

# Sendmail 360° Messaging Assessment™

## OVERVIEW

Email continues to be the most widely used communication vehicle with over 130 billion email messages sent each day. It is estimated that one in five emails contain a legal, compliance or financial risk, while email fraud and forgery, a tactic often used in phishing attacks, spam and other malware, continues to dramatically rise.

The Sendmail 360° Messaging Assessment program is a comprehensive assessment of your organization’s entire messaging flow that delivers critical information about your company’s data loss exposure, the reliability, scalability and efficiency of your organization’s infrastructure and the overall effectiveness of your gateway security practices.



## COMPONENTS

- Compliance Risk
- Secure Messaging
- Authentication
- Email Architecture
- Inbound Efficiency
- Hardware Refresh
- Operational Metrics

## MESSAGING ASSESSMENT COMPONENTS

There are seven components to the Sendmail 360° Messaging Assessment program. Businesses have the flexibility to choose only those assessment components that address their current requirements.

### Compliance Risk Assessment

Businesses of all types and sizes are confronting the complex challenge of managing enterprise risk related to the insider. Regulatory compliance regulations such as HIPAA and GLBA, corporate governance policies, and privacy concerns are just a few of the risks which need to be managed. To manage these risks, businesses must first clearly determine where the organization is vulnerable. This vulnerability information provides the organization with the baseline data required to formulate a comprehensive plan for addressing their compliance risks.

#### Description

The Compliance Risk Assessment measures the security and compliance risks occurring in the corporation's message flow. The Compliance Risk Assessment is a two step process that includes an interactive workshop session and a 48-hour analysis period that looks for real compliance risks in your corporation's outbound email. Sendmail's findings and recommendation follow in an executive report.

The entire process is designed to be non-intrusive, driven primarily through interactive workshop sessions with key stakeholders from IT, Messaging, Security and Compliance departments.

### Secure Messaging Assessment

With 80% of enterprise compliance and security violations occurring in email, businesses require a more effective way of securing their email communications. Email messages containing sensitive, confidential or regulated information need to be discovered in-line and automatically encrypted to avoid potential damage to brand and corporate assets, and to comply with government regulations.

#### Description

Sendmail first performs a detailed assessment of the organization's secure messaging requirements and then applies proven best-practices to deliver a comprehensive guide for improving messaging security.

### Authentication Assessment

One of the major flaws of email today is its lack of authentication. This means that anyone on the Internet can send email to anyone else while claiming to be a third person. The most common example of this kind of email forgery is phishing scams which are designed to steal account numbers and other private customer information. This type of fraud can have serious consequences for any business including loss of reputation and high value customers.

#### Description

The Sendmail Authentication Assessment identifies the major components of risk for a corporation and provides a detailed set of email authentication best-practices.

**Eighty percent of enterprise compliance and security violations occur in email.**

## Email Architecture Assessment

Email continues to be the most widely used business communication vehicle and uptime and reliability is mandatory to an organization's success. As organizations have grown and adapted to the latest threats and technology, messaging infrastructure has grown substantially creating complex environments that require heavy administration with a high total cost of ownership.

### Description:

The Email Architecture Assessment provides an organization with a high level assessment of the email infrastructure and business email requirements. Sendmail identifies areas of potential security risk and possible vulnerabilities. Deliverables include an executive summary addressing the scalability, reliability and efficiency of the infrastructure with recommendations for improvements.

## Inbound Efficiency Assessment

Mitigating the risks of spam, viruses and malware are critical to the organization. Spam and virus engines, content filtering, mailstore processing and storage all consume valuable bandwidth and resources. If an organization can eliminate unwanted messages at the gateway, the cost savings is tremendous.

### Description

Sendmail's Inbound Efficiency Assessment utilizes best practices guidelines combined with an inbound message review to provide the organization with an assessment summary that outlines recommendations to improve overall gateway effectiveness.

## Hardware Refresh Assessment

As messaging throughput increases and hardware components age, it is difficult to keep the messaging infrastructure at peak performance and efficiency resulting in high costs and degraded ROI patterns.

### Description

The Sendmail Hardware Refresh Assessment provides a detailed ROI analysis for various upgrade and consolidation options for the hardware within your messaging infrastructure.

## Operational Metrics Assessment

In the last few years, state and federal legislators, regulatory bodies and other industry specific groups have implemented a substantial number of regulations designed to force companies to higher levels of accountability and information security standards. Managing these requirements is costly and complex resulting in non-compliance and lack of insight into the messaging operations.

### Description

The Sendmail Operational Metrics Assessment evaluates your organization's email log management and auditing strategies discovered during a remote log assessment and requirements review session.

**If an organization can eliminate unwanted messages at the gateway, the cost savings is tremendous.**

## ABOUT SENDMAIL

Sendmail is the leading global provider of trusted messaging. With 25 years of leadership delivering innovative messaging technology, Sendmail ensures the protection and trust of employee and customer communications. Sendmail technology, driven by the industry's most powerful and flexible policy engine, provides protection where 80% of security and compliance violations occur - within inbound and outbound messaging. Large enterprises in 33 countries, and the majority of the Fortune 1000 trust Sendmail to shield users from unwanted messages, defend the messaging infrastructure, stop data and privacy leaks and effectively manage messaging to maintain brand and shareholder value and support regulatory compliance. Sendmail is headquartered in Emeryville, CA with offices and distributors in Europe, Asia and North America.

Sendmail offers a full range of integrated email infrastructure and security capabilities, including routing, virus protection, spam rejection, content filtering, policy management, traffic control, next-generation sender authentication, and more – everything you need to secure and manage your entire email environment.

## CONTACT US

For more information and further details on each 360° Messaging Assessment component, please contact us at [sales@sendmail.com](mailto:sales@sendmail.com), or phone 877-363-6245.

**Sendmail, Inc.**  
6475 Christie Avenue,  
Emeryville, CA 94608  
Tel: +1 888 594 3150  
Fax: +1 510 594 5429  
[www.sendmail.com](http://www.sendmail.com)