

Data Security & Privacy Certification
Sales Certification Study Guide



Sales Study Guide

Demonstrate your sales knowledge by participating in the Echoworx Data Security & Privacy Certification (DSPC) Program

The Importance of Data Security

- Securing company and customer data is vital to an organizations success
- Many organizations today are ill prepared to deal with identity theft, data thieves, etc
- According to IDC data breaches are more costly than ever:
 - *“... it costs \$6.6 million to rebuild your brand image and retain customers for a typical 1000 employee company”*

Encrypted Data

- The most effective way to achieve data security is to encrypt all confidential information
- Data and email encryption can be hard for companies to understand and deploy
- A managed service model is the easiest way to get encryption deployed within an organization
- Using FTP (File Transfer Protocol) to send large amounts of data across the Internet is not secure

Securing Confidential Information

- **Customer Information**
 - Securing customer information should be the # 1 priority for any business
 - Without customers there is no business
 - Without data security customers will take their business elsewhere
 - Securing customer data results in happy customers

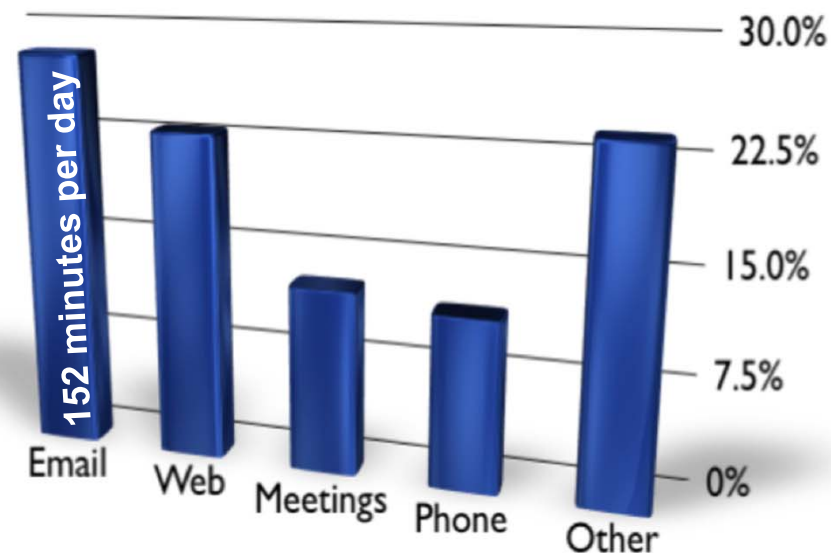
- **Product Information**
 - Protecting product information is a high priority in any organization
 - Protect product information from competitors looking for the next big idea
 - Protect intellectual property from prying eyes

- **Employee Information**
 - Protect employee information such as social security numbers, addresses, telephone numbers, and employment records

- **Company Information**
 - Protect company information such as financial and other business data
 - Leakage of this data could harm a company's reputation and can result in legal action

Why Encrypt Email?

- Email is still the number one business communication tool
- Workers spend 152 minutes per day on average on email

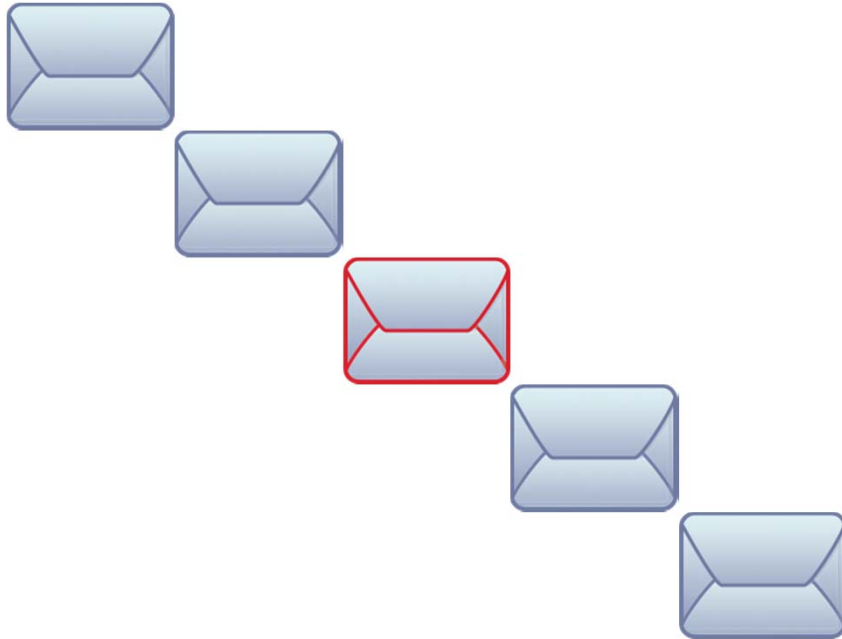


Source: Forrester Research 2009

Why Encrypt Email?

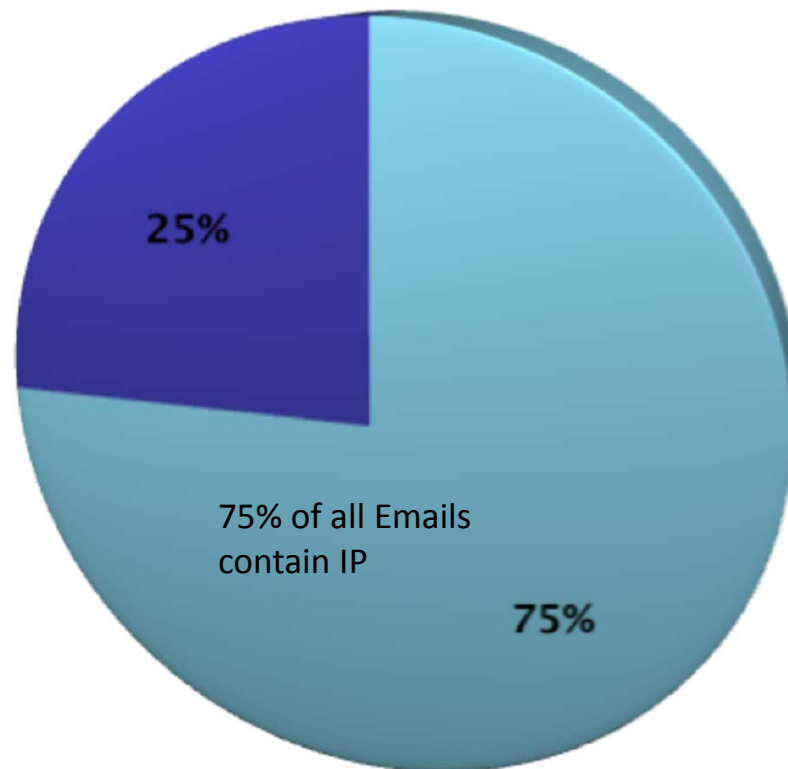
- 1 in 5 outgoing emails contain content that poses a legal, financial, or regulatory risk

Source: Forrester Research 2009



Why Encrypt Email?

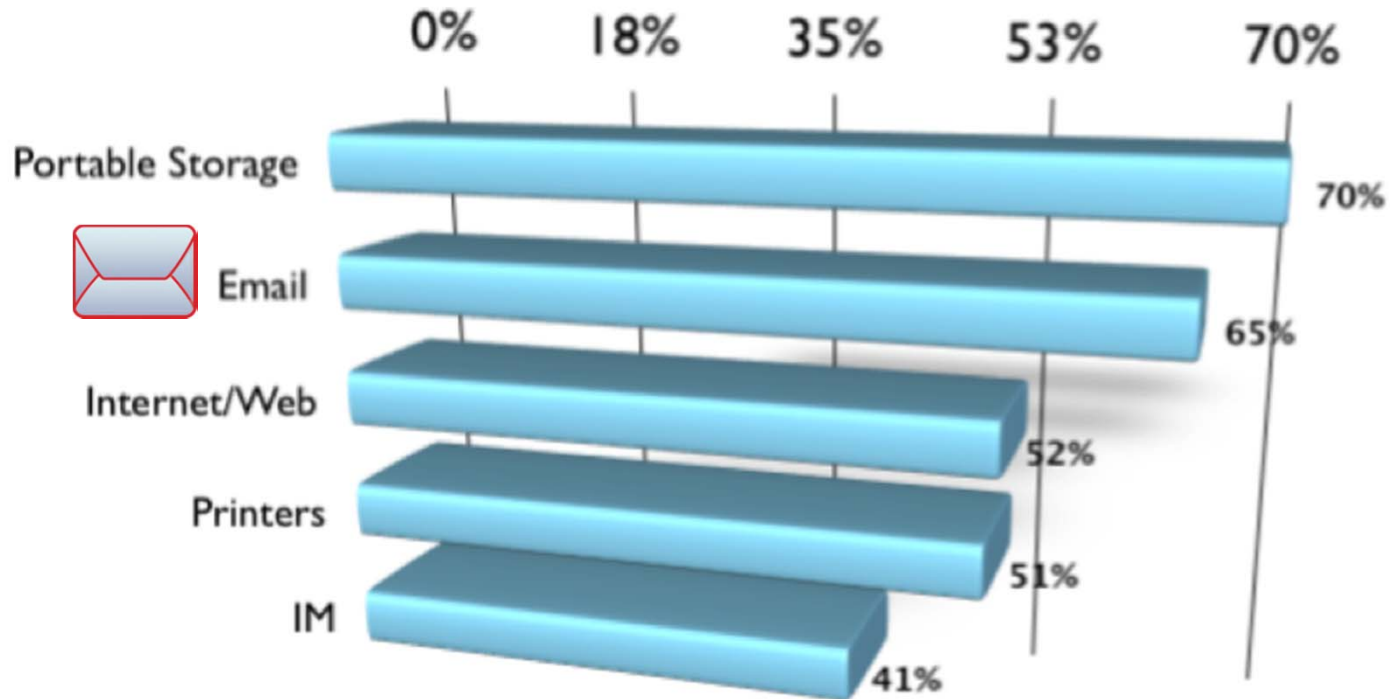
- 75% of all Email contain some Intellectual Property



Why Encrypt Email?

- Email continues to be one of the Most common data leakage channels

Source: Forrester Research 2009



Data Security Goals for all Organizations

1. Know who you are dealing with (Authentication)
2. Keep private information private (Confidentiality)
3. Ensure people don't cheat (Non-Repudiation)
4. Ensure information has not been altered (Integrity)



What is Encryption?

- Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing a “key” to unlock the data
- Another way to look at Encryption: It is a process of converting plaintext into an unintelligible form using a set of procedures and algorithms
- Plaintext is used as input to an encryption algorithm, the output is usually called ciphertext particularly when the algorithm is a cipher
- The use of encryption/decryption is as old as the art of communication. The Egyptians used encryption to securely communicate with each other in wartime
- Cryptographic techniques have been used for centuries to protect confidential information from prying eyes



Building Blocks for Encryption

1. Encryption is used to provide confidentiality and integrity protection to confidential data
2. Digital signatures are used to provide authentication, integrity protection and non-repudiation
3. Checksums / hash algorithms are used to provide integrity protection and can provide authentication



Types of Email Encryption

- **S/MIME** (Secure/Multipurpose Internet Mail Extensions) is a form of email encryption that is included in several email clients by default (such as Outlook Express and Mozilla Thunderbird) and relies on the use of a Certificate Authority (CA) to issue a secure email certificate

How S/MIME works

- The sender gets a certificate issued by a CA that is "installed" on their computer
- The sender emails a digitally signed email to all the people he would like to securely correspond with
- The recipient uses a copy of the senders digital signature to encrypt mail back to the sender
- In order to send encrypted mail, the sender must have both the sender's certificate and the recipient's digital signature on their computer

Types of Email Encryption

- **PGP** takes a de-centralized approach to email encryption
- It does not rely on trusting a Certificate Authority
- The users create encryption keys themselves.
- This allows users to choose:
 - key size (minimum 1024bit, maximum normally 4096bit)
 - an encryption/signing algorithm (eg. RSA, DSA or El Gamal)
 - their own expiry date
- The problem with PGP is that it is complicated to setup and use

- **TLS** (Transport Layer Security) and **SSL** (Secure Socket Layer Security) are less secure forms of email encryption used to encrypt messages from one server to another

Introduction to Public Key Infrastructure (PKI)

- The aim of PKI is to integrate all components of encryption mechanisms and algorithms into a coherent and efficient structure
- If done right, it will answer the following fundamental security needs:
 - Authentication
 - Confidentiality
 - Non-Repudiation
 - Integrity
- The basis of PKI relies on the concept of digital certificates

PKI Basic Functions

PKI will include at least:

- One Certificate Authority which delivers digital certificates
- One Directory that stores active Certificates and/or Revoked Certificates
- One Registration Authority that allows digital certificates' enrollment
- One centralized management

What is S/MIME & Email Encryption

- S/Mime (Secure Multipurpose Internet Mail Exchange)
- Developed by RSA, Microsoft, Lotus, Banyan, and ConnectSoft in 1995
- Implemented at the application layer
- Build on top of PKCS #7 and PKCS #10
- Very strong commercial vendor acceptance
- IETF developed S/MIME v3 (last version)
- Use X.509 certificates

Four Services Provided by S/MIME

<i>Security Services</i>	<i>Security Mechanism</i>
Message origin authentication	Digital Signature
Message integrity	Digital Signature
Non-repudiation of origin	Digital Signature
Message confidentiality	Encryption

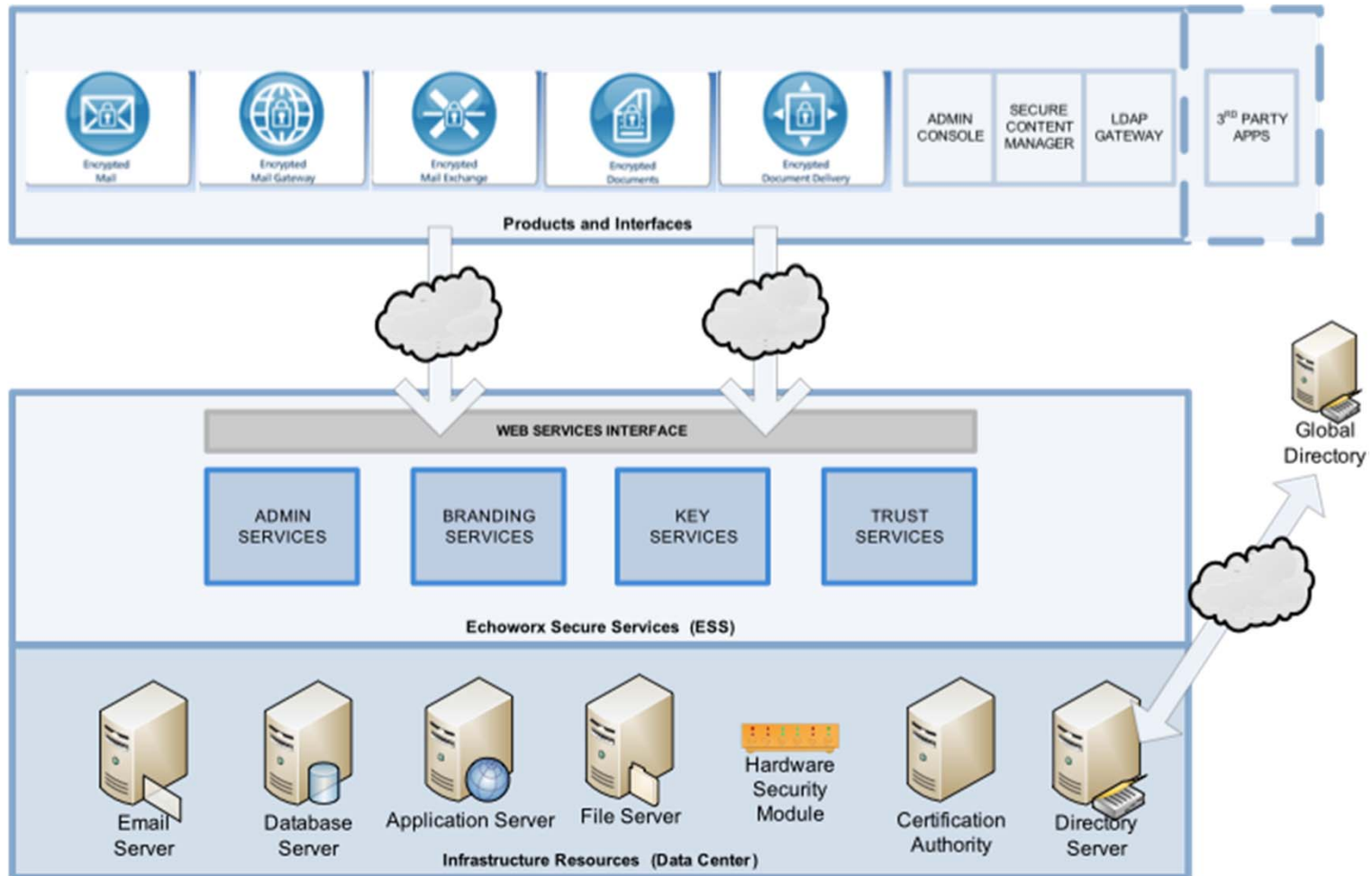
Understanding Email Encryption Products

- Before you can fit an encryption solution to a customer, ask yourself the following questions:
 - Does your customer require end to end email security i.e. from desktop to desktop?
 - Do they have a tech savvy user base or do they need an easy to use solution?
 - Would they benefit from “policy enforcement” ?
 - Is there staff and infrastructure in place to support a security solution or would they prefer a managed encryption platform?

Understanding Email Encryption Products

- The answers to your questions will lead you down one of the following paths:
 - **End to End Email Encryption: Echoworx Encrypted Mail** – Messages are encrypted directly from the desktop by the sender
 - **Policy-Based Encryption: Echoworx Encrypted Mail Gateway** – A solution that relies on encryption, based on pre-defined policies at the gateway rather than relying on the sender to encrypt messages
 - **Web or Cloud Encryption: Echoworx Encrypted Message Exchange** – A service that originates and delivers emails in a secure environment outside of the company network. This service is typically agnostic in its software and hardware requirements and relies on a secure messaging center

Encryption Platform Overview



Encryption Platform Highlights

- All applications are built on common platform and architecture
 - Leverages advanced and automated credential management invisible to Service Providers, Enterprise customers and end users
 - Underpinned by a globally trusted and professionally audited fully managed Public Key Infrastructure
- Designed to meet service provider and enterprise customer needs
 - Delivered as a hosted Software as a Service
 - Multi-tenant design
 - Based on open internet and international standards
 - Non-proprietary; not a point-solution
- Service oriented architecture for all cryptography infrastructure
- Highly distributed and scalable architecture
- Multiple data centers, shared public certificates
- Wide range of applications that cater to different security and usability needs

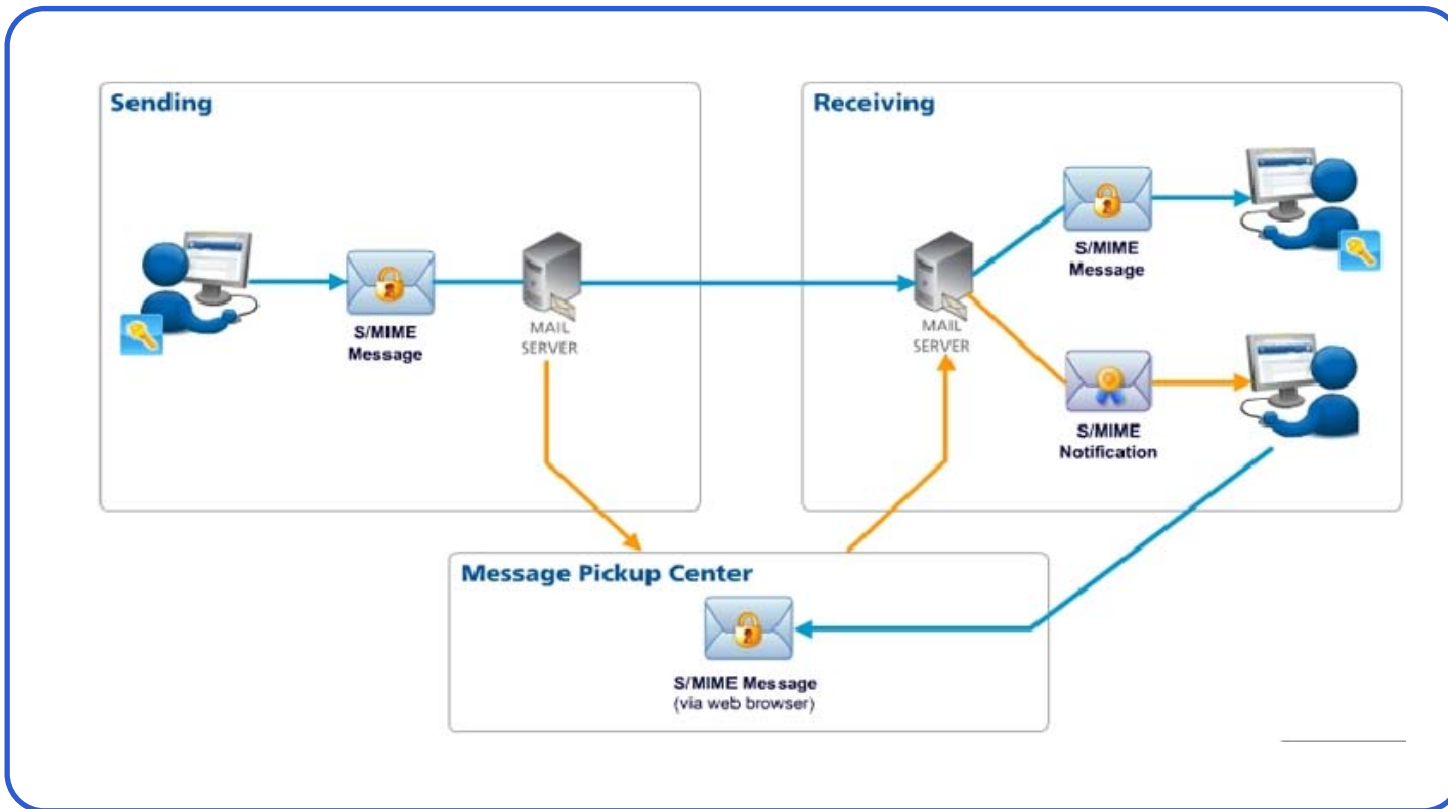
Features: End to End / Desktop Encrypted Mail

- Desktop components to provide end point to end point encryption (S/MIME)
- Desktop applications that use trusted PKI standards to allow for encryption and signing (for non-repudiation) of emails
- Fully managed PKI service to support credential life-time management and recovery
- Seamless integration with popular Email clients (such as Outlook, Lotus Notes, etc.) or stand-alone reader to work with any email client, including web based tools (such as GMail, Yahoo Mail, etc.)
- Centrally and dynamically branded user interface, supports multiple tenancy

Deployment: End to End / Desktop Encrypted Mail

- Desktop applications are “pushed out” with MSI (Microsoft Installer) or are installed as local software (one-time) on each desktop or laptop
- PKI infrastructure and web pickup portal are offsite and fully managed as a SaaS (Software as a Service) model

Overview: End to End / Desktop Encrypted Mail



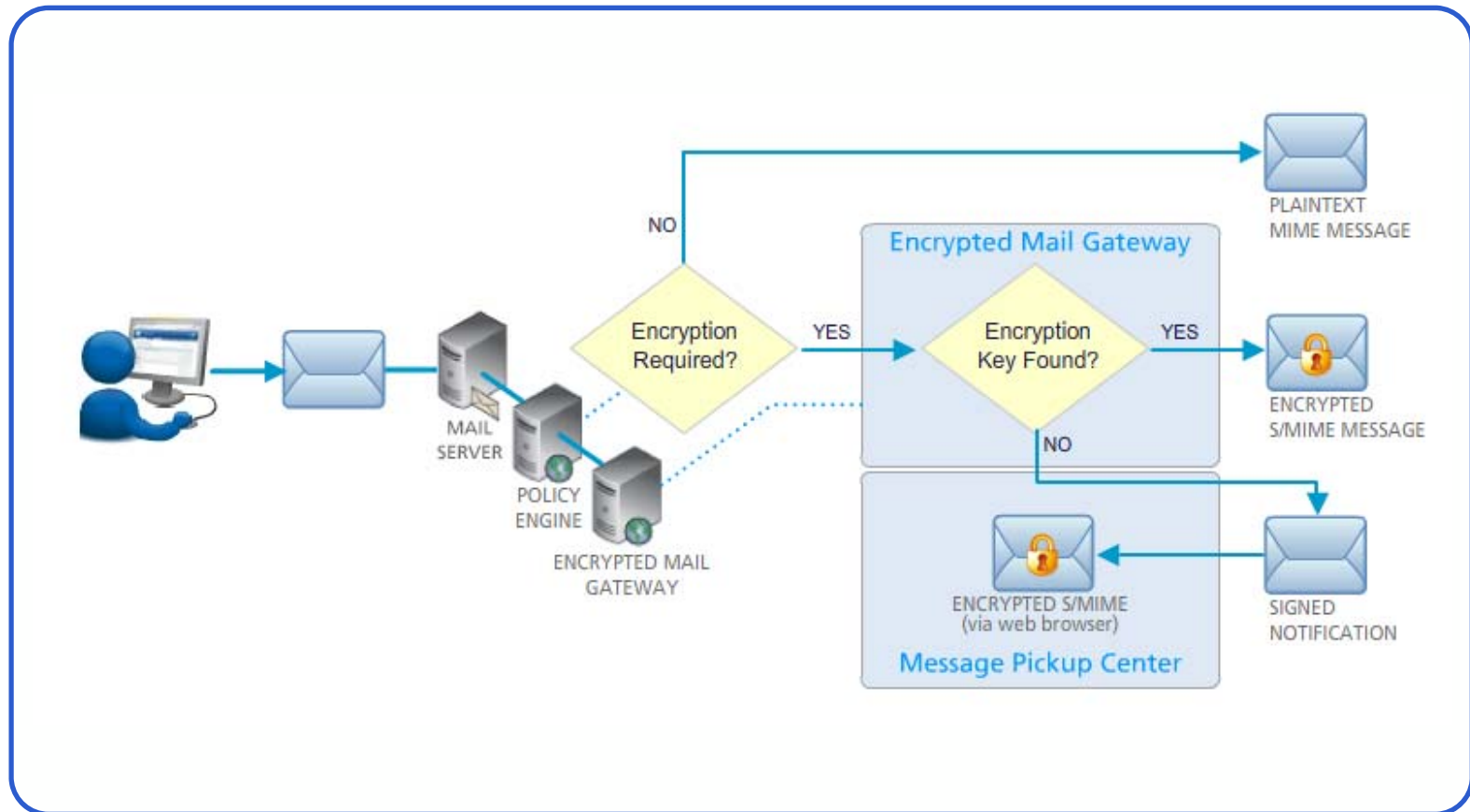
Features: Policy-Based Email Encryption

- Encrypts/decrypts messages to automatically deliver through best available channels
- Allows for encryption based on policy or content rules
- Works with third-party S/MIME and PGP credentials
- Recipients have the choice of web pickup or inbox pick up using PKI security (via Echoworx Encrypted Mail or Echoworx Encrypted Reader)
- Supports multiple tenancy, branding and multiple levels of administration

Deployment: Policy-Based Email Encryption

- Boundary based S/MIME encryption in the cloud (SaaS)
- Customers use their existing TLS channel to deliver messages, no extra deployment is needed
- No tight-integration between the provider and Echoworx is needed, uses standard email protocols for communication
- Typical installations include the Echoworx policy engine residing on premises with the messages travelling via TLS connection to the Encryption engine at an Echoworx secure facility

Overview: Policy-Based Email Encryption



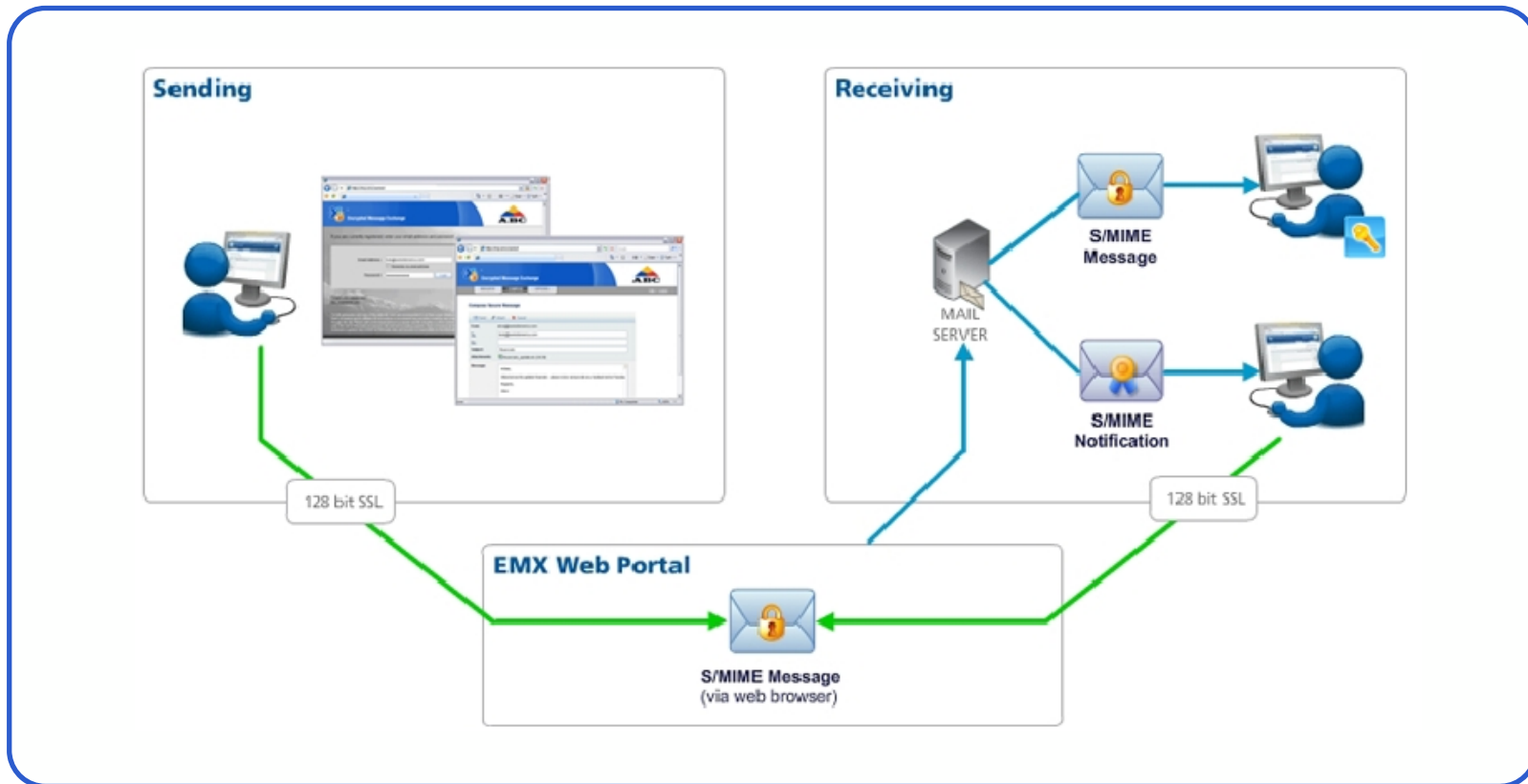
Features: Web-Based /Cloud Email Encryption

- Secure, encrypted communication web portal
- No desktop software needed and can be used by any browser (including mobile)
- Full audit capability around message access (read, notification etc)
- User can choose any of the 12 supported languages, has an inbox, can self manage and compose message
- All messages are kept encrypted at all times

Deployment: Web-Based /Cloud Email Encryption

- SaaS operated model through a secured channel (https)
- Supports different types of uses, such as a closed community portal or as a non-subscriber message pick-up portal
- Supports multiple tenancy, branding without deployment
- Complete “Cloud” solution

Overview: Web-Based /Cloud Email Encryption



Why Encrypt Sensitive Documents?

- Data Leakage
- Since the invention of the floppy disk, data leakage has been on the minds, and often in the nightmares, of all IT security personnel
- You could make the direct correlation between data leakage and the creation of the IT Security industry as a whole

Defining Data Leakage

- Data Leakage happens whenever a system reveals confidential information to unauthorized parties
- The term “system” is used in a way to indicate an organization of trained, knowledgeable people with responsibilities to a company or a physical / conceptual technological infrastructure
- Aspects of data leakage include:
 - The human effect
 - The technology effect

Defining Data Leakage

The Human Effect

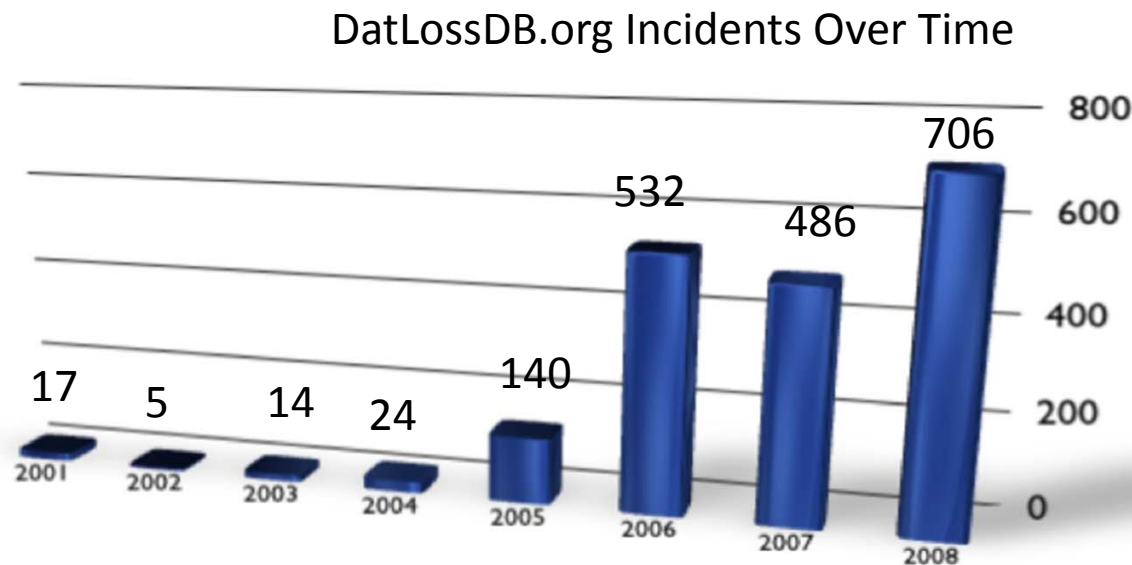
- An employee verbally reveals proprietary information to outsiders
- An employee reveals proprietary information while social networking on Facebook, MySpace, Yahoo! Chat, etc
- An ex-employee discusses trade secrets with a new employer
- An employee inadvertently leaves data in a public place

The Technology Effect

- Malicious hacking or use of virus, bots, and trojans to gain access to critical systems through corporate firewalls and safeguards
- Forwarding secure email communications via unsecure channels
- Downloading sensitive documents to portable devices including thumb drives, CD-ROMs, iPods, and more
- Physically stealing entire laptops, hard drives or thumb drives with proprietary data

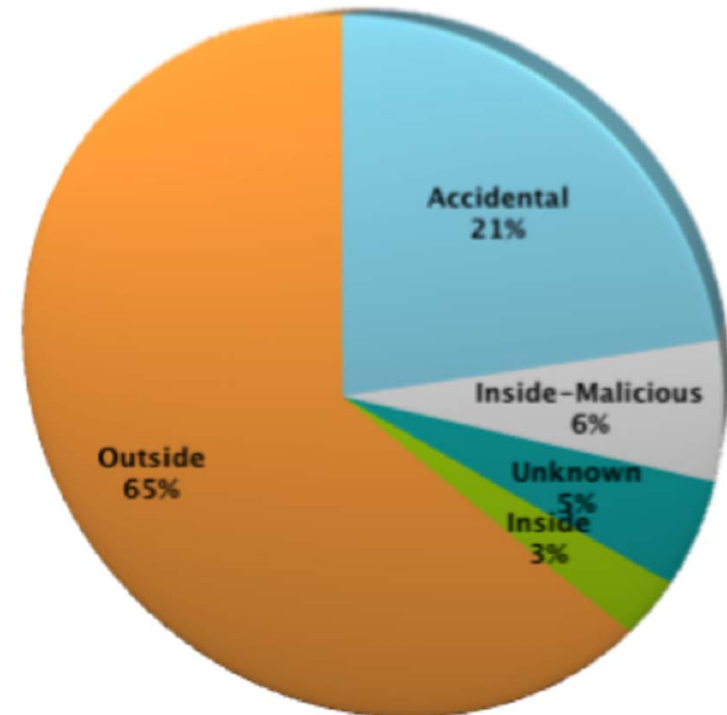
Data Leakage / Breaches Over Time

- Most breaches aren't reported as only a few states require open revelation of breaches to the public.
- Average cost of a data loss incident is \$140 USD per record



Data Leakage by Vector

- 21% of costly data leakage scenarios that were reported were “accidental
- You can’t totally rely on employees to protect data on their own
- Automated technology will have to be leveraged



Incidents by Vector - All Time

The Cost of a Data Breach

- \$140 per record: average cost of data leakage event
- \$14 M cost on average (100,000 records)
- \$5 M: Notification, legal expenses, discounts, telecoms
- \$7.5 M: Opportunity cost: retention and acquisition of customers

How Much Could it Really Cost ...

- \$1.5 M: Productivity losses due to additional load on staff
- ChoicePoint: \$79 per record lost (Gartner)
- \$11.5 M in expenses directly related to exposure
- \$15 M fine by Federal Trade Commission
- Average: \$79 per record disclosed
- 75 out of 150 companies surveyed had a data loss in the last 12 months (Deloitte Survey)

Why not Encrypt everything?

- Encrypting everything is a viable solution only if time and money are not factors in the decision process due to:
 - High up front capital investment in the encryption solution – most are not subscription model-based
 - Investment in newer equipment that can handle the burden of constant encryption
 - Increased training in both solution administration and management
 - Additional administration of password or key management
 - And more ...

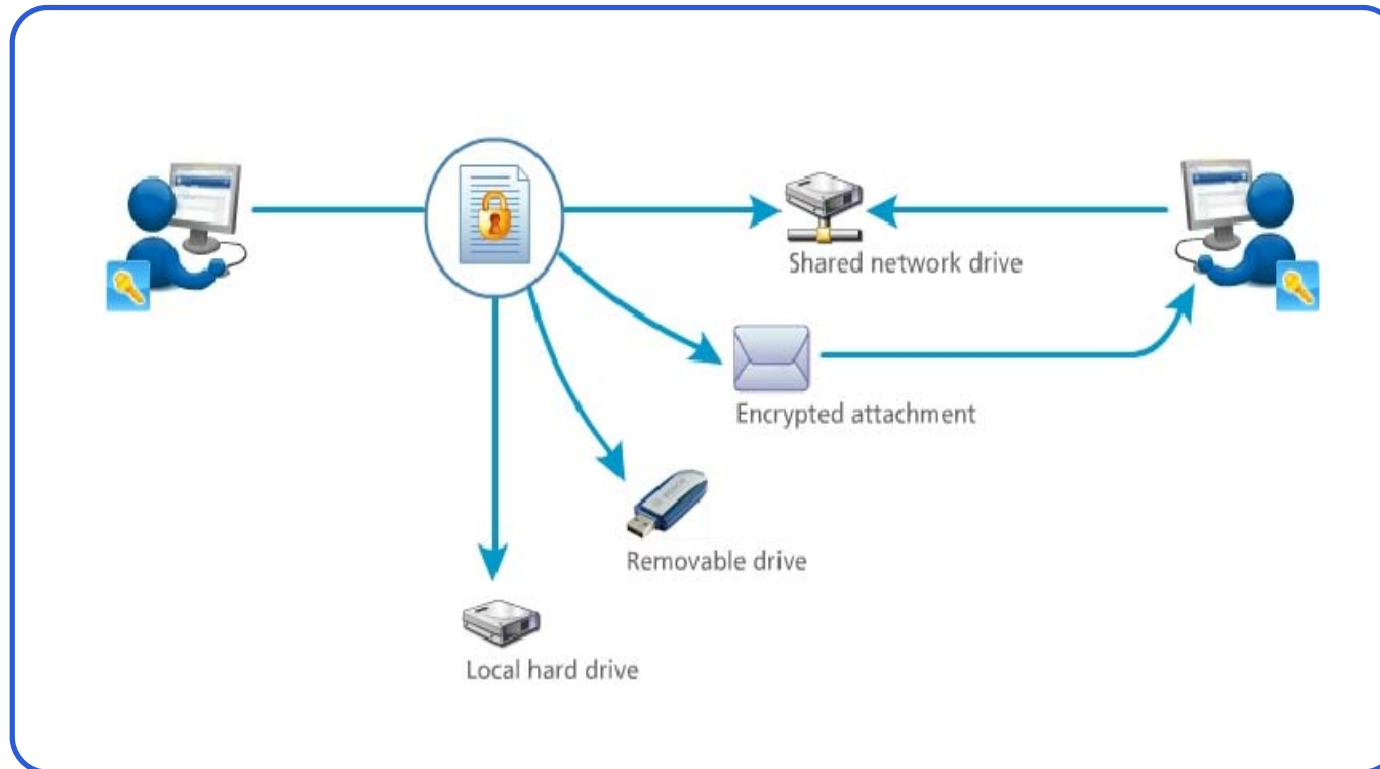
Features: Encrypted Documents

- Users can encrypt any folder /file locally or on a network
- All files written to the folder are encrypted based on the policy set by the owner (policy = who has access to files)
- User just install Encrypted Documents and sign-in
- Targeted to organization who want to enable users to encrypt and protect files
 - in a shared environment (network drives)
 - locally on their laptop
 - flash drives

Deployment: Encrypted Documents

- Based on a File Filter driver that integrates within the OS level
- Deployed either as a push or pull application
- IT Administrators can push the application down to the desktop via a software distribution method such as MSI, SMS, or gold image
- Users can pull down the application to their desktops from a hosted web site
- Credential services managed in the cloud as a SaaS model
- Users can encrypt/decrypt files and folders without having to worry about managing credentials and user certificates
- DLP features prevent users from copying unsecured files to external devices such as USB drives and external media

Overview: Encrypted Documents



Sample Positioning Case # 1

- The IT administrator of a small regional law firm asks if you provide a solution that can help his attorneys secure confidential emails to their clients
- The solution should be easy to use, with a simple click-of-a-button to secure individual emails
- No IT staff available; the solution would rely on each attorney's judgment
- The solution should ensure that the email is secure from the attorney to the client, never traveling without the actual message being unencrypted....

Sample Positioning Case # 1

- You'd recommend Encrypted Mail of course!
- In this case, the key factors you picked up on were:
 - Easy to use
 - No IT staff, so any solution would rely more on the individual attorney's judgment
 - Ensure that the email is secure from the attorney to the client, never traveling without the actual message being unencrypted

Sample Positioning Case # 2

- A National healthcare organization are actively seeking a way to secure emails to comply with HIPAA
- They want to ensure that the messages never leave their environment if they contain certain key words or phrases
- They realize that human error plays a part in everything, and the organization needs a solution that will **AUTOMATICALLY** encrypt emails based on pre-defined policies
- Their requirements include: easy to use, automated, and flexible policy management

Sample Positioning Case # 2

- Being an expert in encryption products, you recommend Encrypted Mail Gateway
- In this case, the key factors you picked up on were:
 - Messages never leave their environment if they contain certain key words or phrases
 - Needs a solution that will AUTOMATICALLY encrypt emails based on certain rules or policies
 - Requirements: easy to use, automated, and flexible policy management

Sample Positioning Case # 3

- A global insurance company uses independent agents to sell its suite of products to the market
- The CIO understands that they have little ability to influence the technical knowledge or infrastructure used by their agents
- Requirements:
 - Ensure that agents send and receive sensitive emails securely
 - They don't want to set policies or train the agents on proprietary software
 - Simple, centralized location that the agents can log into and send or receive encrypted Emails, regardless of their hardware platform
 - Ability to add and subtract authorized users in a quick and efficient manner

Sample Positioning Case # 3

- Web-based cloud email encryption solution like Encrypted Mail Exchange
- Key factors:
 - No ability to influence the technical knowledge or infrastructure their agents use
 - Does not want to set policies or train the agents on a proprietary software technology
 - Simple, centralized location that the agents can log into and send or receive encrypted Emails, regardless of their hardware platform
 - Needs the ability to add and subtract authorized users in a quick and efficient manner

Sample Positioning Case # 4

- Customer requirements:
 - Secure files and records pertaining to all human resource data and company financials
 - Restrict access to certain groups
 - Ability to quickly add and remove employees from the access list for each individual document and folder
 - Automated encryption solution based on pre-defined policies and not at the employees' discretion
 - Under consideration is encrypting everything although they realize this will be cumbersome and expensive

Sample Positioning Case # 4

- Encrypted Documents is the perfect solution
- In this case, you heard:
 - Secure files and records pertaining to everything from human resource information to company financials
 - They want the ability to easily add and remove employees from the access list for each individual document and folder
 - The ability to secure or encrypt the information needs to be automated and based upon company policy
 - Ability to add and subtract authorized users in a quick and efficient manner

DSPC Summary



- Increase Revenue Opportunity
- Higher Confidence in selling Encryption / Security Services
- Opportunity to use DSPC Logos
- Reference Worthy
- Zero Cost to Certify
- Exclusive Pool of Certified / Qualified Candidates
- Simple Re-Certification Process