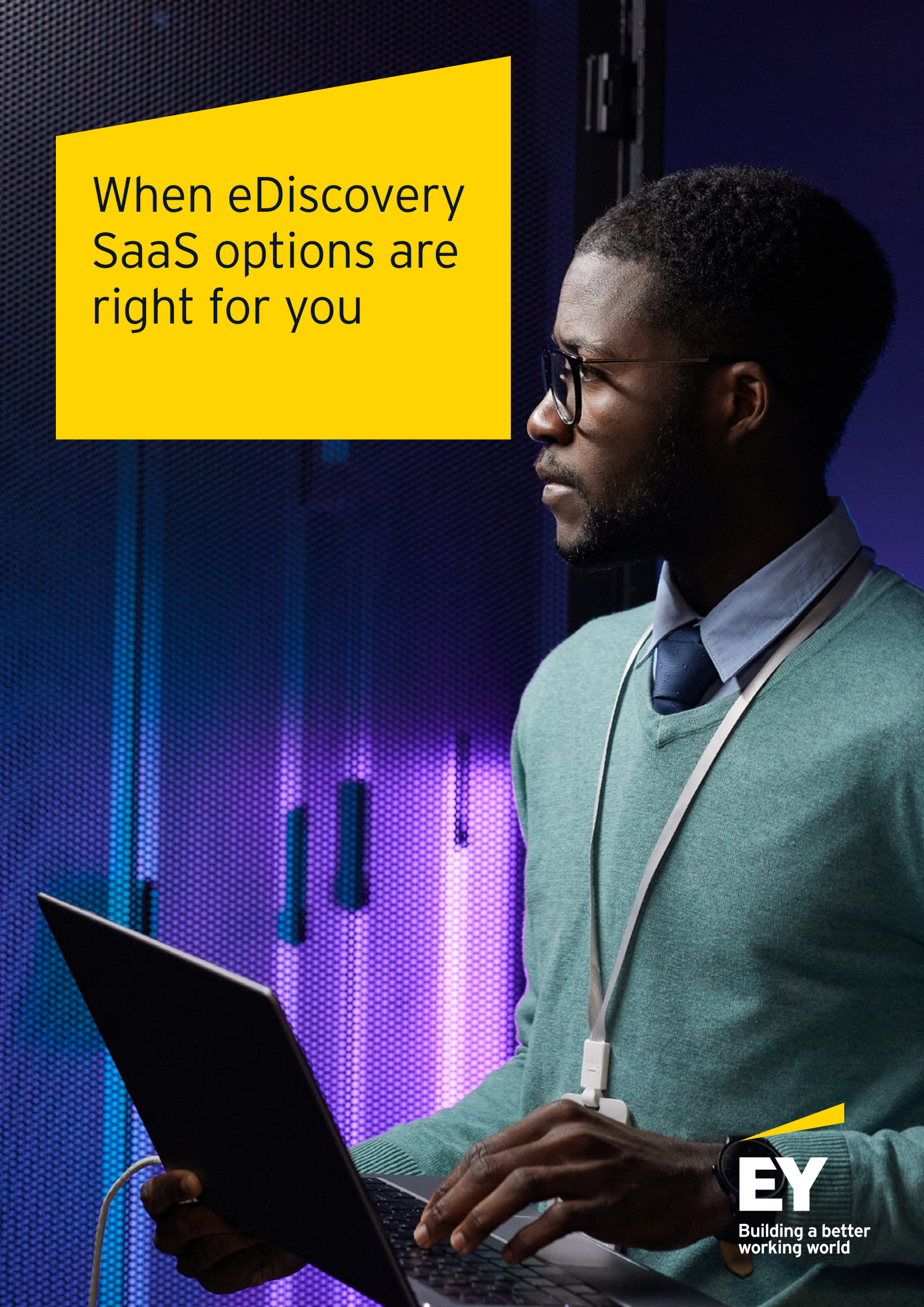
When eDiscovery SaaS options are right for you



Building a better working world

Determining the optimum approach to eDiscovery requires careful evaluation of security, software and socialization issues.

In brief

- While many legal practitioners are turning to Software as a Service (SaaS) for eDiscovery, these options may not meet the specific needs of every organization or every matter. A thorough evaluation of organizational requirements and provider offerings is vital to determining whether eDiscovery SaaS options might offer better value and outcomes than traditional models.
- eDiscovery SaaS solutions have the potential to simplify the eDiscovery process for matters with standard data sources and straightforward review and production requirements.
- Potential "dealbreakers" to using SaaS effectively for eDiscovery include obstacles regarding security measures, software capabilities and socializing changes in an organization.

First, how does eDiscovery SaaS differ from other eDiscovery solutions? Although many eDiscovery practitioners are drawn to SaaS solutions for the potential benefits provided by their hardware setups, it is important to remember that these are software solutions. Traditional eDiscovery service delivery models typically deploy a combination of multiple integrated technologies to provide leading-class software throughout the eDiscovery process; whereas, eDiscovery SaaS providers offer an end-to-end solution within a single software.

eDiscovery SaaS options are not one-size-fits-all solutions for eDiscovery programs, and practitioners should closely analyze their needs to determine when a particular solution works best. A hybrid approach that uses a SaaS solution for routine legal matters and traditional eDiscovery deployment for more complex legal issues may be the most effective answer for many organizations.

The rapidly growing volume and complexity of data has made eDiscovery more expensive than ever, fueling demand for more cost-effective solutions. SaaS can provide predictable, transparent pricing on a subscription or pay-as-you-go model, eliminating expenses such as infrastructure maintenance and software licensing. But eDiscovery SaaS costs are highly variable based on the provider and are not always cheaper than traditional services.

Just as important as the software costs is identifying which solutions are likely to offer the most value and deliver successful outcomes based on specific needs and use cases. Many of our clients report three major "dealbreakers" that have kept them from moving forward with eDiscovery SaaS offerings: security, software and socialization. This article details these considerations and offers questions for assessing whether moving to an eDiscovery SaaS solution is right for your organization.

Security: Can an eDiscovery SaaS provider meet your organization's unique data security requirements?

Although most cloud-based technology providers invest heavily in data security, complying with data privacy and governance requirements for some matters may prove challenging. There may also be risks from data comingling between providers' clients, which could create a requirement for a private client environment, an option that is not always available in the cloud. While data segregation is not always required, clients looking for separate encryption keys, policies and storage locations may be disappointed. More than a third of legal professionals surveyed cited data security and privacy challenges as the biggest disadvantage to a cloud-based system.[1]

For example, consider regulatory limitations on data transfers and storage. The rapid growth in data privacy regulations around the world, such as the EU's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law may require that data be stored in environments whose physical servers are located within a specific geography. Some countries also require special handling for government-related data, as demonstrated by the Federal Risk and Authorization Management Program (FedRAMP) in the US. The European Banking Association requires a flow-down of audit rights, which isn't offered in many cloud environments. Regulatory compliance can come at a premium price and is not possible with every eDiscovery SaaS provider.

Another important consideration is whether anonymized, aggregated client data could become the intellectual property of your provider. This raises the risk of data loss and could violate privacy statutes. Standard SaaS agreements often limit vendor liability for privacy and security breaches, while on-premises service providers are more likely to offer uncapped liability.

When evaluating cloud-based eDiscovery, it is imperative to consider your organization's typical data security profile as well as how the provider can meet any customized requirements that arise. Identifying how an eDiscovery SaaS solution will fit into your existing IT security, support and data governance model is a critical first step in exploring alternatives to traditional delivery models. Highly regulated organizations may have the most difficulty identifying an eDiscovery SaaS provider that can meet their unique data security requirements.

[1] 2021 Ediscovery Cloud Adoption Report, 2021, everlaw.com, https://www.everlaw.com/white-papers/2021-ediscovery-cloud-adoption-report/.

Software: Do your legal matters require customized or integrated software?

While the regularly recognized benefits of eDiscovery SaaS solutions are related to their hardware setups, it is important to remember that software is the main product of SaaS providers, and some end-to-end eDiscovery software may be unable to effectively satisfy customized requirements. Many legal departments and service providers have traditionally leveraged a variety of eDiscovery software solutions across the electronic discovery reference model (EDRM) and could find it challenging to sacrifice some of their current functionality. For example, a workflow with automation functions built to match playbooks and optimize processes will lose all value without integration to the new platform.

When you run a matter through an eDiscovery SaaS solution, you are frequently limited to the technology in that platform, which may lack some functionality that would greatly benefit your work. For example, legal matters that involve a complex variety of data sources, such as forensic laptop images, mobile data or non-standard electronically stored information (ESI), may require additional third-party forensic technology tools to acquire, process and produce data in the formats needed. In some cases, it may even be necessary to leverage multiple providers to collect and analyze data.

It is crucial to identify when these additional tools and methods may be required, as well as the level of integration and access supported by various eDiscovery SaaS platforms.

Performance and scalability may also be concerns, requiring a proof of concept that tests requirements. Consider whether data can be extracted from the cloud back to an on-premises environment or another provider to avoid becoming locked-in to an inadequate service. The inability to manage data backups could also be an issue.

As you evaluate the use of eDiscovery SaaS, it is necessary to consider how capabilities will impact your outcomes. If the SaaS solution has connectors that enable you to collect data directly from your organization's primary data sources and the capability to effectively support your preferred review workflow for this data, then it could help to simplify and streamline your eDiscovery process. Matters with standard data sources and straightforward review and production requirements are ideal candidates for eDiscovery SaaS solutions.

Socialization: What actions are needed to make a successful change to an eDiscovery SaaS?

When assessing potential eDiscovery SaaS options, catalog in detail your must-have capabilities and analyze how those needs can be met and supported by a new platform. eDiscovery SaaS providers typically offer varying service tiers, with self-service solutions being the most common. For simple matters requiring less robust support, this may be acceptable or even preferable. For more complex portfolios, though, consider how eDiscovery will be managed and supported going forward. Even leading-class technology requires the right people and processes for a successful deployment.

Additionally, the transition to utilizing an eDiscovery SaaS platform could require significant time and experienced oversight depending on the complexity of an organization's data footprint and process requirements. For example, current policies, processes and reports will need to be adapted for compatibility with a new platform. Another critical factor to consider is the extent to which legacy eDiscovery data will be either migrated or maintained in an existing environment.

A strong change management plan, including consideration and training for all stakeholders, is also vital to success. All eDiscovery software options should be evaluated from the perspective of legal users as opposed to just the IT department. For example, if in-house or outside counsel do not like the review interface for your selected software, they may resist adopting it and attempt workarounds. Involving these stakeholders in the evaluation process can lead to better experiences and the creation of long-term value for your organization through your eDiscovery program.

Summary

While eDiscovery SaaS solutions may be effective for simple, routine matters, more complex legal work is still likely to benefit from traditional eDiscovery service models. A thorough evaluation is essential and may show that a hybrid approach will deliver optimum outcomes.

Appendix: Questions for evaluating eDiscovery options

When evaluating eDiscovery SaaS options, it is important to ask the right questions to find the best fit for your organization. The explosion of novel, non-standard data makes it essential to select a vendor that can recognize new formats and quickly adapt its practices for collecting, processing and reviewing data.

Below are some sample questions and focus areas to consider when evaluating providers.

Requirement considerations

1. What are the overall drivers for considering an eDiscovery SaaS solution (e.g., lower costs, infrastructure footprint and workflow centralization)?
2. What use cases within your organization align best with eDiscovery SaaS solutions and what is the percentage within your overall eDiscovery program? How does this affect return on investment (ROI) analysis?
3. What are the data security and privacy requirements for your organization?
4. What integrations of custom processes or tools would be critical to meet your eDiscovery needs?
5. Do you have active and involved sponsorship from business leaders for changing the organization's eDiscovery solution?
6. What level of legacy eDiscovery infrastructure will need to be retained? How does this affect ROI analysis?
7. Do you have the experienced resources needed to evaluate and implement eDiscovery SaaS options?

Questions for eDiscovery SaaS providers

Security

1. How is access to data controlled and monitored in your environment?
2. What options do you offer to comply with data privacy and other data governance regulations?
3. Where are your servers physically located?

Software

1. Which phases of the EDRM can be addressed by your solution and which may require additional tools?
2. What file formats are supported for data ingestion and what is your approach for non-standard ESI and other unsupported file formats?
3. How can you integrate your customized processes and technology into your platform?

Socialization

1. What levels of customer service do you provide throughout the eDiscovery process?
2. What support do you offer for transitioning eDiscovery data from other providers into your platform?
3. How do you assist with change management and user training?

Key contract considerations

1. How does the Service Level Agreement (SLA) address resolution and recovery times, acceptable downtime and performance guarantees?
2. Is there a cap for liabilities arising from privacy and security breaches?
3. Who will own anonymized, aggregated client data?

For more information please contact

Todd Marlin
EY Global Forensic & Integrity Services Technology & Innovation Leader
Ernst & Young LLP
todd.marlin@ey.com

Laura Gallichio
Managing Director,
Forensic & Integrity Services,
Ernst & Young LLP
laura.gallichio@ey.com

Michael Pippin
Manager,
Forensic & Integrity Services,
Ernst & Young LLP
michael.pippin@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 010845-22Gbl.
BSC no. 2210-4105616
ED None

ey.com