Everyday Identity

Trust Nothing. Verify Everything. Protect Everyone.

IAM in the Cloud & SaaS Era Checklist

Untracked SaaS Usage (Shadow IT)

- [ ] Have all SaaS apps been inventoried, including employee-created or unmanaged ones?
- [ ] Is there a formal approval and review process for all new SaaS tools?

Inconsistent Authentication Standards

- [ ] Is SSO enforced across all SaaS applications?
- [ ] Is MFA (preferably phishing-resistant) enabled for all cloud accounts?

Exposed or Mismanaged API Keys

- [ ] Are secrets rotated regularly and ownership clearly assigned?
- [ ] Are all API keys and tokens stored in a secure secrets manager (not hardcoded)?

Overprivileged Roles in SaaS Apps

- [ ] Are roles scoped to least privilege by default?
- [ ] Are administrative privileges reviewed quarterly?

Manual Provisioning & Deprovisioning

- [ ] Is user lifecycle management automated via SCIM or workflow integrations?
- [ ] Are accounts deactivated within 24 hours of termination or role change?

Lack of Access Review and Oversight

- [ ] Are third-party vendor accounts subject to the same review process?
- [ ] Are periodic access certifications performed for all high-risk SaaS apps?

Unmonitored Third-Party Integrations

- [ ] Are SaaS integrations and OAuth scopes regularly audited?
- [ ] Are risky or unused third-party app connections revoked promptly?

Quick Tip: *Aim for centralized identity governance and at least 90% compliance across all SaaS tools to drastically reduce sprawl, risk, and audit fatigue.*