PLATOPS

Scale securely from day one

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS	AVG. TO COMPLIANCE	MONITORING

SaaS Security Checklist

Enterprise Readiness & Security Controls for SaaS Companies

Prepared by PlatOps Security Version 1.0 | January 2026

SAAS SECURITY MATURITY MODEL

Security Maturity by Stage

STAGE	FOCUS	KEY CONTROLS	TIMELINE
Seed	Foundation	Basic security, secure development	Month 1-3
Series A	Enterprise Ready	SOC 2, security questionnaires	Month 3-9
Series B	Scale	Advanced security, automation	Month 9-18
Growth	Industry Leader	Zero trust, advanced threat detection	18+ months

REQUIREMENT	% REQUIRING	PRIORITY
SOC 2 Type II	89%	Critical
Security Questionnaire	94%	Required
Penetration Test Report	76%	High
SSO/SAML Support	85%	High
Data Encryption	97%	Critical
SLA/Uptime Guarantee	82%	High
Incident Response Plan	71%	Medium
BAA (if PHI)	100%	Required

The Enterprise Security Tax

Without Security Program:

- 3-6 month sales cycle extension
- 350+ question security questionnaires
- Custom security reviews per deal
- Lost deals to "security concerns"

With Security Program:

- Pre-built trust package
- 1-click questionnaire responses
- Faster procurement approval
- 35% higher close rate

SECURE DEVELOPMENT LIFECYCLE

Secure Coding Practices (8 items)

□ OWASP Top 10 remediation verified
□ Input validation on all user inputs
□ Output encoding to prevent XSS
□ Parameterized queries (prevent SQL injection)
□ Secure authentication implementation
□ Secure session management
□ Security headers configured (CSP, HSTS, X-Frame)
□ Dependency vulnerability scanning

Code Review & Testing (6 items)

□ Mandatory code review for all changes
□ SAST (static analysis) in CI/CD pipeline
□ DAST (dynamic analysis) in staging
□ SCA (software composition analysis) for dependencies

- □ Pipeline runs with least privilege
- □ Container image scanning before deployment
- □ Signed commits required
- □ Branch protection rules enforced
- □ Deployment approval gates for production

Secrets Management (4 items)

- □ Centralized secrets management (Vault, AWS SM)
- □ No secrets in environment variables
- □ Secrets rotation policy (90 days)
- □ Audit logging for secrets access

Secure Development Total: 24 items

MULTI-TENANT ARCHITECTURE SECURITY

Multi-Tenancy Security Requirements

ISOLATION LEVEL	USE CASE	COMPLEXITY
Database-level	Highest security (finance, health)	High
Schema-level	Good balance	Medium
Row-level	Cost-effective, lower isolation	Low

Data Isolation Controls (6 items)

- □ Tenant isolation at application layer
- □ Database-level tenant separation (or row-level with enforcement)
- □ Cross-tenant data access prevention tested
- □ Tenant ID validation on all queries
- □ Tenant-aware caching strategy
- □ Tenant data backup isolation

Tenant Configuration Security (4 items)

- □ Per-tenant security settings
- □ Tenant admin access controls
- □ Tenant-specific audit logging
- □ Tenant data export/deletion capability

Noisy Neighbor Prevention (3 items)

- □ Per-tenant rate limiting
- □ Resource quotas per tenant
- □ Performance isolation monitoring

Multi-Tenant Security Total: 13 items

Enterprise Authentication (8 items)

- □ SAML 2.0 SSO support
- □ OIDC/OAuth 2.0 support
- □ SCIM provisioning support
- □ Just-in-time (JIT) user provisioning
- □ Multi-factor authentication (MFA) available
- □ Enforceable MFA for enterprise plans
- □ Session management controls
- □ Configurable session timeouts

Access Control (6 items)

- □ Role-based access control (RBAC)
- □ Granular permission system
- □ Admin role separation
- □ API token management
- □ IP allowlisting option
- □ Audit logging for access events

Password & Credential Security (4 items)

- □ Secure password requirements (NIST 800-63B)
- □ Password breach detection (HaveIBeenPwned)
- □ Secure password reset flow
- □ Account lockout after failed attempts

Authentication Total: 18 items

API SECURITY

API Security Stats

STAT	VALUE
SaaS APIs exposed	500+ avg
API attacks increase	+300% YoY
Breaches via API	41%
APIs with auth issues	34%

API Security Controls (10 items)

- □ OAuth 2.0/API key authentication
- □ Rate limiting per API key/user
- □ Input validation on all endpoints
- □ Output filtering (no data leakage)
- □ API versioning strategy

□ API documentation with security notes

□ Regular API penetration testing

API Monitoring (4 items)

□ API usage analytics per customer

□ Anomaly detection for API abuse

□ Error rate monitoring

□ Latency monitoring and alerting

API Security Total: 14 items

DATA PROTECTION & PRIVACY

Encryption Requirements (6 items)

□ Data encrypted at rest (AES-256)

□ Data encrypted in transit (TLS 1.2+/1.3)

□ Database encryption (transparent or field-level)

□ Backup encryption

□ Key management (customer-managed option)

□ Encryption key rotation

Data Privacy Controls (6 items)

□ Data processing agreement (DPA) available

□ GDPR compliance (EU customers)

□ CCPA compliance (CA customers)

□ Data retention policies documented

□ Data deletion capability (right to erasure)

□ Data export capability (portability)

Data Residency (3 items)

□ Data residency options (US, EU, etc.)

□ Cross-border transfer documentation

□ Regional deployment capability

Data Protection Total: 15 items

INFRASTRUCTURE & CLOUD SECURITY

Cloud Security Posture (8 items)

□ Cloud security configuration baseline

□ CSPM (Cloud Security Posture Management) tool

□ Infrastructure as Code (IaC) security scanning

□ Least privilege IAM policies

Container Security (4 items)

- □ Container image scanning
- □ Base image hardening
- □ Runtime container security
- □ Kubernetes security (if applicable)

Monitoring & Detection (4 items)

- □ Centralized logging (SIEM)
- □ Security event alerting
- □ Intrusion detection
- □ Anomaly detection

Infrastructure Security Total: 16 items

COMPLIANCE & CERTIFICATIONS

SOC 2 Roadmap

PHASE	DURATION	ACTIVITIES
Gap Assessment	2-4 weeks	Identify control gaps
Remediation	2-4 months	Implement controls
Type I Audit	4-6 weeks	Point-in-time assessment
Observation	3-6 months	Operate controls
Type II Audit	4-6 weeks	Operating effectiveness

SOC 2 Readiness Checklist (10 items)

- □ Security policies documented
- □ Access control procedures
- □ Change management process
- □ Incident response plan
- □ Vendor management program
- □ Employee security training
- □ Vulnerability management
- □ Logging and monitoring
- □ Business continuity plan
- □ Risk assessment process

CERTIFICATION	WHEN NEEDED
ISO 27001	International enterprise
HIPAA/BAA	Healthcare customers
PCI-DSS	Payment processing
FedRAMP	Government customers
GDPR	EU customers

SECURITY QUESTIONNAIRE ACCELERATION

Common Enterprise Questions (Top 20)

1. Do you have SOC 2 Type II certification?
2. How is data encrypted at rest and in transit?
3. Do you support SSO/SAML?
4. What is your incident response process?
5. How do you handle data breaches?
6. What is your data retention policy?
7. Do you conduct penetration testing?
8. How is access to customer data controlled?
9. What is your backup and disaster recovery?
10. Do you have a vulnerability management program?
11. How do you vet third-party vendors?
12. What security training do employees receive?
13. How is customer data isolated?
14. What is your SLA and uptime guarantee?
15. Do you offer data residency options?
16. How can customers export/delete their data?
17. What compliance certifications do you hold?
18. How do you handle security vulnerabilities?
19. Do you have cyber insurance?
20. What is your change management process?

Trust Center Essentials

- ☐ Public security page/trust center
- ☐ SOC 2 report (NDA download)
- ☐ Penetration test summary
- ☐ Architecture overview
- ☐ Data flow diagram
- ☐ Subprocessor list
- ☐ Security contact information

Minimum Viable Security (30 items for Seed/Series A)

Week 1-2: Foundation

- □ Enable MFA for all employees
- □ Implement SSO for internal tools
- □ Configure secrets management
- □ Enable audit logging
- □ Set up security monitoring

Week 3-4: Development

- □ Implement secure coding guidelines
- □ Add SAST to CI/CD pipeline
- □ Enable dependency scanning
- □ Configure branch protection
- □ Implement secrets detection

Month 2: Infrastructure

- □ Review cloud IAM policies
- □ Configure VPC/network security
- □ Enable encryption at rest
- □ Implement backup strategy
- □ Set up monitoring/alerting

Month 3: Compliance Prep

- □ Document security policies
- □ Implement access reviews
- □ Configure SSO for customers
- □ Create incident response plan
- □ Start SOC 2 preparation

CHECKLIST SUMMARY

Total Controls by Category

CATEGORY	COUNT	STAGE
Secure Development	24	Seed
Multi-Tenant Security	13	Seed
Authentication	18	Series A
API Security	14	Series A
Data Protection	15	Series A
Infrastructure	16	Series B
Compliance	10	Series A

PRIORITY	CONTROLS	TIMELINE
P0 - Ship Blockers	15	Before launch
P1 - Enterprise Ready	30	Series A
P2 - Scale Ready	35	Series B
P3 - Industry Leader	30	Growth

Ready to Get Started?

Let our team of security and infrastructure experts help you achieve your goals faster.

100%
AUDIT PASS RATE

60+
ORGANIZATIONS SERVED

8-12 wk
AVG. TIME TO COMPLIANCE

24/7
MONITORING & SUPPORT

Get Free Assessment

Book Strategy Call

SaaS Security Services

Email: hello@platops.com Phone: (202) 864-1197 Web: platops.com

This document is provided for informational purposes only. Requirements may vary based on your organization's specific circumstances. PlatOps is a registered trademark. Redistribution without permission is prohibited.