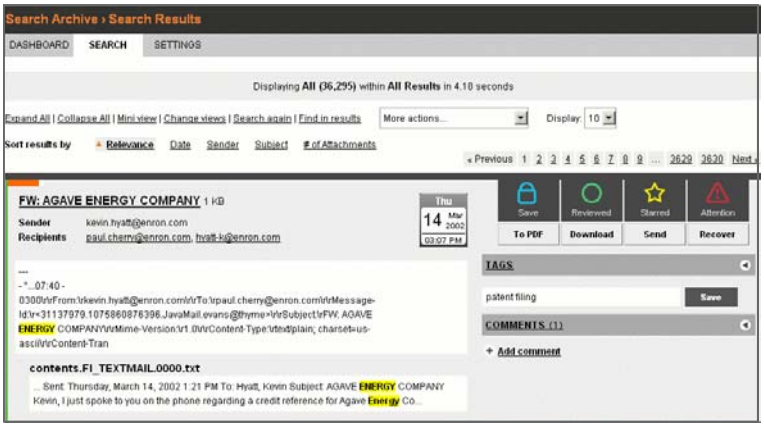
BlueTie inbox innovation™

BlueTie Archive Services

BlueTie Archive Services offers a simple and convenient way to meet your legal compliance and email auditing needs. All inbound and outbound email and attachments are permanently and securely stored online, and can be accessed and searched from any computer with an Internet connection. Our powerful search & retrieval interface lets you search messages and attachments by keyword, sender or recipient, date range and more, enabling fast and convenient review and action.

Advanced Search and Discovery

Add Comments ● Export Results ● Legal Hold
Tag Keywords ● Flag for Review



Automatic Back-Up of Messages & Attachments

- Capture all inbound and outbound messages
- Maintain a secure and tamper-proof copy of all business correspondence
- Implement with a few simple clicks

Powerful Search & Retrieval

- Retrieve accidentally or intentionally deleted messages
- Respond quickly to unexpected legal requirements, i.e. subpoenas, preservation orders, or litigation discovery
- Audit employee email for harassment, improper disclosure of confidential information, etc.

Lifetime Retention with Unlimited Storage

- Satisfy legal and business retention requirements
- Allow users to delete email with the knowledge that it can be retrieved from archive if needed later
- Predictable and affordable costs

Secure and Reliable: All archived data is replicated across multiple data centers. SSL encryption and adherence to DoD AES standards ensure that no data is accessible in clear-text.

Unlimited Storage: While other vendors charge a variable price for archival that increases as the amount of data stored increases, with BlueTie Archive Services you receive unlimited archival storage and no hidden fees.

All Data Searchable at All Times: To minimize their costs, other vendors move older data to offline or near-line storage, dramatically increasing the time required to conduct audits or comply with requests for discovery. With BlueTie Archive Services all data is kept online and immediately accessible for searches.

Email Archival & Auditing: It's Not Just for Finance & Healthcare Anymore

A 2008 report prepared by Forrester Consulting* reveals the level of importance US companies are placing on email archival and employee email monitoring. 70% of companies surveyed were "concerned" or "very concerned" about ensuring compliance with financial disclosure or corporate governance regulations, while 68% were "concerned" or "very concerned" about ensuring that email not be used by employees to disseminate company trade secrets or valuable intellectual property. The statistics below explain the reason for this high level of concern:

- **24%** of companies surveyed had been ordered by a court or regulatory body to produce employee email within the past 12 months. That number jumps to **34%** for companies with 20,000 or more employees.
- **44%** of companies surveyed had investigated a suspected leak of confidential or proprietary information via email in the past 12 months.
- **26%** of companies surveyed had terminated an employee for violating email policies within the past 12 months.
- **29%** of companies surveyed employ staff to read or otherwise analyze the content of outbound email. That number rises to **41%** for companies with 20,000 or more employees.

* "Proofpoint: Outbound Email and Data Loss Prevention in Today's Enterprise, 2008", Forrester Consulting, May 2008

220 Kenneth Drive | Rochester, New York 14623 | Phone: 1-800-BlueTie | Fax: 585.586.2268 | www.BlueTie.com

BlueTie inbox innovation™

BlueTie Archive Services

Compliance & Litigation Support

Email has become the lifeblood of modern business, and today most firms use email for taking orders, giving approvals, formalizing contracts, and discussing sensitive personnel issues. As a result, the corporate email system now contains a great deal of sensitive information. As dependence on email and its use have grown, so has its level of governmental and legal scrutiny. Email is now just as admissible in court, and just as critical for businesses to maintain, as are paper-based records.

Although firms in the financial services and healthcare industries face the most difficult data retention requirements, all organizations regardless of their industry are well-advised to maintain an archive of all email communications - just as they maintain insurance policies to mitigate other business risks. The alternative may include heavy fines from regulatory agencies, and presumed guilt or damaged reputation if subpoenaed records can't be produced.

A proactive email archival or automated auditing program can allow your business to take control of the situation before it becomes a problem.

BlueTie Archive Services capture, index, and store audited email for easy retrieval through the search and discover Web interface.

Employee Email Monitoring

The convenience and ubiquity of email - despite the many benefits - has exposed businesses to a wide variety of new risks, and firms of all sizes and within all industries have expressed a high level of concern about managing and enforcing outbound messaging policies that ensure that employees' email messages comply with internal rules, best practices for data protection, and external regulations.

It is often all to easy for employees to inadvertently or intentionally distribute highly sensitive information to unauthorized parties, leading to fines, legal complications, or loss of competitive advantage.

"23% of companies surveyed said their business had been impacted by the improper exposure or theft of sensitive information or intellectual property via email."

BlueTie Archive Services lets you define filters that scan each employee email message, flagging any messages containing those keywords you've defined as potentially worrisome. Flagged messages can be reviewed by your designated HR, compliancy, or legal staff, and appropriate action can be taken as necessary. Flagged messages can be tagged by category, routed to specific personnel for review, or filed for future reference.

Summary of Key Email Archiving Requirements

INDUSTRY	KEY REGULATORY BODIES/STATUTES	GENERAL REQUIREMENTS
Financial Services	Securities and Exchange Commission (SEC) Financial Industry Regulatory Authority (FINRA)	Maintenance schedules for records How records are to be maintained How records of communications with clients are to be maintained and supervised
Healthcare and Life Sciences	Healthcare Insurance Portability and Accountability Act (HIPAA) Medicare Conditions of Participation	Maintenance schedules for records Disposition of records
Government Agencies	General Records Schedules from the National Archives and Records Administration	Each agency develops its own retention policy
Automotive	Auto Industry Action Group (QS-9000)	Maintenance of quality performance records, internal quality system audits, and documents
All Commercial Enterprises	Federal Rules of Civil Procedure Sarbanes-Oxley Act Gramm-Leach-Bliley Act Internal Revenue Service	Maintenance schedules for records How records are maintained

* "The Impact of Regulations on Email Archiving Requirements", Osterman Research, Inc., 2005

BlueTie inbox innovation™

Email Archival & Auditing

Federal Rules of Civil Procedure (FRCP)

The U.S. Supreme Court ratified changes to the Federal Rules of Civil Procedure in 2006 which altered the rules of discovery in a legal proceeding from a focus on policies for electronic records retention, disposition and preservation, to a focus on procedures that will streamline evidence presentation. As a result, businesses, non-profits, and government agencies must now be prepared to answer key questions such as:

- Where is the data in question?
- What actions were taken to preserve it?
- How can the data be searched and reproduced?
- What is the company's established data retention / deletion policy?

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 was enacted in the wake of several major corporate and accounting scandals. Its provisions affect email retention, integrity and oversight. Sarbanes-Oxley applies to all publicly-traded companies and the CPA's and attorneys associated with these companies.

- Possible fines of up to $1,000,000 or sentences of up to 20 years can result from the destruction, alteration, mutilation or concealing of electronic documents in an official investigation.
- Minimum retention periods defined for all accounting records, work papers, communications, file attachments, and documents, including email.
- Requires companies to maintain all documents including electronic documents that form the basis of an audit or review for seven years.

Freedom of Information Act "Sunshine Laws"

The federal government and nearly all state governments have established "Open Records" laws. The purpose of these laws is to provide a level of transparency to the activities of government agencies and officials for their citizens. There are no specific guidelines on how long emails must be retained. However, IT departments of these agencies must comply with the request for information which, in the absence of an email archiving solution, typically includes the laborious process of the restoration of backup tapes and the manual search across multiple mailboxes. In many cases, this search only produces a fraction of the emails pertaining to the request.

Graham-Leach-Bliley Act (GBLA)

The GLBA became effective in 2001. The law applies to banks, brokerage firms, tax preparation companies, insurance companies, consumer credit reporting agencies and a wide variety of other financial services firms. Violations of the GLBA may result in a fine of up to $100,000 dollars and 5 years in jail. The primary focus of the GLBA is the protection of customers' personal financial information.

- Regulated organizations must insure the security and confidentiality of customer records and information.
- Access to all records must be carefully controlled to prevent substantial harm or inconvenience to any customer.
- Storage of sensitive customer information must be protected by strong access control and secure passwords.
- Sensitive customer information must be protected in case of physical disaster or technological failure.

BlueTie Archive Services help organizations comply with these and other regulations by securely capturing, indexing and storing copies of auditable email for fast and easy retrieval through the search and discovery Web interface.