Exchange

Meet compliance needs with Microsoft Exchange

As the volume and importance of digital information grows, regulatory compliance schemas are broadening to encompass an ever-larger share of data that companies use and produce. A wide variety of businesses must consider compliance-related issues such as immutable email archiving, eDiscovery, and Data Loss Prevention (DLP) when planning their email infrastructure. Relevant regulations include the following:

The Sarbanes-Oxley Act requires publicly traded companies to control, protect, and retain financial data and related files—a regulation that is widely interpreted to include email.

The Gramm-Leach-Bliley Act requires financial institutions to safeguard clients' private information.

The Health Insurance Portability and Accountability Act requires that healthcare organizations adopt medical information security, privacy, and data standards to protect patient information.

The Federal Rules of Civil Procedure require organizations to be able to retrieve electronically stored information—including email—in a timely manner upon request during litigation.

68%

of companies send sensitive data via email.

Meeting compliance requirements related to email would be challenging under any circumstance, but it is even more so in light of the explosive growth in email volumes. In 2011, according to the International Data Corporation (IDC), more than 1.8 zettabytes (trillion gigabytes) of data were created and replicated[1]—almost an order of magnitude higher than in 2006, just

[1] Digital Universe to Add 1.8 Zettabytes in 2011, 2011, EMC, http://www.datacenterknowledge.com/archives/2011/06/28/digital-universe-to-add-1-8-zettabytes-in-2011/

©2013 Microsoft Corporation. All rights reserved.

five years before. According to the same study, enterprises have liability for up to 80 percent of that data. A survey conducted by Harris Interactive in March of 2012 showed that 68 percent of companies send sensitive data via email.[2]

IT managers need to comply with industry regulations by preserving data in a way that is both immutable and accessible. In addition, they must also deal with the risk that users will unintentionally create data leaks, typically due to a lack of awareness or education. For example, in April 2012, a physician at the University of Arkansas for Medical Sciences emailed a document containing the un-redacted personal financial information of 7,000 patients to an outside party.[3] Businesses need tools that can prevent this type of common but potentially disastrous error.

While the responsibilities of IT professionals grow, their relative numbers dwindle. Worldwide, data is expected to grow 44 times over the next 10 years, whereas the number of IT professionals will less than double. At the same time, one survey shows that a majority of attorneys expect the number of eDiscovery matters they handle and the costs of those matters to increase.[4] Given the increased compliance demands, it is becoming the responsibility of all IT professionals to actively manage security needs. Microsoft understands and addresses these challenges. The data protection and archiving features of Exchange are designed to help IT professionals meet compliance challenges in a world where the volume of email data continues to grow. Exchange also enables them to delegate compliance responsibilities to the right people—without granting unnecessary administrative privileges—via Role Based Access Control (RBAC).

These new and improved features include:

- Cloud-based email hygiene with Exchange Online Protection
- DLP technology to identify, monitor, and protect sensitive information
- In-place email archiving, hold, and native data governance to preserve email as long as necessary
- Advanced, easy-to-use eDiscovery tools to locate information in the organization, with advanced delegation capabilities through RBAC
- Integration with SharePoint for safe team collaboration with site mailboxes

Move email protection to the cloud with Exchange Online Protection

Exchange Online Protection (EOP) is the Microsoft cloud-based email protection service, which works with Exchange on-premises and online. Companies using Exchange Online Protection no longer have to worry about the disparity between data volume and staff available to manage it. They also benefit from email protection that is continuously updated to deal with present and emerging threats. Microsoft security researchers constantly monitor spam, phishing, malware, and network attacks globally—and update EOP to protect against them. The EOP service uses a sophisticated multi-engine malware detection approach to catch viruses and spam messages before they are delivered. This is critically important, because, according to one study, more than two-thirds of intentional corporate data breaches involve malware.[5] Even the most security-conscious companies would find it difficult to maintain the level of security vigilance, innovation, and virtually unlimited scalability EOP provides.

[2] Sharing Sensitive Information via Email..., 2012, TechJournal, http://www.techjournal.org/2012/03/sharing-sensitive-information-via-email-ftp-poses-enterprise-challenges/
[3] Top 10 Data Breaches Include Public Health Departments, 2012, Government Health IT, http://www.govhealthit.com/news/top-10-data-breaches-include-public-health-depts?page=0,1
[4] 2011 Cost Savings and Challenges in E-Discovery Survey, 2011, The Huron Legal Institute, http://www.huronconsultinggroup.com/library/2011-challenges-e-discovery.pdf
[5] 2012 Data Breach Investigations Report, 2012, Verizon, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

©2013 Microsoft Corporation. All rights reserved.

To keep customers' email available 24/7, EOP uses a globally load-balanced network of data centers to provide five nines (99.999%) network uptime. The service can actually increase email reliability by queuing email for up to five days, thereby eliminating bounces if on-premises email servers go down. EOP is also highly scalable: when organizations grow, the service grows with them, seamlessly.

Moving email hygiene to the cloud also has a number of operational benefits. Microsoft designed EOP to help customers offload the costly, repetitive, and unproductive aspects of email protection such as purchasing and servicing hardware, applying software updates, and managing network connections. At the same time, EOP gives customers control over what really matters to their businesses. Organizations can set specific filtering rules and policies through an easy-to-use, web-based administration tool. Exchange Online Protection also delivers comprehensive reporting, auditing, and message trace capabilities.

Companies using Exchange Online Protection no longer have to worry about the disparity between data volume and staff available to manage it.

Use sensitive data safely with Data Loss Prevention technology

Any business that handles personally identifiable information (PII), financial data, intellectual property, or other sensitive information in the daily course of business is likely to be subject to compliance requirements. These organizations need ways to use sensitive information appropriately, keeping it safe without affecting worker productivity. Data Loss Prevention technology in Exchange uses deep content analysis to identify, monitor, and protect sensitive information. Exchange includes dozens of ready-to-use DLP templates based on common regulations from ten countries in areas such as healthcare, PII, financial data, and more. Independent software vendors can also build specialized policy templates that can be imported into Exchange. In addition, Exchange administrators can easily create DLP policies in the Exchange Administration Console.

DLP policies can include rules, actions, and exceptions, and use the full power of Exchange transport rules. Upon identifying sensitive information, DLP technology can automatically take action, such as applying Information Rights Management protection, appending a disclaimer, generating an audit log, sending the message for moderation, or preventing a message from being sent.

DLP technology works with a new feature called Outlook Policy Tips that informs users of a potential policy violation before it occurs. Policy Tips aid users to identify sensitive data in emails and educate them about related company policies. This ongoing education helps users manage data appropriately and avoid sending sensitive data to unauthorized users.

Manage data with large mailboxes, in-place archiving, and retention policies

With growing volumes of email data, organizations used to face a difficult choice: keep email archives on slow, expensive, third-party archiving systems, or limit the amount of historical email available to users. With Exchange, organizations can provide users with large mailboxes and keep archived and current email data in one system through in-place archiving

©2013 Microsoft Corporation. All rights reserved.

technology. This provides a number of advantages. Users get a best-in-class, full-fidelity email experience with archived mail, almost identical to what they experience with their primary mailbox. They no longer have to waste time managing their inboxes to stay within quotas, and they also don't need to store messages in .PST files outside the control of Exchange administrators and backup policies.

With Exchange, IT administrators have the flexibility to balance fast storage performance and low-cost scalability targeted to business needs. They can manage and search archived and current email through the unified Exchange interface, and no longer need to deploy and maintain a separate archiving infrastructure. The unification of primary and archive email stores also means they have one centralized place to manage compliance and retention.

With large mailboxes, organizations need efficient, automated ways to manage message retention and expiration. Exchange provides easy-to-manage policies for controlling how long messages are kept, so users do not have to worry about it. Retention policies can apply to messages, folders, or even entire mailboxes. Organizations can achieve all these benefits for Exchange archives on-premises or in the cloud using Exchange Online Archiving.

With growing volumes of email data, organizations used to face a difficult choice: keep email archives on slow, expensive, third-party archiving systems, or limit the amount of historical email available to users.

Make data tamper-proof with in-place hold, and search efficiently

A key element of email compliance is the ability to capture and store email immutably. At one time, virtually the only way to enforce immutability was through journaling—basically, forwarding email to a special, separate archive deployed and managed independently from Exchange. Many organizations enforce immutability using write once, read many (WORM) storage, which can be expensive and makes eDiscovery more time consuming. Today, Exchange makes immutable archiving simple with in-place hold technology. Now, an IT administrator can easily place a group, a user, a mailbox, or even individual items on hold from the Exchange Administration Console. When a held item is deleted, purged, or altered, Exchange keeps a copy in a folder that is invisible to the user but subject to eDiscovery. Unlike WORM storage, which simply stores copies of messages, Exchange captures and preserves all edits to items at a granular level regardless of whether the action was performed by a user, an administrator, or even an automated tool.

Timely eDiscovery is crucial to an effective compliance program. Since Exchange can keep archived and active email data in one system, it makes searches easy. Authorized personnel such as a compliance officer can search across Exchange, SharePoint, and Lync from the intuitive, web-based eDiscovery Center. Searchable items include email, instant messages, calendars, and contacts, as well as SharePoint documents, sites, file shares, blogs, wikis, and more—all from one straightforward interface.

©2013 Microsoft Corporation. All rights reserved.

Exchange

For greater efficiency, IT administrators can use role-based access control to delegate search, hold, retention policy management, and HR/legal personnel audits without providing full administrative privileges. Finally, auditing capabilities built into Exchange can record configuration changes and compliance activities.

Timely eDiscovery is crucial to an effective compliance program.

Audit logs can be used to prove due diligence and, if necessary, pinpoint tampering by an administrator. This makes Exchange more secure and less volatile to corruption.

Collaborate while maintaining compliance with site mailboxes

With site mailboxes, Exchange works in conjunction with SharePoint to give users the ultimate collaboration tool, while keeping data safe. In a site mailbox, members of a SharePoint site can access project emails and documents in a central location—from Outlook on the desktop or the SharePoint site itself. Users view site mailbox emails just as they would any other Exchange message, while SharePoint enables versioning and coauthoring of documents. Site mailboxes can be searched using the Exchange eDiscovery Center, and all emails and documents stored in the site mailboxes can be put on legal hold. Additionally, site mailboxes adhere to the life-cycle policies applied to the SharePoint site with which they are associated.

Transform email data from a challenge to an asset

Exchange helps organizations maintain compliance while reducing costs, improving security, and boosting employee productivity. Businesses can move email hygiene to the cloud with EOP, stopping viruses and spam before they get close to the company's network. New DLP technology enables organizations to work with sensitive information safely, and helps everyone better manage data risk. In-place archiving and large mailboxes eliminate the need for third-party archives. Built-in eDiscovery functionality makes it easy to find needed information across email (held, archived, and current), documents, and other data types. By integrating all of these data protection features into one system, Exchange greatly simplifies IT infrastructure and helps reduce costs, allowing organizations to manage compliance issues efficiently and employees to use email without fear of sending sensitive information to unauthorized people.

Learn more

- Learn more about Advanced Email Security
- Try Exchange Online or evaluate Exchange Server 2013
- Take a deep dive into Simplified Archiving and Faster eDiscovery
- Learn more about Data Loss Prevention (DLP) and Protection

©2013 Microsoft Corporation. All rights reserved.