

SecureAuth for Google – Full Functionality

	Google Alone	Google + SecureAuth
2-Factor User Authentication	Yes	Yes
Forces Uses to do 2-Factor (Not User Opt out – necessary for PCI DSS, NCUA, HIPAA/HITECH, FFIEC, etc.)	No	Yes
Users Use their own AD (or other) ID	No	Yes
Users User their own AD (or other) password	No	Yes
Users get Active Directory SSO (Desktop SSO)	No	Yes
Users get Web SSO into other on-premise web apps (.NET, J2EE)	No	Yes
Users get Web SSO into other SaaS apps (Salesforce, Concur, SuccessFactors)	No	Yes
Password Synch from local directory (AD/LDAP) -> Google	No	Yes
Multi-Domain Google Authentication from local (AD/LDAP) directory	No	Yes
Dynamic Account Provisioning from enterprise DataStore	No	Yes
Local Logging (Syslog) of Google Authentications	No	Yes
Low-Friction (User unaware of 2Factor-Auth) Mode of Google Authentication	No	Yes
Certificate based Google Authentication (Non- Phishable, prevents MITM)	No	Yes
VPN Integration of 2-Factor Authentication	No	Yes
Local AD/LDAP Account tools: - AD/LDAP User Account creation - AD/LDAP 2-Factor Password Reset - AD/LDAP Profile User Self-Modification - AD/LDAP Help Desk User Management	No	Yes
iOS Google Password Provisioning (AD or other directory)	No	Yes
iOS Google ID Provisioning (AD or other directory)	No	Yes
iOS Google x.509 Provisioning (From AD or other Directory)	No	Yes