AppOmni

SaaS Security Checklist

AppOmni's SaaS Security Checklist is based on best practices recommended by our team of security experts. It's designed to be utilized alongside cybersecurity models such as the NIST Cybersecurity Framework, ISO-27000, and the CIA triad.

The checklist contains seven key categories and is designed to serve as a guide for organizations looking to build successful SaaS security programs.

Configuration & Posture Management

Verify that your SaaS security program supports third-party application management as well as data access management. Expertise should be embedded in the product with guidance and advice offered to your team so their time and energy can be focused on mitigating the highest risk misconfigurations and data exposures.

- [ ] 3rd-party app visibility
- [ ] Custom configuration checks
- [ ] Custom policy scanning
- [ ] Settings & configuration monitoring
- [ ] Compliance policies
- [ ] Data leak prevention
- [ ] Data access management & permissions
- [ ] Access control
- [ ] Privacy control
- [ ] Expertise in security policies & compliance
- [ ] User inventory

But Don't Stop Here!

When it comes to SaaS security, many companies don't go any deeper than configuration management. This leaves their business-critical applications and sensitive data at risk. A successful SaaS security program requires several additional components.

In addition to Configuration and Posture Management, a successful SaaS security program also includes the following functionality:

Deep Security Architecture

Ensure you have deep security coverage for your most business-critical SaaS applications. Depth of coverage delivers effective SaaS security to protect and monitor your entire SaaS ecosystem. Additionally, running comprehensive security checks provides a clear look into the SaaS ecosystem, integrations, and domains of risk.

- [ ] Extensive security coverage & capabilities
- [ ] Easy to expand as you scale
- [ ] Unlimited security checks for these areas: 2FA requirements, role assignments, user password policies, admin & elevated permission assignments to users, 3rd-party app inventory, 3rd-party app scope & permission tracking
- [ ] Support for common use cases: Pre-SaaS Implementation, Securing Current SaaS Platforms, Post-Breach Security, M&A Due Diligence, IPO Preparation, 3rd-Party App Inventory, Auditing Permissions Hierarchy, Shifting to a Hybrid Workforce

Continuous Monitoring & Threat Detection

Embrace automated tools that continuously monitor the millions of policy settings and permissions in your SaaS platforms. Look for a tool that offers continuous monitoring and visibility to identify SaaS risks and manage data access.

- [ ] Always-on continuous monitoring
- [ ] Suspicious activity alerts
- [ ] SaaS event log monitoring
- [ ] Case & service management

Automated Workflow

Create an automated security workflow that provides a structured way to identify, detect, protect against, respond to, and recover from security threats. These workflows are designed to establish and enforce consistent data access policies across all SaaS applications to stay vigilant for possible areas of exposure.

- [ ] Aggregated & normalized SaaS activity events
- [ ] Automated remediation workflows
- [ ] Integration with existing security workflows
- [ ] Alerts on deviations from application-specific user settings
- [ ] Scanning of APIs, security controls & configuration settings
- [ ] Least privilege access & role-based access control

DevSecOps

Utilize DevSecOps to shorten the development cycle while maintaining enterprise-level quality control. DevSecOps provides automation, continuous monitoring, and better communication between teams and ensures that security can be integrated in all project phases.

- [ ] Integration with SSO/SAML providers
- [ ] SaaS data classification & mapping engine
- [ ] Multi-vector approach for risk assignments
- [ ] Custom policies that automatically scan development environments
- [ ] Continuous issue identification & remediation advice
- [ ] Always-on, point-in-time SaaS incident response
- [ ] Authentication flows for single sign-on

Governance & Risk Compliance

Establish and maintain a SaaS governance or assurance plan that implements security measures to reduce risk associated with SaaS apps. The plan should include compliance frameworks, documentation, and due diligence for ongoing monitoring and risk reduction.

- [ ] Compliance mapping
- [ ] Centralized location for cross-SaaS configuration review & analytics
- [ ] Continuous monitoring for SOC2, ISO 27001, NIST-CSF, NIST 800-53, SOX
- [ ] Built-in, always-on SaaS compliance reporting for SOC2, ISO 27001, NIST-CSF, NIST 800-53, SOX

System Functionality

Look for system requirements and onboarding capabilities that help set up your SaaS security program for success. Your solution should be easy to deploy and allow your security team to easily add and monitor new applications as your SaaS environment lives and grows.

- [ ] Robust APIs
- [ ] Low false positives
- [ ] Quick deployment
- [ ] Customizable alerts
- [ ] Guided onboarding process
- [ ] Collaboration with existing security & IT teams
- [ ] Global onboarding
- [ ] UX tailored to all levels of technical expertise
- [ ] Integrations for safe onboarding
- [ ] SaaS-delivered solution that connects within minutes

CONCLUSION

There are many considerations when it comes to SaaS security and the stakes can be high. The goal of a successful SaaS security program should be to decrease the level of risk across your SaaS environment through full and continuous visibility into security settings and configurations, data access management, and third-party application coverage.

AppOmni's patented technology deeply scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent. Businesses and enterprises can establish rules for data access, data sharing, and third-party applications that will be continuously validated. AppOmni was founded by enterprise security veterans with frontline experience preventing and stopping cyber threats. Our leadership team brings expertise and innovation from leading SaaS providers, high-tech companies, and cybersecurity vendors.

Reference our Quick Start Guide to put this checklist into action, or get in touch to discuss these recommendations in more detail.

To learn more, email us at info@appomni.com or visit appomni.com.

AppOmni is a leading provider of SaaS Security Management software. Its patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. AppOmni makes it easy for security and IT teams to protect and monitor their entire SaaS environment, from each vendor to every end-user.

2022-08