and whether it's still appropriate, audit prep becomes a fire drill — or worse, a liability.

Key compliance and governance goals supported by full access visibility:

- ✅ Role-based access enforcement
- ✅ Segregation of duties
- ✅ Real-time access revocation
- ✅ Audit trail generation
- ✅ Continuous access certification

Whether you're facing internal audit, board-level risk reviews, or external attestation, visibility across your SaaS stack gives you something most orgs can't deliver: proof of control

8. The Access Visibility Checklist

Ask yourself:

☑ Can you list every third-party app connected to your Google or Microsoft workspace?
☑ Do you know who still has admin access to your most sensitive SaaS tools?
☑ Can you tell which accounts haven't been used in the last 90 days?
☑ Are you alerted when MFA is disabled or bypassed?
☑ Do you track access drift as users change roles, move teams, or leave?
☑ Can you generate an access report for any application within minutes, not days?
☑ Are your user credentials continuously checked against dark web breach records?

If you're unsure about even one of these, you don't have full visibility. **And if you don't have full visibility, you don't have full control.**

9. What To Do Next

Access visibility is no longer a "nice to have." It's **essential** for compliance, security, and resilience.

✅ Reassess how you track SaaS access across your environment
✅ Align IT, security, and app owners around access reviews
✅ Implement continuous visibility—not annual snapshots

The cost of not knowing who has access to your SaaS environment far exceeds the investment in proper visibility tools. In an era where the average security team manages hundreds of applications, manual access tracking isn't just inefficient—it's a business risk.

About FrontierZero

FrontierZero is built for a world where security perimeters no longer exist—and identities, apps, and AI tools now shape the real attack surface.

As the only SaaS Security Posture Management (SSPM) platform based in the UAE, FrontierZero gives organizations in compliance-driven sectors full visibility into how SaaS tools are actually used—not just which ones exist. We track the full lifecycle of SaaS risk: every identity, every integration, every behavioral anomaly.

Our identity-first approach connects to your SaaS environment in minutes and starts mapping hidden threats immediately—whether it's an employee connecting a Shadow AI tool via OAuth, a service account with risky permissions, or a login pattern that breaks the norm.

By focusing on behavior instead of static roles, FrontierZero helps security teams surface what actually matters:

- Unknown apps with full data access
- Accounts that bypass MFA policies
- Unusual downloads, device changes, or login anomalies
- Excessive permissions tied to abandoned or shared accounts

All of this is continuously updated and delivered through a real-time SSPM platform built for scale, speed, and simplicity.

FrontierZero is the visibility layer modern companies need to stay ahead of compliance audits, stop insider threats, and finally get control over their SaaS sprawl—without adding complexity or overhead.

✅ Want to see what your real SaaS perimeter looks like?

Start Your Free Trial Today