AppOmni

Secure Your SaaS Data

SaaS Security Posture Management Checklist

Critical components of a comprehensive SaaS security solution and program.

AppOmni's SaaS Security Checklist is designed to help Security and IT teams build successful SaaS security programs. It is developed by our SaaS security experts and modeled on best practices as outlined by the NIST Cybersecurity Framework, ISO-27000, CIS Critical Security Controls and the NCSC's Shared Responsibility Model.

Configuration Management

Look for a SSPM tool that offers continuous monitoring and visibility to identify SaaS risks and manage data access. Establish your security posture by defining configuration settings for your SaaS apps. 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 first.

- [ ] Support for all SaaS apps in your ecosystem, including standardand custom apps
- [ ] 24/7 continuous monitoring for unlimited number of supported apps
- [ ] Custom system and User settings configuration checks and policy scanning
- [ ] Out-of-the-box & customizable SaaS security policies created and maintained by experts
- [ ] Measure SaaS Security Posture and Risk Reporting Over Time
- [ ] End-User Permission Management
- [ ] SaaS Security Baseline SaaS Development
- [ ] Configuration Drift Detection
- [ ] Automated Detections of Misconfigurations
- [ ] End-User Context
- [ ] Centralized Security Controls
- [ ] User Audits and SaaS Inventory

Security Architecture

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.

Ensure you have deep and broad security coverage for all your SaaS applications. Depth and breadth of coverage delivers effective SaaS security to protect and monitor your entire SaaS ecosystem. Additionally, running comprehensive security checks provides observability into the SaaS ecosystem, integrations, and domains of risk.

Unlimited security checks for these areas:

- [ ] Password Policy Enforcement
- [ ] MFA Enforcement
- [ ] Conditional and Role-Based Access Controls (RBAC)

SaaS-to-SaaS App Management

Verify that your SaaS security program supports third-party application management. Inventory all installed 3rd party apps and control access levels for SaaS-to-SaaS connections. Track and monitor all SaaS-to-SaaS app access through comprehensive security checks to have a full understanding of your risk exposure. Look for an SSPM solution that is equipped with the following third-party monitoring tools to prevent unauthorized access.

- [ ] Automated SaaS-to-SaaS Discovery
- [ ] 3rd-Party App Scope & Permission Tracking
- [ ] 3rd-Party Inventory of Every Add-On, API Extension, Utility or 3rd Party Integration
- [ ] Discovery of Permission Access Level
- [ ] Ability to Approve or Remove Apps
- [ ] Baselining of 3rd Party Apps
- [ ] Settings Detection
- [ ] Installation Dates & End User Analytics
- [ ] Ability to Search & Filter
- [ ] Security Risk Rating of App & Publisher

Deep Data Exposure Prevention

Verify that your SaaS security program supports data access management. Quickly identify SaaS data exposed on the public Internet and other critical data leakage gaps. You need full control over your Users' data access and actions. Look for a SSPM solution that allows you to control access to each End-User with granular roles and robust environment restrictions while also safeguarding sensitive data.

- [ ] Data Exposure Prevention
- [ ] Data Access Management
- [ ] Visualization of Data Exposure
- [ ] User Access and Permissions
- [ ] Customizable Policies to Govern What End-Users & Systems Can See & Do
- [ ] Customizable Policies to Monitor that End-Users Maintain Access & Permissions
- [ ] Least Privilege Access
- [ ] Role-Based Access Control with Predefined Roles
- [ ] Inventory of Settings, RBAC assignments, and End-User Types
- [ ] Combine Roles to Create Permissions Unique to Your Requirements

Threat Detection & Activity Monitoring

Embrace automated tools that continuously monitor the millions of policy settings and permissions in your SaaS platforms. Act on threats and suspicious activity with custom alerts and guided remediation steps. Create an automated security workflow that provides a structured way to detect, protect against, respond to security threats and events. These workflows are designed to establish and enforce consistent data access policies across all SaaS applications to stay vigilant for possible areas of exposure.

- [ ] Visibility into Security Events
- [ ] SaaS Event Log Monitoring & Drift Detection
- [ ] Always-on, Continuous Monitoring of Policy Settings & Permissions
- [ ] Out-of-the-box & Custom Suspicious Activity Detection & Alerting on Deviations from Specific Settings
- [ ] Integrated Workflows with SIEM, SOAR or Security Data Lake
- [ ] Incident Detection & Response, including Case Management
- [ ] Guided Remediation
- [ ] Automated Remediation Workflows
- [ ] Aggregated & Normalized SaaS activity Events
- [ ] Scanning of APIs, Security Controls & Configuration settings

DevSecOps

Utilize DevSecOps to shorten the development cycle while maintaining enterprise-level quality control. It is essential to use a SSPM solution in the Secure Software Development lifecycle. 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
- [ ] Authentication Flows for Single Sign-on (SSO)

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 to Internal Policies
- [ ] Compliance Mapping to Regulatory Frameworks, including SOX, SOC2, ISO 27001, NIST CSF, NIST 800-53, and CPS 234
- [ ] Built-in, Always-on & Point-in-time SaaS Compliance Reporting for SOX, SOC2, ISO 27001, NIST-CSF, NIST 800-53, CPS 234
- [ ] User Access and Permissions
- [ ] A Centralized GRC view for SaaS Estate Configuration Review & Reporting

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 grows.

- [ ] Quick Deployment
- [ ] Guided Onboarding Process
- [ ] Integrations for Safe Onboarding
- [ ] Support for Custom SaaS apps
- [ ] Robust Platform APIs
- [ ] Customizable Alerts
- [ ] Low False Positives
- [ ] UX Tailored to all Levels of Technical Expertise
- [ ] Integration with Ticketing Systems

There are many considerations when it comes to SaaS security and the stakes are high. The goal of a successful SaaS security program should be to decrease the level of cyber risk across your SaaS environment. You can only realize this by adopting a best-in-breed tool that enables continuous monitoring and visibility into SaaS security and configuration settings, including data access and SaaS-to-SaaS app management.

AppOmni is the leading provider of SaaS security. AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organizations to secure mission-critical and sensitive data. Its 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. With AppOmni, organizations can establish rules for data access, data sharing, and SaaS-to-SaaS applications that will be continuously and automatically validated. The company's leadership team brings expertise and innovation from leading SaaS providers, high tech companies, and cybersecurity vendors.

Get in touch to discuss these recommendations in more details or visit **appomni.com**.