Email Privacy
How Nudge Security safeguards your data

Nudge Security's patented approach to SaaS discovery uses email analysis powered by machine learning to uncover SaaS assets and activities. While this method provides unrivaled visibility of your SaaS landscape and a fast, lightweight deployment, we recognize that email is a sensitive resource for organizations. As such, we go to great lengths to safeguard your email and data privacy.

This data sheet describes how Nudge Security works to uphold our responsibility to protect and limit access to your email data. For additional questions and materials, please reach out to us directly at security@nudgesecurity.com.

Secure by Design

While this document does not attempt to describe our security program at length, it's important to know that our product and company are built on a foundation of security expertise gained through decades of experience building and operating security products for some of the world's largest enterprises. We are security people at heart, and as such, we take a security-first design approach to everything we build and operate, ensuring that we have the right infrastructure, automation, and monitoring controls in place from design to deployment.

For more information on our security program and compliance attestations or to request our compliance reports, including our SOC 2 Type 2 report, or other security information, please visit the Nudge Security Trust Center on our website.

Read-only access to Google Workspaces and Microsoft 365

Nudge Security's primary method of SaaS discovery works by analyzing mailboxes for evidence of SaaS activities. To do this, we rely on read-only API access to your Google Workspaces or Microsoft 365 domain, granted by your administrator during the initial setup of Nudge Security. Read-only access means that Nudge Security does not require any permissions that would allow us to modify or delete contents of mailboxes. This makes Nudge Security less permissive than the average SPAM filter or secure email gateway.

For more detail on all of the OAuth scopes Nudge Security uses and how, please see the following:

OAuth scopes list for Google Workspaces
OAuth scopes list for Microsoft 365

Scanning machine-generated emails

We use the Microsoft and Google search APIs, which allows us to be highly selective in our search queries and thus narrow the scope of the email dataset we analyze. We limit our search algorithms to inbound emails only, meaning that we never look at outbound emails sent by your employees or emails sent among employees within your domain.

Our machine-learning algorithms are trained to specifically look for machine-generated emails from SaaS providers, either known senders whose email communications we have already analyzed (e.g., no-reply@box.com) or by recognizing patterns that SaaS providers commonly use for email communication (e.g., subject: account password reset). This latter approach gives us a unique ability to identify new SaaS providers as they emerge without prior knowledge of their services or email communications.

SOC 2 Compliant

CCPA Compliant

Auditing our access

In addition to narrowing our email dataset, we also maintain a record of all the search queries we perform and the identifiers of every email analyzed. You can request this information at any time. Alternatively, your email administrator has the ability to review and verify the searches performed by Nudge Security from within your Google Workspaces or Microsoft admin console.*

*In Google Workspaces, API call events are available only for *Enterprise Plus*, *Education Plus*, *Enterprise Standard*, *Education Standard*, and *Cloud Identity Premium*.

Ephemeral, in-memory email analysis

No human eyes ever have access to the contents your emails. All email analysis performed by Nudge Security is done in memory with serverless ephemeral workers, where no employee can access it. During analysis, Nudge Security identifies and pulls out the relevant metadata from the email, such as application name, user account name, OAuth grants, timestamps, etc. and sends this event information to be stored in your SaaS inventory. All email contents and the ephemeral workers performing the analysis are destroyed after every job, persisting only for seconds during the job and never longer.

Deprovisioning and data deletion

Nudge Security not only maintains your right to destroy your data in the product and delete your instance, but we also make it very simple and straightforward to do so. Under the Settings tab in Nudge Security, you'll find options to delete all data and revoke access from your Microsoft 365 or Google Workspaces domain. Microsoft and Google administrators also have the ability to delete the application from within the respective admin consoles.

Employee transparency and trust

Compared to other methods of SaaS discovery available on the market today, Nudge Security promotes employee trust and transparency. Unlike other "big brother" approaches that rely on network monitoring, endpoint agents, or browser extensions, Nudge Security does not perform user activity monitoring or keyboard activity monitoring to track or collect data about your employees' online activities.

In contrast, Nudge Security was built with every employee in mind. Nudge Security administrators can extend platform access to all employees with an "individual access" role, which allows employees to view their own SaaS footprint. This encourages employees to disentangle their corporate identities from any personal or non-work-related SaaS usage, which often occurs by mistake. More so, this promotes a culture of trust, transparency and personal responsibility as it relates to safe and compliant SaaS use at work.

Get started with a 14-day free trial with zero commitment.

nudgesecurity.com