AppOmni

The SaaS Security Prioritization Checklist

A practical framework for building a scalable SaaS security program

You don't need to secure every SaaS application at once. The most effective security teams start with the applications that store the most business-critical data, then expand their program over time. Use this checklist to assess your current maturity and prioritize the actions that reduce risk first.

WALK

Secure your business-critical SaaS applications

GOAL

Build a strong security foundation around the SaaS applications that matter most.

INVENTORY & PRIORITIZATION

- [ ] Identify your business-critical SaaS applications (Salesforce, Microsoft 365, ServiceNow, Workday, Claude, etc.)
- [ ] Rank applications by data sensitivity, business impact, and attack surface
- [ ] Identify privileged users and administrative accounts
- [ ] Document third-party integrations and connected SaaS applications

SECURE CONFIGURATIONS

- [ ] Establish secure configuration baselines
- [ ] Enable multi-factor authentication (MFA) wherever supported
- [ ] Eliminate single-factor authentication for privileged accounts
- [ ] Review administrator roles and remove excessive permissions

VISIBILITY

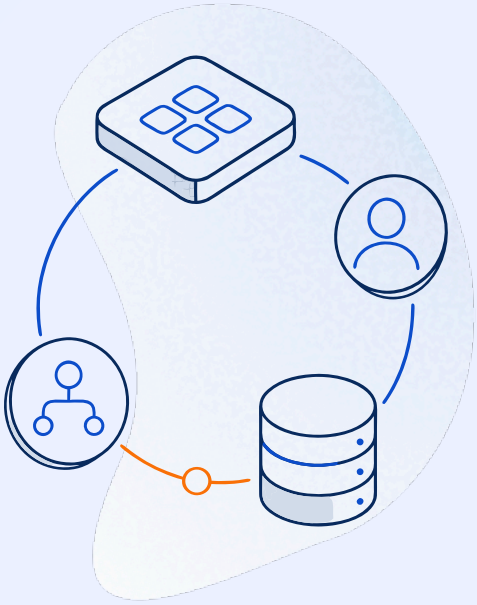
- [ ] Centralize SaaS audit logs
- [ ] Validate visibility across identities, configurations, and application activity
- [ ] Confirm security teams can investigate activity within critical applications

RUN

Operationalize SaaS security

GOAL

Turn one-time security projects into repeatable operational processes.



GOVERNANCE

- [ ] Define ownership using a RACI model
- [ ] Assign security, IT, application owners, and business stakeholders
- [ ] Document configuration standards for critical SaaS applications

PROCESSES

- [ ] Review new SaaS purchases before deployment
- [ ] Include procurement in security reviews
- [ ] Apply Zero Trust principles to users, identities, applications, and integrations
- [ ] Standardize remediation workflows across application owners

COLLABORATION

- [ ] Establish recurring SaaS security reviews
- [ ] Share posture findings with application owners
- [ ] Track remediation progress against agreed SLAs

FLY

Continuously reduce SaaS risk

GOAL

Move from periodic audits to continuous monitoring.

CONTINUOUS MONITORING

- [ ] Monitor for configuration drift
- [ ] Detect excessive permissions as environments change
- [ ] Continuously review connected applications and third-party integrations
- [ ] Identify inactive, orphaned, and unnecessary accounts

DETECTION & RESPONSE

- [ ] Feed SaaS telemetry into SIEM and SOAR platforms
- [ ] Monitor for suspicious identity behavior
- [ ] Monitor both human and non-human identities
- [ ] Review service accounts and API identities regularly

AI READINESS

- [ ] Inventory AI-powered SaaS applications
- [ ] Identify AI agents with access to sensitive data
- [ ] Apply least privilege to AI identities
- [ ] Continuously monitor AI access and behavior

SaaS security doesn't have to be overwhelming. Start with the applications that have the greatest business impact, then expand your program with repeatable processes and continuous visibility. That's how you reduce risk without overwhelming your team.