cerby

Securing Corporate Social Media Accounts

A Practical Playbook for IT Leaders

cerby

Table of Contents

cerby

Executive Summary

At 8:00 a.m., your marketing team launches a global campaign across LinkedIn, TikTok, and Facebook. By 9:15, screenshots are everywhere: your verified account is posting offensive content and draining ad budget after attackers hijacked credentials left behind by a former agency partner. Social media accounts represent critical brand infrastructure with massive, often overlooked security risks. These platforms operate outside enterprise identity systems, leaving IT with zero visibility into who has access, when credentials are shared, or how accounts are managed. Marketing teams fill the gap with spreadsheets, shared passwords, and manual processes that create soft targets for attackers.

The business impact is severe. Security breaches average $4.4 million in total costs while 22% of global ad spend is lost due to fraud. With 57% of organizations facing phishing attacks daily, targeting the exact identity gaps that social platforms expose, the window for action is closing.

This playbook helps IT leaders bring corporate social media accounts under enterprise identity and access management (IAM) controls without slowing down marketing. It covers key strategies for enforcing access controls, automating user provisioning and deprovisioning, and establishing centralized visibility where none exists today. By adopting these approaches, organizations can eliminate long-standing blind spots in the marketing stack and manage social media accounts with the same level of security, governance, and control as the rest of their enterprise applications.

$4.4m

averaged in total costs by security breaches

Source

22%

of global ad spend is lost due to fraud

Source

cerby

The Growing Security Gap in the Marketing Stack

Social Media is a Business-Critical Risk

Social media is more than just a marketing channel, it drives brand visibility, customer engagement, and revenue growth. Ad spend alone is projected to reach $276B globally by 2025 and social commerce revenue is expected to reach $1T by 2028. That makes these platforms one of the most visible and valuable parts of the modern enterprise stack—yet one of the least protected.

A single compromised account doesn't just derail a marketing campaign, it can impact revenue, ad budgets, and erode brand trust in full public view. But these mission-critical platforms were built for consumers, not enterprises. They lack the identity and access controls IT leaders rely on to secure every other business application. For modern enterprises, protecting social media accounts is no longer optional, it is essential for safeguarding revenue and reputation.

Why Attackers Target Social Media

High-value, low-security targets

Social media accounts offer immediate access to millions of followers, large advertising budgets, and direct customer communications. Yet 89% of enterprises fail to enforce multi-factor authentication (MFA) or passkeys for these accounts, leaving them highly vulnerable to takeovers.

Public breaches cause outsized damage

Unlike backend system breaches that may go unnoticed for months, social media compromises play out in real-time with millions watching. The 2020 Twitter Bitcoin scam reached 130 high-profile accounts simultaneously, demonstrating the platform-wide impact possible from identity system failures.

Weak identity controls make compromise easy

Many business applications are secured through IAM, with centralized authentication and governance. Social media accounts are not. They rely on shared credentials, personal emails, and individual phone numbers. Attacks don't need to be sophisticated—basic phishing, password reuse, and credential stuffing are often enough to gain access to these critical accounts.

cerby

The Business Case for Action

For IT leaders, the choice is clear: bring the social media stack under enterprise identity and access management or accept escalating risk to brand, budget, and reputation.

1,000%
Increase in social media account takeovers between 2021-2022
Source

$84B
is lost annually to ad fraud, expecting to reach $170B by 2028
Source

66%
of consumers say they won't do business with a company that experienced a major security breach
Source

53%
of account takeovers involved social media accounts, making them the most commonly hacked
Source

Why Social Media Breaks Traditional Identity Security

The Ideal Enterprise App Security Model

Enterprise applications are expected to integrate seamlessly with identity providers like Okta or Microsoft Entra ID. When they do, IT gains two critical capabilities:

Centralized authentication

Users access applications through federated single sign-on (SSO) with enterprise-grade
MFA policies. IT defines and enforces password complexity, rotation schedules, and authentication methods—rather than relying on end users to implement security best practices.

Automated lifecycle management

When employees join, change roles, or leave, HR system updates automatically trigger provisioning and deprovisioning across all connected applications. Access rights stay aligned with job responsibilities and are removed immediately when employment ends—eliminating orphaned accounts and the risk of unauthorized access.

This is the ideal foundation of enterprise identity security. But it only works when applications natively support integration with IAM systems—and many social media marketing platforms don’t. Even those with partial controls lack the enterprise-grade capabilities required for secure access management.

cerby

The Social Media Integration Problem

Social media platforms operate as disconnected applications outside this model. They are most often managed by marketing teams and they were built for consumers, not enterprises. As a result, they lack the identity and access features IT depends on elsewhere, creating gaps such as:

Accounts tied to personal profiles

Many social media platforms require users to sign up with personal profiles to create and manage business accounts. This design choice means corporate social media access is inherently tied to individual employees' personal identities, creating ownership confusion and recovery nightmares when employees leave or change roles.

No IT oversight

IT lacks visibility into who has access to these accounts, password strength, whether MFA is enabled, and how credentials are being updated and shared. Responsibility for security falls on marketing team members.

Insecure authentication practices

Without IT oversight, employees choose their own passwords (often weak or reused) and decide whether to enable MFA. Convenience frequently wins over security, leaving accounts vulnerable to common attack methods.

Shared logins with no traceability

Corporate accounts require access from multiple marketing team members, agencies, and contractors. To make this work, teams fall back on sharing logins by passing around credentials. The result: insecure credential sharing and no way to identify which individual accessed an account or performed a specific action.

MFA doesn’t work for shared accounts

MFA on social platforms is tied to one person’s phone or email. To keep accounts usable across teams, many organizations disable MFA entirely—trading security for convenience and increasing risk exposure.

Contractor and agency access risks

External partners often retain access after projects end, either through delayed deprovisioning or because recovery credentials are tied to their personal information.

Ghost accounts accumulate

Over time, organizations lose track of dormant or unofficial accounts created by employees, contractors, or agencies. These unmanaged accounts create hidden exposures that can be exploited months or years later.

Limited enterprise integrations

Some social media applications support SAML and/or SCIM, but standards adoption is inconsistent and incomplete across platforms. Even when available, these integrations don’t solve broader challenges like shared access, seamless MFA, and auditability.

cerby

Why Existing Approaches to Social Media Security Don't Work

Marketing self-management

Most organizations default to letting marketing teams handle social media access entirely. Marketing creates accounts using personal emails and manages team access through informal processes. When new team members join campaigns, credentials get passed around and when people leave, no one enforces password resets. This approach creates massive security blind spots: IT has zero visibility into who has access, credentials proliferate uncontrolled, and former employees often retain access indefinitely.

Spreadsheets, emails, and chats

Storing passwords in spreadsheets or sharing them over email and chat provides no encryption, no audit trail, and no policy enforcement. The result is uncontrolled credential sprawl and constant risk of compromise.

Password managers (EPMs)

Password managers help store credentials, but they don't solve the core problems of social media access. MFA enforcement is inconsistent across social platforms, and users can disable it. The need to share accounts inevitably leads to credentials being passed around outside the EPM vault, creating risks. Most critically, corporate social accounts remain tied to individual emails and phone numbers, leaving ownership and recovery outside enterprise control. And because password managers don't deliver user provisioning and deprovisioning, they fail to deliver true identity automation and governance.

Native social media platform capabilities

Every platform provides different, limited controls, but they rarely integrate with enterprise IAM systems. Managing access across LinkedIn, TikTok, Instagram, X and other platforms separately only creates more fragmentation and risk.

Custom automation scripts

Automating on/offboarding processes requires ongoing development resources and deep API expertise for each platform. When platforms change APIs or deprecate features, those custom solutions break.

Social media was built for consumers, not enterprises, which is why conventional tools and approaches can't close the identity security gap.

cerby

The Solution: Bring Identity Controls to Social Media Accounts

Social media platforms are unlikely to ever deliver full enterprise-grade identity security. Enterprises need their own control layer—one that provides centralized credential management, organizational account ownership, secure sharing, automated provisioning and deprovisioning, properly assigned permissions, and complete IT oversight—regardless of the limitations of the platforms themselves.

Secure Credential Management & Authentication

Current State

Users manage their own credentials, often creating weak or reused passwords, storing them insecurely (e.g., in spreadsheets), and disabling MFA to reduce friction. Security teams lack the ability to enforce password policies, rotate credentials, or ensure MFA is consistently applied. Users must also log in manually to each social media platform, adding complexity and risk.

Target State

The organization centrally manages credentials with automated password rotation and enforced MFA. Security teams can set granular controls—for example, allowing users to only login with credentials or allowing them to view, edit, rotate, or share credentials when appropriate. Users enjoy a seamless one-click, SSO-like experience when accessing social media accounts.

Business Impact

Greatly reduces credential risk, removes the burden of managing and using credentials and MFA codes from users, and ensures all activity is auditable and tied to enterprise identities.

Centralized Account Ownership

Current State

Social media accounts are tied to individual employees' emails, phone numbers, and MFA factors. This makes collaboration insecure and inefficient—credentials and MFA codes must be shared—and creates single points of failure. If an account owner leaves or becomes unavailable, the organization risks losing access to critical accounts.

Target State

Accounts are registered using organization-owned emails, phone numbers, and MFA factors, effectively creating enterprise-managed service accounts. Ownership shifts from individuals to the organization, making access durable, consistent, and centrally managed.

Business Impact

Preserves business continuity when employees or external partners leave and reduces risk by enabling robust security controls such as enterprise-wide MFA enforcement (with seamless auto-fill of codes) and secure account sharing.

cerby

Secure Account Sharing

Current State

Individuals share access with teammates or external partners by distributing personal account credentials and MFA codes. This creates security risks, audit blind spots, and lingering "ghost accounts" as access remains long after it's needed.

Target State

Internal employee access is managed through enterprise lifecycle processes, while marketing teams can grant external partners time-bound access that automatically expires. Credentials remain in use but under secure measures—with enforced MFA and centralized access revocation via password rotations. All access is logged for visibility and auditability.

Business Impact

Reduces risk, lowers administrative effort, accelerates collaboration, and ensures compliance with complete, traceable access records.

Automated Provisioning and Deprovisioning

Current State

Managing user access is manual, slow, and error-prone. New employees often wait for access, while departed users retain it for too long, leaving behind orphaned and unmanaged accounts.

Target State

Provisioning and deprovisioning are automatically triggered by events in HR systems through the organization's identity provider (IdP). Employees receive the right access on day one and lose it immediately upon departure without IT involvement. The same automated processes used to manage core enterprise applications are applied consistently to social media platforms.

Business Impact

Reduces administrative workload, eliminates orphaned access, and ensures access always stays aligned with employment status.

cerby

Properly Assigned Permissions

Current State

Social platforms offer role-based permissions (e.g., admin, editor, viewer), but in practice too many users are assigned admin rights. Account sharing compounds the problem—collaborators might unintentionally get admin permissions like the ability to change passwords or delete accounts.

Target State

Role assignments are mapped automatically from an authoritative source such as groups in the identity provider. For example, members of the "Executive" group may receive admin rights, "Marketing" members editor rights, and everyone else viewer access. Roles are always current, correct, and aligned with organizational policy.

Business Impact

Eliminates overprivileged access, brings social media accounts under the same role-mapping mechanisms as other enterprise applications, and ensures employees and partners have the precise level of access they need to work securely.

IT Visibility & Oversight

Current State

IT lacks a centralized view of social media accounts—who has access, whether MFA is enabled, or how credentials are being shared. Audits are challenging since data is scattered and requires manual efforts to compile.

Target State

Oversight of all social media accounts is centralized in a single platform. IT gains real-time visibility, audit logs, and enforcement capabilities equivalent to those applied to other enterprise apps in its ecosystem.

Business Impact

Removes social media as a security blind spot, enables consistent policy enforcement, and provides full auditability for compliance and risk management.

cerby

Implementation Roadmap for IT Leaders

Phase 1

Foundation

(30 days)

1. Audit current state
Document every corporate social media account, connected app, and current access holder

2. Assess risk exposure
Calculate potential cost and risk from current manual processes and shared credentials

3. Establish governance framework
Define roles, responsibilities, and approval workflows for social media access

Phase 2

Security Controls

(60 days)

4. Deploy centralized credential management
Migrate shared passwords to secure, auditable systems with automated password rotation capabilities

5. Enforce MFA universally
Replace individually owned email, SMS, and MFA with centrally managed alternatives

6. Automate provisioning workflows
Connect account creation/deletion to identity platforms and project lifecycles

Phase 3

Continuous Improvement

(90+ days)

7. Enable real-time monitoring
Deploy anomaly detection and automated alerting for unusual access patterns

8. Integrate compliance reporting
Connect social media logs to feed existing SIEM tools and GRC workflows

9. Optimize based on usage
Refine roles and permissions based on actual business requirements

cerby

The Strategic Value of Comprehensive Identity and Access Management for Social Media

While other organizations manage social media access through ad-hoc processes, enterprises with mature IAM controls gain security and operational advantages:

Operational efficiency

Automated provisioning and deprovisioning eliminate manual ticket workflows and reduce help desk burden. IT teams spend less time on access requests and credential resets, and more time on strategic initiatives.

Security posture

Strong, centralized access controls and continuous monitoring extend enterprise security to previously disconnected applications. Consistent authentication policies and real-time threat detection reduce attack surface across all business-critical platforms.

Risk mitigation

Comprehensive identity lifecycle management eliminates orphaned accounts and unauthorized access. Automated offboarding and access reviews prevent insider threats and reduce breach exposure.

Compliance readiness

Continuous audit logging and automated access certifications satisfy regulatory requirements without manual evidence collection. SOC 2, ISO 27001, and industry-specific compliance becomes streamlined and repeatable.

Cost control

Eliminating manual access management processes and preventing security incidents delivers quantifiable ROI through reduced IT overhead and avoided breach costs.

cerby

Conclusion: Social Media is Critical Business Infrastructure

Social media accounts require the same identity and access management rigor applied to ERP, CRM, and other mission-critical systems. Organizations that extend their identity and access control strategies to include social platforms gain measurable advantages in risk reduction and operational efficiency.

The implementation path requires three immediate actions:

Conduct a comprehensive audit

Document all social media accounts and quantify current manual processes, including IT time spent on access requests, security gaps, and compliance risks

Evaluate specialized security solutions

Traditional password managers and native platforms cannot provide the lifecycle management and access controls social media applications require. Assess solutions designed for security and access management across non-integrated applications

Execute a controlled pilot

Select high-risk accounts to demonstrate automated provisioning, centralized access controls, and auditability capabilities

The secured outcome: your marketing team launches that same 8:00 a.m. campaign. Automated deprovisioning blocked former employee access. MFA policies and access controls prevented credential-based attacks. Integrated security monitoring flagged suspicious third-party connections. When auditors request access documentation, IT generates comprehensive reports instantly.

This is the operational advantage gained when IT applies the same security rigor to social media as other mission-critical enterprise applications. IT leaders who move first won't just prevent incidents—they'll prove that oversight and governance can accelerate operations, not slow them.