

InComparison



Email archiving best practices

...a competitive overview of major players in the market

An InComparison Paper by Bloor Research
Author : Fran Howarth
Publish date : September 2011

Email archiving should be considered to be part of a broader email management solution that includes mailbox management, policy enforcement, security, continuity and e-discovery. For best results, all of these capabilities should be tightly integrated as part of one unified system.

[Fran Howarth](#)

Executive summary

Email is of vital importance as a communications and collaboration tool as it is one of the prime ways that business information is communicated and shared. This makes its storage and archiving a necessity for maintaining and improving productivity by being able to retrieve information as it is needed. Yet operational efficiency is not the only driver for investing in email archiving technology. Owing to the amount of business information that it contains, email constitutes the leading type of evidence requested for litigation purposes and its preservation is also essential for complying with the requirements of a variety of governmental and industry regulations.

Today, there is a range of choices to be made when deciding to deploy an email archiving solution, from on-premise installations of software and/or appliances, to hosted cloud-based services, to a hybrid mix of the two. The information presented in this report is intended to help organisations with their evaluations of the major players in the market for email archiving technologies. It is intended to be read by organisations of all sizes in any vertical industry.

Key recommendations

- The technology must be tightly integrated with the email system in use to ensure all messages, their attachments and associated metadata are captured. Check which email clients are covered. To reduce training needs and to aid in user productivity, look for products or services that use the native interface of the email client for the archiving service.
- Archiving is part of a broader email management solution that includes security, continuity and e-discovery. Look for a solution that is built on a unified platform and that provides a single, consolidated administration console.
- The technology should offer powerful indexing and search capabilities, including the provision of user self-service directly from within the email client itself.
- It should provide centralised archiving and management for enforcing policies, and for providing a reporting and audit trail for governance and compliance purposes.
- The security of the system or service is important for risk management and should be tightly integrated. Consider such factors as granular access controls, especially for privileged users, logging of all activity, encryption for data at rest and in transit, and security controls such as anti-malware.
- For hosted, cloud-based services, key considerations include the provisions of the SLA, data centre coverage in terms of number and location, as well as the security of the data centres, backup and disaster recovery provisions, and availability of email services should an outage occur. Downtime is a major drain on productivity, so look for a system that provides for continuity of service so that users continue to receive emails and can search the archive even during an outage.
- Consider the options provided for mobile device connectivity and needs for archiving other types of content.
- The system or service should provide good levels of support for e-discovery and record retention regulations for compliance purposes and to help the organisation to avoid fines or sanctions. Review the vendor's position on complying with intelligence-gathering legislation such as the Patriot Act.
- Review the financial viability of the vendor, the strength of its business model and its ability to execute on it, its longevity as a business supplier and the availability of existing clients as references.
- Consider the roadmap and enhancements planned within the contract term offered. Check this against the vendor or service provider's history of innovation and delivery over the past two years at least.

The importance of email

Since its inception, the use of email has risen dramatically. A survey of 1,800 knowledge workers in six countries by Platronics, entitled "How we work", that was published in 2011, looked to gauge how people communicate in business today. It found that, among communications tools used, the use of email has seen the greatest increase, with 78% of respondents saying that its use had increased dramatically since 2005. Furthermore, 83% cited email as being the communications tool that contributes most to their success and productivity at work.

However, email is more than a communications tool. It has become a platform for sharing information, collaborating around documents and managing group discussions, and today the majority of all business data is held in email. Not only do a vast proportion of emails contain business data, but it is estimated that 60% to 70% of business-critical information is, at some point, contained in email. According to Osterman Research, the average mailbox contains 250 megabytes of critical business information. This makes it extremely important that such records are kept and stored in an accessible manner so that information can be retrieved when needed and can be re-used for other purposes.

Email also constitutes the leading type of evidence requested by courts during litigation. Numerous surveys point to the rise in both the number of lawsuits requiring e-discovery as well as the sanctions for non-compliance, especially where the organisation was unable to produce all the required documents. Whilst the bulk of cases are seen in the US, e-discovery cases are becoming increasingly commonplace in other regions. According to researchers IDC, who conducted an online poll of 115 legal professionals in large US organisations that was published in January 2010, the number of respondents facing more than 100 lawsuits rose from 27% in 2008 to 46% in 2009. It also found that 70% of respondents were involved in international litigation.

There are also numerous government regulations and standards that demand that organisations maintain records, including email correspondence, for specified periods of time, some affecting specific industries or types of organisation, others more general in nature. Examples of these in the US include SEC Rule 17a-4, Sarbanes-Oxley, the Federal Rules of Civil Procedure, NARA Electronic Records Management regulations and FINRA Rule 3110. The US also has the Patriot Act, which allows for the interception and inspection of enterprise email. In the EU, each member state tends to have its own national laws governing records retention with the majority requiring records to be maintained for an average of five years.

The need for email archiving

For the reasons given above, more and more organisations are taking a more proactive stance to the retention and archiving of emails. In a survey undertaken by Computerworld of 111 email managers that was published in January 2010, 59% of respondents cited the need to locate business records and contacts as the reason they need to search for emails, 49% to recover deleted emails, 40% as part of an internal HR investigation, 29% for compliance purposes and 19% for legal discovery.

To be able to cater to these needs, emails need to be stored in a secure, centralised repository. However, it is still too often the case that emails are filed locally on users' own hard drives, or within the email systems themselves. Given the sheer volumes of emails received and sent, this makes it a difficult task to search for and retrieve emails as and when needed and it also places the onus on users to decide what to keep and what not to. This leads to the danger that emails that contain information pertinent to a lawsuit or that need to be kept for regulatory compliance purposes could be deleted, requiring the time and expertise of the IT department to retrieve the email; or lost, requiring that the information be produced again. Further, if the emails are stored on a laptop, they could be gone forever if that laptop is lost or stolen.

Such scenarios pose risk to the organisation, are a drain on productivity and the assistance of IT may be beyond the means of smaller organisations that lack the IT resources with the relevant experience or time to perform the task of restoring deleted emails. They could also leave the organisation facing sanctions for non-compliance with regulations or for failure to be able to produce evidence required in a legal dispute.

What organisations need is the ability to efficiently and securely collect and preserve emails. Those that don't will end up spending more than their competitors when required to produce emails and are likely to face more sanctions for non-compliance. However, this is something that is not being lost on organisations. According to the results of a survey released in January 2010 by the Enterprise Strategy Group, 87% of respondents stated that they were planning to budget for technology to support e-discovery requirements during 2010. The same survey also found that 22% of respondents have the job title "e-discovery manager", which provides an indication of how serious the problem is becoming.

Choosing a solution to the problem

With the need to archive emails so stark, organisations must make a decision as to how to solve the problem. There are technologies that automate the processes and can be installed within the organisation's network and are managed by themselves as packaged software and/or appliances. This is the way such technology has traditionally been delivered. Early systems were mainly focused on the needs of large enterprises, and many were focused on the needs of specific industries, financial services in particular. To deploy such technology, the organisation needs to purchase hardware to run the systems and software licences for all who require them, and then must dedicate resources to the administration and management of the system.

Some five years ago, technology deployed in-house was preferred by many, especially those in the financial services sector who were adamant that they would never store emails offsite and who felt that bandwidth and security were issues that made offsite archiving impractical. Today, the massive volumes of email that are produced and stored makes in-house archive management a complex and costly task and even those in highly regulated industries such as financial services are looking for alternatives.

In recent years, an alternative has been developed—that of subscribing to a hosted archiving service, managed by experts. There are a variety of vendors offering such services, some of which are highly specialised in email management, including archiving, security, continuity and e-discovery; and others that offer such services as part of their information management portfolio. Since they are provided on a subscription basis, the costs of such a service can be lower than for technology deployed in-house as no specialised hardware is required, software licences do not need to be purchased upfront and the organisation does not need to dedicate resources to the administration and management of the system. This makes it an alternative that is an attractive option for organisations of all sizes—from the largest geographically dispersed multinational that will benefit from a unified email archiving service across all locations in which it operates to a small company that lacks the IT resources required to manage its archiving needs itself.

What email archiving technology or services must provide

The following are some of the key features to look for when evaluating products and services.

One unified service

Email archiving should be considered to be part of a broader email management solution that includes mailbox management, policy enforcement, security, continuity and e-discovery. For best results, all of these capabilities should be tightly integrated as part of one unified system, built on a common architecture for an amalgamated service, with one single, centralised management point that provides policy enforcement, management reports and an audit trail for governance and compliance purposes.

User experience

There are a number of capabilities that are essential components of any email archiving technology or service. Of primary importance is that it is tightly integrated with the email system that is in use in the organisation so that all messages sent and received, including their attachments and associated metadata, are captured by the system, including those that users place in their personal archive. It must also provide powerful search capabilities that can quickly and accurately search through the archive and that allows users access to both current and historical emails and their attachments directly from the email client with which they are already familiar for efficiency and ease of use. For example, a system that uses the features of an email client that users are already familiar with, such as the icons and drag and drop features of Outlook, rather than opening up a new frame or web page, will be most easily accepted by users and will allow them to quickly search for old emails, when needed, directly within the email client itself. This will also help users to become familiar with the system so that training requirements are lessened. As well as this, many offer access via a browser or a mobile device for added convenience.

Centralised control

The system should also have one central storage system and one centralised management interface for ease of use and administration and for providing management reports that give visibility over how well the system is working. The central management console should also provide log analysis that will form the basis of the audit trail that is necessary for

corporate governance and regulatory compliance purposes. Centralised management will also ensure that policies can be managed and enforced for security controls, data retention and destruction periods, access controls by role in the organisation and policies regarding acceptable use. Retention period policies should take into account the requirements of the various regulations and industry standards with which the organisation must comply.

Security

Security is another important consideration. Granular access controls are required, with all access records logged to show the actions of all users, and encryption for all messages when stored in the archive or in transit between the email system and the archive is necessary for ensuring that data cannot be improperly accessed or leaked out of the organisation. Even though the organisation will almost certainly be using its own malware controls, the system should also include its own checks to ensure that all emails stored in the archive are malware-free.

Continuity

Where the use of cloud-based hosted email archiving services is being considered, organisations should look at what the service provider has in place for business continuity. Today's always-on generation demands access to emails from wherever they are, whenever they want. Therefore, the service should provide guarantees regarding service availability. Some providers offer a gateway service for providing service availability even in an outage, so that uninterrupted access is provided to both current and historical emails, and so that regulatory compliance requirements such as email retention can continue uninterrupted even in the event of a server outage.

e-discovery support

With e-discovery cases on the rise for organisations of all sizes, including international litigation, an email management and archiving system should store not just every message that passes through the email server but also detailed information related to all messages for non-repudiation purposes. This includes all attachments as well as metadata associated with each message, such as data regarding what policies were applied to each message, from which service they were sent and proof that the message was actually delivered. For

What email archiving technology or services must provide

chain-of-custody purposes, the email stored in the archive must be the same as the one delivered to the recipient, and emails in the archive should be encrypted and tamper proof. Because the archive is tamper proof and emails are stored in a location other than on hard drives and email servers, it is also fully compliant with forensic evidence requirements, as well as the mandates of various government regulations and industry standards. So that the archive is non-contestable, each message should be stored in at least two, if not three, separate locations and the system should be capable of enforcing legal holds, as well as retention and destruction periods according to the requirements of the regulations with which any particular organisation must comply.

Data centre coverage

The number and location of data centres should also be considered. Not only should the service provider have ample data centre resources to ensure that data is not only securely backed up and failover services can be provided in the event of a service failure at the primary data centre, but also organisations should evaluate in which jurisdiction data is being stored. The issue of data centre jurisdiction is important given the growth in international litigation. According to a recent report by Bloomberg Law, the growth in multi-jurisdictional investigations has been one of the most notable emerging trends of 2010, especially those invoking the Foreign Corrupt Practices Act, and individuals at corporates are being increasingly targeted in 2011. The ramifications of this are shown in the 7th Annual Litigation Trends Survey, published by Fulbright & Jaworski LLP in 2010, which shows that more than 40% of respondents have encountered an actual or threatened dispute involving privacy and data protection and 39% have encountered privacy and data protection issues when data is transferred from the EU to the US.

Evolving issues

One of the main issues concerns the use of the Patriot Act and other intelligence-gathering legislation from the US to compel organisations to hand over information to the US government, with such requests sometimes accompanied by a gagging order that prevents the recipient of the request from disclosing that the order has been issued. Therefore, organisations may not even be aware that these instruments are being used against them. If the hosting company is a

wholly owned US company, it and its subsidiaries in foreign countries are subject to the Patriot Act throughout its operations. However, some such companies state that they will abide by the Safe Harbor framework as set out by the US Department of Commerce regarding the collection, use and retention of data from the EU, the European Economic Area and Switzerland.

Because of these issues, many countries, including the UK, Australia, Canada, the Netherlands, France and Norway, have put in place blocking statutes that prohibit the gathering of business-related information to be used in foreign litigation and that provide for prison sentences, fines or both for transgressions. With regard to the French blocking statute, law firm Gibson Dunn states that these statutes should be interpreted as preventing the formal collection by US courts of any documents, testimony or information from French nationals under the Foreign Corrupt Practices Act. However, US case law has determined that sanctions, such as contempt of court, can be imposed by US courts. Recipients of such orders must face a choice of breaking national laws or provoking the wrath of US courts.

Therefore, this is an issue that must be considered when deciding to transfer data to a US-based cloud service provider, especially if a Safe Harbor framework is being used, under which it would be allowed for data to be copied from a European data centre to one in the US, making that data vulnerable to discovery requests under the Patriot Act. Therefore organisations should look for a provider that has a local cloud infrastructure to mitigate concerns about storing data in an offsite location and should scrutinise the terms and conditions of the service to ensure that hosted data is secure and will reside only in data centres within the EU, including secondary data centres for geo-redundancy.

Even if the organisation is a US subsidiary based in a foreign country and therefore subject to US discovery requests, it should seek assurances from the service provider that procedures for dealing with such requests are tight, with only a very limited number of people within the organisation provided with the means to comply so that due consideration will be given to the validity of the request and so that not just anyone in the organisation can hand over data. Similar consideration should be given to the procedures employed for encryption key management. All messages should be

What email archiving technology or services must provide

encrypted with a key that is unique to each customer and stored securely, with controlled access to keys very limited to just a few people, and with more than one person required to authorise the release of a key. The data should be stored on a backend grid that is independent of the actual email archiving application. Therefore, if customer data is removed from the archive infrastructure, the data cannot be read except through the application itself. Such measures will help to protect data stored in a multi-tenant cloud-computing environment.

However, the issues of US e-discovery laws notwithstanding, there are discovery requests with which organisations will need to comply and there are a number of capabilities that a service provider should offer to support their customers in such litigation. The technology provided should include functionality for imposing retention periods according to the needs of the regulatory compliance mandates that their customers face, as well as providing and enforcing secure destruction when the retention period has been reached to avoid organisations exposing information that is no longer valid, and which could be harmful to them. The system must have strong iterative search and retrieval capabilities, including the ability to recover deleted emails, and should be able to enforce acceptable use policies to avoid potentially incriminating emails being produced and stored in the archive. All metadata should be stored, providing details regarding the authenticity and integrity of all emails held in the archive for complying with chain-of-custody requirements and to provide proof of delivery. This metadata should also prove that security controls have been applied to all messages, such as scanning for viruses. This metadata will also be useful in identifying the source of any data leak so that remedial action can be taken. For litigation purposes, the system should also provide for legal hold requirements to be imposed and adhered to so that information cannot be altered once a discovery request has been received.

In-house versus cloud-based deployments

There are many well-designed in-house email archiving solutions that give fine-grained control over all aspects of the email archiving and retrieval process. However, such systems are generally costly to deploy in terms of the hardware and software licences that need to be purchased upfront, providing limited flexibility into scaling up or down the solution as required. Implementation times are also generally quite long, averaging six to ten months for a large enterprise across its operations. Some in-house systems have also been developed as part of larger information management portfolios and many such capabilities have been acquired, rather than built from the ground up. In some cases this has led to a confusing array of products being offered, some with overlapping capabilities. With acquisitions on-going for some vendors, the future direction of some products offered is unclear.

Notwithstanding the legal issues discussed earlier—which could affect any organisation that is wholly owned by a US company or that has operations in the US, even if its deployment is in-house—the use of cloud-based email archiving services is an attractive alternative for many organisations. Such services can provide access to a unified email management platform that includes guarantees over availability, reliability, security and business continuity. With access to the archive provided via the email client itself, or a browser or mobile device, such services are useful for organisations with geographically dispersed offices, providing one unified archive across all locations, or for those that need to support a mobile workforce. They also provide smaller organisations with access to enterprise-class services, without the need to administer and manage the service themselves. As such, they will also appeal to those organisations that lack the in-house IT resources required to administer the system.

Offered via a subscription model whereby organisations only pay for those users who need access, providing the flexibility of being able to scale up or down the number of users as circumstances change, the use of cloud-based services lower the capital expenditures associated with a technology deployment, such as hardware purchases. According to technology consulting firm Booz Allen Hamilton, the lifecycle costs of using cloud-based services are 65% lower than for other technology delivery models and provide cost-benefit ratios ranging from 5.7 to nearly 25. According to law firm Quarles & Brady, the savings organisations will make by using a cloud-based email archiving service will not be absorbed by the additional costs and risks of moving to the cloud, which include the loss or alteration of data and its associated metadata, potential violation of international data privacy laws, co-mingling of data and sanctions related to failure to properly implement litigation holds. To mitigate these risks, organisations should insist that the service agreement with their cloud provider specifies where data will be held, provides a detailed mechanism for how litigation holds will be implemented, and addresses how metadata will be created and stored in a cloud environment.

Overview of the major players

Autonomy

Autonomy was founded in 1996 and describes itself as a provider of infrastructure software for enterprises. It has a heritage from research at Cambridge University in the UK, where it still maintains one of two headquarters, the other being in California. Its last reported full-year revenues were US\$870 million in 2010 and its expected turnover in 2011 is in the region of US\$1 billion. Around two-thirds of its revenues are for its core enterprise search engine, and it offers a range of other products, including those for customer interaction, information governance, business process management, web content management, web optimisation and rich media management and analysis, as well as email management, archiving and e-discovery. Autonomy has seen a compound annual growth rate of 55% over the past five years, although much of this has been owing to the acquisitions that it has made, rather than organic growth. Autonomy reports that it has 36 offices worldwide and that 70% of its revenues are from the Americas.

In August 2011, HP announced its intention to acquire Autonomy for US\$10.2 billion in order to enhance its enterprise information software. Speaking at the time of the announcement, HP's CEO, Léo Apotheker, stated that the acquisition of Autonomy will help position HP as a leader in the enterprise information management market. What the acquisition does show is that HP recognises the value that organisations are now placing on the management of unstructured data. Whilst many applauded the deal, HP made other announcements about its future strategy at the same time, such as selling off its hardware businesses, which were not well received by the market, causing its share price to fall heavily. Since the ramifications for Autonomy are not known at this point, this evaluation refers to Autonomy's capabilities at the time of the proposed acquisition.

Many of Autonomy's archiving, records management and e-discovery capabilities come through acquisition, including Zantaz, an email archiving and litigation support company, for US\$375 million in July 2007 and enterprise content management company Interwoven in January 2009 for US\$775 million. In June 2010, it made a further acquisition by taking over CA Technologies' information governance business to improve its enterprise archiving and search capabilities. Its latest acquisition was in May 2011 of Iron Mountain

Digital for US\$380 million for further capabilities in archiving, e-discovery, and offline and online backup, as well as specialised products for compliance requirements of financial services organisations.

Current offering

Autonomy's "meaning based computing" unstructured information indexing and analysis platform, called the Intelligent Data Operating Layer (IDOL), underpins all of its offerings, including its hosted archiving services.

Autonomy's archiving, e-discovery and compliance products are offered under its Protect product line, which is one of three. It offers both on-premise and hosted offerings, often through partners such as Huron, Deloitte and Ernst & Young, as well as hybrid deployments, covering content management, e-discovery review, production and early case assessment, policy management and legal hold, and archiving and records management. Its background in unstructured content means it can offer its customers the ability to search audio and video files, as well as electronic records. As well as a range of email systems, its products support mobile devices, instant messaging, social media and SharePoint. Autonomy also offers e-discovery services that complement its technology and hosted services.

Autonomy aims to address all aspects of the Electronic Discovery Reference Model (www.edrm.net), from identification, preservation and collection of records, to processing, review, analysis and production.

Autonomy's enterprise archive solution was renamed to Autonomy Consolidated Archive (ACA) in 2010 when it released a consolidated product that aggregated the capabilities it had acquired prior to that date. The product is available as on-premise technology, as a hosted option, or a hybrid mix of the two. It offers archiving with compliance, records and content management, legal and backup capabilities and supports a wide range of content types and languages. Autonomy's aim is to support the entire EDRM process from identification to collection to review and production. The product utilises the IDOL platform to provide advanced classification, analytics and search capabilities. ACA is complemented by End-to-End eDiscovery and Autonomy Records Manager for supporting the entire EDRM process.

Overview of the major players

Autonomy offers the Autonomy Digital Safe cloud-based products in three packages, ranging from archiving and basic e-discovery at the low end to a full-fledged consolidated archiving and governance platform at the top end. All of these products can also be provided as an appliance for onsite deployment. Autonomy maintains four SAS 70 Type II certified data centres in the US, Canada, the UK and Europe.

Autonomy claims that its Safe Harbor Framework certification emphasises its commitment to ensuring the security of the data of organisations in the EU.

Strategy

Autonomy's strategy is to support its customers throughout the EDRM lifecycle, which it is doing through a combined strategy of organic development and acquisition. Having traditionally focused on enterprise customers, its cloud-based offerings extend its appeal further into the SME sector. Some of the companies that it has acquired were focused primarily on this sector, as well as being strong in the North American market. It aims to provide a wide range of options for its customers, including a hybrid on-premise/cloud offering that it has been developing over the past three years.

Post-acquisition, Autonomy's strategy will be more strongly influenced by HP, although Autonomy is likely to remain as a relatively autonomous division within HP. For the acquisition to succeed, HP will need to focus on the further development of Autonomy's products in the long term. In the short term, there remains a great deal of integration work remaining regarding recent acquisitions made by Autonomy.

Market presence

Autonomy has historically focused primarily on the enterprise sector of the market and claims all of the top ten financial services institutions worldwide use its archiving products, as well as global companies, including 86 of the Fortune 100. Also particularly strong in the legal sector, Autonomy claims the top ten global law firms as its customers.

For the financial services market, Autonomy offers products specifically aimed at compliance needs in that vertical, as well as a healthcare division that focuses on cloud archiving. It also has technology specifically for the legal market. Selling its archiving services worldwide, Autonomy has a strong presence in Europe.

Strengths

Autonomy is considered to be a market leader in information governance owing to the wide range of products that it offers and the wide range of content types that it covers, being especially strong in the area of unstructured information through its IDOL platform. It is considered to be a market leader in the enterprise archiving market, complemented by a broad set of information governance technology and services.

Weaknesses

Much of Autonomy's capabilities in the archiving market have been obtained through acquisition and significant integration work remains. This has led to a number of rebranding exercises recently that have been confusing. Its integration of Iron Mountain's capabilities could be challenging and could pose questions for existing customers since Iron Mountain's technology was previously powered by technology from Mimecast, which Autonomy states was not included in the terms of the acquisition. Its traditional focus has been on enterprise customers and, as it moves more to a SaaS model, it could be challenged to serve the needs of the SME sector as it has been considered to be weak in sales to, and support for, this sector. Its on-premise technology is considered to be resource-intensive and products are expensive when compared to competitors.

The fact that products have been purchased through multiple acquisitions means that, whilst they may over time be integrated, with IDOL as the common underlying platform, they are not a unified solution. Much development also remains and Autonomy has always been tight-lipped about its product roadmap.

Overview of the major players

Google

Google was founded in 1998 and is active in the areas of internet search, cloud computing and advertising technologies. Headquartered in California, Google has offices worldwide and employs around 24,400 people. A public company, Google received revenues of US\$29.3 billion in 2010.

Google's email archiving service was acquired from Postini in 2007, along with email and web security services, in order to boost the business appeal of its Google Apps products. Its archiving product can be bought as a standalone product or as an add-on to Google Apps.

Current offering

Google's cloud email archiving services are designed to complement its Gmail product and are integrated with its secure messaging services, but are provided as an add-on service at extra cost. Support is also provided for Microsoft Outlook and other email clients. Its message discovery services are priced at US\$25 per user per year or US\$45 per user per year for advanced message discovery, which includes up to ten years retention for emails. However, there are minimum purchase requirements. Tight integration with secure messaging services provides anti-spam and anti-virus protection, as well as content policy management and encryption. Its message encryption service is also priced separately at US\$35 per year for a minimum of 100 users. Phone-based support is available for customers spending in excess of US\$1,500, although it does operate an online forum for its customers to discuss technical issues and solutions.

Google enhanced its email archiving service in 2010 with a new message log search feature to allow emails to be searched for and analysed, with the associated metadata stored in a log file. Prior to this, administrators had to go through customer support to access this data. This service allows administrators to monitor all messages received and sent to check to see if they have been delivered, quarantined, archived or encrypted. The service includes the ability to transmit messages using policy-based Transport Layer Security protocols for added security.

Google's email archiving service allows emails to be retained for up to ten years and includes services such as legal hold and retention policies, and integrated spam and virus filtering

for message security. To ensure that there are no service disruptions or lost messages, it has a patented real-time, pass-through architecture that guarantees email delivery through spooling even if the email server goes down. Once the server is restored, all emails will gradually be delivered to users' normal mailboxes. It provides guarantees of 99.999% availability for message processing and claims to have the capacity to handle billions of transactions per day.

The SLA offered by Google includes guarantees of 99.999% service availability, 100% anti-virus protection, 60 seconds or less latency for email delivery, 98% capture of junk mail, 0.0003% spam false positive rates, 100% email delivery assurance and 100% guaranteed client service response.

Strategy

Little has been seen in the way of new features to its web and email security services being released since Google acquired Postini in 2007 and it is unclear what new features are planned on the roadmap. However, it has made enhancements to its archiving and discovery capabilities. In this market, Google views Microsoft as its primary competitor.

Market presence

Google has a large installed base for the products that it acquired from Postini, claiming to have more than 35,000 customers using these services.

Google has a wide network of its own data centres and guarantees that all messages are held in at least two geographically separated facilities.

Strengths

Google's email archiving services are a relatively cheap option, offering a range of basic services that are integrated with other product offerings, including email and web security.

Although Google is somewhat tight-lipped about the extent of its data centres, it is known to have numerous facilities throughout the world, including at least 12 in the US. The two largest known centres in Europe are located in Belgium and the Netherlands. It is thought that there is a data centre in Australia.

Overview of the major players

Weaknesses

Although Google has a wide network of data centres, it has suffered several service outages. Some customers also report mail delivery failures and high false positive rates for spam, above the 0.0003% stated in the SLA offered. Google offers its customers credits if these thresholds are breached.

Language support is limited, with emails searchable in English only. However, the user interface has been localised in French, German, Spanish and Japanese. Instant messages and social media are not supported and the compliance requirements for specific regulations are not provided. Its e-discovery services are slated as being simplistic and mailbox management is lacking. It is criticised for its customer support and has had a visibly poor record of service outages.

Overview of the major players

LiveOffice

Founded in 1998, LiveOffice is a privately held company that is focused on email and other content archiving. All other services that it offers, including spam filtering and malware protection, are provided via partnerships. In 2009, LiveOffice achieved revenues of US\$26.1 million, representing growth of 16.5% over the previous year. However, its strategy of partnering with other technology vendors led to it achieving sales growth of 111% in the first quarter of 2011 compared to the same period in 2010.

Current offering

LiveOffice offers a range of products that are sold as packaged bundles according to customer need, including products for compliance, policy, discovery and mailbox management. Its core product is its Personal Archive that allows emails to be stored, searched and retrieved, although the interface lacks the familiarity of the native email client. Its Discovery Advisor offers additional e-discovery capabilities, including legal hold through a partnership with compliance vendor Zapproved. LiveOffice has its heritage in serving the financial services industry and its Advisor Mail is targeted at the needs of financial institutions, including message pre-review and post-review. Its products currently support nine languages and more will be added in the future.

LiveOffice's products provide archiving capabilities for Microsoft products, as well as support for other email clients that include Domino and GroupWise. LiveOffice also has partnerships with SaaS vendors Salesforce and SuccessFactors for archiving their content, provides optional integration with instant messaging through a partnership with Actiance (formerly FaceTime Communications), social networking and SharePoint applications through partnerships, and supports a range of smartphones.

In the latest release, LiveOffice claims to have expanded the e-discovery capabilities of its products to allow greater collaboration among legal teams and other stakeholders in the organisation. New features added in 2011 to its Discovery Archive product include more granular controls over legal hold enforcement, and retention policy management to allow greater customisation to meet specific needs of organisations. In 2011, it released an upgrade to its Personal Archive to provide a more intuitive user experience, including enhancements to its search capabilities and expanded language

and browser support. Upgrades to its Advisor Mail product have been made with the needs of its financial services clients in mind.

LiveOffice guarantees its customers the provision of unlimited storage, deployment within five days without a setup fee, and 99.99% uptime for its service. Its security services include secured data centres, encryption for data in storage and in transit, security monitoring and always-on availability.

Strategy

LiveOffice announced in 2010 that it had entered an agreement with Microsoft to resell its email management services. It claims that this has led to it deploying this service for a customer with 120,000 mailboxes under management. Partnerships form a core part of its strategy and other partners include Symantec and Salesforce. It claims that these partnerships are responsible for around 70% of its revenues.

Market presence

LiveOffice is headquartered in California and employs some 200 people. It claims more than 18,000 customers, which are primarily located in North America and Europe, although it states that it has customers in 50 countries across six continents. Until June 2008, it primarily focused on the financial services sector, but has since expanded to address the needs of organisations across verticals that require email archiving services.

Strengths

As a small company, LiveOffice has partnerships with larger, well-established vendors that include Microsoft and Symantec, as well as service providers Salesforce and SuccessFactors. These partnerships allow it greater reach than it could achieve purely by itself as a small company with limited brand recognition.

Weaknesses

Owing to its limited data centre coverage, LiveOffice is best suited to serve the needs of US customers and is less well-served in terms of data centres than its competitors. Its average customer size is small and it lacks large reference customers that can attest to the scalability of its services, although it claims Fortune 100 companies as customers. Although it has expanded beyond the financial services industry in recent years, this still remains a core focus for the company.

Overview of the major players

Although email archiving forms the bulk of LiveOffice's revenues and capabilities, it claims to offer a comprehensive suite of email management services. However, these services are provided through the capabilities of its partners, rather than being a unified suite of products with a common architecture and a specifically built management interface, and its products lack the tightly integrated services offered by some of its competitors. This strategy could also leave it exposed if the terms of those partnerships change. For example, it had a partnership with Mimosa Systems, which was acquired by Iron Mountain, which was subsequently acquired by Autonomy.

There are many reviews of LiveOffice that slate it for its poor service levels, history of outages, and performance of the service, such as slow or non-delivery of emails. The breadth of its services beyond archiving is not as great as its competitors; such as in security, data integrity and e-discovery capabilities, and many are heavily dependent on relationships with third-party providers.

Overview of the major players

Microsoft

Microsoft was founded in 1975 and offers a wide range of computing products and services, including office productivity tools. It maintains its headquarters in Washington State and has offices worldwide. In mid-2011, Microsoft employed more than 90,000 people and achieved revenues of US\$69.9 billion in fiscal 2011.

Current offering

Microsoft has been a hosted email archiving provider since its acquisition of FrontBridge Technologies in 2005. Office 365, which is described as a cloud-based suite of office productivity tools, was launched in June 2011 as the successor to Microsoft's Business Productivity Online Suite (BPOS) of SaaS offerings. It comprises Exchange Online, SharePoint Online and Lync Online, as well as Active Directory Federation Services 2.0 with single sign-on capabilities, which can help in migrations. Its Exchange Online includes archiving capabilities and can be bought as part of the package or as a standalone product.

Office 365 uses the archiving capabilities that were added to the newest Exchange version, Exchange 2010, in 2009. The product essentially provides users with their own personal archive folders, which are managed through the Exchange database. E-discovery capabilities are somewhat basic, focused on search, with some further capabilities such as email monitoring and test compliance searches, role-based multi-mailbox search, legal hold and export. Support for email clients other than Exchange is limited and compliance requirements are only included in the enterprise edition or those tailored for specific enterprises.

There are a variety of licensing options for Office 365, including four enterprise versions that offer varying levels of functionality, with prices ranging from US\$10 per user per year to US\$27. There are two offerings for "kiosk" workers, priced at US\$4 per user per month for the basic version and US\$10 for the more advanced. There is also a version for small businesses priced at US\$6 per user per month that includes a single SharePoint site. Mid-sized businesses are advised to consider the enterprise versions.

Microsoft claims a global network of data centres. Its standard Office 365 products are provided in a multitenant architecture. However,

for organisations with at least 30,000 seats or for government agencies, Microsoft will offer a dedicated, single tenant implementation.

Microsoft has a very wide range of partnerships through which its products can be bought and many partners offer more advanced e-discovery and compliance capabilities by bundling Office 365 with their own products.

Market presence

Although Microsoft has had a hosted email archiving capability since 2005, it lacks recognition in this market. It has stepped up its capabilities with the inclusion of archiving in Exchange 2010, but the functionality is considered to be basic. However, many organisations are considering upgrading to Exchange 2010 and the archiving needs may be suitable for some, although specialist third-party options will likely to prove to be popular, with many vendors offering migration help for customers to Exchange 2010 and Office 365.

Strengths

For some small companies that do not have much in the way of regulatory or e-discovery needs, Microsoft's services provide basic email archiving capabilities at an affordable price. They have the same look and feel as familiar Microsoft products, making them intuitive to use.

Weaknesses

Microsoft's new Office 365 service is based on the archiving capabilities of Exchange 2010, which are considered to be more basic than those offered by more specialised competitors. For example, the ability to enforce archive and retention requirements for compliance are limited as users can over-ride the guidelines provided and institute their own policies. This makes it unsuitable for heavily regulated industries. Support is also limited to email. Many potential customers could do well to supplement Microsoft's offerings with those of a specialist provider based in the cloud.

As a US-based vendor, Microsoft's customers could find themselves subject to the requirements of US data gathering laws, such as the Patriot Act. Its BPOS cloud-based service has also experienced outages in recent years.

Overview of the major players

Mimecast

Mimecast was founded in 2003. Its headquarters are in London and it maintains offices in South Africa and the US. Designed from the outset as an integrated SaaS offering, Mimecast specialises in email archiving, continuity, security, policy management, data leakage prevention, e-discovery, and marketing and attachment management to provide a unified email management service in the cloud, with its services connecting to in-house and hosted email clients. Privately held, its latest round of funding of US\$21 million was received in January 2010. Mimecast was placed fifth in the Deloitte Fast 500 EMEA 2010 Ranking and CEO Survey, which showcases some of the region's most innovative and fast-growing technology companies. Mimecast has achieved revenue growth of more than 300% over the three years to the end of its last fiscal year in March 2011.

Current offering

Mimecast's email archiving service can be provided as a unified email management service, or as a standalone archiving service. It offers an enterprise version of its service, which provides a secure email gateway, content power tools, email continuity and archiving, with optional BlackBerry integration and advanced mailbox management features. It also has a version of its product, called Unified Email Management Express, which is focused on email threat protection and continuity, giving users uninterrupted access to both live email and 58 days of archived messages via Microsoft Outlook and Mimecast Webmail. This is aimed at organisations that have existing email archiving investments. Although its products work with all email servers, it has a particular focus on support for all versions of Microsoft's email offerings with its Mimecast Services for Exchange offering, which tightly binds Exchange to the Mimecast service, offering granular folder structure replication, stubbing and folder-based retention as key features.

Mimecast's archiving service is accessible by browser, BlackBerry mobile devices or Microsoft Outlook. It has a core focus on Microsoft's Outlook email client and offers a service specifically aimed at those organisations looking to migrate to Microsoft's new Office 365 hosted offering. A default period of ten years of emails can be searched through its archiving service.

For streamlining e-discovery processes, all emails are stored with associated attachments and metadata, including receipt and delivery versions and their transactional metadata for non-repudiation, what policies have been applied and any changes that have been made to the message, such as signatures or branding that have been applied to emails for chain-of-custody purposes.

Strategy

Mimecast is a specialist email archiving company and will continue to maintain its focus on this area. Continuing its focus of developing all products itself on one unified platform, Mimecast is currently working on extending its platform to all types of unstructured data in use in an organisation.

Mimecast offers its products direct to enterprises or through a network of partners, and services the SME market through its partners. It is currently looking to further build out its network of channel partners.

Market presence

Headquartered in the UK, Mimecast has a strong presence in Europe and in South Africa owing to its heritage in that country. It established operations in the US in 2008. It claims to have almost 4,000 customers, and is particularly well represented among law firms, servicing more than 60% of the top law firms in the UK. During fiscal 2011, Mimecast claims that its global user base grew from 556,000 to 906,000, and it saw revenues grow by 57%. Mimecast currently has around 250 employees.

Strengths

Mimecast is a specialist provider of unified email management services, the four pillars of which are security, continuity, archiving and policy management. All of its services have been built by Mimecast itself, rather than being acquired, and were built from the ground up as a SaaS offering. Designed to work as a single system, customers benefit from a single administration and management console that provides centralised policy control, reporting and auditing. User productivity is enhanced by the use of the familiar Outlook interface, which reduces the training time and user support required.

Overview of the major players

Mimecast's data centre infrastructure comprises a massively parallel grid infrastructure, with separate grids serving EMEA, North America, Africa and offshore Channel Island locations, each of which has multiple, inter-linked data centres. Its multitenant storage environment provides tenant isolation and encryption for ensuring confidentiality, integrity and availability.

Mimecast is one of the only email archiving vendors that provides guarantees as to the location where a customer's data is stored and has the data centre infrastructure necessary to do this. This is important for customers that do not want any data stored in the US owing to the fact that this may leave them exposed to information gathering legislation enacted by the US that allow the US government to seize data without notice. Its grid infrastructure means that a minimum of three copies of all customer data is guaranteed to be held within a particular jurisdiction in at least two local data centres, lowering inadvertent customer exposure to US laws. It also offers a unique encryption key for each customer to protect them in a multitenant environment, with access to those keys strongly controlled and limited. Emails are stored in a backend storage grid that is separate from the archiving application itself so that no data removed from the system on disks can be accessed except through the application.

Mimecast offers a strong SLA that guarantees 100% virus protection, 98% spam protection and 0.0001% spam false positives, and 100% availability, including via BlackBerry mobile devices. This availability means that email services continue to be provided through SMTP journaling even during a service outage owing to its real-time online queue management capabilities, providing access via Mimecast Web-mail mailboxes to 58 days of archived email as well as live email. It is the only vendor that can provide this service for always-on availability.

Weaknesses

Although it has had a presence in the US for the past three years, uncertainty over the future of the relationship with Iron Mountain following its acquisition by competitor Autonomy could leave it without a strong distribution partner in the US market. However, it claims to have grown its customer base in the US by 81% during fiscal 2011 and has a strong partnership with Microsoft.

Although support is planned for future releases, Mimecast currently does not support archiving of instant messages or SharePoint.

Overview of the major players

Sonian

Sonian is a privately held company that was founded in 2007 as a provider of email archiving services based on public cloud offerings, these being the Amazon EC2 virtual computing and S3 storage cloud platform at present. It is a pure SaaS offering.

In total, Sonian has received US\$14.6 million in funding, including US\$9 million in January 2011 in round B funding from venture capitalists, as well as Amazon and OEM partner Webroot. It intends to use the funding for further development of its archiving platform and for expanding its business. It has around 20 employees.

Current offering

Sonian's products have been built from the ground up, rather than having been acquired from other vendors, based on a mix of Web 2.0 frameworks, open source components and grid computing utility infrastructure so that there is no single point of failure. Emails are pulled from mail servers by Amazon EC2, which encrypts the data and stores it on Amazon S3, with Amazon SimpleDB being used to store metadata associated with documents. Sonian has developed proprietary technology for management functions and it has designed a secure web portal, hosted on Amazon EC2, through which users access data in the archive.

Known as Archive SA2, Sonian's email archiving service supports a range of email clients, instant messaging and social media. It plans to offer an email continuity service option during 2011.

Sonian offers an SLA with 99.99% uptime and a guarantee that all data is separated in customer-specific silos so that no data can be inter-mingled. Encryption is deployed for data in storage and in transit and the service allows administrators to set retention and purge periods. It states that it offers support for compliance with GLBA, SEC, FERPA, FRCP, SOX, HIPAA and FINRA regulations and also offers basic e-discovery capabilities that include legal hold, search, filtering, tagging and export. Data is replicated to eight data centres, separated into two clusters on the east and west of the US, with optional backup storage in a data centre in Europe. Encryption is provided for data both in storage and in transit.

Pricing for the Sonian service is low. It is available from Google Apps Marketplace for just US\$2 per user per month, including

unlimited storage. If customers wish to import old emails, there is an initial fee of US\$10 per gigabyte for importing legacy data into the archive. The price includes free phone, email or web-based support.

Strategy

Sonian describes itself as a "channel-based company" and its go-to-market strategy is through reseller partners such as Rackspace and Webroot. It is currently looking to expand its range of OEM partners and its strategy is for 80% of its revenues to be made through partners within a year's time.

Market presence

Sonian claims to serve more than 7,000 customers, which range in size from micro-firms to large enterprises, although it primarily targets SMEs. In September 2010, Sonian announced that it had expanded its customer base by 107% in the first nine months of 2010 and increased revenues by 147% over the same period in 2009. However, such high growth rates are due to the fact that it has only been in operation for three years.

Strengths

Sonian is one of the lowest priced services available on the market and is easy to set up and use. It states that leveraging Amazon's infrastructure allows it to keep capital expenditures low so that it can focus on product innovation. It will extend its reach further as it continues to build out the number of partners that are resellers of the service.

Weaknesses

Sonian's mailbox management is provided only for Novell GroupWise and it also focuses on Lotus Domino from IBM. This limits its brand recognition and makes it dependent on the fortunes of its partners. It also faces concerns from potential customers over the security of using public cloud infrastructure from providers that have themselves seen service outages. It states that it plans to deploy its service to other cloud providers in the future to overcome such obstacles.

Sonian states that all data is replicated to eight data centres divided into two clusters on the east and west coast of the US, with an optional backup data centre in Europe. This makes it less suitable for customers outside the US, who could see themselves facing legal challenges over the jurisdiction their data is held in.

Overview of the major players

Symantec

Symantec Corporation describes itself as a vendor of infrastructure software and services for addressing risks to security and system availability. It has its headquarters in California and has operations in more than 40 countries, employing around 17,500 people. A public company, Symantec recorded revenues of US\$6.2 billion in fiscal 2011, of which US\$2.3 billion were in its storage and server management division, of which its archiving and e-discovery capabilities are a part.

Symantec offers both on-premise email archiving technology, in the form of its Enterprise Vault product, as well as SaaS archiving services, which are the result of its acquisition of MessageLabs in November 2008. Its SaaS offering has recently been rebranded Symantec Cloud.

Current offering

Symantec offers a range of options for archiving and e-discovery for on-premise deployment, as a hosted solution, or a hybrid mix of the two.

Its first foray into this market was with its Enterprise Vault archiving platform for on-premise deployment for hosting via partners. It claims that this is the most widely deployed enterprise archiving solution. For a complete archiving and e-discovery deployment, additions are available for Enterprise Vault. These include Enterprise Vault Discovery Collector, which collects, assesses and de-duplicates unstructured data from file stores, network servers, and on desktops and laptops for indexing and adding to the archive. Enterprise Vault Discovery Accelerator provides search, preservation and review capabilities. The technology also works with Symantec's NetBackup and Backup Exec products, both of which support virtual machines. These latter two products are provided in partnership with Nirvanix. A third option has recently been developed that allows on-premise customers to leverage cloud-based storage.

The products support multiple email clients as well as instant messaging, SharePoint, file servers and databases; it provides access from mobile devices, and is aimed at archiving all unstructured information in an organisation. E-discovery features include legal holds and analytics tools for guided review of collected documents. The most recent release has

expanded support for more content types as well as archiving, now being driven by meta-data for needs such as non-repudiation and for maintaining chain-of-custody evidence.

The latest version—Enterprise Vault 10—was released in August 2011. Features added allow faster search, provide for more granular policies to be created for archiving and retention, and extend e-discovery to social media sites.

Symantec's cloud-based service came through its acquisition of MessageLabs in 2008, now rebranded Symantec Cloud. Since the acquisition, Symantec has made investments to expand its product portfolio with archiving, provided through a partnership with LiveOffice, and endpoint protection capabilities, which have been added to the existing web security, email security, email encryption, email management and instant messaging services. Additional data centres have been established and more resources have been added to develop and support the business.

Its cloud service has recently been rebranded Symantec Enterprise Vault.cloud. It works with a range of email clients that include Microsoft Exchange, Lotus Domino and Sendmail, as well as supported Microsoft Office and PDF attachments, and provides support for mobile devices. For security, all messages are encrypted, which can be customisable according to policies set by the organisation, based on Transport Layer Security protocols to encrypt the whole email connection. All messages are stored in redundant offsite data centres and the service supports e-discovery and compliance needs such as legal holds, and collaborative review and categorisation to help cull large volumes of email. Enterprise Vault Mailbox Continuity.cloud is available as an optional extra through a partnership with Dell MessageOne to facilitate high availability by providing a failover system that is activated in minutes when needed so that service is disrupted for only a short period of time in the event of an outage. There is also a service aimed specifically at the healthcare sector—Symantec Health Safe—that allows for the archiving of medical images.

The SLA offered for the Symantec Cloud service guarantees 99% anti-spam effectiveness, 0.0003% false positives, 0.0001% anti-virus accuracy, 100% email service availability and

Overview of the major players

email scanning within 60 seconds. Money back remedies are offered if these targets are not met, although Symantec publishes data that shows that the targets are routinely exceeded. For archiving, 99.9% uptime is guaranteed.

Strategy

Symantec's strategy is to provide a complete end-to-end solution for archiving and e-discovery, collecting all unstructured information in the enterprise and providing technology for streamlining all processes that make up the electronic discovery and records management model (www.edrm.net). In line with this, it has continued development of both its on-premise and cloud-based offerings and acquired Clearwell Systems, an e-discovery specialist, for US\$390 million in 2011. According to Symantec, this was a strategic move designed to provide it with an end-to-end EDRM solution to compete more effectively with companies such as EMC and IBM and it carefully considered its choices as the intention was to make only one acquisition, not multiple. It has announced that it expects to release a suite of integrated products, combining its existing capabilities with those of Clearwell Systems, in the first half of 2012. The intention is to retain the Clearwell brand name owing to its widespread recognition in the legal sector. Examples of what this integration will bring include search-in-place technology for e-discovery archives, using backup software for legal holds, and bringing metadata about file creation and ownership into Clearwell data sets.

Symantec has stated recently that further development of SaaS cloud-based services is a key priority for it and its intention is to develop these services into a US\$1 billion business. It will continue to expand its portfolio, which includes archiving, endpoint protection and on-line backup, is looking to expand its channels to market and is investing in a next-generation portal and architecture.

Market presence

Symantec's Enterprise Vault and associated products are aimed primarily at the enterprise space and are used by more than half the Fortune 100, although the vendor claims to also have SME customers. For its Enterprise Vault product, it states that more than 16,000 organisations use its archiving and e-discovery solutions, translating to more than 31 million users. It also claims 21,000 customers of its cloud services range from small businesses to large enterprises. The Symantec Cloud

infrastructure spans four continents and comprises 14 data centres and two network operating centres.

Strengths

Symantec is a large, well-resourced technology vendor that is particularly well known in the enterprise space. Its on-premise solution provides an integrated solution supporting email and other content archiving, mailbox management, automated categorisation of records and e-discovery. It also provides a cloud-based solution for smaller companies in particular and for geographically dispersed organisations. Integration of these two capabilities will allow organisations to choose a hybrid option should they wish this. Its e-discovery capabilities will be enhanced in 2012 with the release of solutions integrating technology from the newly acquired Clearwell Systems. Figures provided by Symantec show that it regularly exceeds guaranteed service levels for its cloud-based offering.

Weaknesses

The majority of Symantec's products were acquired, starting with Enterprise Vault, which came with its acquisition of Veritas in 2005, whilst others are provided through partnerships, which could leave it with gaps if the terms of those partnerships change or its partners are acquired. This strategy means that it offers bundled, rather than unified, solutions that were developed by multiple suppliers or provided through partnerships. Symantec also has much further integration to do owing to its recent acquisition of Clearwell Systems.

Symantec still requires further development of its e-discovery capabilities to better compete with pure-play vendors in particular. Its cloud-based services have only been developed fairly recently and it is better known in terms of such services for its email security and web security services. Its on-premise technology is complex and takes time to implement. Symantec's own deployment to 17,500 employees took four months to compete.

Data reference section

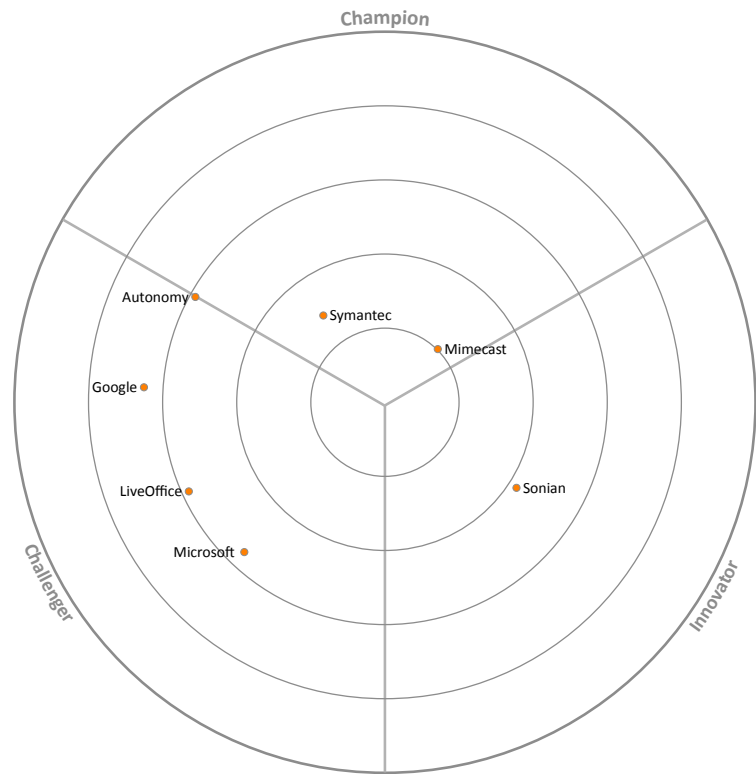


Figure 1: the vendor landscape

The information used in making these evaluations has been drawn from a variety of sources, including published and unpublished sources. Technology and service providers have been evaluated for their capabilities in offering email management, archiving, security, continuity and e-discovery services. The evaluations take into account their financial stability, brand and market share, their current offerings in this market sector and future direction, market presence, and perceived strengths and weaknesses. The information provided does not constitute a direct endorsement of any of the organisations. Where the diagram is concerned, the closer to the centre the vendor is positioned, their offerings are considered to be the most fit for the purpose intended.

Summary

The market for email archiving is showing fast growth owing to the need to control risk and increase productivity in organisations, where email has become an essential business collaboration and communications tool. It is also an essential capability for meeting litigation where requests are made for electronic documents to be provided as evidence, of which emails are an important part, as well as for complying with the records retention requirements of a host of governmental and industry regulations.

Not all email archiving systems or services are equal. Among the differences is the way that they are delivered, catering to the varying needs of different types of organisations. When selecting a system or service, it is essential that more than just basic archiving is provided, such as ancillary products and services for managing needs such as those related to e-discovery.

Further Information

Further information about this subject is available from
<http://www.BloorResearch.com/update/2108>

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Fran Howarth Senior Analyst - Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.



Copyright & disclaimer

This document is copyright © 2011 Bloor Research. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



2nd Floor,
145-157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com