

CRITICAL IAM STRATEGIES TO STAY CYBER-SAFE

In 2023, cybercrimes, including data breaches and identity theft, impacted over 353 million users, with

DAMAGES PROJECTED TO REACH

\$10.5 Trillion
by 2025.

As organizations adopt cloud and IoT, the expanding attack surfaces make IAM (Identity Access Management) crucial for securing digital assets, enhancing efficiency, and ensuring compliance.

80%

say better IAM could have prevented some or all attacks. ([One Identity](#))

49%

ranked IAM as one of the top five essential security skills in their organization, the highest percentage among responses. (ISACA)

“

What's needed today is a zero-trust mindset for cyber hardening industrial systems in a way that secures identities and blocks attacks. Identity and Access Management (IAM) needs to be a priority for real-world operations. Technologies exist to offer protection without a complete infrastructure overhaul.



Roman Arutyunov
Co-Founder and SVP of Products at Xage Security

Cost of Cybersecurity in 2024

- ▶ **\$4.88 million**, up 10% from last year- global average data breach cost in 2024 ([IBM](#))
- ▶ Data breaches can cost \$1.3 million in lost business. ([IBM](#))
- ▶ AI and automation reduce breach costs by **2.2%**. ([IBM](#))

600% increase in cybercrime due to COVID-19 pandemic with a cost impact of about

1%

of global GDP.



Understanding IAM

Identity and Access Management (IAM) is a framework for managing digital identities and controlling access to data.

- ▶ **User Authentication:** Verifies identities with passwords, biometrics, or MFA.
- ▶ **Access Control:** Grants access based on user roles.
- ▶ **Provisioning:** Automates access rights for new or departing employees.
- ▶ **Monitoring:** Tracks user activities for compliance.

Assessing IAM Needs & Best Practices

- ▶ **Assess Needs:** Conduct security audits, map user roles, and evaluate access controls.

Analyze: Review users, resources, and compliance requirements.

Best Practices:

- ▶ Conduct regular security audits.
- ▶ Enforce multi-factor authentication.
- ▶ Apply the principle of least privilege.
- ▶ Use encryption and automate user provisioning.

IAM Implementation & Partnerships

- ▶ **Partner with Experts:** Work with experienced IAM providers.
- ▶ **Setup Support:** Assist with installation.
- ▶ **Integration:** Ensure compatibility with existing systems.
- ▶ **Testing:** Identify and resolve issues.
- ▶ **Guidance:** Navigate implementation challenges.

As cyber threats become more sophisticated, a robust IAM strategy is your frontline defense. Stay ahead of cyber threats with a tailored IAM solution.

Contact us today to secure your business and safeguard your future.