

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

**FACILITATING EMAIL DISCOVERY & PRODUCTION
WHITE PAPER**

Dell | Modular Services

www.dell.com/modularservices



ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

OVERVIEW

Email is the most widely used method of business communication. Throughout all organizations – corporate planning, product development, sales, legal, and finance – sensitive information is being sent by email. An overwhelming number of users send and store sales proposals, marketing plans, competitor profiles, contracts and intellectual property via email. In many companies, email has become the enterprise filing cabinet – it's the place where individual workers store and organize, their personal work communications and files.

When companies are sued, electronic data such as email is the first target of legal discovery. With increases in the frequency of major lawsuits and the volumes of electronic data, e-Discovery is becoming a major headache for most organizations. According to Fulbright's 2007 Litigation Trends Survey, 60% of the average company with more than \$1 billion in annual revenue is currently facing at least one law suit with more than \$20 million at stake. Even one in three of the average mid-sized companies, with \$100-\$999 million in revenue, are currently facing at least one lawsuit of that magnitude. Nearly 40% of the largest companies spend over \$5 million annually on litigation.¹ As data volumes continue to double every few years, the proportion of legal costs allocated to discovery continues to rise at an alarming rate.

Often referred to as e-Discovery, Electronic Discovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. In the process of electronic discovery, data of all types can serve as evidence. This can include text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites, and computer programs. Even malware such as viruses, Trojans, and spyware can be subpoenaed and investigated. Electronic mail (email) and instant messages (IM) are viewed as less formal correspondence than written memos and letters and become an especially critical source of evidence in civil and criminal litigation.

For most organizations, email search and retrieval is the costliest, most time-consuming, and most difficult e-Discovery task. A company with 1,000 employees will likely produce as many as 100,000 email messages every business day. Once messages are sent, they are stored on servers, backup tapes, and individual users' computers where they typically remain for years. When companies are sued in the United States, they will be required to search through all email messages for relevant communications and documents. In the case of *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, email from more than 700 employees were requested. The email had been saved to 93 back up tapes and cost the organization six months and \$6.2 million to restore.² According to Gartner, IT departments in companies with five or more \$1 million plus cases per year should budget at least \$500,000 and one full time equivalent for e-discovery this year.³

Proactive management of information remains the goal of many organizations. In their annual survey, Fulbright and Jaworski state that:⁴

- 60% of companies surveyed with more than \$1 billion in annual revenue is currently facing at least one law suit with more than \$20 million at stake
- Nearly 40% of the largest companies spend over \$5 million annually on litigation.
- Despite good intentions, 27% of U.S. companies believe that the new federal rules on e-Discovery have made the problem of managing e-Discovery issues during litigation more difficult.
- Over half of the companies surveyed had at least 6 law suits pending; 13% had over 50
- The industries most frequently targeted were insurance, energy, and construction followed by banking and financial services.
- Regulatory litigation ranked third in the top litigation concerns of corporate counsel.

With lawsuits becoming more of a certainty, senior executives are mandating changes in the way that organizations store electronic data and comply with e-Discovery requests.

¹Fulbright and Jaworski, "2007 Litigation Trends Survey."

²*Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 U.S. Dist. LEXIS 3196, 52 Fed. R. Serv. 3d (Callaghan) 168 (E.D. La. Feb. 19, 2002).

³Gartner, "E-Discovery: Project Planning and Budgeting 2008-2011," Debra Logan, John Bace, February, 2008.

⁴Fulbright and Jaworski, "2007 Litigation Trends Survey."

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

THE REVISED FEDERAL RULES OF CIVIL PROCEDURE (FRCP)

While a variety of prominent court cases over the last decade have established the need for email discovery and production, recent changes to the Federal Rules of Civil Procedure have codified the specific requirements for electronic discovery.

The Federal Rules of Civil Procedure govern the conduct of all civil suits brought in Federal district courts. While they do not universally apply to state courts, many states have implemented their own e-Discovery requirements based on the FRCP rules. Consequently most organizations create policies in compliance with these rules.

On December 1, 2006, the FRCP were revised with the addition of new amendments that govern the collection and production of evidence. These new amendments must be adhered to when producing all types of evidence, including electronic materials. In fact, several of the amendments directly impact email management. Rules of note include:

Table 1: Federal Rules of Civil Procedure Requirements Governing e-Discovery

Rule Number	Summary	Ramifications
Rule 26(a)	States that electronically stored information is discoverable.	Counsel must be prepared to produce all relevant e-documents.
Rule 26(f)	Parties must meet early in the process to discuss e-discovery issues	Need to be able to identify early on what they can and cannot produce. Accuracy is important, as the court will require counsel to meet their discovery commitments.
Rule 26(b)(2)	Provides guidelines on when cost or effort can be used to justify not producing an e-document.	Effective email management must be in place to allow you to quickly determine if there are e-documents that you can only retrieve at great cost or effort.
Rule 26(b)(5)	Limits the damage caused when privileged information is inadvertently provided to opposing counsels.	Allows counsel to be thorough in the sharing of information and still have a safeguard to protect the organization.
Rule 37(f)	Addresses the loss of evidence through routine email purging.	Must be able to illustrate purging policy and demonstrate compliance with all rules requiring the safeguarding of evidence.

This table reflects Dell's view of compliance with the statutes and standards as of July 20, 2008 and may be superseded by changes in the statutes/standards. This information is not intended as legal advice and may not be used as such. Nor does this information reflect a full and exhaustive explanation of all relevant statutes and standards. You should seek the advice of your own legal counsel on any legal compliance questions.

This table reflects Dell's view of compliance with the statutes and standards as of July 20, 2008 and may be superseded by changes in the statutes/standards. This information is not intended as legal advice and may not be used as such. Nor does this information reflect a full and exhaustive explanation of all relevant statutes and standards. You should seek the advice of your own legal counsel on any legal compliance questions.

The stakes of litigation are very high and the FRCP dictates the rules of engagement for electronic discovery. Organizations that are unable to comply with these rules may be penalized in court and may risk fines, or even worse, unfavorable court rulings. Companies that are able to effectively manage electronic evidence will have a strategic advantage in their litigation efforts.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

THE ROLE OF EMAIL RETENTION AND ARCHIVING IN MANAGING E-DISCOVERY

Electronic documents usually far outnumber paper documents and are much more difficult to recover due to their volume, backup and retrieval methods, and restoration costs. While discovery of electronic media can be simple and cost-effective if the information is stored in a searchable format, most organizations have not taken the necessary steps to organize and manage digital information in a way that provides for rapid retrieval. In fact, the cost and difficulty of producing e-documents has led some opposing counsels to begin using e-Discovery as a legal tactic, increasing their e-Discovery requests to place financial and hardship burdens upon defendants.

While there are many types of electronic documents – email messages, digital transaction records, web pages, spreadsheets, databases, etc., email is uniquely challenging when it comes to e-Discovery. A typical 1,000-person company may have hundreds of millions of messages stored across hundreds of computers and tapes in many different locations. With the FRCP, it can be difficult to comply with email discovery requests without a centralized email archive and sophisticated tools for e-Discovery search and retrieval.

The e-Discovery savings from one major lawsuit can fund an email archiving initiative. With the average billion-dollar company facing more than 50 new lawsuits each year,⁵ companies are seeing the cost benefits of centralized email archives and are rapidly adopting them. When correctly implemented, these archives provide direct access to all email messages sent and received within the company's stated retention period.

HOW TO CHOOSE AN EMAIL ARCHIVE

When choosing an email archive solution, there are countless numbers of options to wade through. Narrowing the options down will save you hours of research and ensure that you ultimately select the solution that meets your needs and accomplishes your goals. While archive evaluation is complex, it should begin with five key questions:

1) Does the archive support complex enterprise models for email retention and deletion?

Email retention can be a difficult balancing act as organizations must trade-off their desire to delete messages with regulatory requirements, legal holds, and business needs that mandate the retention of email. When it comes to legal holds, or a hold on the deletion of all email meeting a certain criteria ordered by the court, it's important to prevent spoliation risk by ensuring the preservation of messages—past and future—related to an ongoing legal dispute. For these reasons, it's important for an archive to be able to manage multi-layered retention and deletion rules and to be able to institute effective legal holds. In particular, it is essential for administrators to be able to set granular retention policies on a user, group, location, department, or operating company basis. While it may seem reasonable to archive messages based on content, this is not feasible with today's technology. Many email messages that must be retained for lawsuits and compliance do not have keywords or context to support content-based archiving.

2) Will you be able to import all email into the archive?

For an archive to be effective, it needs to hold all company email. To do this, it must allow the import of historical messages from the primary email environment. In addition, it must be able to capture all future email: internal, external, text, and attachments. If information is left behind or not searchable, you will still need to manually search those remaining sources during the legal discovery process.

⁵Fulbright and Jaworski, "2007 Litigation Trends Survey."

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

3) Does the solution provide the full scope of needed archiving services?

There are many reasons why companies implement email archiving solutions: to meet e-Discovery requests, to improve the reliability of the primary email system, to reduce the size of primary email data stores, to improve email back-up and disaster recovery, to provide better end-user search, or to manage email retention and meet compliance requirements. It's important that an organization adopt a single archive to meet as many of these needs as they expect to develop. If organizations are forced to adopt multiple solutions because their e-Discovery archive does not meet all enterprise requirements, all of the archives will become discoverable, making it very difficult for organizations to manage retention and deletion policies and e-Discovery searches. In addition, since the largest cost of archiving is storage, organizations will wind-up paying significantly more if they choose to implement a multi-archive strategy.

4) Will the archive continue to run if email goes down?

Email outages are frequent occurrences and many organizations rely on their archives as an email substitute during an outage. If email or other IT services are unavailable, and the archive stops either collecting email or providing access for e-Discovery, employees will resort to using personal email accounts to continue business transactions, and deadlines for production of evidence may be missed. All of these messages will be sent outside of the corporate email system resulting in a loss of intellectual property that will be expensive and extremely difficult to recover during e-Discovery. Many organizations opt to use a managed services solution to prevent this problem from occurring.

5) Does the solution support your legal discovery workflow?

Legal discovery is a complex process that includes search, retrieval, redaction, and production. Every organization has a different process for managing discovery. It's important that the solution is flexible and able to support a variety of workflows. In particular, look for solutions that are able export messages to PST files or to export mail to a dedicated mailbox for legal review.

These five questions touch many of the most important criteria for selecting an email archive to support e-Discovery under the new Federal Rules of Civil Procedure. While many archives claim to meet these requirements and look the same, the following nine real-world archiving problems should provide further guidance on the selection of an archiving solution.

NINE COMMON PROBLEMS AND ESSENTIAL SOLUTION REQUIREMENTS

In real world use, archives that look similar often perform very differently. Here are a few problems that organizations commonly encounter with email archive solutions. When evaluating archives, be sure they can solve each of these problems:

PROBLEM 1 – SEARCHING BY USER

Many users have multiple email aliases within an organization such as psmith@, paulsmith@, NASales@, WorldWideSales@, Corporateteam@, etc., making it difficult to locate email for particular individuals. Many archives have no idea who the users of an email system are; they require the legal team to track every email address used by a particular user and to incorporate all of those address into every email search. This inevitably leads to incomplete searches that can damage the e-Discovery process.

Requirement – Email archiving solutions must be “user aware.” In a Microsoft® Exchange® environment, the archive must communicate with Active Directory to track every end user’s individual aliases along with any distribution lists in which they participate. In addition, the archive should allow the legal department to search for messages by user, without requiring the searcher to know which email address may have been employed by the user.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

PROBLEM 2 – AVOIDING ROGUE EMAIL ACCOUNTS

In the modern era, every individual has one or more personal email accounts in addition to their primary work account. When corporate email systems go down, users depend on these personal accounts to continue business operations during the outage. Messages that should be subject to corporate retention and deletion policies are stored in personal accounts outside of the corporate environment. These messages are invisible to the corporation and are expensive to locate and retrieve. While the messages are invisible to your counsel, they will have been received normally by other parties and may already be in the hands of your opposing counsel, creating a potentially hazardous legal situation.

Requirement – Ensure that the potential for email downtime is eliminated and that the archive will continue to function normally during an outage of the primary email system.

PROBLEM 3 – IMPLEMENTING DYNAMIC LEGAL HOLDS

During a lawsuit, it's important to eliminate spoliation risk by ensuring that no email related to the lawsuit is destroyed. Legal holds are often ordered by the court, and must be applied to prevent the destruction of existing email messages and of future email related to the lawsuit as soon as litigation is reasonably anticipated. This request will likely become more and more common during the early "Meet and Confer" requirements of Rule 26. Frequently, this is accomplished by preventing the deletion of messages by a user or group for the duration of the lawsuit. However, many archives cannot support legal hold policies by user or group, causing this to become a complex and expensive manual operation. Consequently, some email archives require all users to operate under the same generic retention policy, requiring companies to prevent deletion of all historical email.

Requirement – Email archiving solutions must be able to implement legal holds by user or group so that email related to lawsuits is not destroyed. Email archives must be linked to the directory and fully user aware. In addition, they must allow legal holds to be placed on a user-by-user basis. The best solutions allow users to apply legal holds to any part of an organization such as a location, department, or group based on information gathered from Active Directory®.

PROBLEM 4 – CENTRALIZING DISPERSED MESSAGES

In most companies, messages are stored in a number of locations. In addition to the primary email server, messages are commonly archived by individual users in .pst files stored on the desktop and placed on backup tapes managed by IT.

Requirement – Email archive solutions must be able to import existing messages from the primary environment, backup tapes, and local .pst files. In addition, they must eliminate the need for storage of email on the desktop. For backup tapes, they must eliminate the need to keep tapes beyond your shortest retention period.

PROBLEM 5 – SEARCHING ATTACHMENTS

Email messages are comprised of headers, body text, and attachments. Most archives do a great job of searching the first two. Attachments, however, can be much more difficult. Attachments can be any type of data file. Many archives can only search a limited number of text files, leaving the legal team to manually cull through thousands of files in esoteric formats to ensure full compliance with discovery requests. In some cases, the application that created the original file may no longer exist or may not be supported by current operating systems. It is the job of the archiving system to be able to read and parse attachment that may be contained in email.

Requirement – An email archiving solution must be able to search through the full text of any file contained in the email system. This means that the archive must be able to read, parse, index, and search more than 200 file format types that constitute the vast majority attachments.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

PROBLEM 6 – GUARANTEEING SECURITY

Email archives hold massive volumes of confidential information and corporate intellectual property. Therefore, it's essential that archives be secure both from intrusion and from improper use. Many archives suffer from three distinct security problems. First, they are not fully integrated with corporate authentication systems. In this case, access to a company's library of historical messages can be compromised if a simple password is hacked. Second, many archives store data in plain text, making the data store vulnerable to probing if it is accessed. Finally, many archives do not have the ability to restrict legitimate users, such as an outside counsel, to searches directly related to a particular legal matter. These limitations create large security vulnerabilities that put corporate data at risk and may prevent the corporate security team from adopting the solution.

Requirement – Email archives, especially archives delivered as a managed service, should meet three essential security requirements. First, they should be fully integrated with corporate authentication systems so that users access the archive with the same secure password that they use on all other corporate systems. Second, all stored archived data should be fully encrypted to prevent access at the data store level.

Most importantly, the archive application should be designed to allow a "scoped review" where users such as an outside counsel can be provided limited search capability that may include a specific set of users, mailboxes, departments, operating units, or even content-specific search terms. In a typical case, there will be different reviewers, each of which play a unique role in an investigation or legal discovery case. Typically, a company's inside counsel, outside counsel, and HR department will need to search email. To protect intellectual property and sensitive communications not related to the investigation, it is essential to limit each user's review capability by mailboxes, user, dates, content, or any other search criteria. This way, reviewers can be assigned an appropriate role with the case, allowing them to find the information they need without unnecessarily providing global access to all archived email communications.

PROBLEM 7 – MANAGING MULTIPLE ARCHIVES

Given the importance of email communication to most businesses, there has been a proliferation of solutions to help administrators and users get the most out of their email environment. Solutions exist to improve end-user search, reduce data store size and improve reliability, ensure that email communication is in compliance with federal and local regulations, prevent email downtime, and facilitate email disaster recovery. Unfortunately, many of the solutions deliver their benefits by storing a copy of related email messages. When this happens, the messages are often retained beyond their scheduled retention period, creating a new nightmare of distributed discovery whenever a legal search is executed.

Requirement – Corporations must implement a centralized archiving architecture where messages are retained solely in the primary system and a complementary email archive. If companies want the benefits of compliance, storage management, continuity, recovery, and end-user productivity in addition to the required e-Discovery capabilities, they should choose a multi-featured archive that meets all of these requirements.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

PROBLEM 8 – IMPLEMENTING GRANULAR RETENTION POLICIES

If legal strategy determined email retention policies, most companies would dispose of all email as soon as it was received and read – unless it was subject to a legal hold. However, most email retention policies balance legal's desire to delete messages with a company's compliance requirements, business needs, and other factors. For example, many firms save email for finance and senior executives for longer periods, often seven years, to comply with Sarbanes-Oxley. For an employee in the human resources department, messages may be saved for five years or more to comply with a variety of federal regulations such as OSHA and the Family and Medical Leave Act. For users elsewhere in the organization, such as product development, messages may be purged much more rapidly. Unfortunately, some email archives are unable to support these sorts of granular message retention policies. Many archiving solutions require all users to have the same retention period of either one, three, five or seven years. This forces organizations to save more mail than they want to, raising costs and adding a risk that they may need to produce incriminating email messages long after they could have legitimately been deleted.

Requirement – EMost organizations need to implement complex retention policies that provide for varied retention periods by user, department, job function, level, or operating company. It's important that these rules can be applied granularly – so that a company can choose options such 100-days or 9-years as their business may demand. In addition, these rules must be easily balanced with legal holds, which must take precedence over any other retention or deletion policy.

PROBLEM 9 – FACILITATING LEGAL DISCOVERY WORKFLOW

When a lawsuit occurs, a strong email archive can enable a legal team to find relevant email messages in just minutes or hours, depending on the complexity of the discovery request. However, searching and retrieving messages is just part of the legal workflow related to discovery and production. If an email archiving solution forces users to follow a single proscribed workflow, or limits the ability to export messages for review and redaction, it may add costs or delays to the legal discovery process. Many e-Discovery services or solutions require customers to submit special requests for extracting email or producing email, and often charge for production. Look for a solution that provides you with the capability to provide quick self-service searches. This will lower costs, production times, and will result in iterative searches that provide better results.

Requirement – A strong email archive will provide sophisticated capabilities to search and retrieve email messages by any user, group, or search criteria. Once these messages have been retrieved, it's important that they can be exported to a dedicated mailbox for review, or even better, to a legal support system where they can be organized with other electronic materials for legal review, redaction, and production.

Unfortunately, many email archiving solutions are afflicted with one or more of these nine problems. Finding a solution that addresses all of these problems will assure that you can meet your e-Discovery and archiving needs effectively and efficiently.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

Dell EMS Rapid Archive and Enterprise Archive Provide Effective E-Discovery

For legal officers, CIOs and email administrators, email can be a no-win proposition fraught with risk. Too often, their job is on the line if they are unable to:

- Easily implement message retention policies
- Quickly and easily find required messages to meet e-Discovery, HR, or compliance requests
- Put in place legal holds to prevent destruction of electronic evidence
- Effectively manage email performance including preventing downtime, eliminating data loss windows from tape backup, and controlling the size of large mail stores

While piecemeal solutions exist to solve many of these problems individually, the result is overly complicated, expensive, and difficult to manage and maintain. That's why Dell developed its Email Management Services (EMS). EMS addresses all of these concerns in simple, SaaS solutions.

Dell EMS archiving solutions help companies streamline e-Discovery and meet the full requirements of Rule 26. They provide granular control of retention and deletion rules and simple methods to execute dynamic legal holds. By implementing Dell EMS Rapid Archive, companies can become prepared to meet the critical requirements of the FRCP discovery rules in as little as a day. By implementing Dell EMS Enterprise Archive, companies easily archive messages based on company policies, improve the performance of production email systems, make email messages available during production outages, and enable rapid discovery of email for legal or HR purposes. Dell EMS archiving solutions can help ensure email never goes down (including BlackBerry®* devices) and can also help ensure that there is never data loss in a disaster recovery situation.

Graphic 1: Dell EMS Rapid Archive

Type	Policy Name	Retention	Statistics	Actions
1	Jameson Lawsuit Legal Hold	99999 days	Users: 0 Messages: 0 Total size: 0 bytes	Select Users Edit Delete
2	Hot Coffee Legal Hold	99999 days	Users: 0 Messages: 0 Total size: 0 bytes	Select Users Edit Delete
3	Compliance Group	730 days	Users: 0 Messages: 0 Total size: 0 bytes	Select Users Edit Delete
4	Finance	540 days	Users: 0 Messages: 0 Total size: 0 bytes	Select Users Edit Delete
5	Company Wide Retention	360 days	Users: 0 Messages: 0 Total size: 0 bytes	Select Users Edit Delete
6	Default	5 days	Users: 0 Messages: 127 Total size: 1.1 MB	Select Users Edit Delete

See the Storage Report section for a complete list of storage across the different policies

Create a new retention policy

*BlackBerry Wireless Continuity is dependent on the availability of the customer's BES server.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

Dell EMS provides a secure, cost-effective “Store Once, Use Everywhere” email archiving service for email continuity, recovery, storage management, legal discovery, and compliance. Dell EMS archiving services are designed to meet e-Discovery requirements of the largest corporate legal departments:

GRANULAR RETENTION AND DELETION POLICIES

Powerful Retention Policy Management: End users frequently wear multiple hats that subject them to different retention policies. Dell EMS supports the most flexible and granular user-based retention policies of any leading archive. For example, Membership-Based retention policies allow mail to be retained based on the current membership of the user, while Capture-Based retention policies allow mail to be retained based on the membership of the user at the time of capture. This enables you to implement policies such as: “all of the mail that John received as a Stock Broker is being retained for six years, while all the mail that John received as a Sales rep is retained for three years.”

Policy Management Automation: Archiving alone is not sufficient. Email must be saved and deleted according to corporate retention policies. That places an added burden on administrators to assure that all users are covered under the appropriate policy. Using information from Active Directory, new users are automatically placed under the appropriate retention policies based on their group membership. This reduces the chance of human error along the lines of, “I forgot to add them to the policy.”

COMPLETE ENTERPRISE ARCHIVING SOLUTIONS

Message Capture: End users are unreliable and can't be counted on to archive their own documents. Dell EMS captures the messages BEFORE they reach recipients' mailboxes so that all messages are archived, regardless of user behavior, automated mailbox rules, or other caveats.

Historical Import: E-Discovery is not limited to the date that you installed an archive solution. All email must be captured. Dell EMS allows you to import all email currently in Exchange Server, legacy systems, and .pst files into the EMS archive.

Continuity, Recovery, and Storage Management: Managing email is difficult and fraught with risk. When email goes down or data is lost, organizations will be unable to meet mandatory court and compliance requirements. Dell EMS Rapid Archive and Dell EMS Enterprise Archive help ensure that email never goes down and that messages are never lost. In addition, EMS Enterprise Archive includes storage and mailbox management capabilities that can reduce the size of mail stores by as much as 80% while providing users with infinitely expandable mailboxes. This helps improve system performance and dramatically decreases back-up, recovery, and maintenance windows. By providing comprehensive archiving services, Dell effectively eliminates the needs for multiple archives of record that can complicate discovery processes.

EFFECTIVE TOOLS FOR E-DISCOVERY

Dynamic Legal Holds: When companies enter into litigation, investigations, or compliance inquiries, it is important to prevent the destruction of electronic evidence. Dell EMS makes it easy to create and implement dynamic legal holds by user, department, location, or operating company that suspend the scheduled destruction of messages until the legal hold has been officially lifted.

Effective Search & Retrieval: The most important component of an e-Discovery solution is the ability to search and retrieve email to collect messages for legal production and defense. Dell EMS uses world-class search technologies to locate messages—usually in less than a second—by any criteria. EMS supports complex discovery criteria including searches by user, department, group, date range, and message content. EMS is fully synchronized with Active Directory. This allows the legal department to search all the mail of a selected user or group by name without knowing the specific email addresses, aliases, and distribution lists they participate in.

Since important content is often contained within attachments, the EMS e-Discovery interface also provides integrated sub-second search of 400 types of attachments by any criteria.

ESSENTIAL ARCHIVE REQUIREMENTS FOR E-DISCOVERY

ENTERPRISE-GRADE SECURITY

Scoped Reviewers: Administrators often need to delegate search access to the legal department and other reviewers to conduct e-Discovery searches, investigations, and compliance reviews. The users, who may be consultants or outside counsel, often have a limited scope of inquiry. Unfortunately, most archives allow reviewers to see all mail and documents for all users. Dell EMS allows administrators to set granular search permissions that cover the specific users, mailboxes, and content-areas that reviewers are allowed to explore.

Archive Security: Dell EMS protects the security of email using strong-key encryption, secure transport, a customer-specific key for storage to ensure that passwords remain secure. Unlike other solutions, no VPN or dedicated network is required to secure email.

Dell EMS Rapid Archive provides legal departments with powerful retention, e-Discovery and legal hold tools that can help them meet the full requirements of Rule 26 and other relevant regulations. Dell EMS Enterprise Archive meets the CIO and email administrator's comprehensive requirements for email archiving, continuity, storage management, and disaster recovery. In summary, EMS provides one of the most comprehensive email archiving and management services available today. With hundreds of companies depending on it today, EMS has become the leading email management platform for companies that use Microsoft Exchange.

CONTACT DELL TODAY

For additional information including pricing and a free demo, please visit www.dell.com/modularservices

© Dell 2008. The Email Management Services, EMS, and AlertFind are trademarks of Dell. Microsoft, Outlook and Active Directory are registered trademarks of Microsoft Corporation in the United States and/or other countries.