

Market Guide for E-Discovery Solutions

Published: 27 June 2019 **ID:** G00388272

Analyst(s): Julian Tirsu, Michael Hoeck

E-discovery solutions facilitate digital discovery and provide administration of legal matters. Controlling risk and cost remain the primary business drivers for seeking comprehensive and more effective e-discovery solutions. I&O leaders can use this guide to help choose a solution for their needs.

Key Findings

- End-to-end e-discovery solutions are gaining momentum in the market with their ease of use, and more competitive and straightforward pricing structures.
- The native e-discovery capabilities offered by Microsoft through its Office 365 Security & Compliance Center continue to attract interest as the functionality continues to improve.
- As the scope of data sources for e-discovery broadens, requirements to search and preserve data across both on-premises and cloud repositories become more difficult, which can lead to overinvestment in technology and processes.
- The e-discovery service market continues to experience consolidation through mergers and acquisitions, though little differentiation is offered across services provided.

Recommendations

To maintain and optimize existing data center infrastructure, I&O leaders should:

- Select e-discovery solutions strategically, by establishing the maturity of in-house e-discovery processes and teams, since end-to-end solutions may not be suitable for all organizations.
- Engage all stakeholders when selecting an e-discovery solution by reviewing privacy and regulatory requirements in order to identify technology capability gaps in your process and needs.
- Leverage enterprise technologies and data connectors to search across all data sources by combining areas like collection, legal hold and similar infrastructure components from more end-user functions. Assess features like analytics, early case assessment and document review by weighting requirements accordingly.

- Use service providers when required, as they are often best-positioned to handle complex high-stakes cases, by working closely with the internal IT and legal teams during all matters.

Strategic Planning Assumption

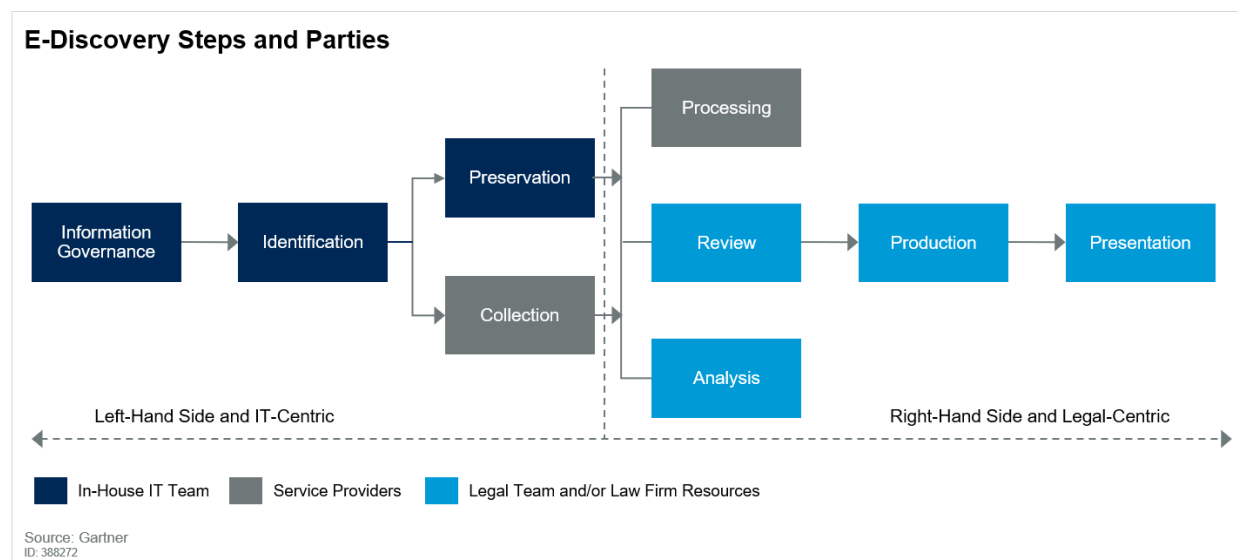
By 2023, more than 70% of enterprise IT leaders will upgrade to end-to-end e-discovery software to reduce time and legal spend, up from 10% in 2019.

Market Definition

E-discovery solutions automate and facilitate the electronic discovery (e-discovery) process, which includes the identification, preservation, collection, processing, review, analysis and production of digital data in support of the common law discovery process in litigation or other investigative proceedings.

To gain a basic understanding of the typical e-discovery process, apply the Electronic Discovery Reference Model (EDRM) — an established and accepted framework by e-discovery practitioners (see Figure 1). Commonly, the “left-hand side” of EDRM is used to refer to the steps containing information governance, identification, preservation and collection, and the “right-hand side” to processing, review, analysis, production and presentation.

Figure 1. E-Discovery Steps and Parties



This division of the two sides primarily reflects the different focuses of processes and engaged teams. The IT team usually leads tasks on the left-hand side, while legal teams (litigation support, compliance, legal department, general counsel’s [GC’s] office) are responsible for the right-hand side tasks. Accordingly, the technology solutions supporting the left-hand side are often familiar to

the IT team, and the legal teams are the typical consumers of the right-hand side systems. For litigation matters, it is common to engage service providers and law firms for some of the work as well. In Figure 1, the color-coded boxes represent typical parties engaged in e-discovery matters. Successful e-discovery projects demonstrate efficiency across all teams that can work in a collaborative and coordinated manner.

Market Description

E-discovery is typically project-based or ad hoc (as opposed to operationalized processes and tasks) and results from a trigger event. These trigger events include:

- Lawsuit or audit (initiated by another party or oneself)
- Internal investigation (i.e., employee-filed complaint or other types of HR-related issues)
- Due diligence process (such as for potential merger and acquisition transactions)
- Investigations (launched by regulators such as Securities and Exchange Commission [SEC], Department of Justice [DOJ], Financial Industry Regulatory Authority [FINRA] or state agencies)
- Freedom of Information Act (FOIA) and General Data Protection Regulation (GDPR) requests
- Post-data-breach assessment (after a cybersecurity event, assessing liabilities or anticipating lawsuits)

Depending on the nature of triggering events, e-discovery projects may not need to go through the entire EDRM process, nor does every project have to follow the steps in the linear manner depicted in Figure 1.

Technology

Various technologies are available to automate and support e-discovery processes. Many only target certain steps of the EDRM. The following six capabilities can be used to evaluate the range and strength of various e-discovery technology solutions:

- **Predictive Coding (or Technology-Assisted Review [TAR]) and Early Case Assessment (ECA):** Predictive coding, or TAR, is a machine learning process that uses software to reduce the number of nonresponsive or irrelevant documents that must be reviewed manually. ECA is the process of gathering potential evidence early on in a legal matter, and is based on data analytics, often with advanced data visualization design. Both TAR and ECA are typically used to help gain insight into data sources and to facilitate culling the data being collected, preserved, processed and reviewed.
- **Forensic Data Collection:** This is the process of gathering electronically stored information (ESI) that could be potentially relevant to an e-discovery matter, regardless of where the data resides. This capability ranges from being able to collect from various data sources (email, document, application, website content, voice, video, etc.) to various data hosts and storage media (server, hard drive, cloud, mobile device, backup tape, etc.). During the data collection process, data integrity must be protected. Collected data could be placed in a virtual repository,

tagged in place (data stays in the original repository) or copied to a separate repository. This process needs to be extremely accurate, especially when involving device collection, which can be intrusive, time-consuming and costly.

- **Legal Hold Management:** This is a process used to preserve all forms of potentially relevant information after receiving an information record request issued by a government entity or anticipating an audit, investigation or litigation.

Legal hold could be achieved in two ways: in place (content tagged and held in its original repository) or collected (content collected and copied/encrypted into a virtual container before loading into a processing/review system). Either way, integrity of the held content is protected, and the chain of custody is tracked through system auto-audit logs. As an adjunct to the hold process, legal hold has evolved to a complete business process that can include questionnaires, workflow and personnel tracking.

- **Processing:** Several activities are involved in processing, including importing ESI from forensics, and converting, reducing, and ingesting data for legal review. This is typically handled through deduplication and renders all the various data formats to be viewable natively or as required by review platforms.
- **Review:** The review technology is aimed to specifically support legal practitioners and typically evaluates ESI for relevance and privilege in terms of context. Potentially relevant digital data is exposed through a set of workflows that enable legal professionals to tag the data for relevancy to the case in hand. The outcome is a production dataset with proper redaction for court or the original entity that requested them.

Services

E-discovery services typically include the following:

- Consulting (expertise in legal and technology capacities)
- Managed review (hosting technologies and providing legal review resources)
- Project management (litigation support and project coordination)

E-discovery projects can be costly, complex, unpredictable and non-negotiable. The number of e-discovery cases an organization has to deal with varies widely, depending on its business sector, size and regulatory landscape. It is difficult for an organization to establish a repeatable process and gain efficiency if the number of cases is small and they are random. Investing in a complete set of in-house capabilities may not be cost-effective. Leveraging service providers for some or all of the cases can be strategic and sometimes the most viable solution.

Even for large organizations with a high volume of e-discovery projects, combining in-house and service offerings can enable cost and risk control. In general, service providers are engaged to support the right-hand side tasks (processing and review). Increasingly, large organizations take a hybrid approach. For example, having the same review technology in-house as well as retained service providers allows the organization to move a case to the service provider without dealing with

technology platform issues. The common practice has been to take care of average cases in-house and send extra volume or high-profile cases to service providers.

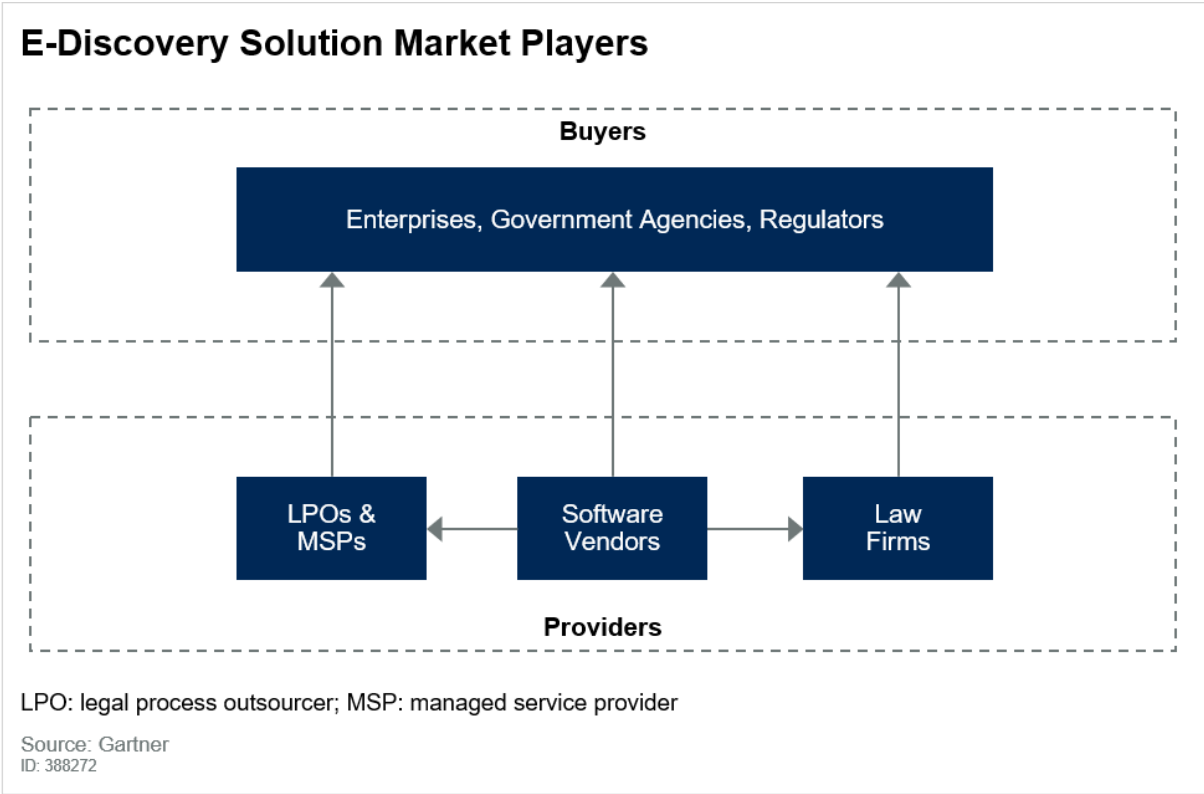
Market Direction

Three Types of Solution Providers

The multiteam, project-based, highly unpredictable and non-negotiable nature of e-discovery projects has led to a complex and fragmented market. Solution providers tend to focus on a few areas of the EDRM or become “best in class” for certain capabilities. While it is possible to leverage a single technology platform or outsource to a single service provider, most organizations have multiple technology tools in-house plus service providers to complete the support of their e-discovery needs.

The e-discovery market is served by three clusters of providers: law firms, service providers and software vendors. The ultimate buyers of e-discovery solutions are enterprises (IT and legal teams), government agencies and regulators. While law firms and service providers (in the form of legal outsourcing providers [LOPs] or managed service providers [MSPs]) are service providers, they are also software consumers. Software vendors serve both e-discovery solution buyers and service providers (see Figure 2).

Figure 2. E-Discovery Solution Market Players



Pricing

Typically, e-discovery software can be deployed in three different models: on-premises, hosted and SaaS. The pricing structure differs accordingly (see Table 1).

Table 1. E-Discovery Software Pricing Structure

Deployment Model	Pricing Structure	Cost Unit	Per
On-Premises	Perpetual license and maintenance	By module	Server or user or custodian
Hosted by MSP	Processing	By data volume (collected)	GB
	Analysis (filtering, ECA)	By data volume (uploaded)	GB
	Accessing	By number of users	User
	Hosting (storage)	By data volume (reviewed)	GB
SaaS	Subscription	All-inclusive	GB or user

Source: Gartner (June 2019)

Pure service components are often charged based on the types (consulting, review and project management) at an hourly rate. Often, service providers also offer pricing quotes in three different flavors: project-based, fixed fee or a la carte.

Market Adoption and Growth

The e-discovery software market is in a phase of high growth, with increasing maturity, innovation and consolidation. New players are entering this market to capitalize on the growing opportunities, while existing vendors in adjacent spaces (such as archiving, cyber security and enterprise legal management) are acquiring and adding additional e-discovery functionality to their offerings.

Data growth is the primary driver for first-time buyers, as well as market demand for more modern and scalable e-discovery solutions. Organizations in the highly regulated sectors (such as banking, finance, insurance, healthcare, pharmaceutical, and oil, gas and energy) in mature and litigious economies (North America and the European Union) are the main e-discovery solution buyers. In recent years, the number of cross-border discovery cases has continued to rise because of business digitalization and globalization.

Changes in local data protection and privacy laws and rules have led to localization of e-discovery services. Many of these cross-border cases require local support (both jurisdiction-specific and language expertise). With the expanded use cases of investigative matters (for example, internal HR investigation, post-data-breach assessment, FOIA request), e-discovery solutions are increasingly adopted by organizations across all sectors and less mature economies.

Market Analysis

The Push for End-to-End Solutions

In the e-discovery market, “end-to-end” can be interpreted in different ways. This Market Guide defines it as covering the nine steps depicted by the EDRM (see Figure 1). Historically, best-of-breed products are typical as a result of mergers and acquisitions or due to a lack of cohesive platform design. In reality, because of multiple review platform heritages (arising from law firms using different review providers in the past) and different procurement owners (such as IT, compliance and legal), organizations have adopted and continue to use multiple tools for their e-discovery needs. Vendors are now making a push to market their solutions as being end-to-end. However, buyers should note that some solutions may not be continuous, as there are multiple moving parts when it comes to implementation.

The drawback of a best-of-breed approach is that organizations have to manage a set of fragmented and overlapping technologies. E-discovery, by nature, is often project-based. It is challenging to have a consistent and holistic approach in orchestrating the different pieces required for each case or investigation. Therefore, having an end-to-end approach is highly attractive. Today, this end-to-end demand is being translated into a single or integrated platform, where data can be

moved easily, efficiently and securely. This approach enables organizations to achieve optimal results in terms of cost and risk control, defensibility, and duty to preserve.

For the short term, conducting an e-discovery assessment exercise (see “Defining Your E-Discovery Process Will Lower Costs and Reduce Risks”) and consolidating e-discovery software tools and service providers should be treated as a best practice. The long-term implementation of end-to-end solutions encompasses business buy-in of information governance, effective vendor management, multimatter capability, process reusability and a set of integrated systems that provide the optimal outcomes for e-discovery.

Migration to Microsoft Office 365

Office 365 has sparked a wider interest among Gartner clients in the topics of e-discovery and archiving. Many of these organizations have had some exposure to e-discovery requests, and the adoption of Office 365 and related SharePoint, OneDrive, and Teams elements has caused organizations to re-examine and invest further in these areas. Microsoft’s aggressive roadmap sends a clear signal that it is committed to e-discovery. This should further attract interest from buyers, many of whom fall outside the realm of the heavily regulated and litigated, and include more midsize enterprises.

Office 365 is the next step for organizations that are planning a move to the cloud, with most of the focus for e-discovery on Outlook email and Microsoft documents. Legal hold, preservation, search and tagging functionalities are readily available in Office 365. Microsoft has released an Advanced eDiscovery refresh, with new capabilities including additional custodian intelligence and communications, automated collection, and processing to improve working with content within a case, as well as native review and annotation capabilities.

This combination of data location (Office 365), archiving, and e-discovery will force many vendors to put a bigger emphasis on, and set of capabilities around, information and compliance management, and potentially add value-added services through partnerships or acquisitions. An example of this shift is the focus e-discovery vendors are putting on information governance and file analysis technology that enable organizations to index, classify, report, and migrate data located in file shares, email systems and content management repositories.

Hybrid Discovery: On-Premises to Cloud

There are many issues that organizations will have to confront in considering SaaS-based e-discovery solutions: data residency, privacy, encryption (both at rest and in motion), and SLAs for response timeliness are but a few. The sizable technical requirements and resources that cloud-delivered e-discovery requires, as well as the increasing demand from enterprises, will create even greater conflict in the market between e-discovery vendors and larger infrastructure providers. This can also lead to fragmented processes and overlapping technology capabilities.

The question of bringing e-discovery in-house and organizations taking greater responsibility for information governance and ownership of processes, such as collection and preservation, has largely been settled. However, data for e-discovery usually spans live systems, archives and sometimes backup tapes, and organizations have wildly different degrees of usage and volume,

depending on litigation demands. E-discovery's accuracy needs to be guaranteed, as the legal team requires confident assurance that all potentially relevant data is within search parameters.

In order to guarantee data identification and collection quality, IT tends to err on the side of being overly inclusive in its data preservation approach. This only adds to IT management overhead and on-premises storage costs. As data moves into the cloud (technology adoption) and toward the edge (wider usage of mobile devices), the number of data sources broadens, and organizations are looking for greater cloud flexibility where capabilities can be “dialed up” and “dialed down” as needed. Established processes, methods and technologies may not be enough. Indexing and classification services, for example, will work better and be less bandwidth- and resource-intensive if they are located closer to the data source.

The Future of E-Discovery Service Providers

The e-discovery service provider market has consolidated quite a bit in the past two years and will continue to do so. Those companies that do not have their own proprietary software must sustain a business model that is built on economies of scale, established relationships or differentiated services. The subtle competition between service providers and their software vendors drives down prices, spurs innovation and ultimately benefits consumers in the e-discovery market. While differentiation remains difficult for service providers, efficiency and cost predictability have become core competencies, along with a focus on delivering cost-effective e-discovery technology and services.

In addition, some e-discovery service providers rely on relationships with law firms or GCs to gain work and sustain their business. However, the unpredictability and the pressure of quickly getting resources together make the market for e-discovery services volatile. Large consulting firms often win business via global expertise and cross-sell via other arms of the consulting engagement. Providers that can't secure a steady stream of cases will face challenges if e-discovery is their only business.

Therefore, we will see more service providers in the area of information governance — not so much the technical aspects of it, but the legal ones. Clients who are frequently engaged in e-discovery exercises have begun to understand that the ultimate answer to decreasing cost and risk, while still meeting regulatory and legal obligations, is to take a more proactive view of information management. One way to achieve this is by seeking technical solutions that allow for indefinite expansion of information stores. One of the bigger trends related to this has been a serious examination of retention policies and, more importantly, how to enforce them.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The vendors listed in this Market Guide deliver most of the capabilities or services described in the e-discovery definition. Some solutions focus more on the left-hand, IT-centric side of the process, while others concentrate on the right-hand, legal-centric side. These vendors often differ on technological, service, business model and go-to-market elements. As a result, client organizations are advised to ask these vendors about their technology capabilities, service focus, delivery models, industry expertise and cross-jurisdiction support. This is not an exhaustive list of providers. See Table 2 for a representative list of e-discovery technology providers and Table 3 for service providers.

Table 2. Representative Software Vendors in E-Discovery

Vendor	Product or Solution
AccessData	AD eDiscovery, Summation, Forensic Toolkit (FTK)
Casepoint	Casepoint
Cicayda	Reprise Review, Fermata Legal Hold
CloudNine	Explore, Concordance, LAW
Congruity360	Discover360, Hold360, Classify360
DISCO	DISCO
Everlaw	Everlaw
Exterro	Legal Hold, Legal Project Management, E-Discovery Data Management
IBM	StoredIQ for Legal, Atlas, eDiscovery Analyzer, eDiscovery Manager
iCONNECT Development	iCONNECT-XERA
Ipro	Automated Digital Discovery (ADD), Eclipse, Eclipse SE, eCapture
Knovos	eZReview, eZManage
Lexbe	Lexbe eDiscovery Platform
Logikcull	Logikcull
Mindseye	Mindseye eDiscovery Platform
Nextpoint	Nextpoint
Nuix	Nuix Ringtail, Nuix Workstation
ONE Discovery	EC3
OpenText-Catalyst	Insight Discovery
OpenText-Guidance Software	EnCase eDiscovery,
OpenText-Recommind	OpenText Axcelerate
Relativity	RelativityOne
Servient	Servient

Vendor	Product or Solution
Thomson Reuters	eDiscovery Point
Venio Systems	VenioOne
Veritas	eDiscovery Platform
X1	X1 Search, X1 Distributed Discovery, X1 Social Discovery
Zapproved	Z-Discovery suite: Legal Hold Pro, Digital Discovery Pro
ZyLAB	ZyLAB ONE

Source: Gartner (June 2019)

Table 3. Representative Service Providers in E-Discovery

Provider	Proprietary Software or Solution
Conduent	Viewpoint Integrated Analytics
Consilio	Sightline
Deloitte	
Driven	
Epiq	
EY	
FRONTEO	Lit i View
FTI Consulting	
Integreon	
KPMG	
KLDiscovery	
Lighthouse	Spectra, Navigate, SmartSeries
Navigant	
PwC	
Ricoh	Remlox Remote ESI Collection, RICOH eDiscovery On Demand
UnitedLex	

Source: Gartner (June 2019)

Market Recommendations

General counsel, chief compliance officers, chief information officers (CIOs) and their teams should consider the following recommendations for e-discovery solutions in any investigative or legal cases they initiate or support:

- Select e-discovery SaaS solutions strategically. Depending on the maturity of in-house e-discovery processes and teams, SaaS solutions may not be suitable for all matters.
 - Small and less complex cases are good fit for in-house teams leveraging SaaS options. Such cases can be categorized as:

- Data volume below 1TB
- 75% or more of data is regular business email (Microsoft Exchange)
- Low profile (i.e., no tight court deadline, reasonable opposing parties, no reasons for causing mass media attention)
- Single jurisdiction
- Consider a SaaS provider's terms and conditions (see "Toolkit: Minimize SaaS Risk and Cost by Efficiently Negotiating Optimal Contract Terms and Conditions.")
- Engage service providers when necessary. Service providers are often best-positioned to handle "one off" high-stakes cases.
 - Identify your e-discovery needs:
 - Number of cases per year
 - Average size of cases
 - Data sources
 - Internal resources and capabilities
 - Retain multiple service providers based on your needs.
 - Review contractual terms carefully, and, in particular, clarify costs associated with retrieving data, including coding data from service providers' repositories (this is an item that often does not get enough attention and sometimes can be costly).
 - Request updates from service providers on data encryption, protection and handling of privileged data.
- Engage all stakeholders (at minimum, IT and legal teams) in selecting a solution provider.
 - Weight and balance requirements across stakeholders accordingly. E-discovery offerings are a combination of infrastructure and application, and result in numerous buying criteria: scalability, repository support, deployment options, end-user features, ease of use and related application criteria.
- Leverage enterprise technologies (enterprise search and archive) as well as data connectors in order to pull all data sources together. Take advantage of mobility management suites, and endpoint data management and other data connector solutions for mobile and social data preservation needs.
 - Include mobile data in data preservation scope, even if the majority of your cases do not require you to do so.
 - Participate in organizations' user training and follow their user policies (such as a bring your own device [BYOD] policy, social media use guidelines).
 - Keep knowledge up to date in terms of e-discovery support capabilities from other adjacent technologies (such as archive).

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

“Defining Your E-Discovery Process Will Lower Costs and Reduce Risks”

“Make E-Discovery Stronger Through Information Governance”

“Corporate Legal and Compliance Technologies Primer for 2019”

“Why ‘Store Everything’ Is Not an Effective Information Governance Strategy”

“Magic Quadrant for Enterprise Information Archiving”

“Critical Capabilities for Enterprise Information Archiving”

Evidence

The analysis and advice provided in this document are built from constant scanning of the market, as well as from the aggregation of analysts’ experience and ongoing interactions with end users and technology providers. We used a range of sources to feed our perspective on the topics discussed in this document:

- Gartner customer inquiry and conversations
- Previous Gartner analysis of e-discovery and related technologies

Gartner analysts also leverage secondary sources of information, including surveys, financial earnings and media reports.

Note 1

Representative Vendor Selection

The vendors and service providers named in this guide were selected to represent the types of solutions as discussed in the Market Description and Analysis sections that (1) offer a combination of installed or hosted software applications and solutions; or (2) offer fully managed hosted software and service solutions using customized installations of commercial software or offerings unique to the provider. In addition, these vendors and service providers are mentioned during our engagements with buyers and stakeholders throughout the year. The vendors and service providers included in this research do not constitute an exhaustive list of the e-discovery solutions in the market.

GARTNER HEADQUARTERS**Corporate Headquarters**

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters

AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit <http://www.gartner.com/technology/about.jsp>

© 2019 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."