Nightfall

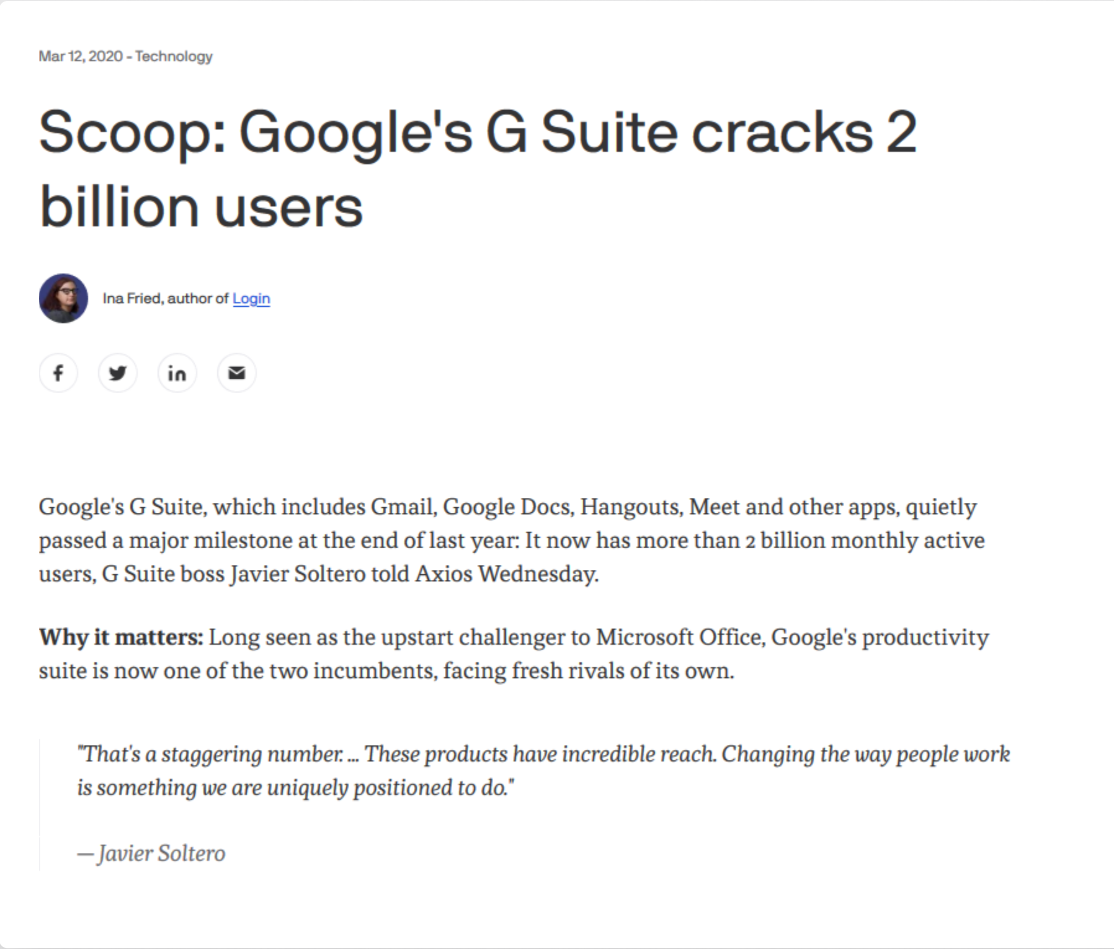
Guide to Data Loss Prevention in Google Drive

Google Drive in the context of data exposure

Google Workspace (formerly Google Suite) is among one of the most popular productivity platforms embraced by organizations today. With over 6 million customers and over 2 billion monthly active users, Google Drive is used by companies large and small to create, edit, and share files on a daily basis.

As platforms like Google Drive supplant traditional productivity tools, which ran locally as opposed to in the cloud, organizations are discovering that an ever growing amount of their sensitive data now lives in the cloud. Cloud platforms like Google Drive lack comprehensive out-of-the-box security options to help manage the proliferation of sensitive data in these environments, and organizations cannot rely on traditional enterprise security solutions to protect data in the cloud.

Without a dedicated security solution to address the problem of sensitive data leakage in cloud environments, organizations will remain at increased risk of incidents that violate data compliance policies and result in unauthorized data exposure. This ultimately increases business costs in the form of compliance violations, reputational harm, and related expenses.



Mar 12, 2020 - Technology

Scoop: Google's G Suite cracks 2 billion users

Ina Fried, author of Login

Google's G Suite, which includes Gmail, Google Docs, Hangouts, Meet and other apps, quietly passed a major milestone at the end of last year: It now has more than 2 billion monthly active users, G Suite boss Javier Soltero told Axios Wednesday.

Why it matters: Long seen as the upstart challenger to Microsoft Office, Google's productivity suite is now one of the two incumbents, facing fresh rivals of its own.

> *"That's a staggering number. ... These products have incredible reach. Changing the way people work is something we are uniquely positioned to do."*
>
> *— Javier Soltero*

How does Google Drive increase security risks?

Google Drive, like many collaborative SaaS platforms, has several attributes that can increase security risks for organizations.

- **Always on.** Cloud environments like Google Drive are readily accessible at any time from anywhere and cannot be deactivated or otherwise reconfigured outside of account settings provided to users by the service provider.
- **High volume of users and activity.** Cloud environments, especially collaborative SaaS platforms like Google Drive, are a central point of access for most organizations that have multiple teams using these platforms to communicate and collaborate. The large footprint of these tools means that there's a large volume of users both inside and outside of your org, who are creating, modifying, and sharing documents on a daily basis.
- **Permissions vary across files and users.** Because these platforms involve collaboration across roles and teams, every user will need access and permissions managed according to their role. Google Drive specifically manages permissions at the file level, allowing the creator and editors of a file or folder to determine how to share it.
- **Troves of unstructured data.** Environments like Google Drive are intended for sharing word processing documents, images, videos, and other unstructured data which makes it difficult to parse for sensitive content.

What is data loss prevention (DLP)?

Data loss prevention is an access control that ensures confidential information is kept on a need-to-know basis. DLP scans for content within messages and files to determine whether an unauthorized disclosure of business-critical information has occurred and can provide automated remediation on the basis of your established data security policies. Additionally, DLP can provide alerts and analytics that help organizations understand risk and employee behavior over time.

Like other always-on, SaaS environments with high volumes of activity, Google Drive makes violations of data security policies more likely, leading to data leakage risks as well as data compliance violations.

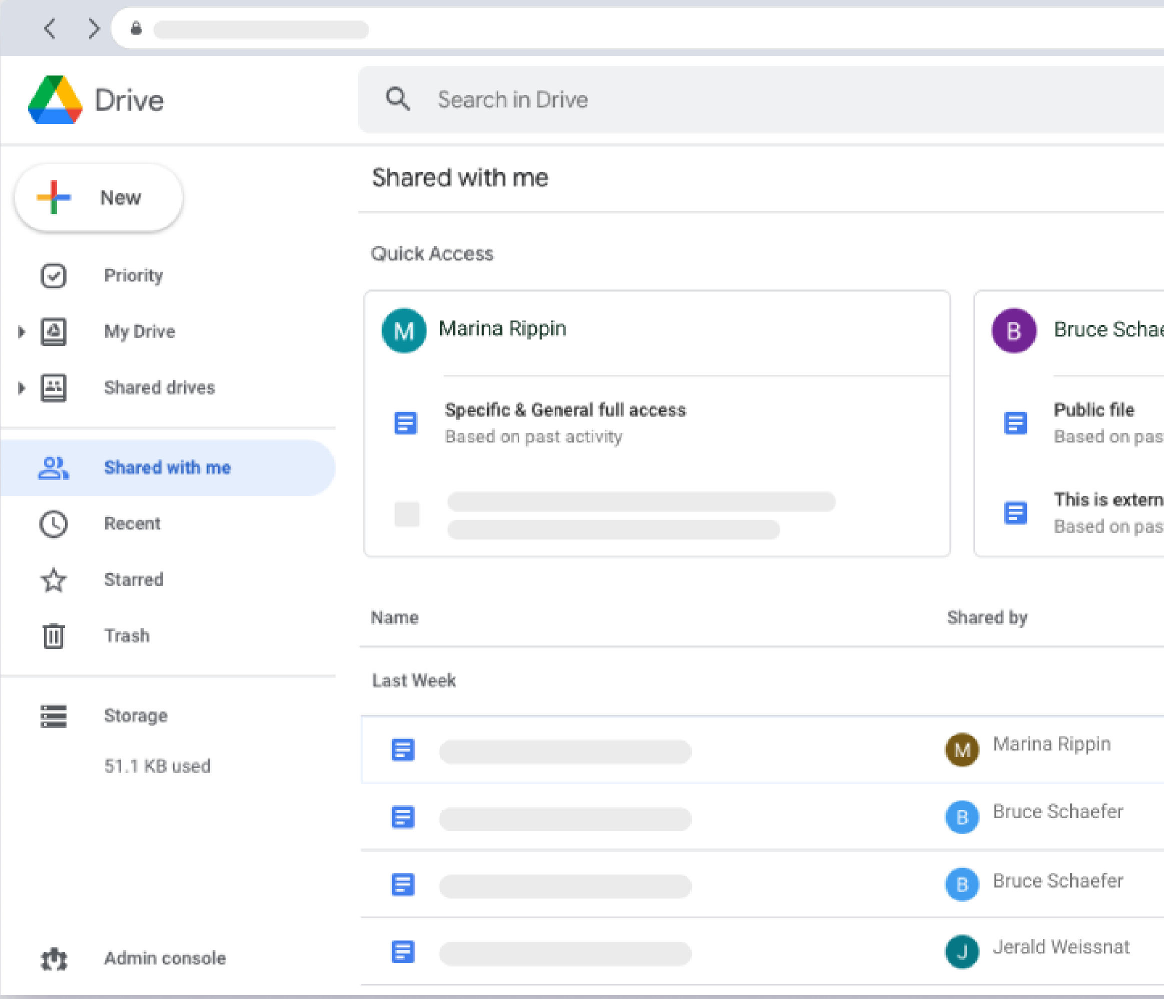
Organizations need to use tools like DLP in order to put into place controls that will help enforce data security best practices by preventing unauthorized parties from accessing documents and folders with sensitive information.

What risks does Google Drive introduce?

With entire organizations now working remotely, the adoption of SaaS and other cloud tools has increased significantly. Unlike traditional productivity and development tools, SaaS and IaaS platforms are always-on systems where any number of contributors share and store business data in environments not owned or managed by an organization's IT department. Without cloud data loss prevention this can easily create scenarios where data policy and security best practices are difficult to maintain or enforce without excessive time or resource commitment.

Key takeaway

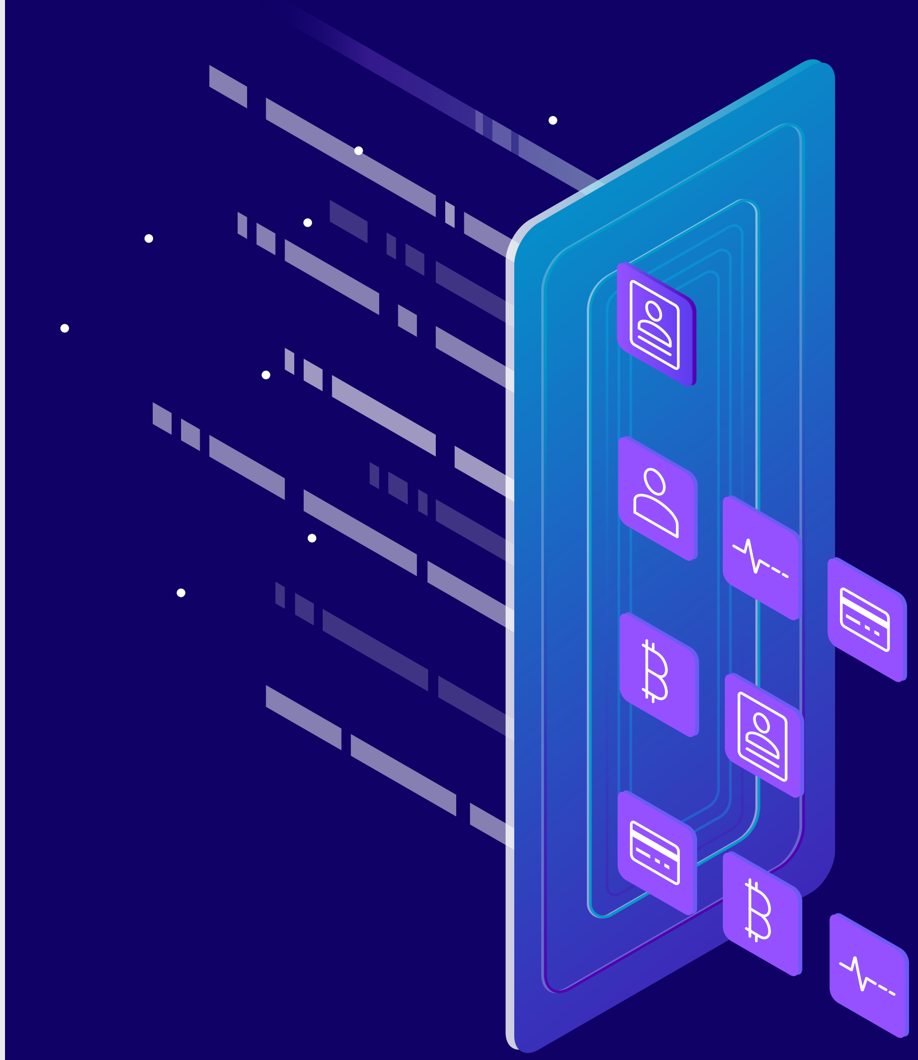
Environments like Google Drive increase the likelihood that unauthorized individuals can edit, view, download, copy, or otherwise gain access to files containing sensitive data through improper permissioning and poor management of accounts, files, and folders within an organization's Google Drive. Additionally, Google Drive provides limited visibility into when and where these incidents occur, making it difficult to enforce your organization's data security policies.



How does DLP work?

DLP helps organizations:

- Discover sensitive data within designated environments.
- Classify data on the basis of predefined token types, like PHI, PII, and other industry standard sensitive data types.
- Protect data with manual or automated redaction, quarantine, or deletion of offending content.



What does Nightfall detect?

Nightfall can detect the following token types within images via OCR and over 100+ file types, including Google proprietary files types:

Standard PII: Age, Credit Card Number, Email, Ethnic Group, Name, Location, Phone Number

Health: ICD, FDA, DEA, NPI, DOB

Finance: IBAN, SWIFT, CUSIP, Routing Numbers

Crypto: Bitcoin, Ethereum, Litecoin Addresses & Private Keys

Network: IP Address, Hardware ID, MAC Address

Custom: API Keys, your application UUIDs, and much more.

IDs: Driver's License Number, Taxpayer ID, Passport Number, Social Security Number, Vehicle ID

What is Nightfall DLP?

Nightfall is a platform to discover, classify and protect sensitve data across cloud SaaS & cloud infrastructure. Nightfall supports compliance efforts with a number of industry standards like PCI DSS, GDPR, HIPAA, CCPA, and much more. Additionally Google Drive is just one of the many platforms Nightfall secures.

Nightfall works by continuously monitoring data flowing in and out of data silos and classifying that data with machine learning. Data marked as sensitive can be automatically quariented, deleted, and redacted with workflows

Key Benefits

- Get started now for free - no setup or tuning required.
- Leverage 150+ pre-tuned, standard detectors of PII out of the box.
- Rich analytics to examine all your PII risk, both in real-time and historically.

Discover

Continuously monitor data that is flowing into and out of data silos.

Classify

Machine learning classifies sensitive data & PII automatically

Protect

Automated workflows for quarantine, deletion, redaction, alerts, and more.

Want to learn more about Nightfall?

To get started with Nightfall, request a demo or email us at **sales@nightfall.ai** with any questions.

Request a demo

About Nightfall

Nightfall is the industry's first cloud-native DLP platform that discovers, classifies, and protects data via machine learning. Nightfall is designed to work with popular SaaS applications like **Slack**, **Google Drive**, & **GitHub** as well as IaaS platforms like **AWS**.

Nightfall