8 Best Practices for Robust IAM Strategy

Identity and Access Management (IAM) is the best defense to secure an organization.

However, IAM can also be the weakest link if not implemented properly.

In fact, unauthorized access is among the highest ranked attack vectors for cybercriminals.

1 Zero-in on Identity

Centralize security controls around user and service identities.

2 Embrace Zero-trust

Presume no user is trustworthy unless proved otherwise.

3 Implement MFA

MFA enables multiple layers of authentication, ensuring extra security.

4 Robust Passwords

Ensure users set strong passwords and update them regularly.

5 Limit Privileged Accounts

Restricting the number of users having privileged access reduces risk.

6 Go Passwordless

Improve user experience with email, SMS or biometrics based logins.

7 Access Audits

Regularly conduct access audits to review, revoke, or restrict access.

8 Stay Compliant

Adhere to regulatory compliances like GDPR, CCPA, and HIPPA.

Securely Connect Every User to the Right Level of Access with **Veritis IAM Services!**

Let's Talk!

veritis transcend

1-877-VERITIS (283-7484), 972-753-0022

connect@veritis.com