RedHelm

Action Guide:
How to Strengthen Your Identity Security Strategy

1 Understand Your Identity Environment

Create visibility across the identities interacting with the organization.
Include:

- Employees
- Administrators
- Contractors
- Vendors
- Service accounts
- Applications
- Cloud workloads
- AI tools and integrations

Identify which identities can access business-critical systems and sensitive information.

2 Strengthen Authentication

Implement **multi-factor authentication** broadly, prioritizing:

- Administrative accounts
- Critical applications
- Remote access
- Financial systems
- Email
- Privileged users
- Cloud platforms

Review MFA coverage regularly rather than assuming deployment means universal protection.

3 Understand Your Identity Environment

Implement **multi-factor authentication** broadly, prioritizing:

- Does this person still need this access?
- Does this account require administrative privileges?
- Could permissions be reduced?
- Are privileges permanent when they could be temporary?
- Has access accumulated because someone's role changed?

Reducing unnecessary permissions reduces the potential blast radius of a compromised identity.

412.349.6680 www.redhelm.com

4 Protect Privileged Accounts

Identify and govern privileged identities separately.
Use **privileged access management** practices to:

- Monitor administrative activity
- Separate standard and administrative accounts
- Review privileged access regularly
- Limit standing privileges
- Remove unnecessary administrative rights
- Protect privileged credentials

The identities capable of causing the greatest damage should receive the strongest controls.

5 Establish Identity Lifecycle Governance

Create consistent processes for:

Joiners → Movers → Leavers

Access should evolve alongside the individual's relationship with the organization.

Do not focus only on onboarding and termination. Role changes should trigger access reviews so employees do not accumulate unnecessary permissions over time.

6 Continuously Review Access

Identity security should operate as an ongoing governance process.
Regularly review:

- Privileged access
- Dormant accounts
- Third-party accounts
- Administrative permissions
- Critical application access
- Cloud permissions
- Service accounts
- Exceptions

The goal is ensuring that today's access decisions still make sense tomorrow.