



Cybersecurity Assistance for Nonprofits

SaaS Security Features Checklist

What to Look For *and Demand* in Your Team's
Cloud Subscriptions: A Practical Checklist for
Essential Security

First Edition

October 2026

As the 501Secure program enters its third year, our expert volunteers continue to serve the nonprofit community with practical cybersecurity information, awareness programming, expert guidance, and free services.

We hope you find this checklist helpful when evaluating cloud software subscriptions and vendors.



Questions about this guide or the 501Secure program contact the 501Secure Team at info@501Secure.org.

For immediate cybersecurity assistance, email help@501Secure.org.

SaaS Security Feature Checklist

By Raymond Osei
GRC Coordinator and Documentation Specialist 501Secure



Central Management of User Logins and Account Access

Technical Term: IAM - Identity and Access Management

IAM is the system used to control who can access your organization's applications and data. It helps make sure employees, contractors, and volunteers only have access to the information they need for their jobs.



One Primary Login Account to Access Multiple Separate Tools and Apps

Technical Term: SSO - Single Sign-On

Single Sign-On allows users to access multiple applications with one set of login credentials. This reduces password fatigue and makes it easier for staff to securely access the tools they need. It also affords the ability to rapidly revoke access to data and accounts if user credentials are compromised or an employee separates from the organization.



Rules That Block or Allow Sign-Ins Based on Specific Conditions Like Device or Location

Technical Term: Conditional Access

Conditional access can be device or user policies to add extra security rules before someone can sign in. For example, it can require additional verification if a user is logging in from a new device, unusual location, or outside normal work hours.



Options to Require a Second Verification Step Beyond a Password for Account Sign-In

Technical Term: MFA - Multi-Factor Authentication

MFA requires users to provide an additional form of verification beyond a password, such as a mobile app notification or security code. This helps protect accounts, even if a password is stolen.



Option to Give Users Access Based on Their Specific Job Duties

Technical Term: Role-Based Permissions

Role-based permissions allow access to be assigned based on a person's job responsibilities. This helps prevent staff from seeing or changing information that is not necessary for their role.



Mandatory Security Settings Instead of Just Opt-In Settings

Technical Term: Global Enforcement vs. Self-Selected Setup

This determines whether administrators can require security settings for all users or whether users choose their own security options. Organization-wide enforcement provides more consistent and effective protection. For organizations that must adhere to compliance standards, global security control is essential.



Admin Tools to Check Which Users Have Set Up MFA and What Method They've Chosen

Technical Term: Admin MFA Audit Functions

MFA audit functions allow administrators to see which users have enabled MFA and identify accounts that may not meet security requirements. This helps ensure security policies are being followed.



Available Methods for the Second Sign-In Step, Such as an Authenticator App, Hardware Key, or Text Code

Technical Term: MFA Options

MFA options are the different ways users can verify their identity, such as authenticator apps, text messages, email codes, or passkeys. More options provide flexibility while supporting different user needs.



Backup Steps for Users to Regain Account Access If They Lose Access to Their Second Sign-In Option

Technical Term: MFA Recovery Options

Recovery options help users regain access to their accounts if they lose their phone, security key, or authentication method. Strong recovery processes reduce downtime while maintaining security.



Automatically Log User Out After a Set Period of Inactivity You Control

Technical Term: Session Timeout

Session timeout automatically signs users out after a period of inactivity. This helps prevent unauthorized access if a device is left unattended.



Control Over How Long a User Stays Signed in Before Being Asked to Re-Enter Their Credentials

Technical Term: Token Duration

Token duration determines how long a user can stay signed in before they must reauthenticate. Shorter durations improve security, while longer durations improve convenience.



Automatically Requiring Extra Verification or Blocking Sign-Ins When an Attempt Looks Suspicious

Technical Term: Risk-Based Conditional Access

Risk-based access encompasses external risk signals evaluated in real-time and can use information such as unusual locations, devices, or login behavior to identify potentially suspicious sign-ins. Additional security checks can then be required before access is granted.



A One-Click Action to Immediately Log an Account Out Across Every Active Device and App

Technical Term: Suspend All Sessions

This feature allows administrators to immediately sign users out of active sessions. It is useful when responding to a security incident or a compromised account.



Records Showing Where, On What Device, and From What Network Connection a User Signed In

Technical Term: Session Device, Location, and IP Information

Administrators can view where users are logged in from and what devices are being used. This information helps identify suspicious or unauthorized access.



Requiring a User to Choose a New Password on Their Next Sign-In

Technical Term: Forced Password Reset

Administrators can require users to create a new password. This is often used when an account may have been compromised or when security policies change.



Access to Historical Account Activity and Sign-In Records and Control Over How Long They Are Kept

Technical Term: Availability of Logs

Logs provide a record of user activity, sign-in attempts, and administrative actions. They help organizations investigate security incidents and demonstrate compliance requirements.



Tracking Where and On What Devices an Active Login Credential is Being Used

Technical Term: Token Usage Across Devices and Locations

This control determines whether a login session can continue working when accessed from different devices, locations, or IP addresses. Restricting token reuse can reduce the risk of account misuse. This reduces the risk of stolen tokens being reused to break into accounts.



Connecting SaaS Account Activity Records to an External Security Log-Monitoring Service

Technical Term: SIEM Integrations

Security Information and Event Management (SIEM) integration capability allows security information from the application to be sent to a central monitoring platform. This helps organizations detect threats and investigate security events more efficiently.



Connecting Accounts to a Security Tool That Monitors and Protects SaaS Account Access and Activity

Technical Term: CASB Integrations

Cloud Access Security Broker (CASB) integration capability provides additional visibility and security controls for cloud applications. They help organizations enforce account access, monitor data usage, enforce data protection policies, and reduce cloud-related risks. It offers central access control for what would be shadow IT. It is accomplished by combining a CASB with an enterprise level browser.