

I D C V E N D O R S P O T L I G H T

Using a Hosted Service for Holistic E-Mail Management

October 2008

Adapted from *Worldwide Messaging Security 2008–2012 Forecast and 2007 Vendor Shares: Forecast Looks Cloudy*, by Brian Burke IDC # 213571; and *Worldwide Email Archiving Applications 2007–2011 Forecast and 2006 Vendor Shares: Storage Optimization, Mailbox Management, and Records Retention for eDiscovery and Compliance Drive Investments*, by Laura DuBois, IDC # 206729.

Sponsored by Mimecast

Organizations are increasingly beset by policy, regulatory, continuity and security requirements for their data. This is particularly applicable for email, which has become the primary communication and collaborative platform at many organizations. To meet the demands imposed by regulatory requirements – while protecting themselves against litigation-related discovery requests and safeguarding their networks against security breaches – organizations are turning to email management and other messaging solutions that provide functionality for archiving, business continuity and security. According to IDC, the market for email archiving applications alone was \$703 million in 2007, a 34% increase over the prior year's revenues, and IDC estimates that 2008 revenues will approach \$900 million.

The Need for Email Management Solutions

Increasingly complex messaging requirements characterized by worldwide regulatory, compliance and archiving issues in addition to longstanding security concerns are driving the adoption of holistic email management “from the cloud.” Holistic email management solutions from the cloud are hosted services that integrate messaging management with archiving, business continuity and security components. According to IDC, the market for hosted messaging security services will increase from \$443 million in 2007 to nearly \$1.750 billion in 2012, representing a compound annual growth rate of 31.6%. IDC estimates that in many cases, 50–70% of unwanted messaging traffic can be stopped in the cloud before it enters the corporate network. (Cloud-based software, as well as software-as-a-service (SaaS) and hosted messaging security are essentially variations of the same thing; such software is characterized by the software, services, and support offerings that are specifically built and designed for one-to-many delivery over the Internet.) Such integrated solutions are becoming increasingly necessary for many organizations: Since governance, risk management and compliance are intrinsically linked, organizations are looking for messaging solutions that integrate the policy enforcement, hygiene, continuity, retention and discovery issues related to email.

In such a complex and intertwined environment, mitigating messaging risk is no longer just a matter of filtering out spam and malicious code such as viruses, Trojans and worms. At many organizations today, email is the most important messaging application and collaboration platform; typically these organizations no longer deploy email servers to handle email per se – they build complex email infrastructures that are designed to handle numerous regulatory and compliance-related activities such as the enforcement of corporate policies and procedures, archiving data for legal purposes, and as a platform for ensuring business continuity in the event of a disaster.

In effect, messaging solutions need to be much more multi-dimensional and comprehensive. Concerns with data loss prevention and regulatory compliance are driving the need for more

complete messaging solutions that secure both inbound and outbound messaging traffic. In a survey, IDC found that over 25% of respondents said that a leak of confidential data cost them more than \$100,000. In addition, legal requirements – particularly the rules pertaining to the discoverability of electronic information (known as eDiscovery), and legislation mandating data privacy and integrity – are creating mandates for organizations to closely examine their archiving practices and implement messaging solutions accordingly. According to IDC, among the drivers fueling adoption of email archiving are legal eDiscovery, compliance with regulations stipulating record retention and overall mailbox management.

Archiving as the Foundation for Effective Email Management

As email has increased in importance and pervasiveness, archiving email is becoming particularly important. The ability to search retained email files is critical for organizations in terms of compliance, eDiscovery, collaboration and maintaining both the lowest possible recovery point objectives (RPO) and recovery time objectives (RTO) for email. Consequently, organizations need to address the three main components of messaging as they relate to archiving, business continuity and security in a cohesive and coordinated manner. While the exposure of confidential information is now the single greatest threat to enterprise network security according to IDC, organizations that don't archive email and its associated attachments with their potential discovery in mind are leaving themselves open to tremendous litigation risks. Compliance to legislation and bullet-proofing against litigation requires a deliberate approach to archiving email, one that meets retention requirements, supports corporate usage policies, satisfies end-users' information management needs, and provides evidentiary-quality data that ensures chain of custody.

Email is also a critical tool during business continuity incidents where it is often the most effective method to coordinate a distributed workforce and provide updates to help settle the nerves of staff under duress. It is essential that RPO and RTO of email infrastructures be kept to a minimum; building effective email contingency plans for environments with multiple point solutions can be complex and expensive, leading organizations to deploy cloud-based solutions as an alternative. An organization is most vulnerable during an outage, but with an integrated approach, the organization is still able to deliver continuity of policy enforcement, security, data leak prevention, and compliance, in addition to email.

IDC has also identified corporate email as the primary source of data leaks. Traditionally, organizations have deployed data leak prevention (DLP) solutions that often operate in isolation from other messaging-related solutions. Consequently, at organizations where email has become the most pervasive collaborative tool, such a siloed approach may lack the necessary flexible policy controls and investigatory capabilities to effectively manage and contain data leak incidents. Many DLP solutions examine only outbound connections, searching primarily for key loggers, breaches of disclosure policy or social engineering-based attacks, while lacking the ability to detect inbound threats to data leakage such as Trojan horses containing key loggers. Since an archive is critical for investigating whether data leaks are malicious or accidental, as well as to provide quality evidence for disciplinary or legal action, many organizations find that it makes sense to deploy holistic email management solutions.

Messaging solutions require sophisticated IT people with an understanding of “3S” — the convergence of security, storage, and systems management. Maintaining point solutions for archiving, business continuity and security can often stretch IT resources by requiring more administrative tasks, the maintenance of multiple skill sets, and fragmented administrative interfaces.

Business users have their own information needs – such as quick and ready access to historical email messages and their related attachments – that are often at odds with messaging management solutions. In addition, some email management solutions may require end users to access more than one system to search for the information they need. With some traditional on-premise email

management solutions, ensuring both security of the maintained email as well as maintaining the continuity of the archive may limit storage for data such as email.

Benefits of a Holistic Approach to Email Management

For customers in both the SMB and enterprise markets, cloud-based email management and messaging solutions offer significant benefits over on-premises solutions.

Typically, software-as-a-service or SaaS-based solutions require low administrative overhead, and can result in “green” benefits such as reduced power consumption, floor space, etc. With a SaaS-based approach, there is also a reduced need for training internal IT staff, particularly in terms of 3S skills. In addition, solutions available in a SaaS model are more rapidly deployed and often more flexible than on-premises solutions.

SaaS services also focus on the business deliverables, abstracting from the organization the day-to-day management of the underlying technology.

Most important, however, is the holistic approach that a cloud-based email management and messaging solution addresses that typically includes the following components:

- Storage: Archiving, off-site backup, and recovery
- Information management: Consolidated storage and retrieval with centralized categorization for unstructured data. This is important in legal use cases involving eDiscovery in which email is used as evidence. In these situations, it is critical that the "chain of custody" of email messages and related attachments can be verified in order to ensure the evidentiary quality of data. A more commonplace situation where this feature is important is in the accurate quarantining of spam from legitimate email messages, allowing end users to quickly locate relevant messages.
- Continuity: Failover, continuity, and backup for in-house email in the event of a system failure or disaster
- Security: Message receipt/delivery, virus scanning, and content filtering
- Policy: Enforcement of corporate policies such as attachment, disclaimer and acceptable use.

Market and Technology Trends

Email management and messaging solutions are available as both an on-premises software or from the cloud in a SaaS-based model.

According to IDC, the market for email management solutions continues to be competitive among the established players, while new entrants also enter the market. Large, well-established vendors are seeking to move downmarket and transition from a focused to a broader product strategy and mailbox management use case. Smaller, innovative SaaS pure-plays continue to gain market traction, particularly in the SMB space. IDC finds that the movement toward cloud computing and online services such as archiving is significant.

Another factor driving holistic, cloud-based solutions are users themselves. User acceptability is a large barrier to effective messaging solutions; the more individual components the user has to deal with the more they will attempt to circumvent the controls, often leading to breaches of policies and procedures. In addition, during business continuity scenarios where employees are already stressed, trying to remember how to use unfamiliar tools can be a contributing factor to ineffective business continuity planning efforts.

Considering Mimecast

Mimecast is a privately-funded global provider of SaaS-based email management products and services. Founded in 2002, Mimecast spent the first two years building its services and perfecting its platform infrastructure prior to launching into the market. The company's products and services address end-to-end email management issues and include features that address archiving, business continuity, and security. By offering email management in a SaaS model, Mimecast provides customers with email management solutions that do not require hardware, software or capital expenses.

Mimecast employs 140 people, and has 2,000 customers in Europe, North America, Africa, the Middle East and offshore. The company has experienced year-on-year revenue growth of 300%.

Mimecast offers a total end-to-end solution for managing email through its entire lifecycle; the company says its products are available for a cost similar to many point solutions addressing only one single area of email management such as archiving for example. In addition, Mimecast says that the reduced risk and management costs that its SaaS-based products provide can result in additional financial benefits.

According to Mimecast, its products and services allow customers to take an incremental approach to end-to-end email management. Customers can start with email archiving as a service and add rich email management services (e.g.: routing, security, policy control, and continuity) as needed with minimal disruption as the services are already pre-integrated into Mimecast's offering. Mimecast also offers integration with LAN based systems such as Microsoft Outlook and Microsoft Exchange that is designed to provide end users with a seamless experience.

Mimecast provides a solution designed to tackle organizational issues related to corporate governance, risk mitigation and regulatory or legislative compliance of email. The company's solution can be deployed in a manner that is transparent to the end-user business units and staff. According to the company, the Mimecast platform was designed backwards after considering the governance, risk and compliance requirements for email. The considerations for messaging security and the inherent requirements to retain and store email with confidentiality, integrity and availability were all factored into the design of the Mimecast platform. According to Mimecast, its solution can protect organizations against 99% of spam.

The company's technology utilizes a parallel grid distributed filing system based on a parallel computing grid similar to that used by Internet search engines, but optimized for email storage. According to Mimecast, the platform not only provides storage with strong chains-of-custody, it also offers greater performance than even on-site technologies based on state-of-the-art storage arrays.

The company is primarily targeting customers with between 500 and 5,000 seats, although its technology is being used by customers with upwards of 10,000 seats.

The key features of Mimecast's on-demand email management solution include the following:

- Data retention and eDiscovery
- Business continuity
- Advanced email security
- Visibility and reporting

According to Mimecast, its email management service for 5,000 seats is priced at approximately \$6.00 per user per month.

Challenges

Mimecast does face numerous challenges in the highly competitive market for email management and messaging solutions. The company needs to achieve brand recognition among potential customers and channels in the United States. One way Mimecast can do this is by developing a needs-assessment model to help customers decide on the cost-effective blend of its products and services.

As a provider of a SaaS-only solution, Mimecast has to sell the concept to channel partners, and therefore needs to focus on building a solid margin story for them. Mimecast also has to competitively position itself against other email management and messaging solutions vendors that are already well-established in the United States.

Conclusion

Faced with increasing regulatory, continuity and legal requirements, as well as an onslaught of spam and malware, organizations need to take a more comprehensive approach to messaging solutions, particularly in regards to email management. Specifically, organizations need to adopt a more holistic approach to email management that encompasses archiving, continuity and security. Since most organizations rely heavily on email for their communication and collaboration needs, managing email effectively – both in terms of employee productivity, and compliance and legal needs – is critical.

Increasingly, effective email management solutions provide a holistic approach that encompasses the related issues of archiving, business continuity and security. Such an approach mitigates the compliance, legal and security risks that email often unwittingly introduces to an organization, while minimizing the impact on an internal IT department.

IDC believes the market for cloud-based email management and messaging security solutions will continue to grow, and to the extent that Mimecast can address the challenges highlighted in this paper, the company's SaaS-based email management services has a significant opportunity to resonate among customers in the market.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street, Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com