



Cybersecurity Assistance for Nonprofits

Security Feature Matrix

Google Workspace

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 Security Feature Matrix helpful when evaluating cloud software subscriptions and vendors.



Cybersecurity Assistance for Nonprofits

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

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

Security Feature Matrix 2026

Google Workspace

GOOGLE WORKSPACE

Consider: Does your organization need the additional security capabilities enough to justify moving to a higher-cost license? Consider the sensitivity of member information, number of users, use of personal devices, account takeover risk, compliance requirements, and whether lower-cost tiers combined with MFA, least privilege, access reviews, and documented security procedures adequately reduce the organization's risk.

Access Control Capabilities	Business Starter	Business Standard	Business Plus	Enterprise Standard/ Plus
Suspend all sessions	Yes: Admin can sign users out of Google services and revoke active sessions from the Admin console.	Yes: Same functionality as Starter license.	Yes: This includes enhanced security management along with the same functionality as the previous two licenses.	Yes: Includes full administrative session management with advanced security controls.
Token duration	Limited: Google uses default token settings, Admin has limited control over the session	Limited: Same limitations as Starter license.	Yes: Admins can set session length for Google services and require users to sign in again after a set period.	Yes: Admins can configure session length and reauthentication policies using Context-Aware Access.* This feature makes access decisions based on the context of the login, not just username and password.
Conditional access	Limited: Administrators can use fundamental endpoint management and basic account security settings, but cannot create advanced access policies based on device, location, or IP address.	Limited: Administrators can enforce basic mobile device policies, including screen-lock requirements, remote account wiping, device blocking, and inventory tracking. It does not include advanced Context-Aware Access policies.	Limited: Some security settings are available, but advanced conditional access policies are not included.	Yes: Includes Context-Aware Access* for creating advanced access policies based on defined login and device conditions.
Role-Based Access Permissions - Admin and User Access	Yes: Uses Google's predefined administrator roles to assign permissions. User access can also be organized through groups, organizational units, Google service settings, and file or Shared Drive permission levels.	Yes: Same core user and administrator access options as Starter. Shared Drives provide additional organization-owned file access roles for teams.	Yes: Same role and user-access capabilities, with additional security and endpoint management features.	Yes: Supports predefined and custom administrator roles along with groups, organizational units, service access settings, and granular Shared Drive permissions.

Single sign-on	Yes: Supports SAML-based Single Sign-On with compatible identity providers.	Yes: Same functionality as Starter license	Yes: Same functionality as previous license	Yes: Supports advanced SSO integrations and enterprise identity management. Compatible with many SAML 2.0 identity providers.
Global MFA enforcement	Yes: Administrators can require 2-Step Verification for all users or selected organizational units.	Yes: Same functionality as Starter license	Yes: Same functionality as previous licenses	Yes: Includes global enforcement with additional policy controls.
Admin MFA audit functions	Yes: Administrators can view users' 2-Step Verification enrollment status.	Yes: Same functionality as Starter license	Yes: Includes additional security reporting features.	Yes: Enhanced reporting and security insights.
MFA options	Yes: Supports Google Prompt, Authenticator app, security keys, passkeys, backup codes, phone prompts, and SMS	Yes: Same functionality as Starter license	Yes: Same functionality as previous licenses	Yes: Same options with enterprise policy controls.
MFA recovery options	Yes: Administrators can reset 2-Step Verification and issue backup codes for users who lose access to their authentication method.	Yes: Same functionality as Starter license	Yes: Same functionality as previous licenses	Yes: Includes additional enterprise recovery and identity management capabilities.
Session Timeout	Limited: Google uses default web session behavior. Admins do not have full control over web session duration in this tier.	Limited: Same limitations as Starter license.	Yes: Admins can set web session duration for Google services and require users to sign in again after a set period.	Yes: Same session duration control, with additional advanced security controls available through Enterprise features.
Risk-Based Conditional Access Policies	No: Admins cannot create advanced conditional access policies.	No: Same limitation as Starter license.	No: Business Plus has stronger security tools, but it does not include full Context-Aware Access policies.	Yes: Admins can create Context-Aware Access policies based on user identity, device security status, IP address, location, and other conditions.
Device, Location, and IP Information for Sessions	Limited: Admins can review user and device log events, but advanced investigation tools are not included.	Limited: Same functionality as Starter license.	Yes: Includes useful audit and log review capabilities for user and device activity.	Yes: Includes advanced investigation features and Context-Aware Access details for device, IP, and location-based access decisions.
Forced Password Resets	Yes: Admins can reset a user's password from the Admin console.	Yes: Same functionality as Starter license.	Yes: Same functionality as previous licenses.	Yes: Same functionality, with stronger investigation and response tools available.
Availability of Logs	Yes, limited: Admins can access basic audit and user log events.	Yes, limited: Same basic log availability as Starter license.	Yes: Provides useful logging for routine security monitoring.	Yes: Includes advanced security investigation tools and expanded options for monitoring and exporting logs.
How Tokens Are Configured Across	Limited: Google provides default session protection, but admins have	Limited: Same limitations as Starter license.	Partial: Admins can control web session duration, but advanced	Partial: Admins can control web session duration, but advanced device, IP, and location-based session

Locations, IPs, and Devices	limited control over whether sessions are tied to specific devices, IPs, or locations.		device, IP, and location-based session enforcement is not fully included.	enforcement is not fully included.	
Integrations with SIEM or CASB	Limited: Basic logs can be reviewed, but advanced SIEM/CASB-style integrations are not the main value of this tier.	Limited: Same limitations as Starter license.	Limited: Better security features, but advanced log export and security operations integrations are still limited.	Limited: Better security features, but advanced log export and security operations integrations are still limited.	
API Integration for User Provisioning / Deprovisioning	Yes: Google Admin SDK Directory API can be used to create, update, suspend, and delete organizational user accounts.	Yes: Same core API-based user management capabilities.	Yes: Same core API-based user management capabilities with additional security features available within the edition.	Yes: Supports API-based user lifecycle management and can be incorporated into more advanced enterprise identity-management workflows.	
Is this tier worth it?/ Questions to consider	High: The best value for small nonprofits, it includes essential security controls without significant cost. Consider whether the organization stores sensitive client data, has remote staff, or needs stronger retention and investigation tools before staying on this tier long-term.	High: For growing organizations in need of additional collaboration and storage while maintaining strong security. Consider whether the upgrade is solving a real business need, since it does not significantly improve advanced identity controls.	Medium: Worth the upgrade for organizations managing sensitive data or in need of enhanced compliance and security capabilities. Ask whether the organization needs retention, eDiscovery, advanced endpoint management, or better security controls before paying more.	Low: Provides the most advanced security capabilities, but the significant licensing cost may not be worth it unless the organization has strict compliance requirements or high cybersecurity risks. Consider this tier if the organization has HIPAA, grant, contract, cyber insurance, or client data protection requirements that require stronger access control and monitoring.	
Control	Availability / Plan	Control's Purpose/benefits	Compensatory Method	Control Mapping	Documentation Link
Suspend All Sessions	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Allows an administrator to end a user's active login sessions when an account may be compromised. This would help the client respond quickly to another suspected account takeover by removing existing unauthorized access.	If sessions can't be immediately revoked, temporarily suspend the user's account or reset password until the issue is resolved	PR.AA-05	Suspend all sessions
Token Duration	Business Plus, Enterprise Standard / Plus	Controls how long authentication remains valid before a user must authenticate again. This can reduce how long stolen or compromised authentication credentials remain useful.	Use shorter browser session settings, require MFA, encourage users to sign out of public	PR.AA-04	Set session duration Re-authentication Compare Business Editions
Conditional Access	Enterprise Standard / Plus	Controls access based on conditions such as a user's device, location, or IP address. This can help protect the client's email and files when board members access	Enforce MFA, use strong and complex passwords, monitor sign-in activity, and restrict account sharing	PR.AA-05	Context aware access Compare Business Editions

		Google Workspace remotely or from personal devices.			
Role-Based Access Permissions	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Limits what users can access or manage based on their assigned responsibilities. This would help the client prevent board members or volunteers from receiving unnecessary administrative access.	If custom roles are unavailable, use Google's predefined administrator roles and Organizational Units	PR.AA-05	RBAC
Single Sign-On	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Allows users to access connected applications using one organizational identity instead of maintaining separate credentials for each application. This can simplify access for board members and reduce the number of passwords they need to manage.	Require MFA on individual applications if SSO is not configured	PR.AA-03	SSO Compare Business Editions
Global MFA Enforcement	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Allows administrators to require MFA for users instead of relying on each person to enable it themselves. This would help reduce the client's risk of another account takeover caused by a compromised password.	If MFA cannot be enforced immediately, require strong passwords and provide regular phishing awareness training	PR.AA-03	2-Step Verification Compare Business Editions
Admin Audit MFA Functions	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Allows administrators to review which users have MFA enabled and identify accounts that are not properly protected. This would help the client confirm that board members are following required account-security procedures.	Periodically review users' 2-Step Verification enrollment status manually through the Google Admin console and follow up with users who have not enrolled.	PR.AA-05	Enforcing and monitoring requirements/ 2-Step verification reporting Compare Business Editions
MFA Options	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Gives users multiple ways to verify their identity in addition to a password, such as passkeys, security keys, prompts, or authenticator apps. This gives the client stronger authentication options for protecting board email accounts.	If passkeys or security keys are unavailable, then require authenticator apps instead of SMS whenever possible.	PR.AA-03	MFA methods Compare Business Editions
MFA Recovery Options	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Provides methods for restoring access when a user loses their normal MFA method. This would help board members regain access without removing MFA	Securely store backup codes and verify user identity for recovery.	PR.AA-01	Recovery options

		protection from their accounts.			
Session Timeout	Business Plus, Enterprise Standard / Plus	Controls how long a user can remain signed in before reauthentication is required. This can reduce unauthorized access if a board member leaves Google Workspace signed in on a personal device.	Require MFA, encourage users to sign out of shared or public devices, and reset sign-in cookies when needed.	PR.AA-04	Set session duration Compare Business Editions
Risk-Based Conditional Access Policies	Enterprise Standard / Plus	Uses information about a login attempt to determine whether access should be allowed or additional protection is needed. This could help protect the client's accounts from suspicious access attempts involving unfamiliar locations or devices.	Enforce MFA, use strong passwords, monitor sign-in activity, and restrict account sharing.	PR.AA-05	Context-Aware Access Compare Business Editions
Device, Location, and IP Information for Sessions	Business Plus, Enterprise Standard / Plus	Provides information about the devices and locations being used to access organizational accounts. This can help the client identify suspicious access, especially because board members use personal devices.	Review user and device log events regularly, follow up on unfamiliar access, and require MFA for risky accounts.	PR.PS-04	User log events Device log events Compare Business Editions
Forced Password Resets	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Allows administrators to require a user to change a password when credentials may no longer be secure. This would help the client secure a board member's account after suspected password compromise.	If SSO is used, reset the password through the organization's identity provider and revoke active sessions when possible	PR.AA-01	Reset password Compare Business Editions
Availability of Logs	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Provides records of user and administrative activity that can be reviewed after suspicious activity occurs. This would help the client investigate account incidents and determine what happened.	Keep a manual incident log, review account activity reports regularly, and document unusual activity until more advanced tools are available.	PR.PS-04	User log events Compare Business Editions
How Tokens Are Configured Across Locations, IPs, and Devices	Enterprise Standard / Plus	Controls how authenticated access can be used across different devices, locations, or IP addresses. This can help reduce the risk of stolen authentication being reused from an unauthorized device or location.	Require MFA, reset sign-in cookies after suspicious activity, and use trusted devices where possible.	PR.AA-04	Context-Aware Access Assign context-aware access levels to apps Session binding

Integrations with SIEM or CASB	Enterprise Standard / Plus	Connects Google Workspace security information with external security monitoring tools. This could help the client monitor suspicious activity across its systems, although it may be more advanced than their immediate needs.	Use built-in Google logs, alerts, Admin console reports, and manual review before investing in advanced security platforms.	DE.CM-03	Export log events CASB guidance Compare Business Editions
API Integration for User Provisioning / Deprovisioning	Business Starter, Business Standard, Business plus, and Enterprise Standard/Plus	Automates creating, updating, suspending, and removing user accounts when access needs change. This could reduce manual work and help ensure former board members or volunteers do not retain organizational access.	Establish a documented process requiring an administrator to immediately create, suspend, or remove accounts when board members or volunteers join or leave.	PR.AA-01	Directory API