CISO Guide: Do You Really Know Who's Using MFA?

Closing the Gaps in Multi-Factor Authentication Across Your SaaS and Third-Party Apps

Multi-factor authentication (MFA) is now a baseline security control, but enforcement often stops at core platforms like Microsoft 365 or Google Workspace. Many CISOs assume MFA is universally adopted, yet critical gaps persist—especially in third-party SaaS, finance, HR, and project management tools. Attackers know this and are increasingly targeting overlooked apps and exploiting MFA fatigue. This guide explains why visibility and continuous monitoring are essential, and how solutions like FrontierZero can help you prove and enforce MFA everywhere it matters.

1. The MFA Assumption Trap

The reality:

- Many security leaders believe MFA is in place across the organization, but in practice, MFA coverage is often patchy.
- Users may skip MFA enrollment on unmanaged or "shadow IT" apps, or disable it due to perceived inconvenience.
- Security teams lack visibility into freemium, self-purchased, or non-SSO apps, leaving critical accounts unprotected.

The Risks:

- One unprotected admin account on a finance, HR, or project management tool can expose sensitive data or provide a foothold for attackers.
- In a recent dataset review, up to 40% of accounts used a password only, with no MFA enabled.
- Even where MFA is present, 99% of accounts used at least one ***phishable*** method, such as SMS or app-based codes.

2. Why Now? The Rise of MFA Bypass and Fatigue Attacks

Attackers Adapt:

● MFA fatigue attacks ("MFA bombing") bombard users with repeated prompts, hoping they'll approve a fraudulent login out of annoyance or confusion.
● High-profile breaches (Uber, Cisco, Apple) have shown how attackers use stolen credentials and social engineering to bypass MFA—even when it's technically enabled.
● Phishing-resistant MFA is critical, but attackers exploit backup methods and session hijacking to circumvent controls.

Key Trends:

● Credential theft remains the top initial access vector in breaches, accounting for nearly half of attacks in 2024.
● Attackers specifically target apps where MFA is missing or weak, knowing these are often overlooked by security teams.

3. The Visibility Challenge: Where is MFA Actually Enforced?

Common Gaps:

● Third-party SaaS: Many critical apps don't support native MFA enforcement, or are outside IT's administrative control.
● Shadow IT: Employees adopt new tools without security oversight, often skipping MFA setup.
● Backup Methods: Less secure MFA options (SMS, TOTP) can be exploited in downgrade attacks.

What CISOs Need:

● Comprehensive inventory: Know every app and account in use, including unmanaged and free-tier SaaS.
● Proof of enforcement: Be able to demonstrate, not just assume, that MFA is active on every critical account.
● Visibility into methods: Understand which MFA types are used, and where phishable methods are still permitted.

4. Actionable Checklist: Closing MFA Gaps

- [ ] Inventory all SaaS and third-party apps—not just those managed via SSO or central IT.
- [ ] Continuously monitor MFA status across all accounts and apps, with automated alerts for gaps.
- [ ] Enforce MFA enrollment—prompt users to enable MFA, even on apps without native admin controls.
- [ ] Assess MFA methods—identify where SMS or other phishable methods are still in use, and upgrade to phishing-resistant options where possible.
- [ ] Educate users about MFA fatigue and social engineering tactics; train them to recognize and report suspicious prompts.
- [ ] Review and test backup methods to prevent downgrade attacks and session hijacking.
- [ ] Integrate compliance reporting—be able to prove MFA coverage to auditors and regulators.

5. How FrontierZero Helps

FrontierZero gives CISOs the tools to eliminate MFA blind spots and enforce strong authentication everywhere:

Challenge	How FrontierZero Solves It
Shadow IT and unmanaged apps	Automated discovery of all SaaS accounts, including free and self-adopted tools
Lack of enforcement on third-party apps	In-browser prompts and workflows to require MFA enrollment—even where native controls don't exist
Incomplete visibility	Centralized dashboard showing MFA status for every account and app, with real-time alerts for gaps
Weak or phishable MFA methods	Reporting on MFA method types, with guidance to upgrade to phishing-resistant options
Compliance attestation	Audit-ready reports proving MFA enforcement across the environment

6. Best Practices for Sustainable MFA Security

● Balance security and usability: Choose MFA methods that minimize user friction while maximizing protection.
● Prioritize high-risk apps: Focus on finance, HR, project management, and other sensitive tools that may be outside SSO.
● Automate monitoring and enforcement: Manual checks are unsustainable—use SSPM tools to scale your efforts.
● Stay ahead of attackers: Regularly review and update MFA policies as new threats and bypass techniques emerge.

7. Next Steps

● Assess your MFA coverage today: Use the checklist above to identify gaps.
● Engage your IT and compliance teams: MFA enforcement is a shared responsibility.
● See how FrontierZero can help: Request a demo to discover how you can achieve true MFA assurance across your SaaS and third-party landscape.

About FrontierZero

FrontierZero is a leading SaaS Security Posture Management (SSPM) platform, empowering CISOs with unified visibility, automated enforcement, and audit-ready reporting for MFA and more—across the entire digital enterprise.