

# eDiscovery in the Cloud

Aligning your people,  
process, and technology



# Contents

---

Introduction	03
What makes cloud eDiscovery so complex?	05
People: Assembling your eDiscovery task force	07
Process: Vetting and implementing your cloud apps	09
Tech: Finding the right eDiscovery tool	11
The tip of the cloud data iceberg	14
About Onna eDiscovery	15

# 01. Introduction

---

In the past 25 years, cloud computing has gone from conceptual to ubiquitous. With a booming SaaS market, mobile devices as our constant appendages, and the recent work-from-home revolution, the cloud has taken over. And the epicenter of it all is the modern workplace.

With knowledge workers able to work anytime and anywhere, data volume has grown exponentially. In fact, it's estimated that the global datasphere will grow to [175 ZB by 2025](#), with more data being stored in enterprises than all of the world's existing endpoints. In other words, there's a data bubble waiting to burst, and enterprises are the main contributors.

On average, enterprise companies use about [175 apps](#) to get work done, each of those harboring a trove of siloed knowledge. Or, in the case of eDiscovery, pertinent ESI. Finding the information you need (let alone having the confidence that it exists) is no small feat. Dealing with tons of data sources and complex data types in the absence of one-size-fits-all governance capabilities has left legal and IT professionals with a messy maze of data to navigate — wasting both time and resources.



**The good news: You can overcome the challenges of cloud eDiscovery with the right approach.**

**In this eBook, we break down strategies to optimize your people, processes, and technology so you can feel confident about finding the data you need long before urgent matters arise.**

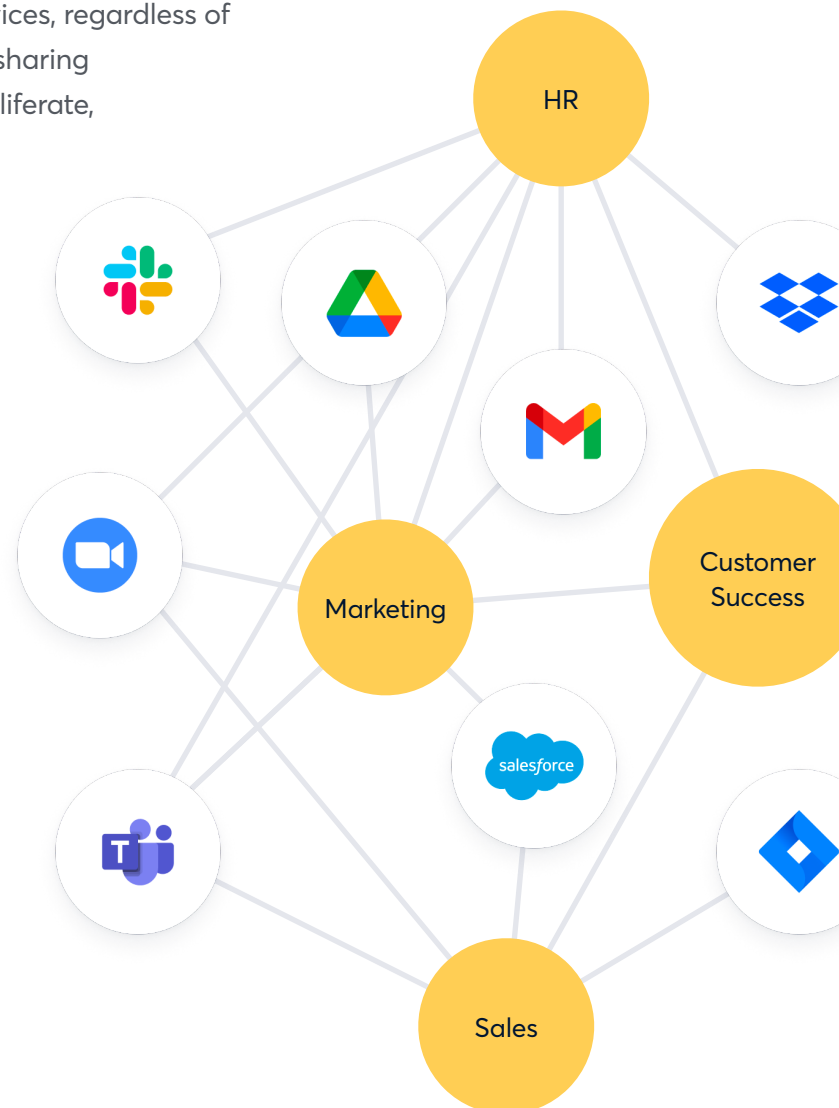
# 02. Cloud eDiscovery

## What makes it so complex?

From tracking analytics for marketing to handling communications for customer success, every department in an organization needs its own suite of tools. Often multifaceted in functionality, compatible with many devices, and easy-to-use, cloud-based tools are a no-brainer for teams that want to boost their efficiency.

**However, the same features that make cloud apps so great to use** are also what make managing the data they produce so challenging. Self-service implementation makes cloud apps easy for just about anyone to install (even without IT's knowledge). "Anytime, anywhere" usability enables users to access apps on many devices, regardless of whether or not they're authorized. File-editing and sharing capabilities make it easier than ever for data to proliferate, transform, and disappear, posing risk for data loss.

Not to mention, what these tools even do isn't always familiar to the legal and IT professionals who are tasked with collecting from them. The kind of data they produce and their retention settings often aren't known until they need to be. When someone does finally take a look under the hood following a discovery request and finds issues, it's often too late.



This is why many legal and IT professionals see cloud apps as a double-edged sword: The tools people need to do their best work vs. the struggle to keep tabs on a plethora of data sources.

This doesn't have to be the case, but it takes a strong organization of people to get there.

# 03. People

## Assembling your eDiscovery task force

---

Although they operate on the front lines, legal and IT aren't the only departments involved in eDiscovery. The foundation of eDiscovery, nay the entire left side of the EDRM, really comes down to one thing — being able to find and access the information you need quickly and accurately. In other words, leveraging a strong information governance (IG) program. However, building that foundation takes contributions from more than just these two departments.

Whether you're in legal, IT, compliance, security, or another IG-adjacent role, you might be familiar with the question, "What data do we have and where does it live?"

Yet, rather than working together to find the answers, IG stakeholders tend to stay in their own lane. In fact, 71.6% of participating organizations [in a recent survey from the Association of Corporate Counsel \(ACC\) and Pagefreezer](#) claim to have IG programs that are in an "early" or "intermediate" stage of development; yet, over 50% of those legal departments cannot confidently produce data without relying on IT. This demonstrates a clear need to set more collaborative relationships from the get go.

# 03. People

## Assembling your eDiscovery task force

There are many reasons IG stakeholders find it easier to work independently, including conflicting priorities and separate budgets. However, because each department harbors a swath of unstructured data, it's imperative that IG stakeholders work closely to connect the dots.

If you're lacking this alignment in your organization, forming an alliance early on with other IG stakeholders can pay off tenfold when it comes to cloud eDiscovery.

### An easy way to start assembling the right teams by assessing who:

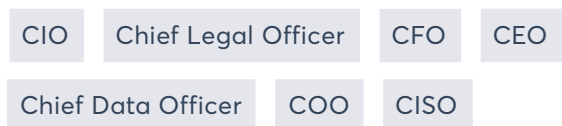
- Helps onboard new technologies
- Leads data security efforts
- Leads data privacy efforts
- Manages data handling & retention policies
- Handles regulatory and audit obligations

### Advocates for a strong IG program:

#### DEPARTMENTS ▼



#### LEADERS ▼



Depending on your company's size, industry, and maturity, you may find that these responsibilities are specialized, overlap, or don't yet exist. The important thing is to take inventory, make the necessary connections to map data, and establish procedures that balance risk and value. The sooner you do so, the smoother and more standardized your eDiscovery process will become.



# 04. Process

## Vetting & implementing your cloud apps

Equally as important as your eDiscovery task force is your process for vetting and implementing cloud apps. Insofar as possible, IG stakeholders should be looped in before employees onboard new tools. We recommend regular syncs with the IT team as a good place to start. And, in the same way IT teams conduct security questionnaires for apps before onboarding, you should consider implementing an eDiscovery questionnaire.

### Use this eDiscovery questionnaire

to cover the basics, but be sure to tailor this to your own unique needs.

01. What advanced search capabilities does the tool have, if any?

02. What retention settings are available and how can they be customized?

03. Can I set legal holds on specific users' data?

☐

Yes

☐

No

If not, what are the data export capabilities? Will any of them compromise or transform the data's integrity?

04. Does the tool offer any API connection exports?

☐

Yes

☐

No

05. Do you work with any trusted eDiscovery partners?

06. Are there any other limitations I should be aware of?

# 04. Process

## Vetting & implementing your cloud apps

---

Bear in mind that some cloud apps' eDiscovery and governance capabilities will be better than others. You should consult with your legal team and greater eDiscovery task force on your standards and weigh the results of your eDiscovery questionnaire against them. More times than not, a vendor will work with you to fill non-negotiable gaps. Whether that means making product enhancements or referring you to a trusted eDiscovery partner, don't be shy about vocalizing your needs.

**Once you've gone through the vetting process and have implemented the app, be sure to record:**

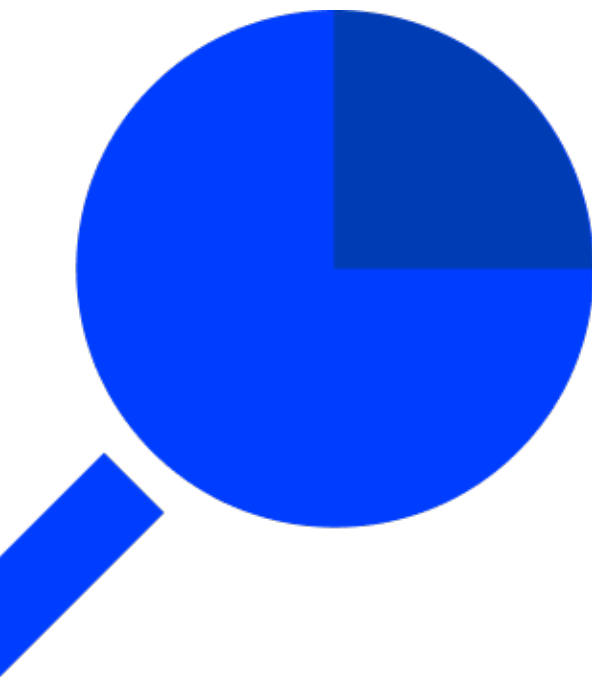
01. What it's used for
02. Any retention policies that apply to its data or usage
03. Any critical questionnaire findings
04. Your plan of action for eDiscovery

This way, when an urgent matter arises, you'll already know how to get a hold of the tool's data. And if you've already missed the chance to vet some of your apps, fear not — it's never too late to go back and do the work. Leverage your eDiscovery task force and vendor support to get the information you need.

# 05. Tech

## Finding the right eDiscovery tool

Although more cloud apps have started to bake eDiscovery and governance features into their DNA, there is still a long way to go. If you're looking for a surefire way to get the job done long-term, you'll find that in many cases, a dedicated eDiscovery tool is your best option. But how can you be certain you're choosing the right one?



There's no straight and easy answer, so a good place to start is by assessing your needs.

- + How large is my organization?
- + How regulated is my industry?
- + How frequently do we encounter litigation?
- + What budget are we working with?
- + How many IG stakeholders can benefit from this tool?
- + How many cloud apps are we looking to collect, preserve & search across?
- + What are these cloud apps' native capabilities and limitations? How can a new tool help solve for them?

By doing so, you can start to get a sense of what kind of tool you need, with which apps it needs to be compatible, and what capabilities you need to fill in gaps. We also recommend thinking about the big picture to make your investment worthwhile. For example, your priority right now might be to find something cheap and easy for Slack. Down the line, however, you may wish you'd considered a tool that can also make light work of Google Workspace, Zoom, Microsoft Teams, and the dozens of other apps you may use. From this lens, leveraging your eDiscovery questionnaire to make sure you know the ins and outs of each cloud app is that much more important.

Beyond app-specific features, your eDiscovery solution should be able to tick off some other crucial boxes as well.

Here are our recommendations for what to look for in a cloud-first eDiscovery tool that will help you increase efficiency and cut back on spending in the long run.

# 05. Tech

## Finding the right eDiscovery tool

- ✓ **Flexible and fast deployment:** Whether it be in the cloud or on-premise, your eDiscovery solution should be compatible with your chosen environment and be able to auto-scale over time.
- ✓ **Progressive cloud compatibility:** Your solution should integrate seamlessly with cloud-based sources that are traditionally harder to process.
- ✓ **Top-tier security:** When it comes to your provider's security structure, be sure to do your homework. It's a good idea to see which security certifications they have, such as the EU-US privacy shield, ISO 27001, and Soc 2 Type II, or other regulations specific to your industry.
- ✓ **Defensible collections:** You should be able to collect as much or as little as you need with your eDiscovery tool. Look for the ability to collect all metadata from the original source, extract all embedded items & .zip files, and preserve files in their native format.
- ✓ **Advanced search capabilities:** The ability to run targeted searches & get fast, accurate results with advanced data capture & processing is a must. OCR and audio transcription is a plus!
- ✓ **Real-time access:** Be sure to ask how often data is refreshed in your eDiscovery tool — it's great if they're able to sync data sources continuously so you always have access to the latest information.
- ✓ **Preservation:** The ability to apply preservation for legal holds across multiple users and apps, all in one platform, is key.
- ✓ **Collaboration & sharing:** Find a tool that makes working with internal stakeholders, outside counsel, and service providers a breeze by only sharing what's relevant and maintaining privacy.
- ✓ **Audit Logs:** Your tool should allow you to maintain and see a comprehensive log of all your data collections and user actions.
- ✓ **Export to review:** Last but certainly not least, you should be able to view clean, comprehensive data exports in your chosen review platform.

# 06. The cloud data iceberg

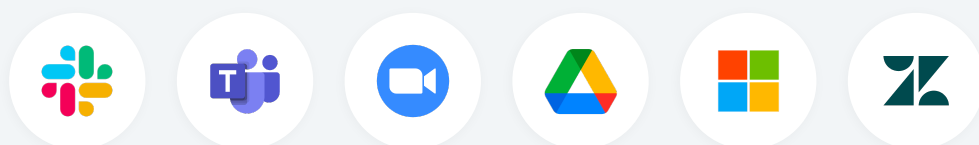
---

The truth is that eDiscovery challenges are only a small symptom of a massive data fragmentation problem. IG stakeholders struggle to find what they need, with most [losing 50% of their time every week](#) (30% searching for, governing, and preparing data, plus 20% duplicating work). As apps continue to proliferate, new data types emerge, and information gets even more siloed, the issue will only compound.

While it's easy to get tunnel vision worrying about one-off data collections and investigations, we urge you to look at the bigger picture and get to the root of the problem. How is your organization thinking about information governance? How are your people, processes, and tech stacking up? Where can you do a better job of maximizing the value of your data and minimizing its risk?

**Although eDiscovery is typically thought of as a niche legal function,** if done right, it can be the impetus for positive change in compliance, security, knowledge management, and more. After all, you can't preserve, secure, or leverage any information if you can't first find it — and whether you're an eDiscovery professional or a knowledge worker, you should be empowered to do so.





## Connect everything, do anything.

When faced with litigation, internal investigations, audits and more, it can be difficult to produce data quickly when it's scattered and siloed across your cloud apps.

Onna eDiscovery helps you effectively collect, search, and access data from all your cloud apps in one place to speed up early case assessment and drive down review costs. Ensure your preserved data is always up to date with automatic syncing and indexing, and minimize risk by controlling data sharing with service providers and outside counsel.

**Sound like the solution you're looking for?**

[See it in action ↗](#)



© 2021 Onna Technologies Inc. ("the author").

The author disclaims all warranties as to the completeness, adequacy, or accuracy of such information and shall have no liability for errors, omissions, or inadequacies herein. The opinions expressed herein are subject to change without notice. Although the author may include a discussion of legal issues, the author does not provide legal advice or services, and its research should not be used or construed as such.