OctoFlow Security Overview

For IT and security teams reviewing OctoFlow

Last updated October 20, 2026 · Applies to OctoFlow v1.8.3 and later
octoflowus.com/security · support@octoflowus.com

What it is. OctoFlow is a Chrome side panel productivity extension, with a companion web app, for individual salespeople. It helps a user track their own professional relationships, log their own outreach activity, and manage a personal to do list. It is a personal productivity tool. It does not integrate with, modify, or extract data from company systems. This page exists so IT and security teams can review OctoFlow quickly when an employee requests it on a managed browser.

QUICK FACTS

Everything on this page can be verified against the Chrome Web Store listing and our privacy policy.

Extension name	OctoFlow, Sales Productivity
Extension ID	aaobogaacakidgajkkfkkafjoeelakdc
Platform	Chrome Manifest V3, Chrome's current extension security standard. Minimum Chrome 114.
Developer	OctoFlow LLC, Denver, Colorado. octoflowus.com
Security assessment	Google OAuth verification approved September 19, 2026 for the gmail.metadata and gmail.send scopes, on the strength of a CASA Tier 2 (App Defense Alliance) assessment by TAC Security passed September 15, 2026. Recertified annually.
Support	support@octoflowus.com, responses within one business day

PERMISSIONS REQUESTED AND WHY

OctoFlow requests six narrow Chrome permissions:

storage	Saves the user's own notes, contacts, and settings in Chrome's local extension storage
alarms	Powers daily reminders, the focus timer completion notice, and the background mail sweep timer for the optional email integration
notifications	Shows productivity reminders as desktop notifications
sidePanel	Renders the app inside Chrome's built in side panel
identity	Opens the standard Google or Microsoft sign in window when the user chooses to connect their mailbox. Used only for optional integrations the user starts; no sign in happens without a click.
scripting	Runs the one time LinkedIn profile read when the user clicks Scan, under the optional linkedin.com permission the user grants at that moment

SITE ACCESS

OctoFlow's network access is limited to its own backend and, only after the user connects them, the official Google and Microsoft mail APIs. It runs exactly one content script, described in the last row:

Google Firebase endpoints	firebaseapp.com, firestore.googleapis.com, identitytoolkit.googleapis.com, securetoken.googleapis.com, cloudfunctions.net: account sign in, optional cloud sync of the user's own data, and OctoFlow's own server functions
gmail.googleapis.com, oauth2.googleapis.com	Official Gmail API. Contacted only after the user connects their Google mailbox in Settings. Header only reads plus sends the user initiated, detailed in the email integration section below.
graph.microsoft.com, login.microsoftonline.com	Official Microsoft Graph API, the Outlook equivalent of the row above. Contacted only after the user connects their Microsoft mailbox.
hooks.slack.com	Optional Slack notifications the user configures themselves. Inactive unless the user sets it up.
mail.google.com (content script)	A small badge in the Gmail compose window showing whether OctoFlow email logging is connected. Display only: it reads no page content, collects nothing, and transmits nothing.

OPTIONAL EMAIL INTEGRATION

Off by default. OctoFlow touches no email of any kind until the user connects their own Gmail or Outlook account through the standard Google or Microsoft sign in window. After connecting, OctoFlow reads message headers (sender, recipient, subject, date, thread id) of recent sent and received mail to log outreach with contacts the user already tracks and to detect replies. It never reads the body of any received email; for Gmail this is enforced by Google's servers, because the gmail.metadata scope refuses to return message bodies at the API level. Sending happens only for email the user wrote in OctoFlow, whether they click Send or schedule an OctoMail campaign or sequence step, from the user's own address through the provider's own API, with no relay or third party mail service in between. When the user connects from the extension, a sign in token is stored in the browser's local extension storage. When the user connects from the web app, or turns on cloud sending for OctoMail, a refresh token is stored server side in the user's own private account record on Google Cloud, readable only by OctoFlow's server functions and never by any browser session; disconnecting deletes it. Emails sent through OctoFlow include a one pixel open notification image so the sender can see opens on their own outreach, and links in those emails pass through OctoFlow's own address so the sender can see which links were clicked and when; the reader lands on the original link. OctoFlow never adds anything to mail the user receives and never reads receipts on it. The user can disconnect in Settings at any time, which deletes the tokens, and can additionally revoke access from their Google or Microsoft account security page. OctoFlow's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. The exact scopes requested:

gmail.metadata	Google: message headers only. Google's API rejects requests for message bodies or attachments under this scope.
gmail.send	Google: sends an email the user composed, on the user's click or a campaign the user scheduled
email (profile)	Google: shows which account is connected
Mail.Read	Microsoft: reads mail to match headers to tracked contacts; OctoFlow requests header fields only
Mail.Send	Microsoft: sends an email the user composed, on the user's click or a campaign the user scheduled
User.Read, offline_access	Microsoft: shows which account is connected; lets the connection survive browser restarts without re prompting

OCTOAI AND AI PROVIDERS

OctoAI is an optional assistant on the Max and Ultra plans. To answer a question, draft an email or write the morning briefing, OctoFlow sends the question and a summary of the asking user's own OctoFlow data (their accounts, contacts, logged activity, tasks, sequences, deals, notes and email engagement) to an AI provider and shows the reply. On Max the provider is the one the user connected, Anthropic, OpenAI or Google Gemini, on the user's own API key. That key is encrypted on our server and never returned to the browser or the extension. On Ultra the request goes to Anthropic on a key OctoFlow holds in Google Secret Manager. A request only ever carries the asking user's own data, never another user's, and on a team plan a manager can ask about a rep only after that rep has switched sharing on. OctoAI reads and drafts. It does not send email, log activity or change records on its own. Under Anthropic's commercial API terms, API inputs are not used to train its models. On Max, the terms of the provider the user chose apply.

DATA HANDLING

The user's data (their contacts, notes, activity history, tasks) is stored locally in Chrome and optionally synced to Google Firebase under the user's own account. Sign in uses an email and PIN flow through Google Identity Platform. Data is encrypted in transit (TLS 1.2+) and at rest on Google Cloud. No data is sold or shared with third parties. Users can delete their account and all associated data from Settings at any time. Full details, including every data category we process and our sub processor list, live in our privacy policy.

WHAT OCTOFLOW DOES NOT DO

No collection of browsing history. No keystroke logging. No reading or scraping of corporate systems or CRM data. No reading of received email bodies, ever: mailbox access is off by default, opt in, and header metadata only, as detailed in the email integration section above. Nothing is added to or read from mail the user receives; the only open notification is on mail the user sends from OctoFlow, described above. Exactly one content script exists, on mail.google.com only, and it is a display only connection badge that reads nothing and sends nothing. No remote code execution: all code ships inside the Chrome Web Store reviewed package. No advertising or tracking SDKs.

FOR IT ADMINISTRATORS

To allow OctoFlow on a managed browser: Google Admin console, then Chrome browser, then Apps and extensions, then add the extension ID aaobogaacakidgajkkfkkafjoeelakdc and set it to Allow install (or approve the employee's pending request). This follows standard Chrome Enterprise extension management. If your organization also restricts which apps may access Google Workspace data, the optional email integration additionally needs its OAuth client allowed under Security, then API controls, then App access control. The Google Workspace admin sheet linked at the top of this page lists the client ID, the exact scopes, and the allowlist steps. For Microsoft 365, the admin sheet linked at the top of this page gives the application ID, the four delegated permissions, and the one click admin consent link for tenants that block user consent. If your review process needs anything else, write to support@octoflowus.com and we will respond within one business day.