

6 Steps to Protect
Google Drive with
Data Loss Protection



The average employee responsible for technology at their company is used to wearing lots of hats and stretching their muscles to take on tasks not included in the job description. Your adaptability is a strength, and likely the reason your team chose to bring you on board. When a task comes around like researching and implementing a new technology, system, or platform, it's not always an open and shut case.

Budget constraints and limited bandwidth are common issues across all teams. If you're used to working on a nimble team or as a team of one, vetting and implementing solutions on your own, requires a lot of steps. In your due diligence, you sit in on demos, you read the help center, and toward the end, you select a vendor of choice. But there's one more step.

You still have to get approval and budget from your stakeholders. And that task is rarely a solo act.

Whether you're a seasoned security professional or someone who's unfamiliar with the risks of data loss in Google Drive, your team is likely working on many competing priorities. Risks associated with not protecting sensitive data in cloud storage platforms like Google Drive should be on the list. Your job is to educate and provide solutions. This guide is written to help you illustrate the potential data protection gaps in a deployment of Google Drive to your team and stakeholders. By the end of this guide, you will be able to cover how to approach solving this data security gap in six steps.



Step 1:

Define your use case



It's important to have an overview of what's in your organization's cloud storage — not just content, but who's viewing and editing files as well as the overall permissions levels within your organization. Google Drive does not provide you with these insights on the platform. Start by understanding what content is stored and which users currently have access in your Google Drive.

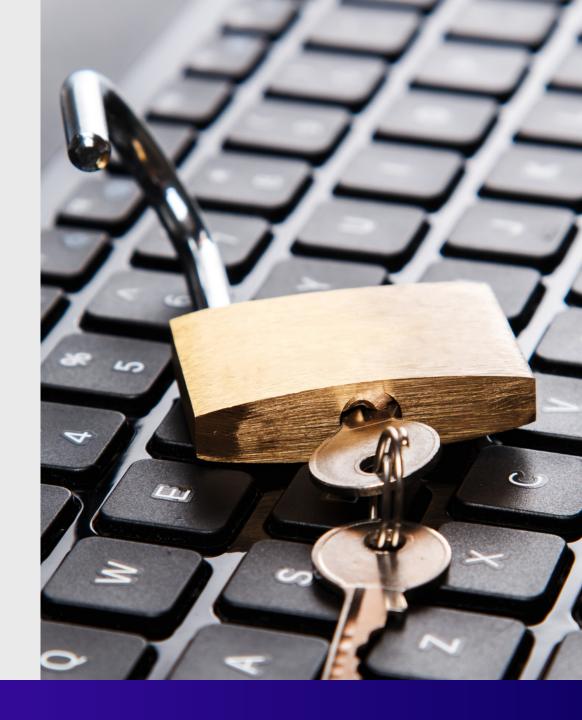
Here are the three most common data security risks companies want to solve for when it comes to cloud storage platforms:

- Share content with the right people. Keep files safe with the appropriate
 permissions settings for each file. Limit certain files to only specified team
 drives to prevent improper access, or allow read-only access to critical
 documents.
- Identify high risk behavior. Look for who is sharing documents inside or outside your organization. Understand who has permissions in your Google Drive, including who has editor and manager powers. You can configure custom policies based on your business needs when you know what's happening with your data.
- Audit your drives. When you see sensitive files set to public access, change
 permissions settings or notify users as soon as possible. Familiarize yourself
 with how permissions settings work in Google Drive, and pay close attention
 to how you're creating and sharing files the default settings may not always
 be the right fit for your desired level of data security.



Here's one way to help your stakeholders understand the value of adding internal policies for managing data security in Google Drive:

"We need to be more aware of how we're sharing content with the right people in our organization. We can have higher visibility into this through our permissions settings. We should be sure that we're setting the right levels of permission and allowing access and edit permissions for documents and files only for the users we want."



Step 2:

Prevent loss of trust



Adding a new process to your security policies can be a hard sell. Decision fatigue from researching solutions likely has your security team feeling fatigued. If you feel you're all out of appeals, play to the bottom line — an assessment of what a failure to protect data truly costs, in both financial and brand reputation terms, will help your team to take notice.

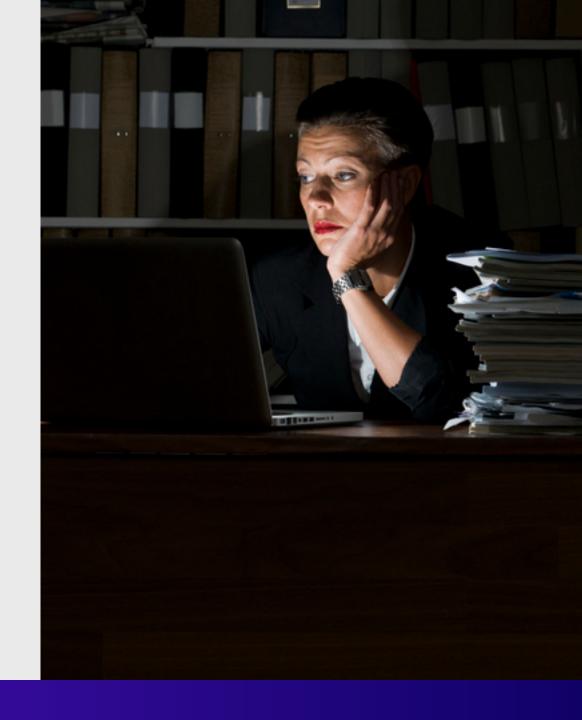
Here are a few stats that could help swing votes in favor of adding data loss protection to your cloud security tech stack:

- According to research from Ponemon Institute in its Cost of a Data Breach Report 2020, organizations spend an average of \$3.85 million recovering from security incidents — and businesses that had not deployed security automation saw an average total cost of \$6.03 million, more than double the average cost of a data breach of \$2.45 million for businesses that had fully deployed security automation.
- The Ponemon report also found that the mean time to identify and contain a breach is **280 days**.
- Tech Beacon reports that **43**% of **CISOs** and security operations managers cite maintaining brand reputation as a driver of primary security spend.



When appealing to your company on the value of protecting data in cloud storage platforms, make it clear what the organization stands to gain with stronger cloud security policies — and the risks they face without securing data and files:

"Securing data in Google Drive has minimal costs up front and costs little to maintain over time. A security event can cost millions in lost revenues and fines plus resources we'd have to allocate toward cleaning up after a data breach. We cannot afford to lose trust with our customers."



Step 3:

Align DLP with security objectives

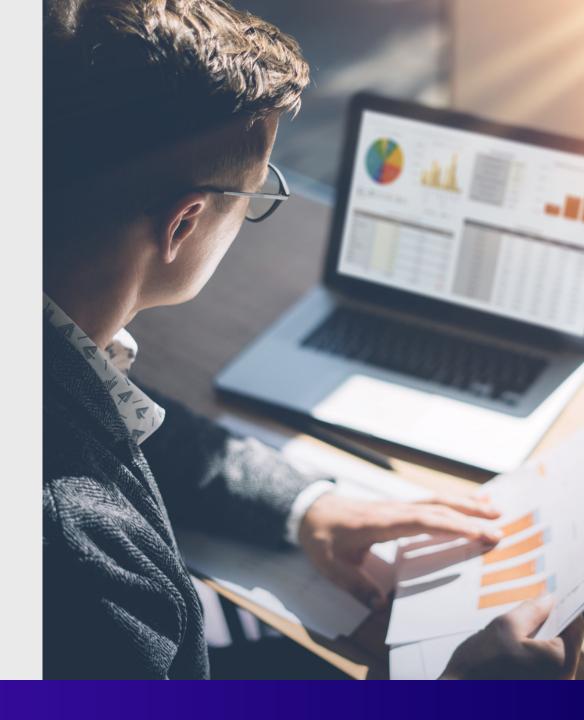


Protecting data specifically in Google Drive, might seem like a niche request, but as adoption of cloud applications and platforms rises, the exposure risk is very real. You can make your business case for stronger data security controls by aligning this request with key security objectives and show how protecting data on the application layer will uplevel the organization's overall security posture, in addition to existing network and endpoint solutions. Prove this by doing your research on which cloud security tools are currently in use and convey how a layered approach to data security can reduce the attack surface.

Read how companies are benefitting from upleveling their cloud data protection:

Improve communication with your customers. Nurture customer loyalty, improve quality of service, and ensure excellent user experience through stronger data security. NorthOne Business Banking uses their existing communication channels and tooling to deliver fast response times and resolutions in real time for their customers with security support from Nightfall.

"Using Nightfall creates the kind of first class customer care we strive for," says Blake Edwards, NorthOne VP of Engineering. "It allows us to reduce risk and keep our team talking to each other and sharing information. People don't have to be solely responsible for safety and security with Nightfall's automated scans. Our communications must be held to the highest bank-grade security standards."



Improve systems efficiency. Engineering teams can focus on creating enterprise applications and delivering other high-value projects to the organization when data is secure. The Calgary Public Library IT interfaces group found an increase in productivity and confluence in their security when they added Nightfall DLP. Historic and automated scans of your cloud systems keep everything running smoothly by detecting important data that could be at risk of leak or loss.

"DLP is a problem that has a very narrow margin of error," says Anton Chuppin, Manager of the IT Interfaces group at Calgary Public Library. "Nightfall solves the DLP problem very well. We are happy to have a tried and tested solution instead of coming up with one on our own."

Increase in sales. Faster and safer communications between teams allowed Springbuk to maintain operations without missing a beat during the COVID-19 pandemic. They rely on Nightfall DLP to secure sensitive protected health information (PHI). By protecting data moving around your company's cloud SaaS systems, your workforce can focus on finding solutions for customers without worrying about exposing sensitive data.

"Maintaining HIPAA compliance is of the utmost importance to Springbuk. Working with Nightfall gives our customers confidence that we take data protection very seriously," says Chris Morrison, Security Coordinator at Springbuk.



By defining your internal security goals, you have the blueprint to explain the benefits of protecting data. Try combining optimal security outcomes with specific OKRs from your teams, like this:

"Increased data protection supports our objectives by allowing us to honor our customer's trust. Improving security for how we store our customer's sensitive information will build trust us and build a long lasting relationship. Security matters a lot to our customers who rely on cloud systems."



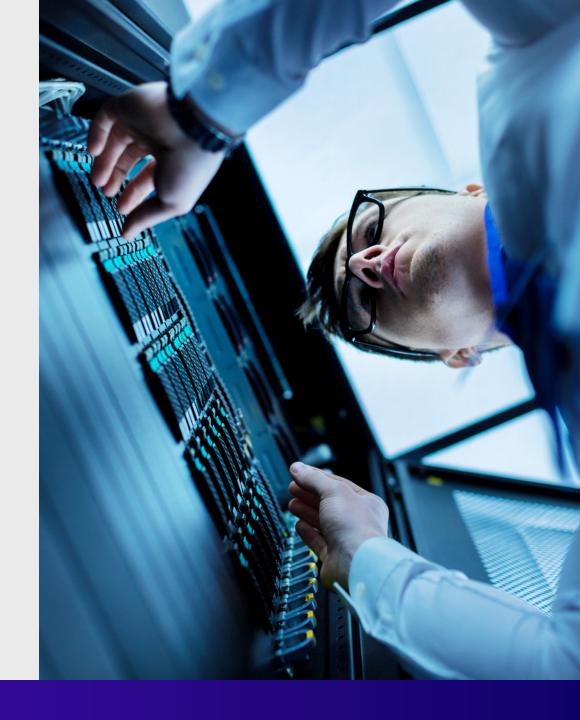
Step 4:

Compare security solutions



Having too many vendor choices could be one of the reasons why your organization may struggle to move quickly. Each option promises a lot — but how can you tell which one is the right fit for your cloud security needs? Get to know the data protection solutions that are out there, and learn how each may fall short for what you need:

- Cloud Access Security Broker (CASB) is a security platform that sits between
 an enterprise network and a cloud provider's infrastructure, allowing for the
 monitoring and blockage of suspicious activity that occur between the
 network layer and the cloud. CASBs also offer limited context with invasive
 installation and difficult deployment. A CASB alone cannot achieve the same
 level of depth in functionality, accuracy in detection, or granularity in
 remediation as a cloud-native DLP solution.
- Google Workspace offers a native DLP solution with limited features and basic alerting. Creating policies tends to be inflexible and scan results can be imprecise. It's difficult to set up granular DLP rules and remediation actions, because admins have few options to define parameters for what to scan and the lack context provided with scan results so not immediate surface where data is at risk of exposure. Google Cloud DLP is available for Enterprise users at an extra cost and is not available for Business tier users.

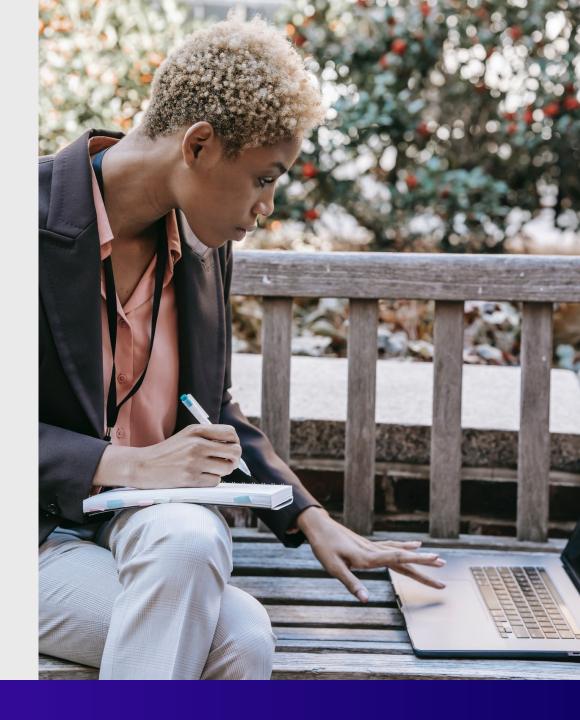


- Legacy DLP secures data on endpoints (devices like laptops, phones, servers) or networks. These options have blind spots due to reliance on regular expressions, outdated detection capabilities, or zero trust policies. These are more rigid ways to protect data that fail to adapt to changing threats and weaknesses within a system. As we've seen during the COVID-19 pandemic, modern security requires creative and flexible thinking. Legacy DLP solutions cannot not address the adoption of SaaS services consumed on multiple devices.
- **Doing nothing** is also an option, though not a good one. If you're reading this, you are looking to protect against a future incident. Perhaps you're being proactive about safeguarding your data and shoring up your SaaS systems. Leaving data completely unprotected should never be a solution.



Recommending data loss protection solutions to your company requires calming fears that adding a new option won't be a drag on existing infrastructure or divert resources (including time and employee bandwidth) during installation, tuning, and operation. Craft your recommendation by demonstrating how the solution benefits add up to a solid investment. Here's an example:

"Nightfall, with its ease of use and best in class machine learning-based detectors, is the best solution because we can protect our sensitive data in Google Drive without complex setup or additional tuning. Nightfall can do it all for DLP, with low false positive scores, custom detectors, and cloud deployment."



Step 5:

Tackle industry security challenges



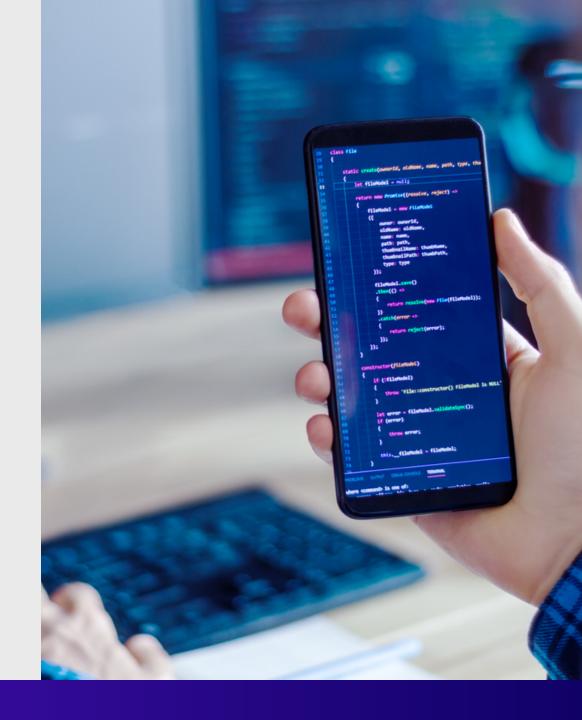
The coronavirus pandemic has amplified the greatest challenges we're facing in cybersecurity. For most industries, mass adoption of cloud infrastructure to support remote work, a lack of security oversight, and third-party risk cause headaches for technology leaders tasked with securing data and files in cloud collaboration tools. Fortunately, increased data security can support these challenges — the first step is to identify specific challenges you're currently facing:

Healthcare security leaders are facing stretched budgets and diverted priorities as their organizations have to place resources toward the immediate response to COVID-19. Even before the pandemic, healthcare tech departments were hindered with budget constraints In today's environment, every penny counts even more. Cloud collaboration tools that enable remote work are necessary and securing these investments with data protection solutions can be cost-effective both in the price and implementation.
 Safeguarding your data to avoid detrimental costs from data leaks is always a smart investment.



- In the financial technology sector, rapid cloud adoption has been widespread

 but hasn't always had the proper oversight and security considerations. As fintech teams ramp up on SaaS and other cloud systems, major data security concerns like compliance and regulation often come in second. The right data protection solution would allow these companies keep the same speed and breadth of adoption around their organization while providing data protection and keeping customers happy.
- One of the hardest hit sectors of the pandemic has been education.
 COVID-19 has forced educators and students to resume classes through distance learning, which has put the spotlight on existing problems of educational technology data security. Many educational tech security systems rely on outdated infrastructure and pass the responsibility to third-party vendors. Student data security is at higher risk as the pandemic stretches on into another school year. Education must continue despite a pandemic and schools must protect student data as we adopt new technology for distance learning.



When you have determined the need for additional data security and protection within Google Drive, approach your leadership team to address your organization's specific needs, unique circumstances, and the bottom line:

"I know our budgets are stretched to capacity because of the pandemic. Improving data security for our organization will help us protect patient, customer, or student data and keep costs down as we scale up our cloud infrastructure. Increased data protection can help address the blind spots in our security with third party risk, remote work, or outdated infrastructure systems."



Step 6:

Gather your advocates



Cybersecurity is a team sport. Even at smaller companies, If you're responsible for data security in your organization, you will have to work with stakeholders and other departments to introduce a new platform. This group can include folks from technology, security, compliance, operations, admins, and many others. To create a successful business case, leverage the data, intelligence, and expertise from your stakeholders.

Successful business relationships are built on making and nurturing connections. You can apply the same thinking to implementing business processes. To build a strong business case, start with the advocates you can trust to establish the new request. Outline how the improvements of increased data security in one core platform, like Google Drive, will benefit other integrated platforms processes:



- Ask your security information team how increased data security would connect to and enhance security information and event management (SIEM) processes and applications. Many security leaders will want to know that your proposed solution will pair well with the existing SIEM.
- Consider the various SaaS apps that connect to Google Drive, and how data could be exposed due to improper security configurations. An operations leader likely has faced that question when implementing or scaling up SaaS systems. Leverage their support to advocate your business case for buying a new solution.
- Talk to your platform or networking team responsible for building programs in the cloud to understand how tighter security policies for cloud storage can benefit laaS systems. It will be important for those teams to ensure secure processes for monitoring data and integrating with log systems.
- Gather data from anyone involved in SOAR security orchestration, automaton, and response. SOAR allows teams to automate certain types of incident response, so understanding the relationship between increased data security for Google Drive and these apps would support the need to minimize risks. SOAR often involves a tiger team assembled from security operations, technology teams, and others responsible for maintaining data security systems and processes.



When trying to rally various teams to select a security solution, the messaging will differ. As you sell your teams on a new solution or vendor, you must uncover solutions for each team and address their expectations. Here are two approaches you can take to contextualize this request with stakeholders and budget holders:

With stakeholders:

"Increasing data security for our organization's cloud storage platform will help our SOAR processes because we'll be able to automatically scan for sensitive data that could be at risk of exposure. What do you think we'll need to share with our VP to start prioritizing data loss protection among other initiatives?"

With budget holders:

"Increasing data security for our organization's cloud storage platform will help our SOAR processes because we'll be able to automatically scan for sensitive data that could be at risk of exposure. What do you think we'll need to share with our VP to start prioritizing data loss protection among other initiatives?"

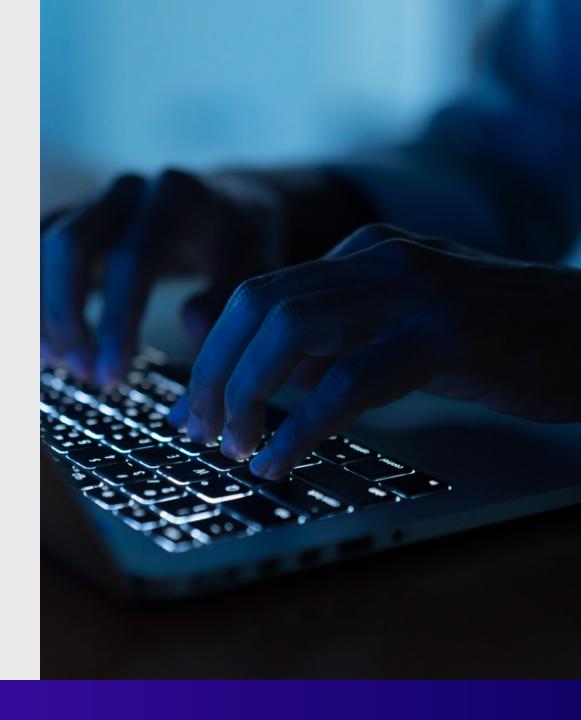


Show your organization why data security for Google Drive matters

We hope this quick guide has illustrated the need for additional data protection in Google Drive for your organization and helps you approach the potentially difficult task of introducing a new platform to your organization. You can use any of the six steps to create the winning pitch, or use all of them together.

For quick reference, here are the six steps summarized:

- Define your **data security use case** based on common Google Drive pain points.
- Prevent data exfiltration and **protect your business** from losing money and trust in data breach events.
- Align data protection with your organization's security objectives to show benefits.
- Compare Google Drive security solutions head to head to find the right one.
- Tackle your industry's **toughest security challenges** with data protection.
- **Gather your advocates** to make the case for increasing data security in Google Drive.



Nightfall for Google Drive allows you to create flexible policies to protect sensitive data for any Google Workspace plan. We discover, classify, and protect data with higher accuracy by leveraging deep learning to scan sensitive data in over 150+ file types like images, documents, and code.

Learn more about Nightfall DLP for Google Drive by scheduling a demo with us at sales@nightfall.ai.

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 <u>Slack</u>, <u>Google Drive</u>, & <u>GitHub</u> as well as laaS platforms like <u>AWS</u>.



