Encryption Buyer's Guide

Email Encryption: It's Time to Buckle Up

While other measures tend to grab more of our attention – email is still the workhorse of the business world containing 75% of the information employees use on a daily basis[1]

Confidence in a connected world. Symantec™

Contents

When is the last time you saw a car commercial that mentioned anything about seatbelts? These days we're so caught up with advanced safety features such as traction control and more airbags ––we tend to forget that seatbelts really do save more than 10,000 lives every year, making them one of the most effective[2] automotive safety measures.

IT security is a similar situation in some ways. There are simple practices that can greatly reduce the risks businesses face, but other measures tend to grab more of our attention. Case in point: email. For all the talk about topics such as cloud computing and virtualization, email is still the workhorse of the business world. In fact, a recent report by the Radicati Group estimates that as of 2012, there were 850 million business email accounts in the world, sending and receiving a total of 89 billion emails per day – or 61 percent of total email traffic. By 2016, this is expected to grow to 65 percent of all email or a total of 101 billion business emails daily.

One reason business email is skyrocketing is that the ways we send and receive email are increasing. Mobile email access, for example, is improving productivity for employees worldwide. As of 2012, 750 million people around the world have been using mobile devices for email, and that's only expected to grow. According to a survey by Dimension Research[3], 79 percent of organizations now report employees storing corporate email on mobile devices.

While the business use of email is increasing, IT is scrambling to deal with other, newer points of attack. They're worrying about their information being stored in the cloud, and headline-grabbing advanced threats that target strategically important facilities.

But are they forgetting that email still contains about 75 percent of the information employees use on a daily basis? Make no mistake, information is the lifeblood of business today – in fact, it makes up 49 percent of the organization's total value, according to Symantec's 2012 State of Information Survey. This isn't just meeting notices and time sheets, either. There is a lot of highly sensitive business information being sent via email every day that requires confidentiality.

Consider just a few examples of information that should be kept from prying eyes:

- Senior management sending important financial documents back and forth about a pending acquisition.
- Executives determining whether or not their financial situation will require widespread layoffs.
- An employee uses a business email account to contact a doctor about the results of a medical test.
- A project manager sends new product specifications to a developer overseas – specifications that a competitor would love to see.

These are not just hypothetical situations. While we tend to think that data breaches involve hackers breaking into sophisticated storage repositories, one email accidentally seen by the wrong person can cause just as much damage to a company.

Last fall[4], an email of unfinished revenue figures was accidentally sent to stock market authorities, costing a large tech enterprise 9 percent of its stock value. In another incident[5], a college football coach was accidentally sent an email that revealed the school was looking for his replacement. And last spring[6] a law school accidentally sent new students a list of personal information – including test scores – of other students.

Either way, like seatbelts in cars, there is one simple solution that we often forget about: Encryption.

Business Drivers for Email Encryption

While email is an extremely useful tool that makes it possible to do business today, it also carries with it several potential avenues for harming an organization. A single email exposure incident can cause all sorts of problems, ranging from a small financial loss to putting an entire business in jeopardy.

Data accounts for a large portion of business' value. The bottom line is, it's important that email be protected every step of the way, from the sender to the recipient.

- **Compliance and Privacy Regulations**
  As privacy concerns continue to gain momentum in our society where more information is sent each day, compliance and privacy regulations continue to grow – with serious consequences for those not following them. Several independent studies have pegged the associated financial losses for poor use of email at several billion dollars annually – and growing.

- **Brand Damage and Loss of Trust**
  Data breaches are receiving more media attention than in previous years and have lead to the public becoming more aware of the tools available for organizations to prevent these mistakes from happening. This increased public awareness also leads to greater risk of lost consumer, partner, and employee confidence along with overall brand damage. This leads to direct financial costs - the 2011 Cost of a Data Breach survey by Symantec and the Ponemon Institute, which found that U.S. organizations lost an average of $3 million[7] due to customer churn following a data breach.

- **Internal Threats**
  We are well aware of malicious outsiders such as hackers, but threats from inside the company can be just as dangerous. Some may be innocent employee mistakes, such as accidentally emailing unencrypted confidential data, while others may intentionally seek to steal or destroy confidential information. Protecting your information from internal threats must be viewed just as importantly as dealing with external attacks.

- **Email in the Cloud**
  With email volumes constantly growing, many companies are now outsourcing email storage to cloud providers. Although potentially advantageous, this practice raises many security questions. What kind of protection can the cloud provider provide? Who is in charge of managing and maintaining the protection? Who controls the encryption keys? What are the legal ramifications should authorities request access to your information?

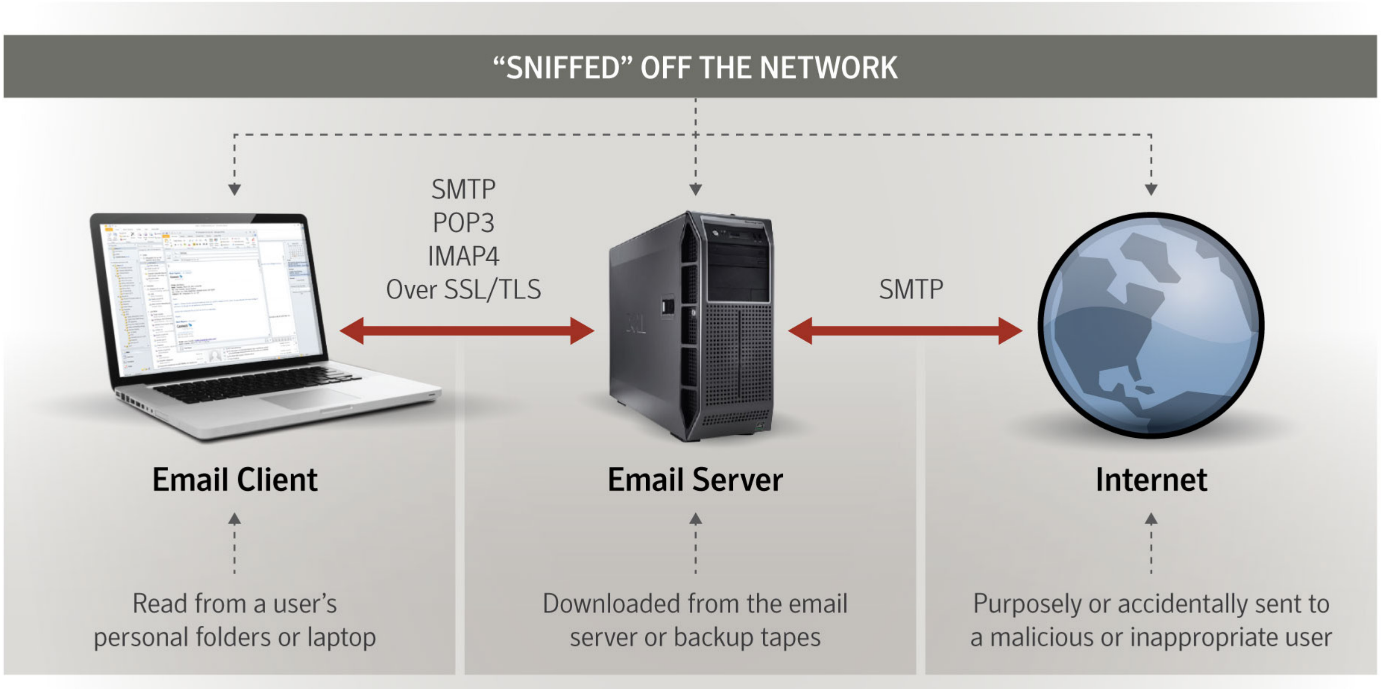
Where Email is Vulnerable

Storing sensitive information in unencrypted email exposes businesses to several risks. Many organizations don't realize that different companies – and different countries – have varying requirements surrounding privacy and the free flow of information.

Research from Forrester reveals vastly different data protection regulations in different countries. China, for example, has virtually no privacy restrictions, with most of Asia having relatively few regulations. Argentina, on the other hand, has strict privacy laws, while neighboring Paraguay has essentially none. It's difficult to know what the situation is when conducting business internationally.[8]

email sent purposely or by accident to malicious or inappropriate user

There are two real worries about people intercepting email. The first is that people with legitimate access, such as email administrators, might be exposed to messages that contain confidential information. This is especially relevant in industries like healthcare and finance, where strict regulations determine what can be sent to whom and who has visibility into what. In this case it may be less an issue of prying eyes than making sure businesses are compliant. The second worry, of course, is that someone could illegally gain access to email that could expose sensitive data. This can happen over wireless networks, such as the free Wi-Fi hotspot at the local coffee shop, or it might happen when someone hacks into a company’s network undetected, giving them access to all the email being sent.


“SNIFFED” OFF THE NETWORK
SMTP
POP3
IMAP4
Over SSL/TLS
SMTP
Email Client
Email Server
Internet
Read from a user’s personal folders or laptop
Downloaded from the email server or backup tapes
Purposely or accidentally sent to a malicious or inappropriate user

What to Look For

With a wide variety of encryption products available, what are the most important considerations? How do you balance affordability with flexibility in case your needs change? It’s important to choose a solution that will not only serve your needs now, but also as your organization grows. A good encryption solution should integrate with other parts of your IT infrastructure so you can work with what is already in place. Here are some important points to evaluate as you look at your encryption options.

Flexibility and Usability

> There isn’t a single way or place to send email. Users should be able to send sensitive information comfortably however they choose, from their desktop, laptop, or mobile device – regardless of whether they are within the organization’s walls or waiting in line for security at the airport.

Encryption should happen behind the scenes, with as little impact on user productivity as possible, regardless of the device. Also, to increase effectiveness and adoption, solutions should minimize the amount of effort users must put forth to ensure your information is protected.

Scalability

Many organizations, when first encountering the need for encryption, see it as an inconvenience rather than strategic tool and opt for a free, unmanaged, or limiting solution at the onset. As they grow however, they find that managing their policies and individual and group encryption keys become exponentially harder as users and roles increase both in number and complexity. When IT no longer has the resources to keep up, or they need new functions that their current encryption solution doesn't provide, they can be forced to deploy an entirely new solution and start from scratch, incurring significant costs.

By choosing an automated solution that handles policy assignment and key management, and allows your organization to add new functionality quickly and easily as you grow, organizations can greatly reduce administrative costs in both the near and far term.

Compliance and Integration

Businesses are responsible for demonstrating compliance with laws and industry regulations concerning the protection of sensitive information. An organization's encryption solution, then, should integrate with other information security tools within the business. Effective eDiscovery, for example, requires the ability to search through email files quickly for legal purposes, including those that are encrypted, to avoid costly penalties and fines. Data loss prevention tools can also be integrated, helping provide more granular security controls and risk mitigation options when tied into an organization's encryption solution.

One of the most important needs in IT today is to not get locked into the technology of one specific vendor. Your encryption solution should incorporate open standards, ensuring that you can keep using the tools that already work for you.

Open Standards

Open standards have been thoroughly tested and form the basis of effecive encryption, and technologies continue to be built on these standards. Proprietary methods will limit your technological options as your organization grows, potentially necessitating a rip and replace if that one vendor can no longer meet your needs. Choosing a solution at the outset that preemptively meets future needs ensures robust security that will not soon be outdated.

Management

As an organization grows, maintaining individual user keys, groups, and associated encryption policies can become enormously difficult for an IT team to do manually – dealing with 20 employees is one thing, but when users swell to even 50 or more, it becomes far too time-intensive. Additionally, as an organization's security model matures, more solutions will come into play adding to complexities.

The right encryption solution should be able to centrally manage all encryption activities from a central point, as well as automatically organize and manage user keys and associated group policies. Tying key management into an organization's Active Directory or other open LDAP architecture can also significantly reduce IT administration costs.

Recovery mechanisms should also be considered. If an employee quits, or is terminated, they might have important information encrypted in their email inbox. Management needs a way to access these emails, so users can't hold company data hostage.

Reporting is also a key factor. Reporting not only enables organizations to prove encryption but also allows them to better understand how and when their users utilize encryption. This is beneficial in better understanding and identifying areas in which employees may need training to improve information security, as well as assessing the security solution's overall effectiveness.

Encryption Solutions

Gateway Encryption

Gateway encryption is the most commonly utilized form of encryption among businesses today and involves the least amount of end user interaction. It allows email to be stored in an unencrypted area within the organization, only encrypted when sent to an outside domain, and provides multiple delivery options.

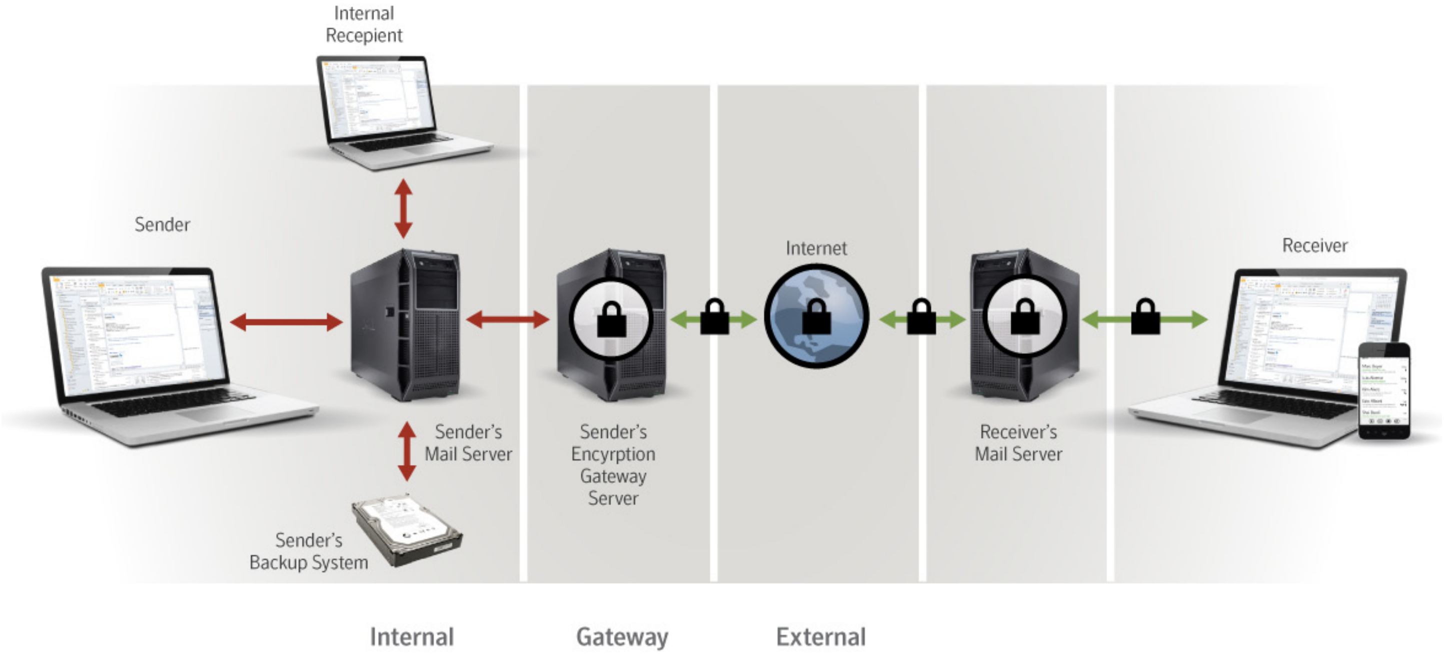
Gateway Encryption at a Glance

- No software needs to be installed at the client
- Email sent are encrypted when they hit the sender organization's encryption gateway, where they are secured based on policy settings before leaving the organization.
- Encryption is based on central policies controlled by IT.
- Data Loss Protection (DLP) solutions can be integrated to strengthen controls and ensure that end users aren't circumventing security policies.
- Eliminates the need for additional actions from the sender's side.
- Multiple delivery options.

Gateway encryption, involves the least amount of end user interaction and allows email to be stored in an unencrypted area within the organization, only encrypted when sent to an outside domain, with several possible delivery options at that point.

Gateway-to-Endpoint

- Provides email encryption from a gateway system within the sender's network to the recipient's endpoint. In this scenario, the message leaves the sender's desktop in plaintext and is encrypted by a gateway solution located near the email server.
- Eliminates the need for any user action on the senders side.
- Provides significant cost savings by reducing user training and IT desktop administration costs and potentially reduces licensing costs by eliminating the need for desktop software.
- Often provides various delivery options for the recepient.



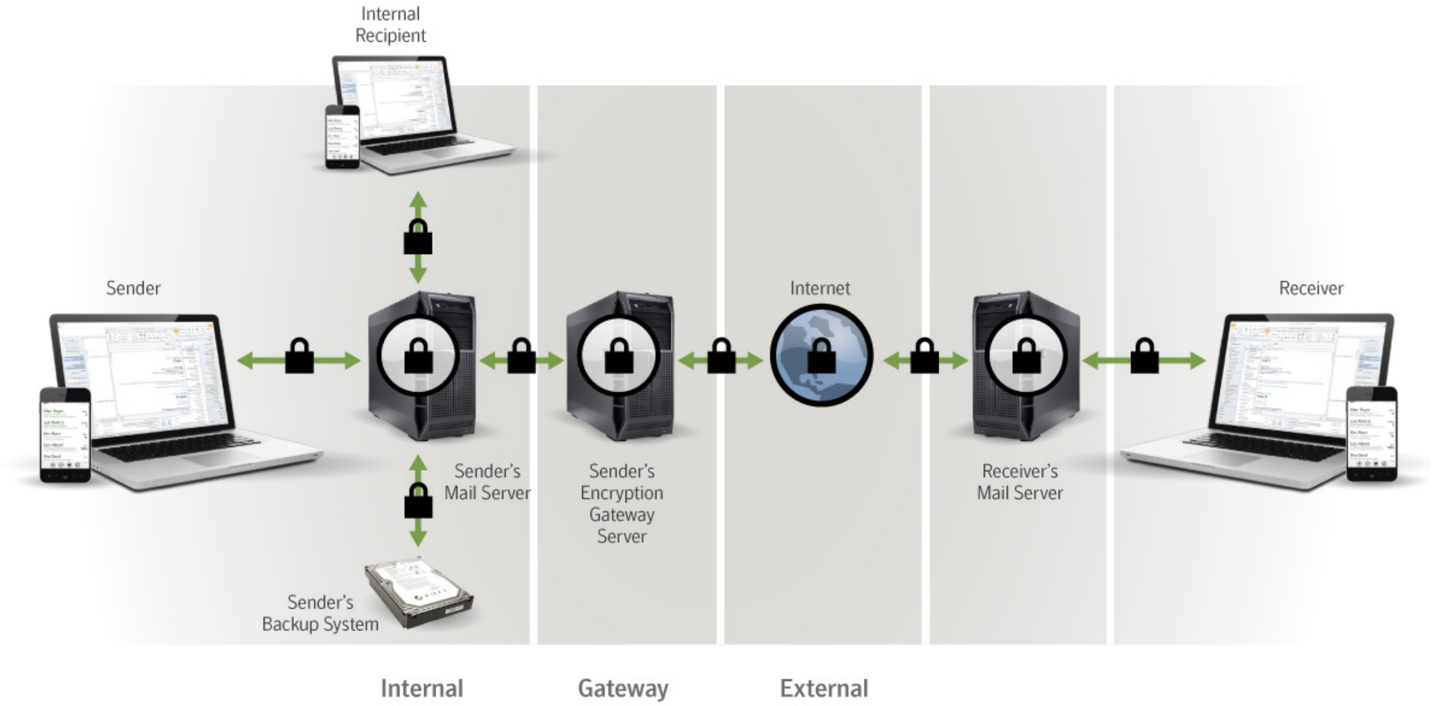
End-to-End Encryption

End-to-End encryption provides the most secure messaging environment and is commonly used by senior executives, boards of directors, and other highly influential roles. Unlike Gateway Encryption, messages are encrypted from the client rather than at the gateway, ensuring the message is secure from start to finish. Common examples of where end-to-end encryption is used are information surrounding mergers and acquisitions, critical intellectual property, or information surrounding stock value and strategic initiatives.

Mobile Encryption:
Often, those using end-to-end encryption are not behind a desk making the user's mobile device one of the most important environments for deploying end-to-end encryption. When employees can improve productivity by sending and receiving email from anywhere, it's important not to compromise security for the sake of convenience.

End-to-End Encryption at a Glance

- Software is installed at the client
- Email is instantly encrypted at the client and remains so until opened at the recipient's end with their own key.
- User activated and automated, policy-defined encryption
- Email is never exposed



Buyer's Checklist

Buyer's Checklist Symantec Encryption Solutions	
Flexibility	□ Can the solution integrate with other existing or future encryption solutions?
	□ What options does the solution allow when the recepient doesn't have an encryption key?
	□ Does the solution allow sending and receiving secure email directly from various mobile devices and tablets without having to log into a web portal?
	□ What options does the solution provide for where encryption occurs?
	□ Is encryption based on Open PGP and/or S/MIME or proprietary methods?
	□ Can the solution support mobile devices? If so, which platforms?
	□ Does the solution offer both gateway and end-to-end encryption?
	□ What other security solutions does the email encryption solution integrate with? Backup? DLP? Anti-Virus/Anti-Spam?
Compliance	□ Does the solution provide comprehensive encryption logs for auditing purposes?
	□ What independent tests have been performed on the vendor's products?
	□ Is the solution FIPS compliant and compatible with standard encryption algorithms such as AES?
Management	□ Does the solution provide policy-defined access to encrypted data if the key owner is unable or unwilling to provide their private key?
	□ Does the solution allow for the separation of duties between various lines of business and email administration?
	□ Will the solution support different encryption methods for different users in the organization, such as end-to-end encryption for Legal and gateway-to-gateway encryption for Marketing?
	□ Does the solution provide an automated key management system?
	□ Can the solution support a rapidly changing email deployment model securely such as storing email in the cloud?
	□ Can the solution manage additional encryption solutions other than email?
	□ Can the solution support automatic user enrollment such as with AD or other LDAP?
	□ Will the solution support automatic generation and management of certificates instead of requiring users to obtain and implement their own certificates?
	□ Can the solution easily handle frequent key changes?
	□ How easily can the solution be deployed on a small scale? Large scale? Incrementally?
	□ What reporting capabilities does the solution provide?

Symantec Encryption Solutions

Symantec Gateway Email Encryption

Symantec Gateway Email Encryption provides centrally managed, standards-based email encryption to secure email communications. By encrypting data at the gateway, Gateway Email Encryption ensures data is protected from unauthorized access in transit, over the public Internet, and at rest on a recipient's mail server. Additionally, automated encryption can be enabled based on recipient domain or other common filtering flags such as credit cards and social security numbers.

Symantec Gateway Email Encryption integrates multiple delivery options for endpoint delivery into a single product:

Gateway-to-Endpoint

- **Web Email Protection**
  This form of gateway-to-endpoint encryption is used when the recipient doesn't have their own encryption key and regular secure communication from both sender and receiver are necessary. When the encrypted email is sent, the end user receives an email informing them they have a secure message in a web portal. The user logs into the portal to read the email and respond securely. All back-and-forth communication takes place within the encrypted environment, making it an ideal solution for secure collaboration.

- **PDF Email Protection**
  This encryption method is especially useful when dealing with one-way communications such as sending monthly statements to customers, where no response is required. The message is encrypted as a secure PDF that is sent to the recipient's mailbox, making it ideal for situations in which individuals need to access encrypted and unencrypted email in the same inbox due to legal reasons or user preference. The user opens the encrypted message as an attachment and enters a user defined password to decrypt it. Often, this method is found in business-to-consumer transactions. This solution is preferred for sending information, rather than collaboration, although a secure reply option is available if necessary.

- **Gateway-to-Recipient**
  Often, one organization is communicating with another organization that also has its own encryption solution in place. When both organizations are using compatible methods, the solution can search for the recipient's key and encrypt accordingly from the sender's gateway, making this the most convenient encryption option when it is available. Otherwise, the process automatically triggers Web Email Protection or PDF Email Protection to ensure that only the proper recipient is able to access the message securely.

Symantec Desktop Email Encryption

Symantec Desktop Email Encryption delivers end-to-end encryption in an easy-to-use interface for employees. Messages are automatically encrypted and decrypted without impacting the user experience, ensuring that full encryption takes place before leaving the user's mailbox for maximum security even within the organization. It delivers the flexibility of automated policy-defined encryption while also allowing users to encrypt their own messages when desired.

Symantec Mobile Encryption

For your employees to enjoy productivity wherever they are, while keeping their communications secure, Symantec Mobile Encryption keeps it simple. Users have access to all their messages without the need to log into external gateways, with no slowdown of their devices. It keeps business data secure while leaving personal information alone, delivering the ideal BYOD environment for iOS, Android, and Blackberry devices.

Symantec Encryption Management Server

Symantec Encryption Management Server automates deployments, provisioning, key management, and policy enforcement for Symantec's encryption solutions from a simple, Web-based management console, reducing administrator workloads and ensuring consistent policy across the organization. An easy-to-use user interface provides administrators both high level and granular reporting capabilities, and staff can quickly add additional encryption solutions and functionality as needed with simple license authorizations without having to install new software.
In situations where a user's key becomes unobtainable, such as when an employee leaves an organization, Symantec offers a unique recovery mechanism called an Additional Decryption Key (ADK). This feature splits a corporate recovery key into multiple pieces among authorized users. To prevent unauthorized use a minimum number of pieces, set by administration, must be combined for the key be activated.

> *Many breaches today are caused simply by user error; not realizing what information can or can't be sent in the open or simply forgetting to encrypt a message.*

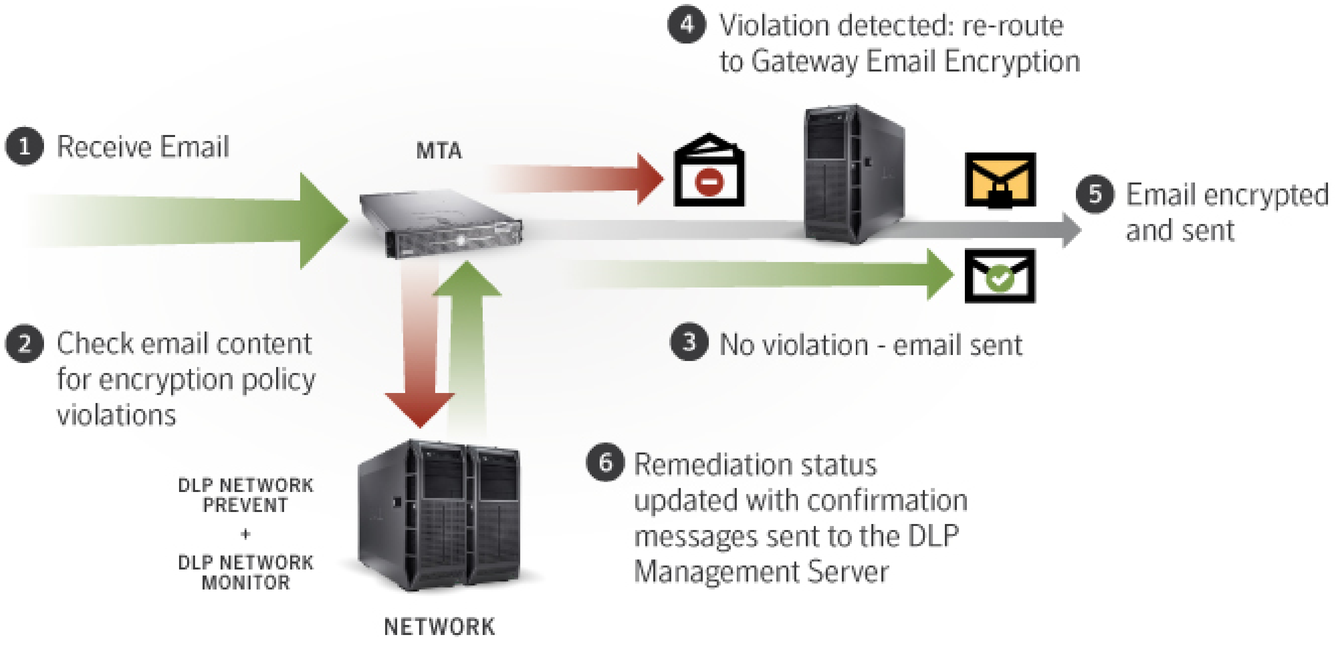
Symantec Data Loss Prevention Network Monitor

Incorporating Symantec DLP Network Monitor into your email solution allows passive deep content inspection of all network communications before it leaves your organization.

Symantec Data Loss Prevention Network Prevent

Symantec DLP Network Prevent for Email redirects, quarantines, or blocks outbound messages containing sensitive data, including messages sent from mobile devices.

When an email is containing sensitive data, administrators have the option of redirecting to Symantec Gateway Email Encryption to prevent any business disruption from a blocked or quarantined message.


4 Violation detected: re-route to Gateway Email Encryption
1 Receive Email
MTA
5 Email encrypted and sent
2 Check email content for encryption policy violations
3 No violation - email sent
6 Remediation status updated with confirmation messages sent to the DLP Management Server
DLP NETWORK PREVENT
+
DLP NETWORK MONITOR
NETWORK

Resources

1. Email Encryption Buyers Guide 2008, An Osterman Research Publication

2. http://www.nsc.org/safety_road/DriverSafety/Pages/SeatBelts.aspx

3. http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

4. http://www.guardian.co.uk/technology/2012/oct/18/google-shares-suspend-email-22bn

5. http://www.cbssports.com/collegefootball/blog/eye-on-college-football/21204371/accidental-email-lets-morgan-state-coach-know-school-is-looking-for-replacement

6. http://blogs.wsj.com/law/2012/04/04/baylor-outs-its-admitted-students-with-accidental-email/

7. http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf

8. http://heatmap.forrestertools.com/

More Information

Visit our website

http://go.symantec.com/encryption

To speak with a Product Specialist in the U.S.

Call +1 (650) 527-8000

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com

Confidence in a connected world.