

**Who else is reading your
email?**

No one!

Are you sure?

Secure messaging from CipherTrust.
Be sure.SM



Secure Messaging • Reliable Appliance • Highly Scalable

Presentation Outline

➤ Security

- Is security really an issue?
- What does CipherTrust offer?
- How does it work?
- Does that meet HIPAA/HCFA requirements?

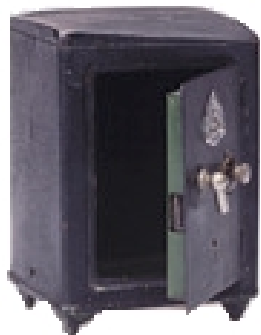
➤ Message management

- What are the issues?
- Is CipherTrust's solution reliable and easy to use?
- Is CipherTrust messaging scalable?

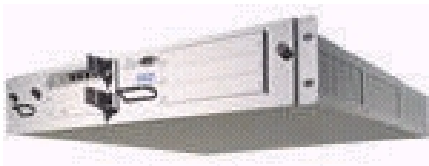
➤ The Bottom Line



We Usually Protect What's Important



Vaults protect
your money



Firewalls protect your
networks and
intellectual property



**What's
being done
to protect
your email?**



“Golden handcuffs”
protect your
employees



Door locks
protect your
offices and homes



Secure Messaging • Reliable Appliance • Highly Scalable

Be afraid...

***Carnivore
Is
coming!***

Be very afraid...



Secure Messaging • Reliable Appliance • Highly Scalable

What About Security?

“When sent via the Internet, E-mail is like a postcard that can be read by hackers or copied in every "post office," or Internet computer, it passes through. E-mail confined to a private network isn't necessarily more secure: Tools for getting to it are readily available to hackers.”

- Fortune

“*Secure email?* Most organizations must securely send e-mail over the internet to business partners, customers, or their employees. Many options currently exist, but a *perfect solution remains elusive.*”

- The META Group



The Need for Security Is Compelling

ORACLE

Fraudulent email used to bilk \$100,000 from Oracle in phony sexual harassment case.

- Source: www.employlaw.com



Merrill Lynch

“... Merrill Lynch will not be responsible for any loss or damage that could result from interception by third parties of any information made available to you ...”

- Source: www.merrilllynch.com

FBI's CARNIVORE

“... there is no substitute for electronic surveillance ...”

- Source: www.fbi.gov

EMULEX

“... The negative statements in the fraudulent press release resulted in unprecedented volatility in Emulex's stock, creating large losses for shareholders victimized by this hoax ...”

- Source: www.emulex.com

Bank of America.



“... Regular non-encrypted Internet e-mail is not secure ...”

- Source: www.bofa.gov



Secure Messaging • Reliable Appliance • Highly Scalable

Currently, Secure Messaging Is Problematic

- Messaging systems are extremely vulnerable
 - Sensitive information is routinely sent through email
 - Email messages travel across the internet in plain text
 - Messages can be viewed, altered, deleted, and saved, with no evidence of tampering
 - Even when using S-MIME, reading email exposes the user name and password when logging in to POP3
 - “Sniffing” software is easy to get and use
 - Carnivore is being deployed
 - Existing certificate-based security solutions are cumbersome and costly to deploy and maintain
 - Most legacy messaging servers introduce significant network security risks



Analysts Agree

“By 2003, 60% of global 2000 organizations will have a formal structure to enable some form of *secure* e-mail delivery over the Internet.”

-The META group



Our Comprehensive Secure Messaging Solution

- CipherTrust provides the *only* comprehensive secure messaging solution
 - Security both inside and outside the firewall
 - Flexible solution supports multiple encryption schemes, including S-MIME and Web mail
 - Vastly reduced certificate management
 - Secure remote management

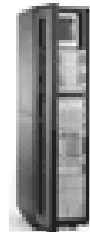


Typical Messaging

Remote Office Network

Sender

... Smith \$1000,
Turner \$1500...



Unsecured
Message
Server

Firewall

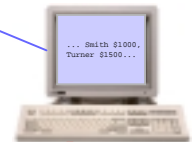
... Smith \$1000,
Turner \$1500...

Internet

Corporate HQ Network

Recipient

... Smith \$1000,
Turner \$1500...



Unsecured
Message
Server

Firewall

Username: Bob
Password: 123

Not Secure

Secure



Secure Messaging • Reliable Appliance • Highly Scalable

CipherTrust Messaging

Remote Office Network

Sender

... Smith \$1000,
Turner \$1500...

... Y&3#@!+PV3~1@
9YH*%\$3@!{?<...

Firewall

CipherTrust
Message
Server

Corporate HQ Network

Recipient

... Smith \$1000,
Turner \$1500...

... Y&3#@!+PV3~1@
9YH*%\$3@!{?<...

Firewall

CipherTrust
Message
Server

... Y&3#@!+PV3~1@
9YH*%\$3@!{?<...

Internet

...Y&0\$A~#^*!...

Not Secure

Secure



Secure Messaging • Reliable Appliance • Highly Scalable

HCFA Encryption and Authentication Standards

Requirements:

Triple 56 bit DES or equivalent for symmetric encryption

1024 bit algorithms for RSA asymmetric encryption; or

160 bits for elliptic curve asymmetric systems

Hardware Encryptors; or

SSL 3.0; or

S-MIME; or

In-stream; or

Offline

Authentication or Identification

CipherTrust:



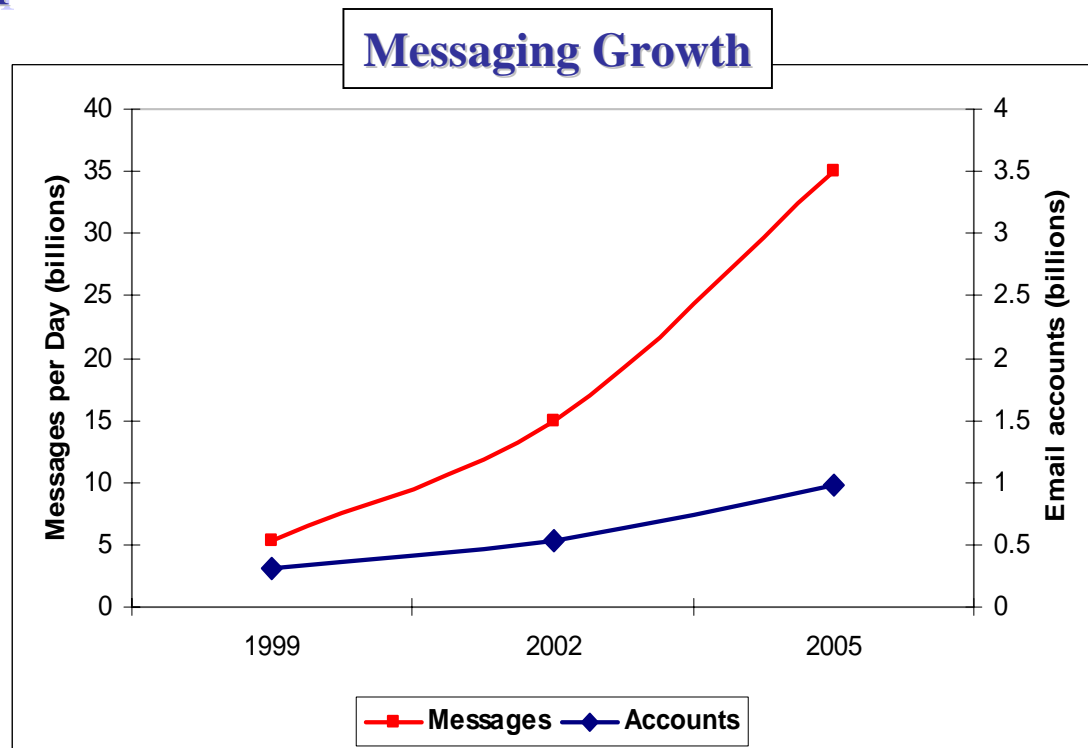
Explosive Growth in Messaging

➤ Messaging is THE killer app for the internet ¹

➤ Up to **75%** of “knowledge exchange” in an enterprise happens using email ³

➤ **46%** of IT managers list email as “mission critical” ⁴

➤ By 2004, more than **1 billion** wired and wireless devices will be used to access email ⁴



	1999	2002	2005
Messages	5.3b ¹	14.9b ¹	35b ²
Accounts	315m ²	530m ²	983m ²

Sources:

1 SG Cowen

2 IDC

3 Gartner Group

4 Statistis Group



Internet Messaging Is Exploding, So Are the Issues

- Message security is a huge issue, but its not the only issue!
- Server reliability and availability
 - Installation of message servers is time consuming and requires experts
 - E-mail infrastructure requires specialized staff to maintain systems
 - Server malfunctions create significant productivity headaches
- Scalability
 - Existing enterprise messaging products don't scale without introducing security or performance compromises
 - Proprietary solutions prevent good security, scalability, manageability and outsourcing



CipherTrust Offers a Scalable, Reliable Appliance

- Appliance eases deployment and administration
- Mission critical reliability for the enterprise
- Highly scalable architecture supports millions of users
- Accommodates tens of thousands of users per server
- Provides much greater message server performance



Summary

➤ CipherTrust Provides:

- Highest level of security and hacker resistance.
- Secure, remote management saves time and money.
- Implementation is fast, thus lower cost.
- Fewer and lower cost personnel needed to install and maintain the servers and applications.
- No need for lengthy administrator training.

The cost of NOT securing your messages could be huge.



The Bottom Line

“CipherTrust is doing for Internet
messaging what Cisco Systems did for
Internet *routing*, ...”

“...we’re putting secure messaging in a box.”



Internet messaging from CipherTrust.

Be sure.SM



Secure Messaging • Reliable Appliance • Highly Scalable