Delinea

Granular Access Control for Corporate Social Media Applications

Protect your brand reputation and sensitive data with enterprise-wide PAM

Social media teams are stewards of an organization's brand reputation, They're responsible for knowing what to say, as well as how to say it, without revealing protected information. Yet, social media teams are among the privileged business users that use web applications with security controls and permissions typically outside the scope of central IT governance. By extending Privileged Access Management (PAM) to web applications, you increase oversight of privileged users so you can answer three critical questions.

1 Who has access to your corporate social media accounts?

Privileged business users often rely on multiple SaaS platforms for social media management. They may lack modern forms of authentication and authorization like multi-factor authentication (MFA) and Single Sign-On (SSO).

Many people, including third-party contractors and agencies, may manage a company's social media presence, using non-domain accounts and workstations outside of your control.

Social media demands constant attention, so teams often share responsibility and people and roles change frequently. Therefore, teams sometimes share privileged credentials, making it difficult to tell who is responsible for a specific activity.

When you incorporate web applications like social media tools into your PAM program, you can validate privileged identities.

2 What can people do with that access?

Access for social media applications is often tiered. Some users can monitor and report. Others can post and share information. A limited set of people may have permissions to post highly sensitive content such as financial disclosures, research and development news, upcoming products, and personal information.

This type of tiering system becomes complicated to manage centrally because each social media application has its own security model and definition of user roles, which don't match the role definitions you use in Active Directory (AD) or other systems.

When you have roles and permissions that tie to central identity management systems, you can manage them more easily and consistently.

3 Can you ensure oversight and reporting?

Enterprises are starting to incorporate social media policy definition and enforcement among the responsibilities of governance, risk, and compliance (GRC) teams. For example, whenever public companies publish an external announcement that could impact their financial health, they must track who authorized it and maintain a detailed audit trail of every person who handled that information. Yet, GRC platforms and traditional access control solutions don't provide sufficient granularity to govern the use of social media applications.

When you track privileged activities with a PAM solution, you can generate detailed reports to share with executives and auditors.

Delinea is focused on the most vulnerable attack vector — privileged access. With Delinea, you can adopt a multi-layered approach that covers your privilege account attack surface from endpoints to the cloud, ensuring protection at every point of the privileged account lifecycle.

Get started fast

There's no need to deploy agents, software, or servers to use Cloud Access Controller. Delinea integrates with existing MFA, AD, and IAM solutions. Plus, you can add MFA and SSO to any legacy or custom apps without writing any code.

Continuous, Intelligent Access Control for all Web Apps

Cloud Access Controller lets you implement and enforce a least privilege policy and Zero Trust access control model for all web applications, including social media platforms. At the same time, you can provide business users the access they need to do their jobs, without causing friction or slowing down their process.

REDUCE PRIVILEGED ACCOUNT RISK

Cloud Access Controller lets you limit access to applications based on users' IP address, location, and browser type.

MANAGE GRANULAR ACCESS

You can give privileged users the access and controls they need, when they need them. For third parties or new users, you can grant temporary access that expires automatically at a time you set.

Access doesn't need to be all or nothing. You can hide or block any sensitive text, buttons, web elements, and specific URLs within any web- based social media application.

INCREASE OVERSIGHT

Delinea makes it easy to record, audit, and review all social media sessions without deploying any infrastructure. You can set notifications to alert you of suspicious behaviors patterns. Out-of-the- box reports help you demonstrate compliance.

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**