

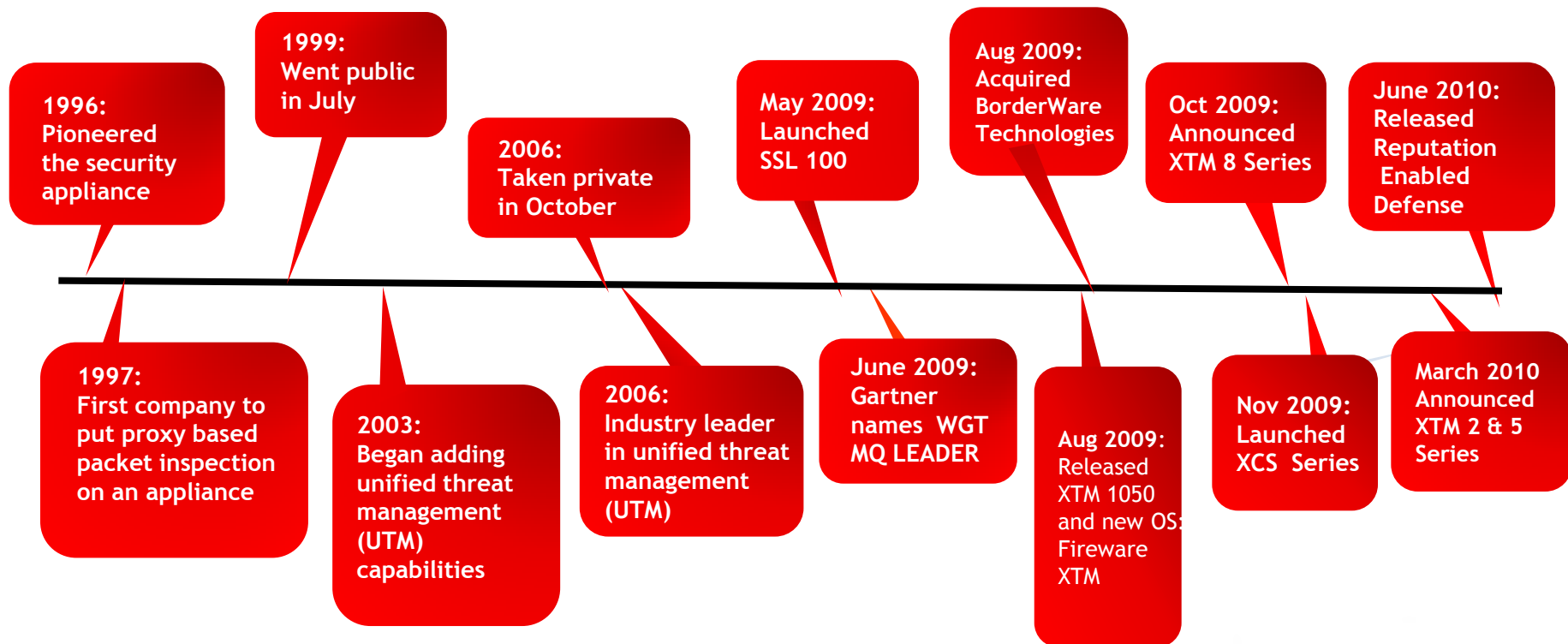
# Get Secured.

WatchGuard XCS Data Loss Prevention

Ensuring Privacy & Security of Outbound Content

# WatchGuard Today

- Started in 1996
- More than 600,000 appliances shipped to business customers worldwide
- 15,000 partners in 120 countries
- A history of innovation, market leadership and outstanding service



# Introducing the new XCS Series: Extensible Content Security highlights

- Powerful anti spam
  - Blocks 98% of spam with 99.9% accuracy inbound and outbound content scanning, threat prevention, and policy enforcement
- Clustering and queue replication
  - Zero messages lost
- Privacy and compliance
  - Email encryption
  - Predefined compliance dictionaries



# WatchGuard XCS Available in 7 Models

- WatchGuard XCS 170, 370
  - SMB
  - Any company needing strong anti-spam



- WatchGuard XCS 570, 770, 770R, 970, 1170
  - MSSP & Data Center
  - Retail (PCI Compliance)
  - Education: Large School Systems
  - Healthcare: HIPAA compliance
  - Finance & Banking: GLB, SOX compliance
  - Government: Federal, State and local



# Who relies on WatchGuard XCS?

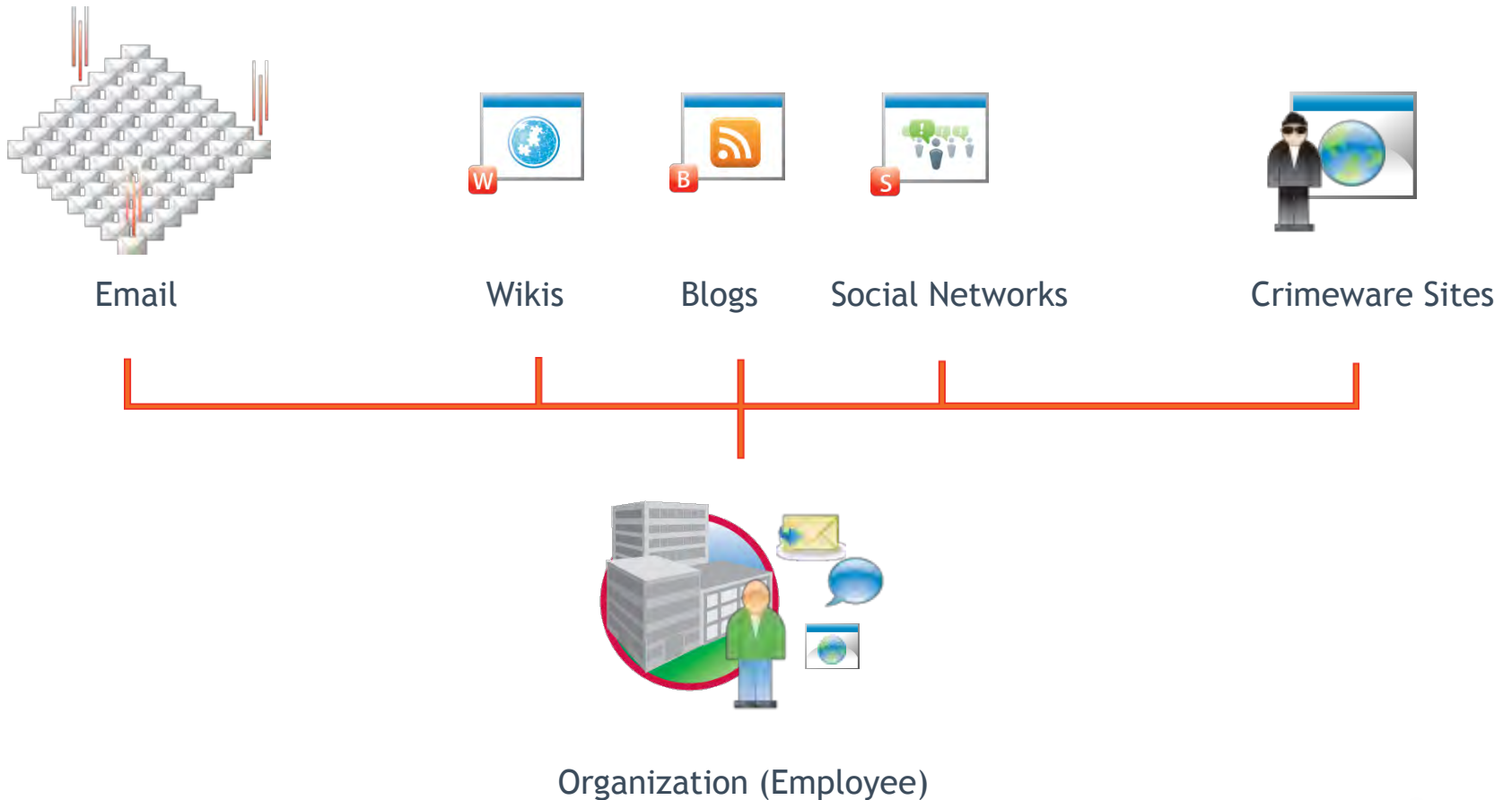
Government	Finance & Insurance	Health Care	Transportation	Technology	Entertainment	Food & Beverage	Retail & Services

Air Transport	Telecom & ISP	Education	Automotive	Manufacturing

# The Data Loss Landscape



# Framing the Problem: Potential for Leaks is Vast



## Data-In-Motion Accounts for 83% of Data Leakage

*“Email has become the de facto filing system for nearly all corporate information, making it even more critical to protect the outbound flow of messages.”*



*“80% of all DLP issues relate to sensitive data being lost across SMTP (Email) and HTTP (Web).”*



FORRESTER

# Data Loss Prevention Is A Top Security Priority



## Risks

3:5 firms experience a data loss or theft event <sup>1</sup>

9:10 data loss or theft events go unreported <sup>1</sup>

1:5 employees have emailed confidential data from their corporate account to a personal one <sup>2</sup>

1 - <http://www.ponemon.org/news-2/7>  
 2 - [Dell + Ponemon Survey](#)

# What our customers are telling us about their data loss concerns...

## Loss of Sensitive Information

“I don’t know how we can control data from being sent in email or uploaded to the Web.”

## Inadvertent Misuse

“Most of our email policy violations and information breaches are accidental!”

## Protect Critical Data

“We need the ability to protect known confidential documents from leaving the organization.”

## Collaboration Risk

“I think some of my employees are sending confidential information via the Web.”

## Granular Compliance Requirements

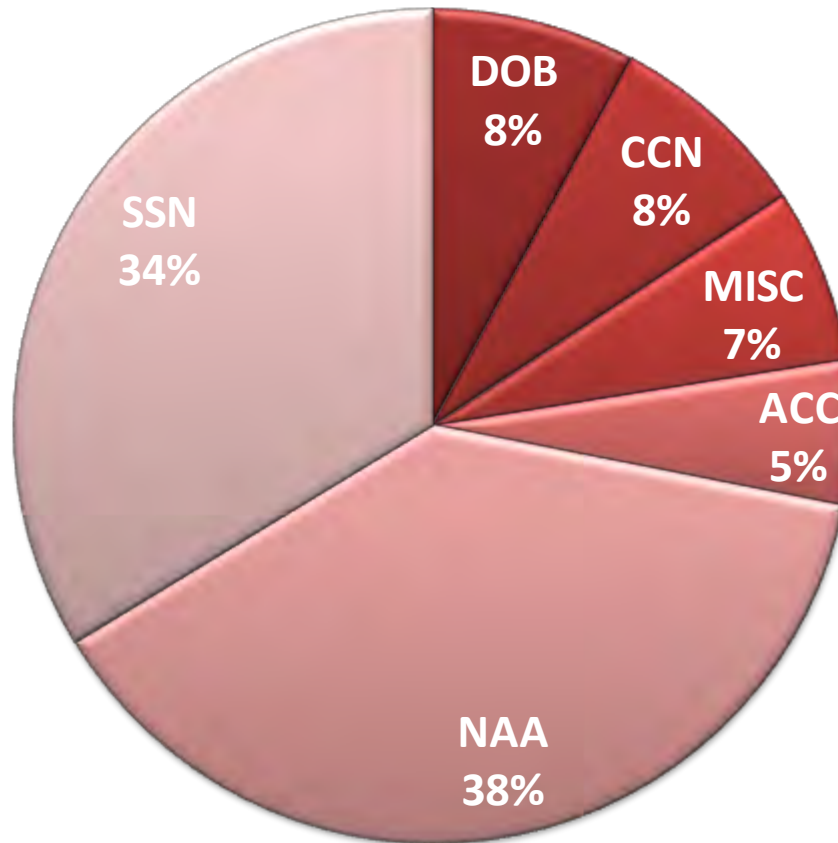
“The auditors are not just checking infrastructure controls anymore; they want to see more specific data-in-motion controls over my sensitive data.”

## The Cost of a Data Loss Incident

- \$6.6 million US per breach
- Negative PR
- Brand erosion
- Lost consumer confidence
- Lost business partner confidence
- Regulatory fines
- Stock market loss
- Legal fees
- Implementation of internal processes

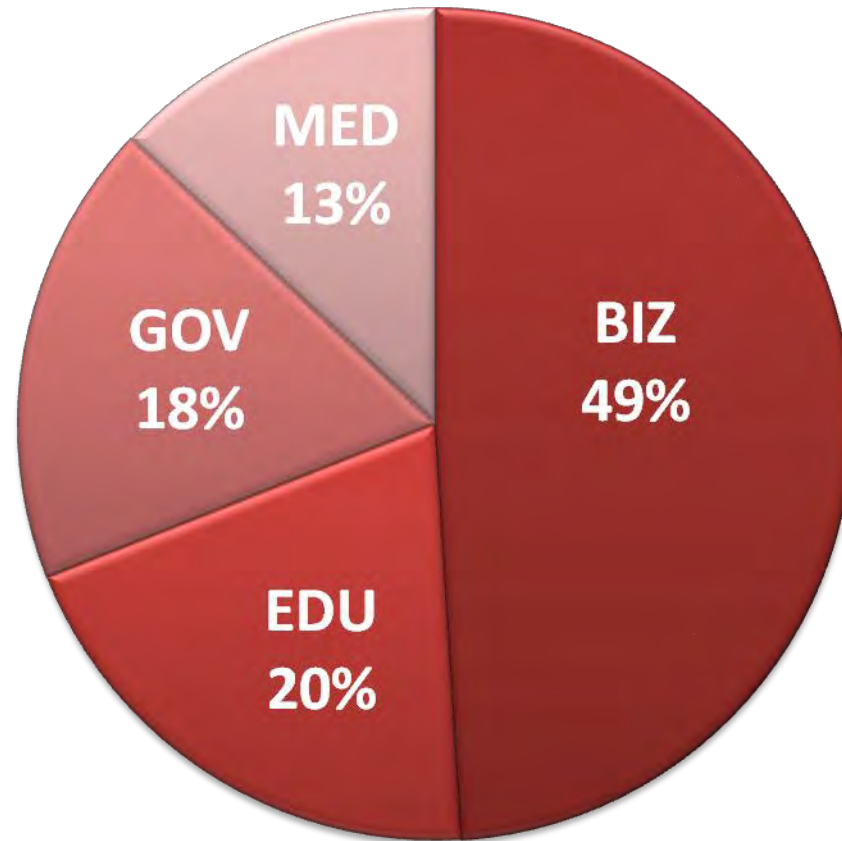
**Can your organization afford a data loss incident?**

# Incidents By Data Type



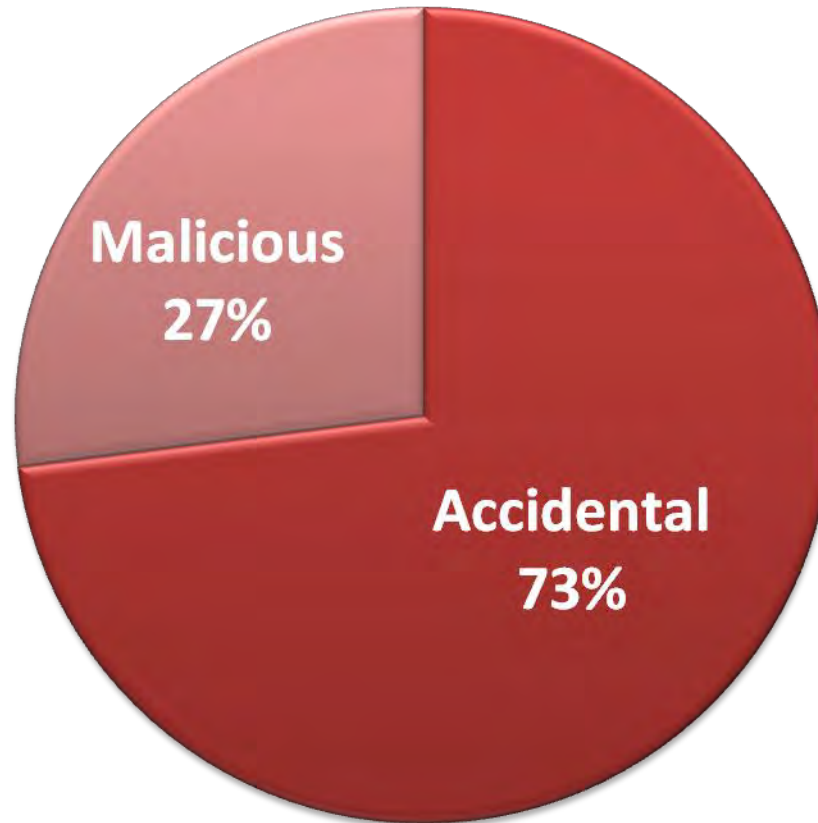
Source: DatalossDB

# All Businesses Are Victims of Data Loss



Source: DatalossDB

# Data Loss Resulting From Internal Sources



Source: DatalossDB

# Exacerbating the Problem: Privacy and Security



Regulations



Internal Policies



Acceptable Use



Intellectual Property



Employee

# Data Loss Prevention



# What is Data Loss Prevention (DLP)?

- Data Loss Prevention is:
  - A business tool that requires a comprehensive strategy
  - Technology that inspects sensitive content, and audits and enforces content use policies
  
- Data Loss Prevention can be used for:
  - Regulatory due diligence
  - Intellectual property protection
  - Accidental data loss
  - Data theft

## Data Loss Prevention as a Tool, NOT as a Silo

- DLP as a Silo...
  - Standalone product that requires agents, gateway and multiple FTEs for technical management and policy administration
  - High upfront expense with high total cost of ownership
  - Disparate and proprietary that does not integrate well with security
  
- DLP as a Business Enablement Tool...
  - Seamlessly integrated with a secure content and threat management platform
  - Scans across email and web with consolidated policies, management and administration
  - Automated with no additional FTEs required
  - Low entry expense with low total cost of ownership

# WatchGuard Data Loss Prevention

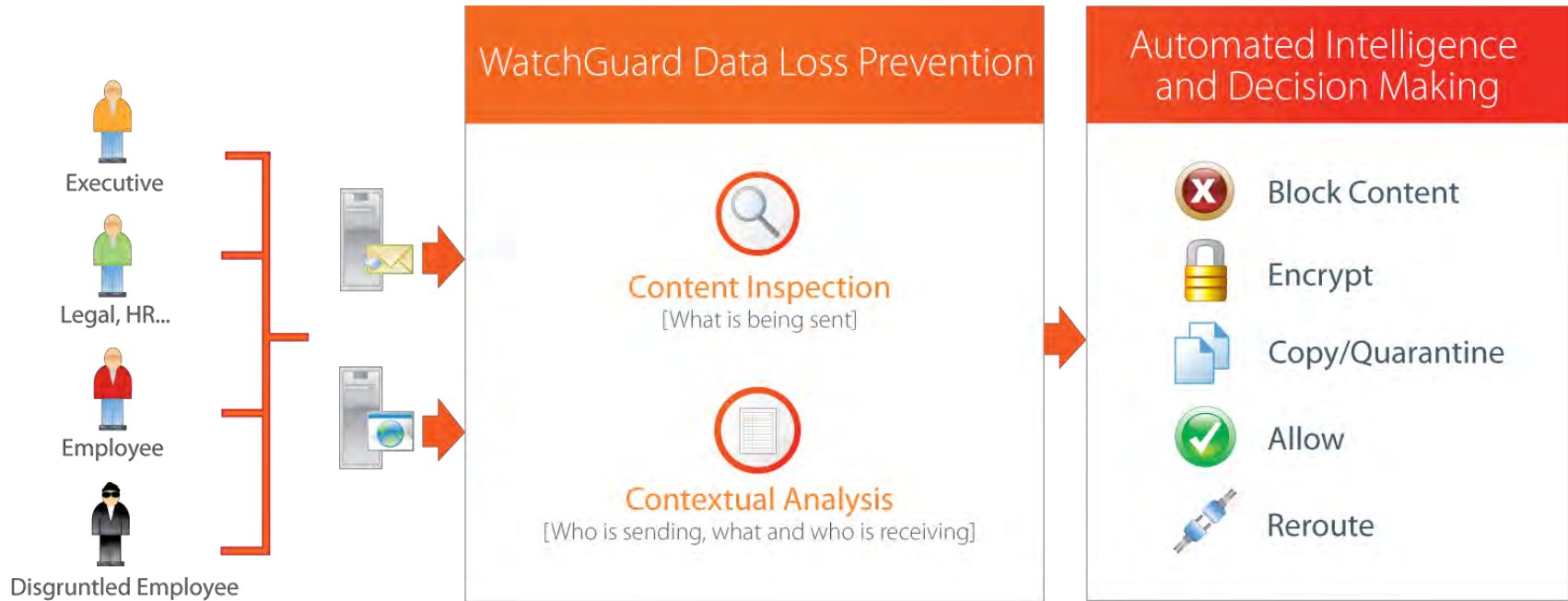
- Deep Inspection
  - Email & Web
  - Content and context scanning
- Consolidated Policy Management
  - Single UI
  - Reporting
- Integrated Remediation
  - Encryption
  - Block or allow
  - Quarantine or reroute
- Instant-On Data Loss Prevention!!!



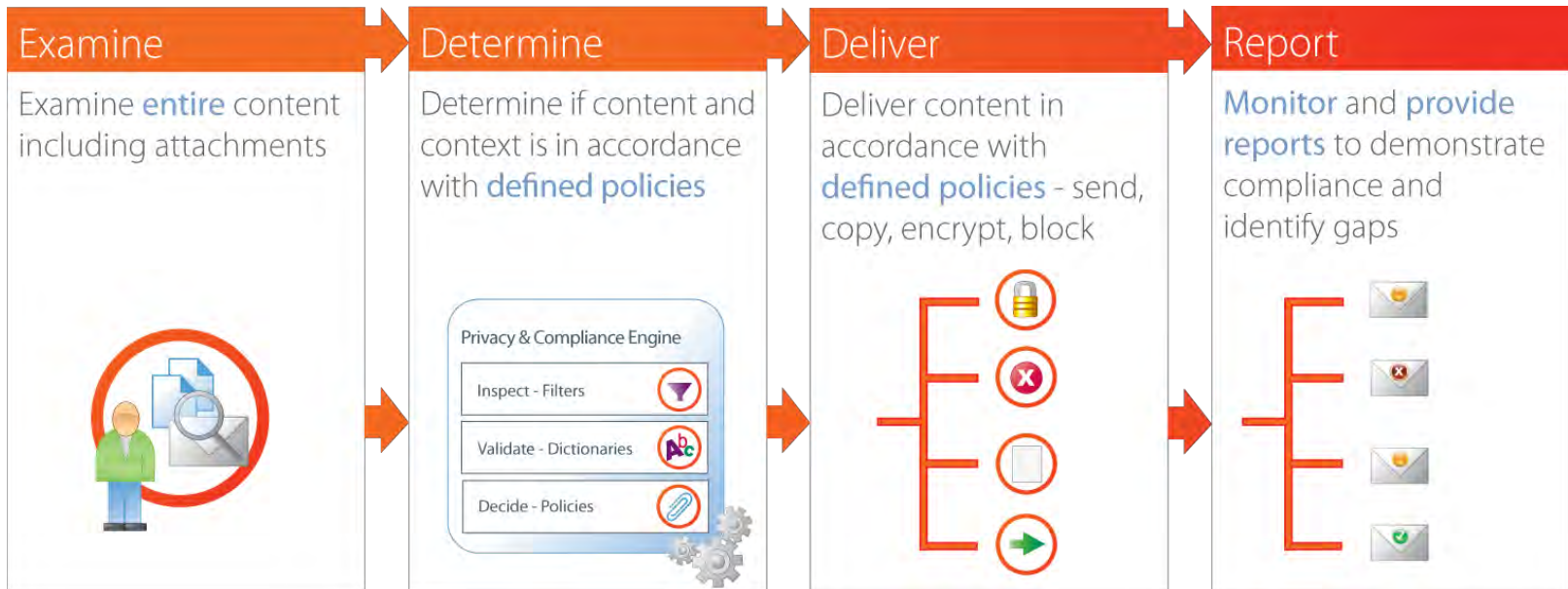
*“The true value of content monitoring and filtering lies in helping management to identify and correct faulty business processes and accidental disclosures.”*

Source: Gartner Research: Content Monitoring and Filtering Helps Find Faulty Business Process, Accidental Disclosures

# The Power of Content & Context



# Seamlessly Integrated Process



# Content Scanning For Accurate Detection of Policy Violations

- Performs deep scanning of attachments in email messages and web requests looking for patterns of text and phrases
- Allows ability to use filter rules and policy settings to scan attachments for specific content that could be a data breach violation



# Compliance Dictionaries

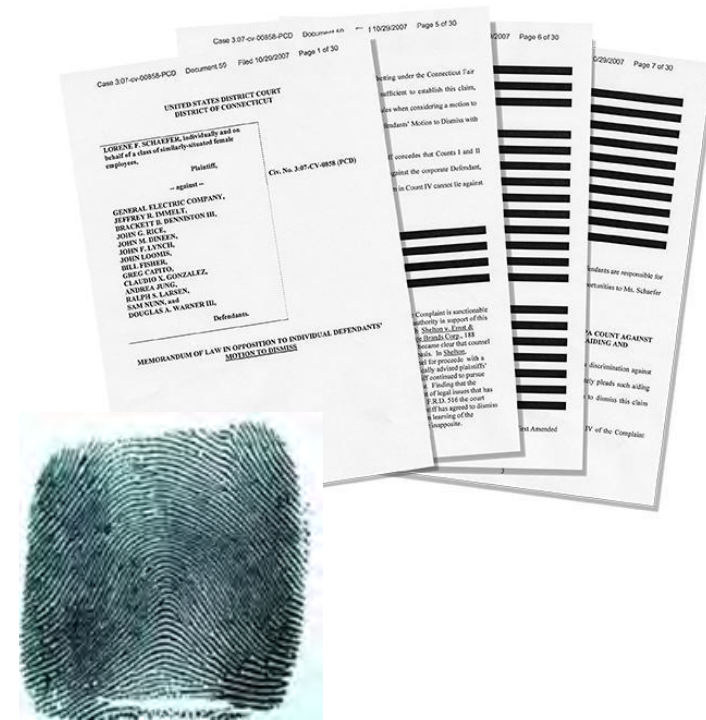
- Content scanning provides ability to upload your own dictionaries or can use included compliance dictionaries
- Contain a list of words and phrases that are checked against text in scanned attachment files and web uploads and downloads
- Weighted thresholds can be set for weighted compliance dictionaries
  - Example: Outbound message contains the phrase “patient number” and the term “diagnosis”; administrator has set weighted threshold for the compliance dictionary to 100
  - Weighted dictionary values:
    - patient number = 50, diagnosis = 50
  - Therefore, message is blocked based on policy set by administrator because combined weighted value meets/exceeds the weighted threshold of 100

# Objectionable Content Filtering for Enhanced Content Filtering

- Defines a list of key words that cause a message to be blocked if any of those words appear in the message
- Predefined lists are configurable and can be customized to meet specific needs of the organization
- OCF words are extracted from messages that disguise words using certain techniques (e.g. use of spacers, underscores, etc.) to block malicious data loss attempts
- Prohibits release of sensitive content outside of the organization

# Document Fingerprinting Protects Critical Business Documents

- Document fingerprinting to detect and protect confidential files and content
- Easily registers sensitive files for whole or partial match
- Scans all outbound messages and attachments
- Assigns a remediation score based on policies



# Protect Credit Card Information to Ensure Customer Privacy

- Supports regulatory compliance for PCI and other types of DLP digital security standards
- Includes predefined regular expression pattern filters that search messages and attachments for specific credit card patterns
- Several default credit card types including Diners Club, American Express, Discover, MasterCard and Visa

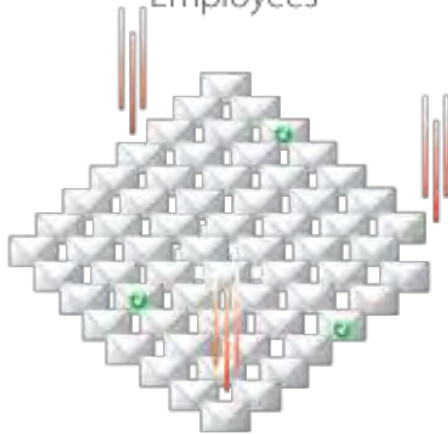
# Email Encryption



# Everyday Messages Contain Private Data



Employees



Partners



Remote Employees



3rd Parties



Ad Hoc

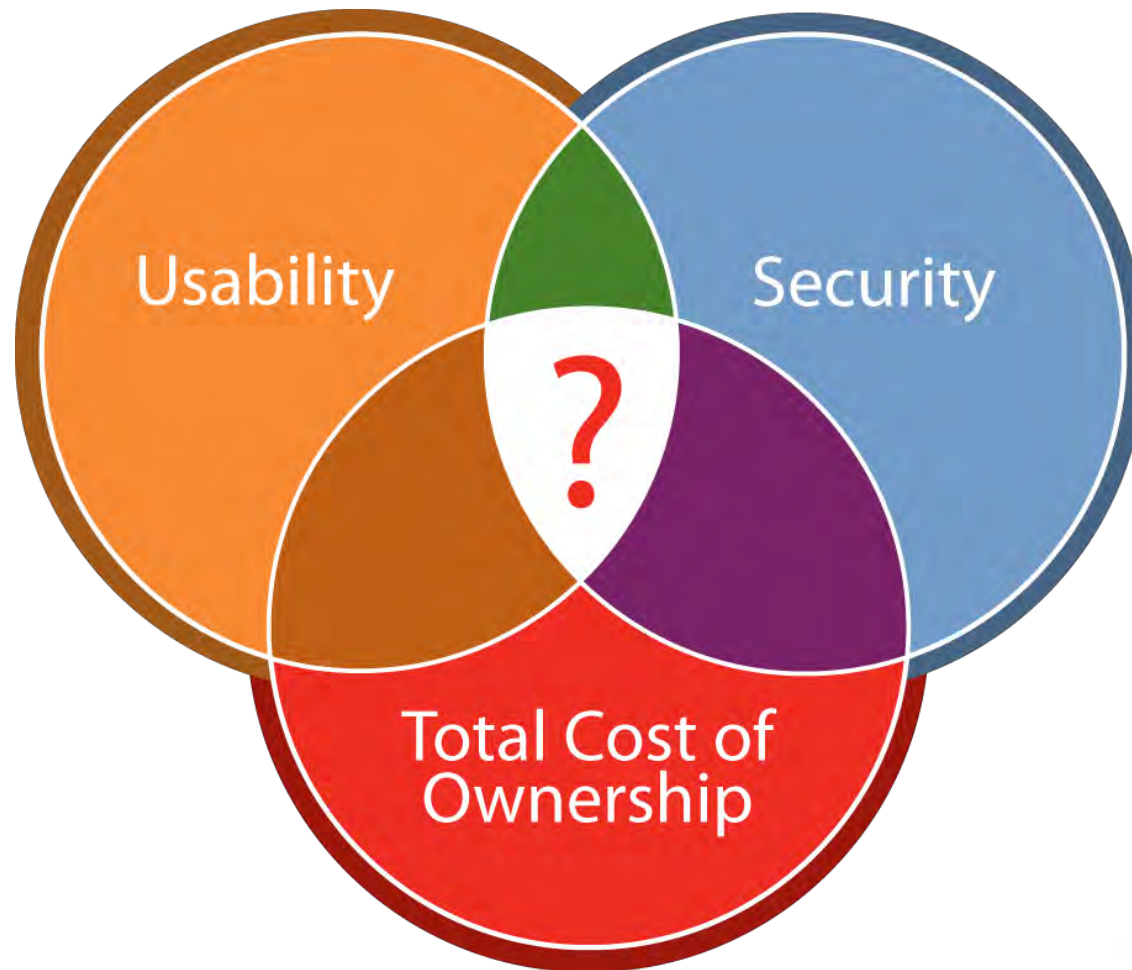
- Privacy
- Compliance
- Sensitive Information
- Confidential Data
- Intellectual Property
- Attachment Risk
- Mandated Third Party Security
- Security Prudence



# Encryption Use Cases

- Business Processes
  - Operations, finance, legal, M&A and HR
  - Sales, purchase orders, quotes and invoices
  
- Compliance
  - PCI, HIPAA, EU Directive, GLBA, PIPA...
  - 3<sup>rd</sup> party communications

# Why Email Encryption Isn't Used By Everyone...



# Secure Email Made Easy With XCS SecureMail Email Encryption

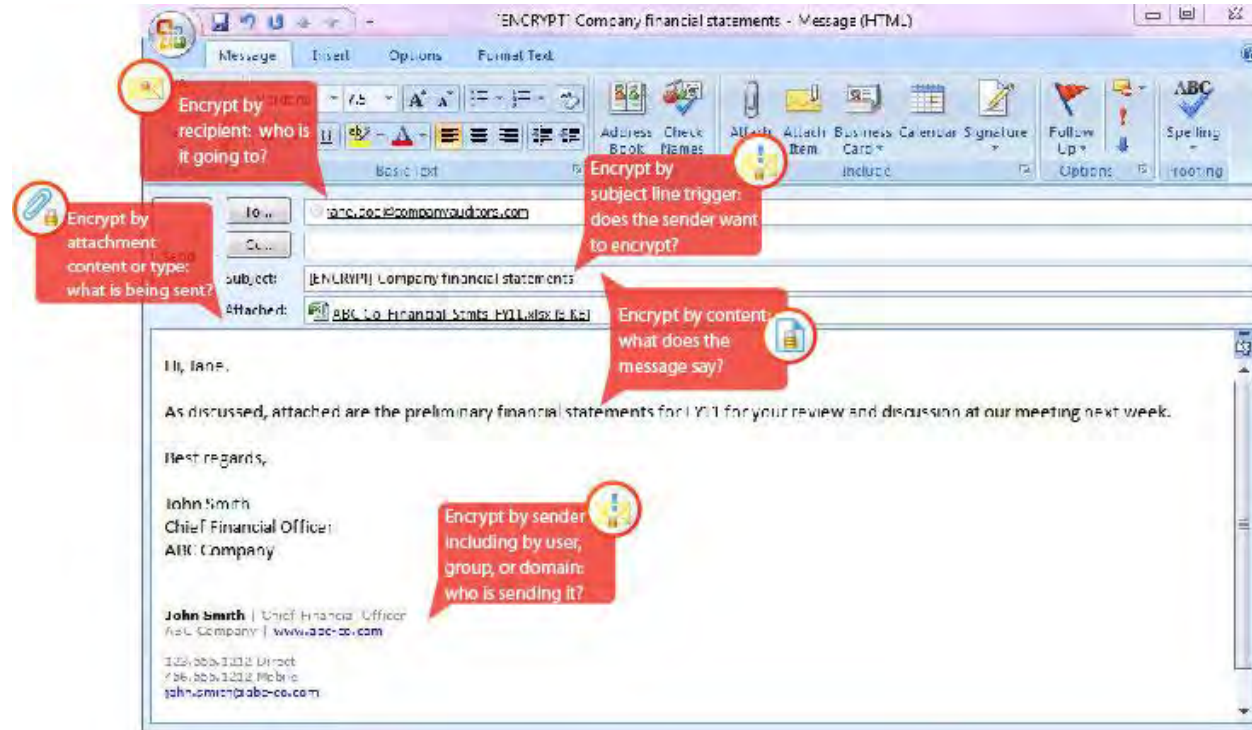
- Provides easy-to-use, transparent encryption to enable organizations to securely transmit and receive private and sensitive information
- Available as an add-on with all WatchGuard XCS appliances, and is tightly integrated within the product to enable instant-on security for confidential, regulated, and business-prudent information
- Effective tool to help you achieve and maintain regulatory compliance and enforce best-practice email protection, without disrupting your business

# Powered by Next-Generation Identity-Based Encryption Technology

- Uses simple identity - an email address as sender and recipient email address as the keys in a public/private key pair
- IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates
- Protection is provided by a key server that controls the mapping of identities to decryption keys
- Provides greater ease of implementation and management
- Eliminates complexity of encryption techniques that rely on long, randomly generated keys that must be mapped to identities using digitally-signed documents, called certificates

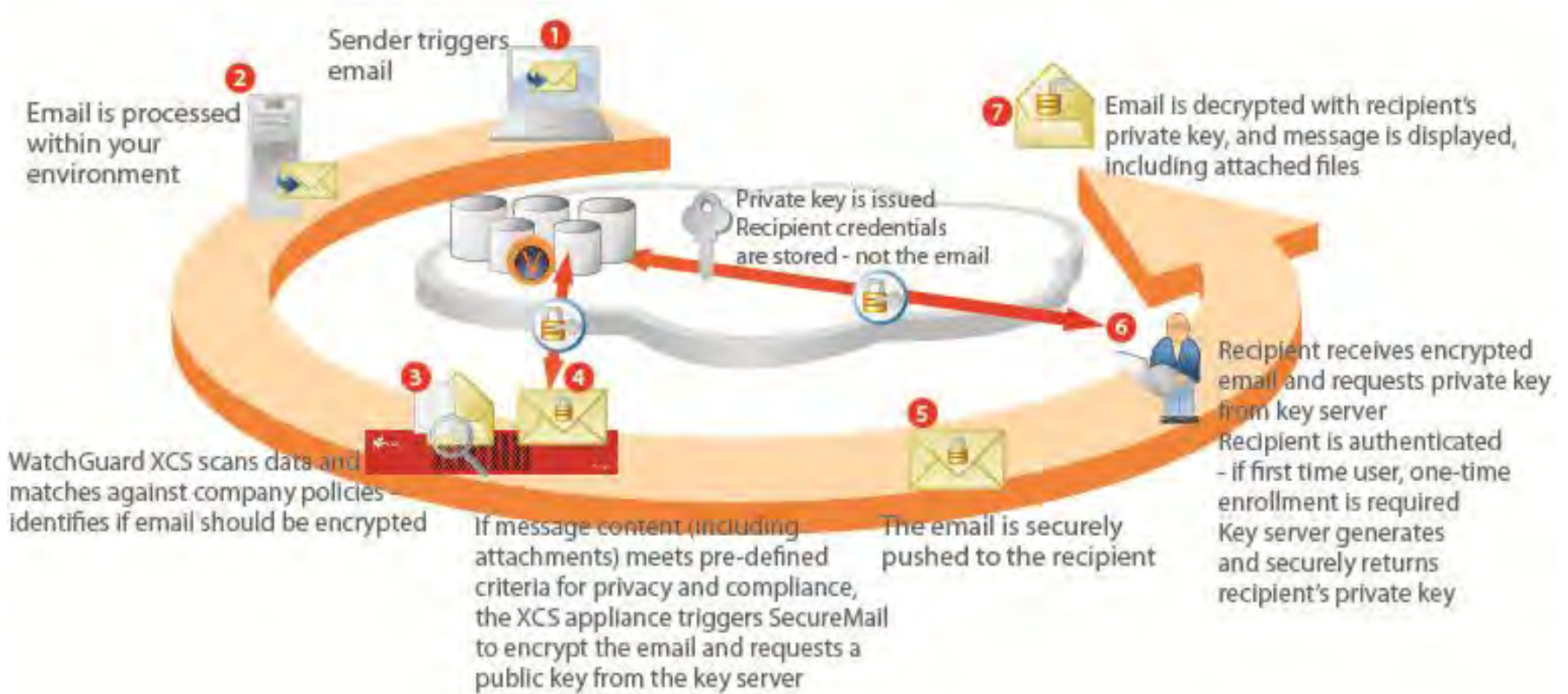
# Transparent, Policy-Based Encryption With XCS SecureMail Email Encryption

- Automates email encryption
- Encrypt based on policies:
  - ✓ Content
  - ✓ Header
  - ✓ Subject Line Trigger
  - ✓ Sender / Recipient
  - ✓ User, Group or Domain
  - ✓ Keywords/RegEx
  - ✓ Attachment Type
  - ✓ Attachment Content



**Senders do not need to make policy decisions.  
Encryption is handled consistently. Accelerates compliance initiatives.**

# WatchGuard XCS SecureMail Email Encryption Subscription



# The Simplified Recipient Experience



message\_z...html  
[Download](#) (16.2 KB)

Download as zip



This is a secure, en



To view thi  
Open the mess

Mobile users - C

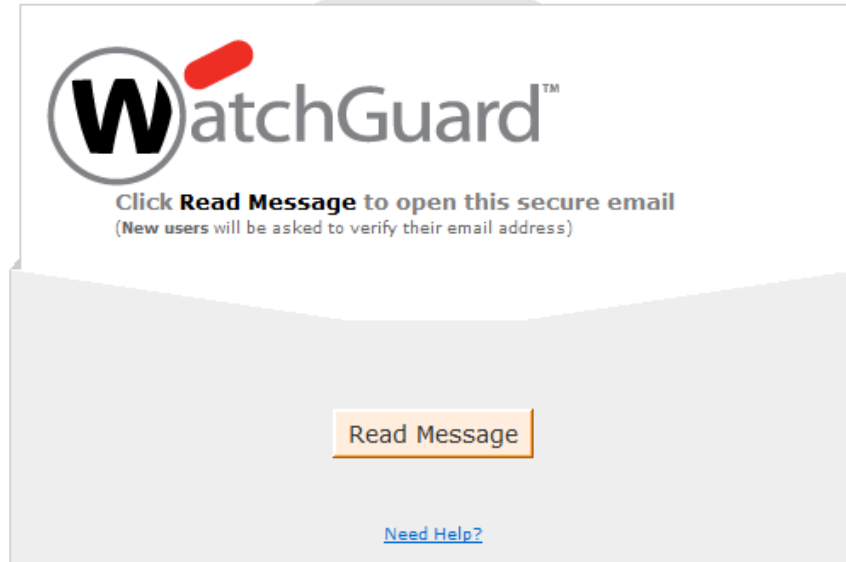
Protected by WatchGuard Technologies

**Confidentiality Notice:** This email, including any  
for the use of the individual(s) or entity to whom  
message in error please notify the sender.

[Need](#)

Email Security Powered by Voltage IBE™

Copy



If you do not see a Read Message button or cannot click on the button, please forward your original email to [zdm@vsn.voltage.com](mailto:zdm@vsn.voltage.com). Within a few minutes, you will receive a link to read your secure message.

Protected by WatchGuard Technologies - [Learn More](#) - [Secure Your Own Email](#)


**Confidentiality Notice:** This email, including any attachments, is confidential and intended solely for the use of the individual(s) or entity to whom they are addressed. If you have received this message in error please notify the sender.

Email Security Powered by Voltage IBE™

Copyright 2003-2011 Voltage Security, Inc. All rights reserved

# One-Time Recipient Registration & Verification Process

- If this is the first encrypted message received by the recipient, he/she is prompted to register with the SecureMail service to create an account and establish a password.
- Recipient must respond to a verification email message before being able to open the encrypted message.



The screenshot shows the WatchGuard registration interface. At the top left is the WatchGuard logo, and at the top right is a 'Help' link. The main content area is titled 'Create a password to continue:'. It contains four input fields: 'Full Name:', 'Email Address:', 'Choose a Password: (6 letters/numbers or more recommended)', and 'Retype Password:'. A 'Continue' button is located at the bottom right of the form. Below the form is a privacy notice: 'You will be asked for this password periodically for security purposes. We will not share your information or sell it to a third party. We value your right to privacy. By clicking 'Continue' we use this information only with your consent.'

Protected by WatchGuard Technologies

Email Security Powered by Voltage IBE™

© Copyright 2003-2011 Voltage Security, Inc. All rights reserved.



The screenshot shows the content of a verification email from WatchGuard. At the top left is the WatchGuard logo, and at the top right is a 'Help' link. The main content area is titled 'Check Your Email'. It contains the following text: 'A temporary message has been sent to your email account to verify your email address. The subject of the message is: **Identity Verification - Do Not Reply** To complete this process: 1. Open the email message 2. Click the link in the email within 2 hours **Note: If you do not receive this message in your inbox within the next few minutes, check your bulk/junk email folder** You may now close this window.'

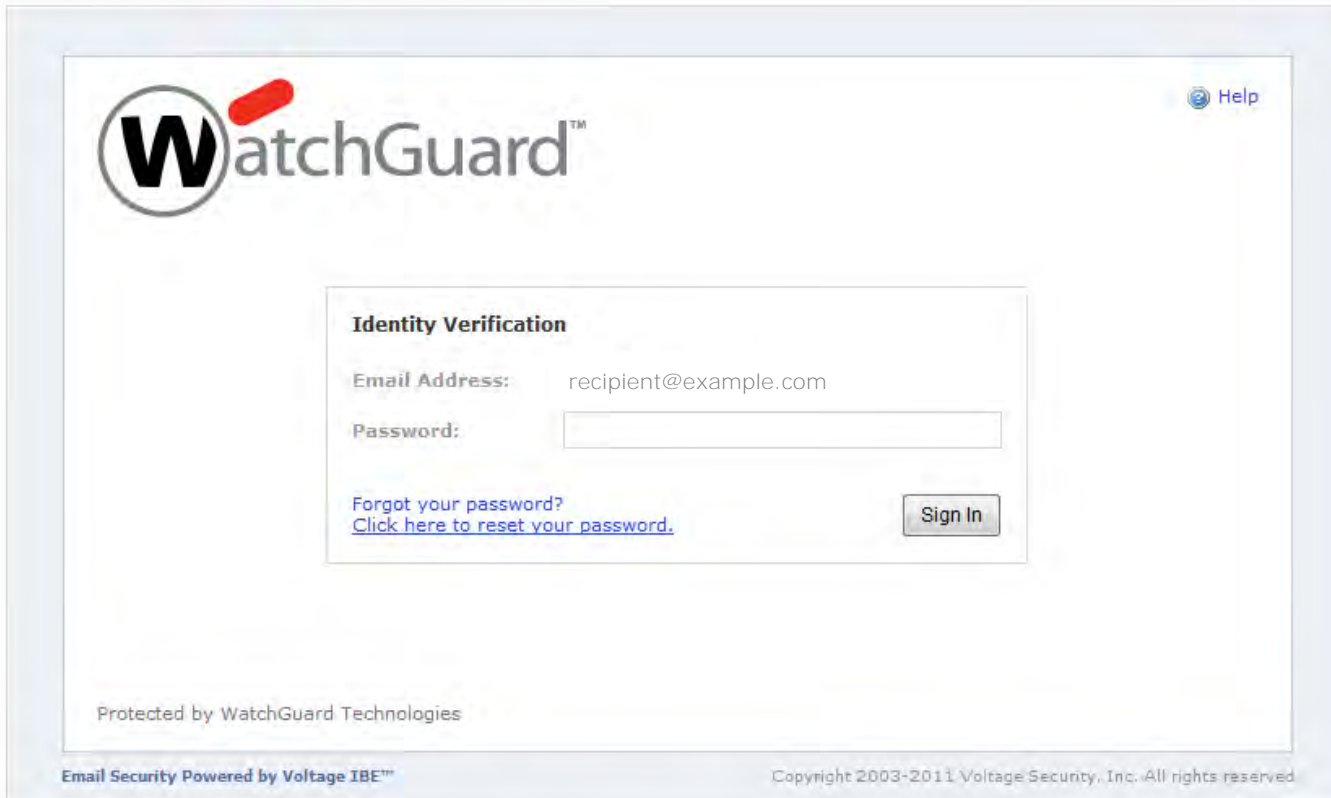
Protected by WatchGuard Technologies

Email Security Powered by Voltage IBE™

Copyright 2003-2011 Voltage Security, Inc. All rights reserved.

# Verification of Recipient Identity

- Recipient's must type their password to verify their identity
- Once authenticated, the secure message is decrypted and displayed.

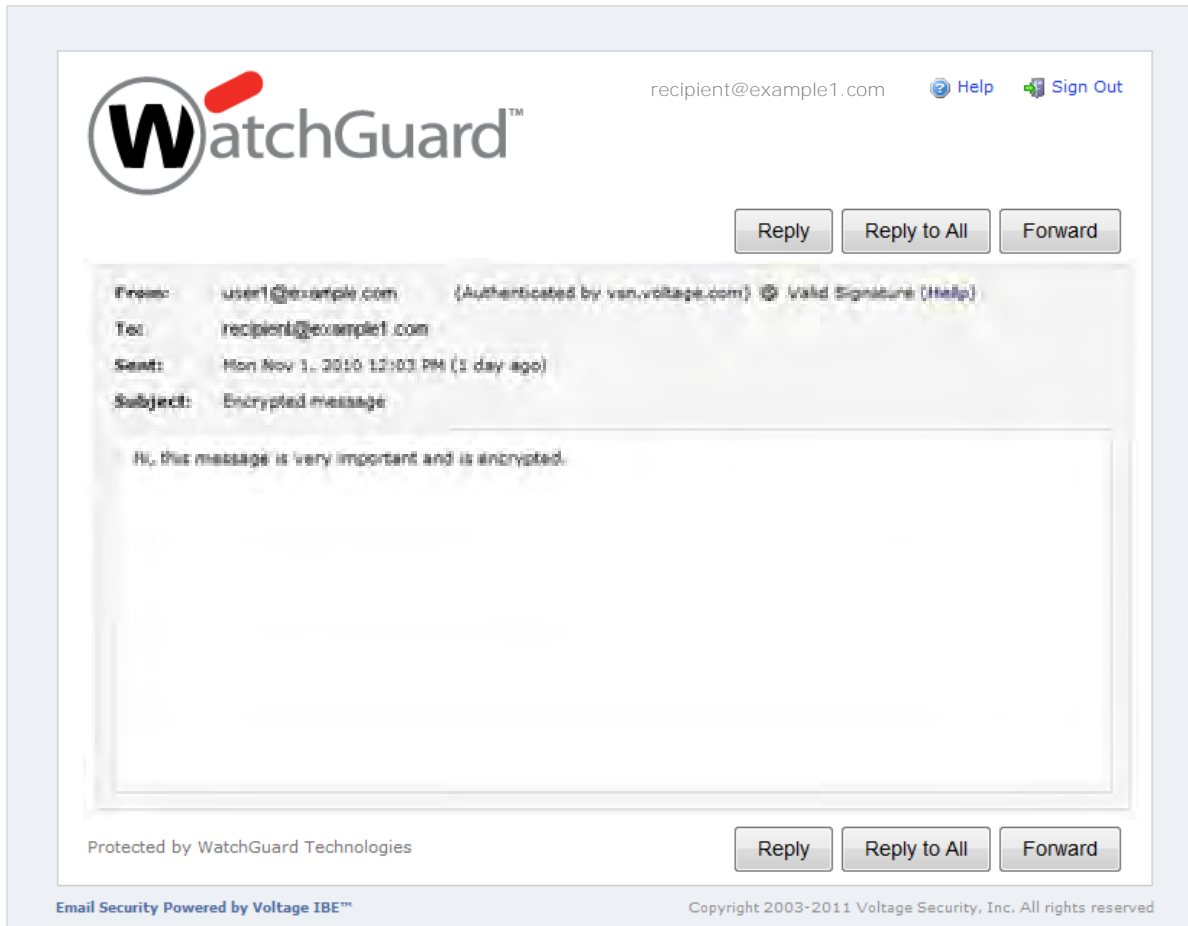


The screenshot shows the WatchGuard Identity Verification interface. At the top left is the WatchGuard logo. In the top right corner, there is a "Help" link with a question mark icon. The main content area is titled "Identity Verification" and contains the following elements:

- Email Address:** recipient@example.com
- Password:** A text input field.
- [Forgot your password?](#)
- [Click here to reset your password.](#)
- Sign In** button

At the bottom of the interface, there is a footer with the text "Protected by WatchGuard Technologies" on the left, "Email Security Powered by Voltage IBE™" in the middle, and "Copyright 2003-2011 Voltage Security, Inc. All rights reserved." on the right.

# Simple External Recipient Experience



- Simple ad-hoc usage – no pre-enrollment
- 100% push delivery method
- Single HTML message envelope format
- Sent to existing mailbox
- Open in browser – no client software to install
- Messages are not stored and do not expire

# Secure Replies & Forwards



- Recipients can securely reply to or forward encrypted messages within the same web-based service that allows them to read the encrypted message.
  - Click **Reply**
  - Type the reply, and click **Send Secure**.
  - An encrypted reply is sent to the sender of the original encrypted message.

# Simplest Mobile Experience



 BlackBerry®



This is a secure, encrypted message.



**To view this secure message:**

**Desktop users** – Open the attachment (**message\_zdm.html**) and follow the instructions.

**BlackBerry users** – [Install the Voltage SecureMail for BlackBerry application.](#)

**Other mobile users** – Forward this message to: [read@watchguard.com](mailto:read@watchguard.com) and check your inbox for a link to view the message.

Simplest decryption for external mobile recipients.  
Business will not be disrupted. Recipients will not become frustrated.

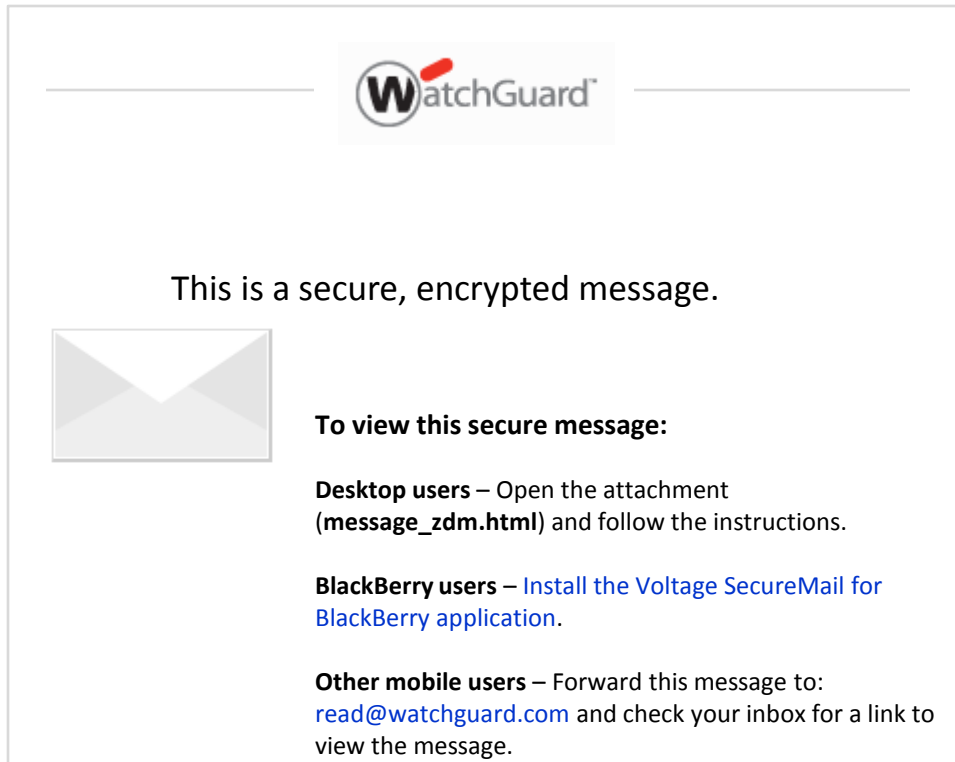
# Cross Platform Forward-and-Decrypt Service



- Recipient clicks on “Other Mobile Users” link in notification message
- The message is forwarded to ZDM Proxy email address at SecureMail cloud
- The recipient receives a new email message with a link to the secure message

Mobile recipients will always be able to decrypt messages.  
Business will not be disrupted.

# Every Element is Fully Brandable



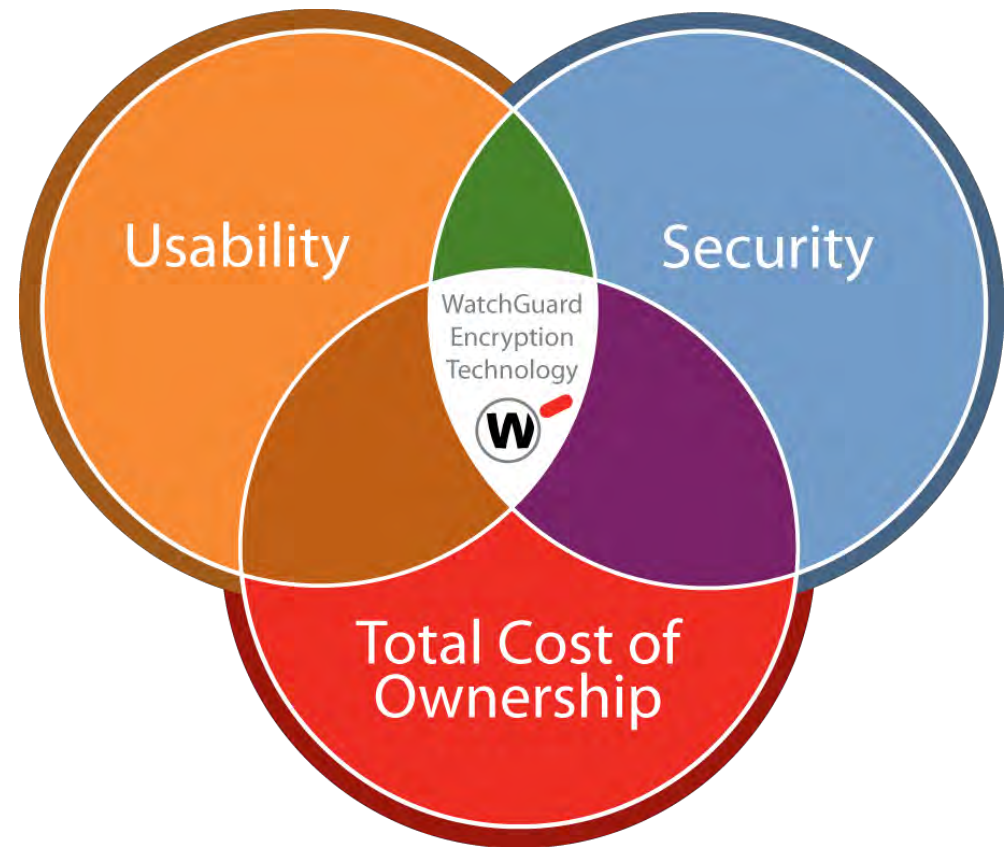
- Allows for unique brand reinforcement of encrypted email, ZDM download pages, and notifications
- Subscribers can use their own corporate logo
- WatchGuard logo is the default if the customer does not purchase a branding subscription
- Ability to customize graphics, borders, fonts, colors, text and links

Promotes corporate brand recognition.  
Reinforces trust and goodwill with recipients.

# Finally...Email Encryption Made Easy!

## WatchGuard Provides a Single, Integrated Solution



- Easiest User Experience
  - No client or plug-in required
  - No certificates
  - No recipient admin-rights needed
- Easiest Deployment
  - Seamlessly integrated within WatchGuard XCS appliances for instant-on use
- Proven
  - Millions of encrypted messages sent per month
  - Worldwide adoption



# Eliminating Security Gaps

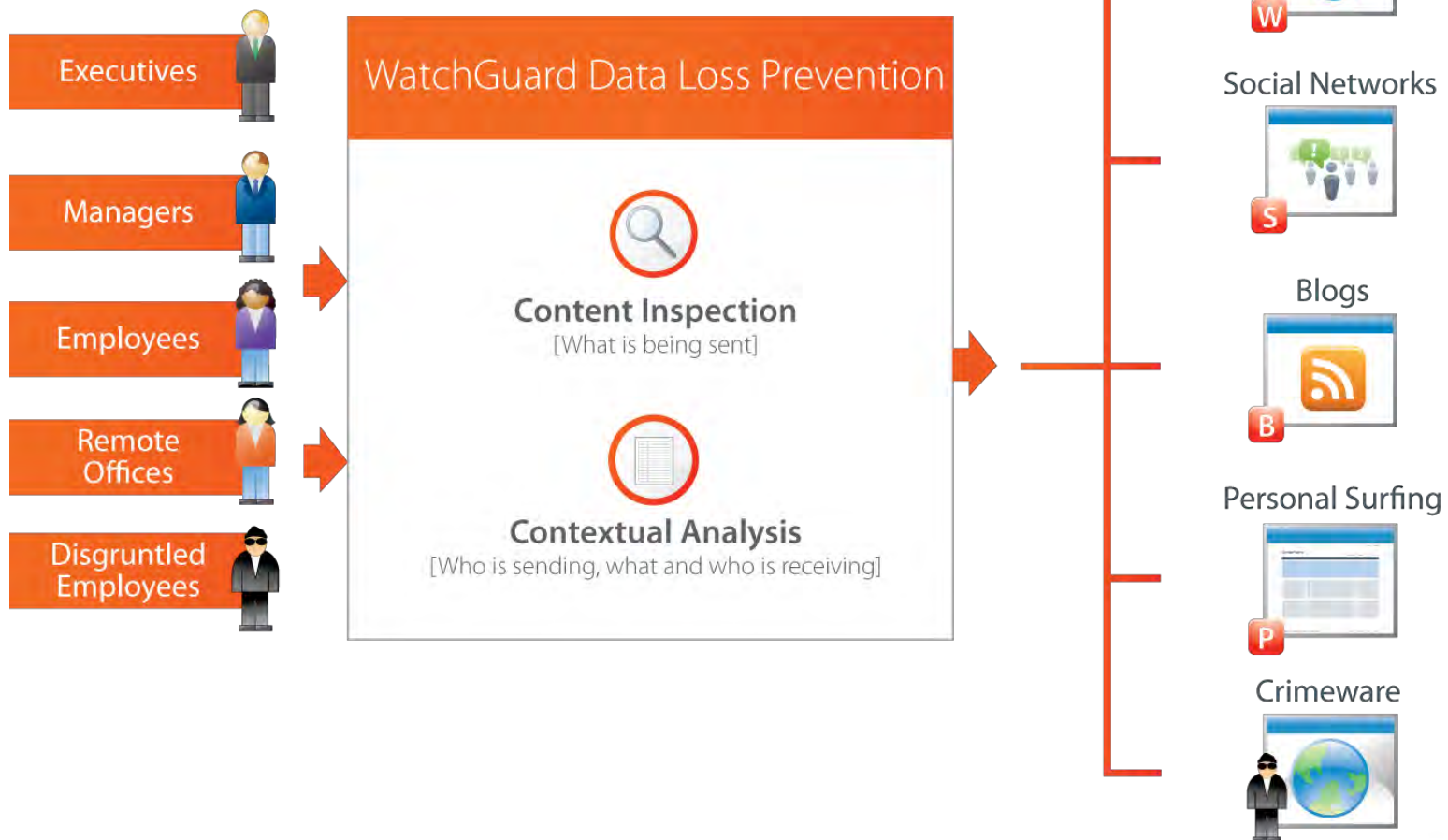


# Extending Data-In-Motion Protection to Web Traffic

<b>Who?</b>	Bob Smith CFO	Bob Smith CFO
<b>When?</b>	Financials.xlsx	Financials.xlsx
<b>Where?</b>	Webmail.com	AuditFirm.com
<b>How?</b>	HTTPS	HTTPS
<b>Verdict?</b>		

# Web Data Loss Prevention

## The Power of Content & Context






# Set-It-And-Forget-It Administration

The screenshot shows the WatchGuard eXtensible Content Security administration interface. At the top left is the WatchGuard logo. At the top right, it displays "eXtensible Content Security" and user information: "User: admin | Host: hostname | [Options](#) | [Logout](#)". Below this is a navigation bar with tabs for "Activity", "Security", "Configuration", "Administration", and "Support". The main content area is divided into several functional groups, each with a sub-header and a list of items:

- Network:** Includes "Interfaces", "Virtual Interfaces", "Performance", "Static Routes", and "Web Server".
- LDAP:** Includes "Directory Servers", "Directory Users", "Aliases", "Mapping", and "Recipients".
- Mail:** Includes "Access", "Delivery", "Aliases", "Routing", and "Mapping".
- WebMail:** Includes "WebMail", "Trusted/Blocked Senders", and "User Spam Quarantine".
- Miscellaneous:** A separate category with a downward arrow.


# Centralized Policy Management For Email & Web

Update "Default"

Policy Summary	
<b>Anti-Spam and Anti-Virus</b> Outbreak Control is enabled. Email Kaspersky Virus Scanning is enabled. Email Kaspersky Spyware Scanning is enabled.   <a href="#">Edit</a>	<b>Content Control</b> Pattern Filters is enabled. Email Inbound Attachment Control is enabled.   <a href="#">Edit</a>
<b>Email</b> Annotations is enabled.   <a href="#">Edit</a>	

**General Settings**

\*Name:  

Default Policy cannot be disabled.

Description:

 The form is ready to submit.

# Detailed Logging & Reporting of Policy Violations

## Message Details for Queue ID 5782A100846267A4

Message:	queue id 5782A100846267A4, size 924 bytes
Message ID:	12c11.0003.00000052@hendrix2.bordenware.com
Prior Message:	
Subject:	Credit Cards
From:	envelope johnsmith@watchguard.com, header johnsmith@watchguard.com
Number Recipients:	1
Source:	outside mail, message was trusted, ssl was not used
Sending Host:	ip 10.10.0.15, helo hendrix2.bordenware.com
Processing Journal:	SAP passed, ReputationAuthority on, PBMF matched, Token Analysis 11, Kaspersky clean, ACS passed, Attachment Control passed
Times:	entered at 2009-10-30 16:20:16, disposed at 2009-10-30 16:20:16

## Message Dispositions

Disposition	Recipient	Date	Policies	Intercept Score
Content: Quarantined	bankfraudguy@domain.com	2009-10-30 16:20:16	Default	0
Details: N/A				
ReputationAuthority		2009-10-30 16:20:16		
Details: ip=10.10.0.15, reputation=0, certainty=0, spamminess=0, infected=0, harvester=0, dnsbl_count=0, dialup=0, scam=0				
PBMF:Quarantine		2009-10-30 16:20:16		
Details: Rule #10, Rank:3, CfgAction:1, inbound:f, option:0, section:content, ptype:regex, pattern:\b4\d{3}[- ]?\d{4}[- ]?\d{4}[- ]?\d{4}[- ]?\b				

# Key XCS Data Loss Prevention Features

- **Single policy administration for DLP across email and web**
  - Eliminates gaps through which data can escape
- **Seamless integrated remediation process**
  - Provides flexibility for policy enforcement without administrator intervention
- **Context scanning is different from content scanning**
  - You need and want both
- **Document fingerprinting**
  - Trains the system on types of data to search for
- **Envelope-based email encryption**
  - Provides affordable protection
- **Compliance**
  - Policy violation logging and reporting for compliance

# Resources for XCS Data Loss Prevention

Available on the WatchGuard Website:

- XCS DLP Datasheet
- XCS SecureMail Email Encryption Technology Note
- Whitepaper: When Pressing the Send Button Results in Compliance Violations
- Case Study: Data Loss Prevention Protects Patient Privacy: National Health Service (NHS), St. Helens and Knowsley Health Informatics Service (HIS)

**Thank you.  
Questions?**

