

Information Leak Prevention Accuracy and Security Tests

Comparative Accuracy Test Findings of PortAuthority Technologies PreciseID™ versus Leading Gateway Vendors

Version 1.0

May 2006

Based on testing performed by and written by:



This document is property of Percept Technology Labs, Inc. and PortAuthority Technologies. All tests, test scripts and suites, test plans, procedures, data collection methods and data presentations are property of Percept Technology Labs, Inc. The testing data referenced in this document was performed in a controlled environment using specific systems and data sets, and represent results related to the specific items tested. Actual results in other environments may vary. These results do not constitute a guarantee of performance. The information in this document is provided "As Is" without any warranty of any kind.

PortAuthority Technologies and the PortAuthority logo are registered trademarks of PortAuthority Technologies. All other trademarks are the property of their respective owners.

Table of Contents

Introduction	4
Information Leak Prevention Technologies	5
Testing Methodology	6
Measuring Success	9
Tested Products	9
Policy Configuration	9
Protected Content Used for Testing	10
Test Results	11
1. Testing for False Positives	11
2. Records Management	14
3. Partial Data Recognition.....	16
4. Data Flooding	17
5. File Type Manipulation	18
6. Information Contained in E-mail Body	20
7. File Format Manipulation.....	21
8. Additional Malicious Testing.....	22
Conclusions	23
Appendix A	25

List of Tables

Table 1: Test results for false positives	11
Table 2: Test results for records management of customer data	14
Table 3: Test for partial data recognition	16
Table 4: Test results for data flooding	17
Table 5: Test results for file manipulation (keyword in files)	18
Table 6: Test results for file manipulation (no keyword in files)	19
Table 7: Test results for confidential information in e-mail body.....	20
Table 8: Test results for file format manipulation.....	21

List of Figures

Figure 1: Classification of Information Leaks.....	7
Figure 2: Map of Test Network.....	8

Introduction

Every year billions of dollars are lost as a result of breaches of secure information from companies and organizations representing a wide variety of industry sectors: financial services, government, healthcare and technology. Since 2005, more than 110 information leaks were publicly reported, affecting some 54 million Americans. According to an independent survey from the Ponemon Institute* completed in September 2005, each individual data breach costs a firm, on average, somewhere between \$5M - \$14M. Studies also show that the number of information leaks is rising and the increased focus in legislative efforts on both the state and federal level underscores the urgency of this issue.

Because information leaks can occur across multiple business applications and channels, it is necessary for firms to employ an enterprise-wide Information Leak Prevention (ILP) solution that accurately monitors and prevents these security breaches across the entire network.

Most companies manage and maintain confidential data that is not properly protected and therefore is susceptible to leaks via outbound protocols such as e-mail, FTP or HTTP. Each company has unique data to safeguard. Whether the company is a bank managing account numbers and Social Security numbers, a government organization protecting sensitive personal data, or an engineering firm guarding its intellectual property, each requires an effective Information Leak Prevention solution.

Information Leak Prevention devices on the market today function by examining outbound communications such as e-mail, web communications, file transfers, instant messaging, etc. When examining e-mails, these devices receive the message, open it, read and analyze its content, and then enforce a policy such as forwarding or blocking the e-mail to the intended recipient based on regulatory or corporate policy requirements.

When comparing Information Leak Prevention technologies, the most critical factor to examine is accuracy. Inaccuracy in identifying sensitive information can result in false positives and false negatives. False positives create unnecessary alarms, erroneously blocking legitimate e-mails, messages and business-critical applications, leading to negative consequences such as:

- Organizations waste resources reviewing safe messages and e-mails, resulting in increased costs.
- Productivity is diminished because important business communications are blocked.
- Employee privacy is at risk if e-mail is incorrectly blocked and reviewed by an administrator.

*NOTE: Ponemon Institute (<http://www.ponemon.org>) conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organization ethics and privacy at Carnegie Mellon University's CIO Institute.

On the other hand, false negatives create a mistaken sense of security leading an organization to believe that there are no policy violations while, in fact, they are occurring. False negatives can compromise the brand, reputation, and competitive advantage of a company leading to an increase in operating costs or a significant loss of revenue.

Information leaks may contain private data or confidential information including:

- New product details or specifications
- New project information
- Confidential client information
- Customer information (Social Security numbers, credit cards, etc.)
- Other proprietary information

An effective Information Leak Prevention technology must eliminate both false positives and false negatives, thus preventing information leaks and data security breaches without interrupting the daily business of an organization, or requiring additional resources to manually examine messages.

Percept Technology Labs, Inc., an independent testing laboratory, was selected by PortAuthority Technologies to establish an open industry testing and evaluation standard for Information Leak Prevention technologies and products. Percept then ran a series of competitive analysis tests to compare PortAuthority's PreciseID™ technology and the company's Information Leak Prevention product, PortAuthority MX with the competitive products and the technologies of the leading e-mail security gateway companies that provide content control and compliance capabilities for outbound content: Ironmail S-10™ by CipherTrust® and Mail Security Gateway 8220 by Symantec™.

Even though PortAuthority products prevent information leaks for multiple protocols, this paper focuses on e-mail transmissions only, to allow for a relative comparison between PortAuthority and the leading mail gateway vendors. This is the first report in a series of several Information Leak Prevention analysis reports that will be used to continue and establish the open industry testing and evaluation standard for Information Leak Prevention.

Information Leak Prevention Technologies

Information leaks can occur whenever users communicate from the "inside out", utilizing a variety of protocols such as e-mail, HTTP, FTP, Instant Messaging or even when printing hardcopy confidential data. An effective Information Leak Prevention solution should include protocol agnostic capabilities to prevent leaks for each different outgoing communications protocol. Content identification is a key capability of this process. Percept Technology Labs, Inc. tested the following three technologies used to identify sensitive information:

- Keyword Content Filtering
- Regular Expression Content Filtering

- **PreciseID Fingerprinting**

When using keywords for identification, an Information Leak Prevention product scans the e-mail body and/or attachment for specific words or phrases – for example, scanning for the word “Confidential.” When one of these words or phrases is found in the document or e-mail body, a policy action is triggered and a resulting action is taken. A policy action may include blocking or quarantining an e-mail and not allowing it to leave the company network. This scanning capability is used by PortAuthority Technologies, Symantec and CipherTrust.

Each of these vendors also uses regular expressions to detect a specific order of digits and characters. For example, scanning for numbers in certain sequence (such as 9-digits for Social Security numbers or 5-digits for ZIP codes).

However, PortAuthority’s PreciseID technology, goes beyond simple keyword or number sequence identification by recognizing actual data rather than only identifying the presence of a keyword, or sequence of numbers inside a document. With PreciseID, the contents of a protected document are scanned at rest, relevant data is extracted and a “fingerprint” representation of the data in the document is created. These fingerprints are then stored in a database and used to identify content in motion. PreciseID identifies documents which do not match the original document exactly and may contain even small percentages of the protected data.

Testing Methodology

Percept’s main focus during this testing was to measure the accuracy of PortAuthority’s PreciseID technology and compare its fingerprinting detection capabilities with other technologies such as regular expression and keyword detection. Percept compared these technologies by testing the Information Leak Prevention capabilities of PortAuthority MX, Ironmail S-10, and Mail Security Gateway 8220. Percept tested the ability of these products and technologies to filter outgoing e-mails while protecting confidential data.

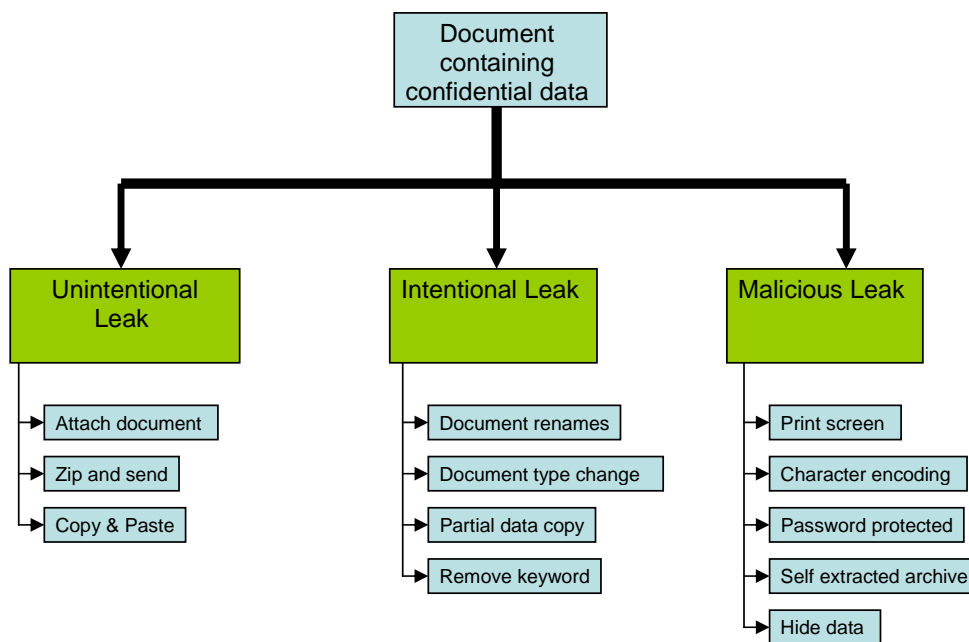
Using a testing standard provided by PortAuthority Technologies as the beginning basis, Percept employed the following nine sections of testing to fully test the capabilities of each product:

1. **False Positives** – Testing for the recognition of legitimate e-mails that should not be blocked by the leak prevention products
2. **Record Management** – Testing for the protection of structured information such as customer data, which includes names, account numbers, Social Security numbers, driver license numbers, and medical insurance numbers.
3. **Partial Data Recognition** – Testing for the protection of small percentages of the original protected document
4. **Data Flooding** – Testing for the protection of data taken from an original source and inserted into a much larger file in an attempt to disguise an information leak.

5. **File Type Manipulation** – Testing for the protection of data "saved as" a different file name/format.
6. **Information Contained in E-mail Body** – Testing for the protection of data copied from a protected document and pasted into the e-mail body.
7. **File Format Manipulation** – Testing for the protection of data altered in its original format. (e.g., font, font size, spacing, order of text, partial deletion of text, letter changes etc.)
8. **Print Screen** – A test created by Percept to test the products abilities to block confidential data that has been converted into a bitmap, jpeg, or gif file (which would constitute a malicious attempt to sneak data past a security device).
9. **Hidden Data** – Testing for the protection of data that has been hidden within a document. For example, adding a picture to cover text.

Within each of these nine test sections, Percept has classified each individual e-mail as an unintentional, intentional, or malicious leak. Each test represents a different scenario of information leak. Please see Figure 1 below for description of this classification.

Figure 1: Classification of Information Leaks



Unintentional Leak (U) – Data leaks caused by someone unintentionally sending out confidential information in an e-mail. Unintentional leaks can occur when a person attaches the wrong document to an e-mail message by mistake or when Microsoft

Outlook completes an email address incorrectly and the message is sent to the wrong recipient.

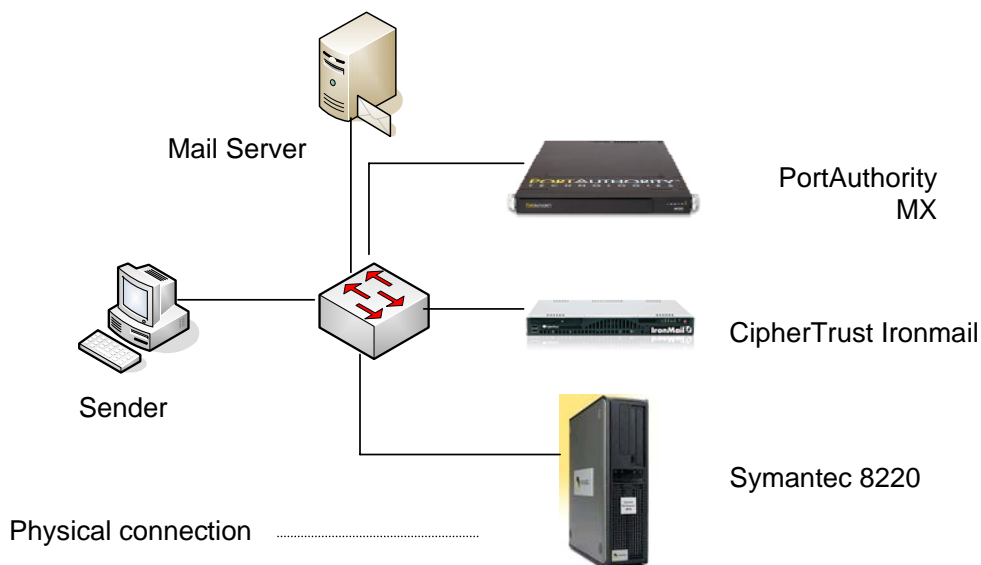
Intentional Leak (I) – Information leaks caused by someone who is aware of company policy, but attempts to send confidential information anyway. Intentional leaks occur when the sender bypasses security devices by doing something like changing a document name or converting it to a zipped archive.

Malicious Leak (M) – Information leaked by someone who deliberately and illegally plans to slip information past a security product is called a malicious leak. Malicious leaks are very rare.

Percept's goal was to measure the accuracy of the PreciseID fingerprinting technology by comparing it with the content filtering technology of the other two products, and test the limits of each technology type. General ease of use, processing speed, and performance were noted as well.

For these tests, Percept set up a small network of computers that included two testing stations to analyze each of the test products. All e-mails originated from one test station, were directed through each product being tested, and then arrived at the second test station where they evaluated for detection accuracy.

Figure 2: Map of Test Network



The software used for testing included *Mail and Collaboration Server* software by DeskNow used as a mail server (SMTP). With this software, Percept set up a recipient (or destination) e-mail account, and an administrator e-mail account, which received notification of blocked e-mails. A total of 72 test e-mails were sent using batch scripts

that utilized *Command Line E-mail Utility* by Febooti Software. This allowed a large number of e-mails to be sent simultaneously.

Measuring Success

Percept Technology Labs, Inc. categorized its test findings into four possible results when sending an e-mail:

True Positive (TP) – the security product correctly identified an e-mail containing confidential information and successfully blocked this e-mail from being sent.

True Negative (TN) – the security product correctly identified an e-mail as NOT confidential and successfully allowed this e-mail to be sent.

False Positive (FP) – the security product incorrectly identified a compliant (non-confidential) e-mail as one that is confidential and incorrectly blocked this e-mail from being sent.

False Negative (FN) – the security product failed to identify an e-mail containing confidential information and incorrectly let this e-mail be sent.

Tested Products

Percept Technology Labs, Inc. tested the following products for this competitive analysis study.

- MX appliance by PortAuthority Technologies
- Ironmail S-10 by CipherTrust
- Mail Security Gateway 8220 by Symantec

(NOTE: All products were installed using the latest software releases as of April 10, 2006)

Policy Configuration

Product configurations for these three products are as follows.

- PortAuthority MX: While there are multiple technologies employed by this product, Percept only tested the Precise ID fingerprinting technology in this analysis. A single document containing the confidential data was fingerprinted. The product policy included only this single document.
- CipherTrust Ironmail S-10: The CipherTrust product policy was set with content dictionaries, keywords and regular expressions.
- Symantec Mail Security Gateway 8220: The Symantec product policy was set with content dictionaries and keywords only.

Protected Content Used for Testing

The following three documents were used for the comparison of the different Information Leak Prevention devices.

- Confidential Information Document 1: “Default Access Control Settings in Windows 2000” – a white paper by Microsoft Corporation. The data in this document was used for the majority of unstructured data testing. The original document contains the keyword “confidential” on page one. To reduce the number of False Positive events, the Microsoft address and ZIP code were removed from page 2 of the document.
- Confidential Information Document 2: A one-page Microsoft Word document used in testing for Section 5.40, 5.41 and all of Section 6.
- Customer Data Document: An Excel spreadsheet containing customer names, account numbers, social security numbers, driver’s license numbers, credit card numbers, and medical insurance numbers.


Test Results

1. Testing for False Positives

This section of testing focused on sending non-confidential e-mails, which have the potential to be incorrectly blocked by the tested products. PortAuthority MX, using PreciselD was capable of accurately identifying a leak without causing any false positives. The other technologies failed to identify the leak and generated false positive alarms.

Table 1: Test results for false positives

Test #	False Positive Tests	Final Results		
	Purpose of test	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products recognize a public document?	TN	TN	TN
2	Can the products recognize a public document with different product settings?	TN	FP	FP
3	Can the products recognize a public doc which includes a keyword?	TN	FP	TN
4	Can the products recognize a public email which contains a keyword?	TN	FP	FP
5	Can the products recognize another confidential with "top secret" in footer?	TP	TP/FN	FN
6	Can the products recognize public document, no keyword, but sharing fingerprint?	TN	TN/FP	TN

 = Test documents that do not contain a keyword.

 = Inconclusive test results.

Detailed Analysis

Mail Security Gateway 8220 had mixed results in this section of testing. While the product did pass several tests, this is due to its inability to scan the contents of e-mail attachments (thereby missing possible false negatives and false positives in these types of applications).

However, this device does have a configuration option that allows a user to block a certain attachment type. The anticipated problem of this feature is that if a user chooses to block all Word documents from being sent, then this feature erroneously blocks non-confidential Word document attachments. In an office environment where hundreds or thousands of documents are sent via e-mail each week, this feature would not be practical. This was the purpose of tests 5.10 and 5.11. Percept used the same document for both tests. In test 5.10 only the keyword filter was enabled. In 5.11 the keyword filter and document type were enabled. As a result, this test created a false positive result. In Test 5.30 the e-mail was designed to replicate the type of e-mail that an employee might send to his boss asking a question. This e-mail contained a keyword and as a result it was incorrectly blocked.

The Ironmail S-10 product showed mixed results as well. In test 5.11 Percept enabled the filter for attachment type and as a result it failed this test. Ironmail S-10 has the ability to scan the contents of the attachments, but it incorrectly blocked test e-mail 5.20, which was a public document containing a marked keyword. Ironmail S-10 also demonstrated limitations in its ability to scan an attachment footer. In test 5.40 Ironmail

S-10 successfully blocked a document which contained a keyword in the footer once, but failed to block the identical document during a retest. Test 5.41 showed inconsistent results as well, therefore Percept deemed these results inconclusive for Ironmail S-10.

PortAuthority MX using PreciseID passed all six tests consistently by correctly identifying and blocking transmission of confidential data in all types of documents and attachments, and allowing all non-confidential data to be transmitted, thus demonstrating the fingerprinting technology's ability to reduce or eliminate false positives.

Test 5.41 was designed specifically to create a false positive for the PortAuthority MX product. Percept was interested in testing a public document, which contained the same template of a confidential document, in order to see if it would be incorrectly blocked. Because PortAuthority MX offers a negative fingerprinting feature, which correctly ignores common data shared in both public and confidential documents, it correctly allowed the e-mail to be transmitted, thereby passing this test.

Figure 3: False Positive detection rate

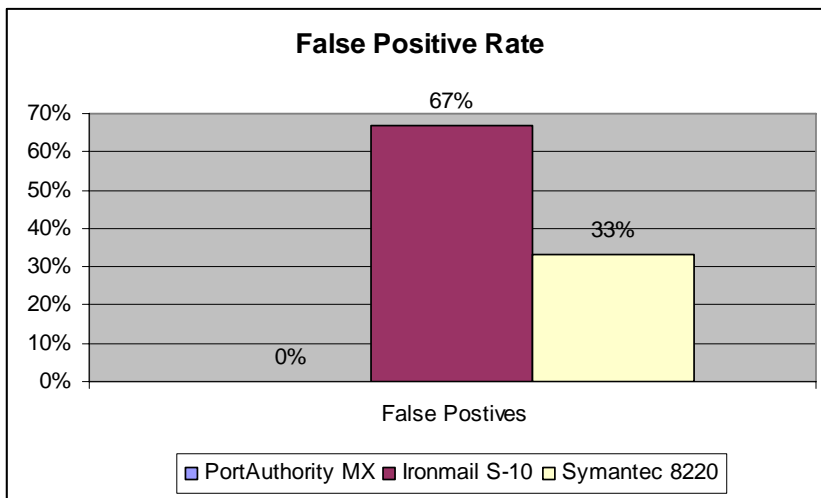
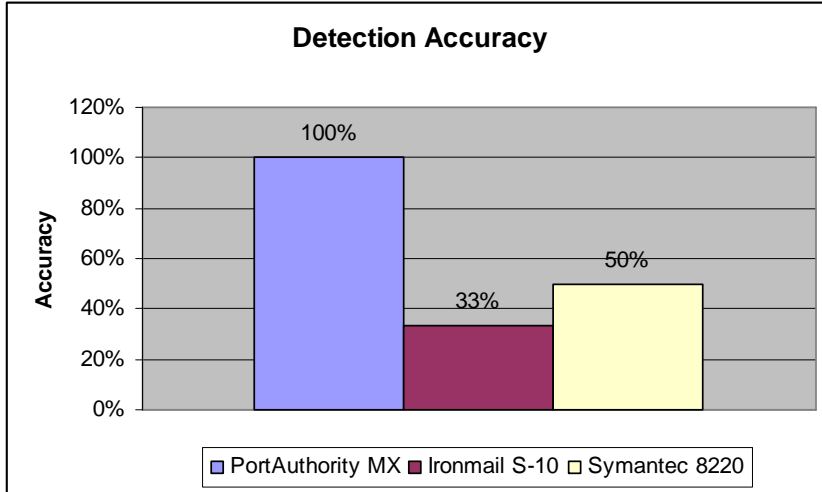


Figure 4: Accuracy Results



2. Records Management

This section of testing focused on each product's ability to identify confidential customer data that should not be disclosed. Data files did not include the exact records and special attention was given to both false positive and false negative scenarios.

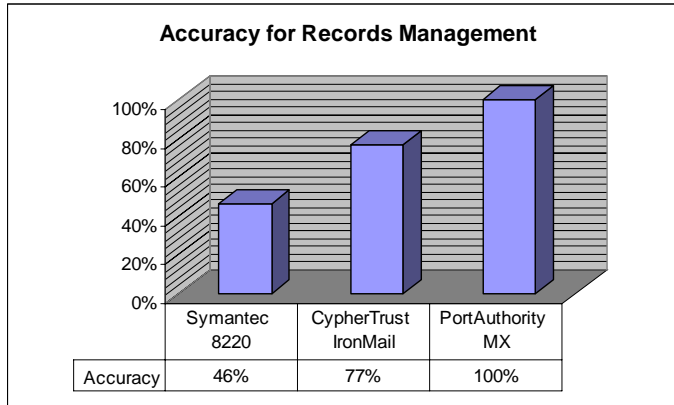
Table 2: Test results for records management of customer data

Records Management – Customer Data Tests			Final Results		
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products identify original list?	U	TP	TP	FN
2	Do the products block a single ssn in doc?	U	TN	TN	TN
3	Can the products block a .pdf containing blocked info 1?	U	TP	TP	FN
4	Can the products block a .pdf containing blocked info 2?	U	TP	TP	FN
5	Can the products recognize a .pdf containing public info?	U	TN	TN	TN
6	Can the products block a .doc containing blocked info?	I	TP	TP	FN
7	Do the products misinterpret public 9 digit numbers?	I	TN	TN	TN
8	Can the products block confidential info in email body?	I	TP	TP	FN
9	Do the products block single ssn in body?	I	TN	TN	TN
10	Do the products block single ssn and wrong name in body?	I	TN	TN	TN
11	Can the products block confidential info in email subject?	I	TN	TN	TN
12	Do the products block single ssn and correct name in body?	M	TP	FN	FN
13	Can the products let unprotected info through?	M	TP	FN	FN

In this section of testing Percept examined each product's ability to protect confidential customer records. This test was not applicable to Mail Security Gateway 8220, which uses keyword technology only and is unable to scan the contents of attachments. For comparative purposes, Percept included the results to illustrate this product's complete inability to filter this information. Ironmail S-10, which uses regular expressions filtering, in addition to keyword filtering, was able to successfully block several of the test e-mails containing confidential customer data. It is unclear how this product failed to block tests 9.60 and 9.80, but on repeated testing these e-mails were consistently missed. Ironmail S-10 showed no false positives during the course of testing, but because this product employs a regular expressions filter, this result is not likely to be consistent in actual usage when the filter would catch any regular expression whether it was confidential or not. Ironmail S-10 successfully identified all of the True Negatives in this section.

PortAuthority MX demonstrated 100% accuracy in this section of testing. PreciseID offers sophisticated data extraction, detection and leak prevention through its ability to match customer names with the relevant account numbers. If these names and numbers appear together in an e-mail or attachment – thereby disclosing confidential information – the e-mail is blocked. If the names and numbers do not match, the message is transmitted because this data does not disclose customer-specific confidential information. This level of protection for this type of data was unmatched in the other technologies tested.

Figure 5: Accuracy Results for Record Management




3. Partial Data Recognition

This section of testing focused on partial data recognition. Rather than simply adding a portion of the confidential document to the e-mail body, it was added as an attached Word document. Once again, the PreciseID technology demonstrated 100% detection of all confidential data with as little as 15% of the original document attached.

Table 3: Test for partial data recognition

Tests for Partial Data Recognition		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products block content of 90% of original?	U	TP	FN	FN
2	Can the products block content of 50% of original?	I	TP	TP	FN
3	Can the products block content of 15% of original?	M	TP	FN	FN

 = Test documents that do not contain a keyword.

Detailed Analysis

Once again, the Mail Security Gateway 8220 product failed all three tests because of its inability to scan the contents of e-mail attachments.


Ironmail S-10 showed mixed results. If the keyword was not present in the attachment, it did not block the data.


4. Data Flooding

This section of testing focused on the ability of each product to identify confidential data that was inserted into both a document and an e-mail body containing a lot of non-confidential data.

Table 4: Test results for data flooding

Data Flooding Tests		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products block confidential data flooded with extra data in document?	M	TP	TP	FN
2	Can the products block confidential data flooded with extra data in document?	M	TP	TP/FN	FN
3	Can the products block confidential data flooded with extra data in email body?	M	TP	TP	TP
4	Can the products block confidential data flooded with extra data in email body?	M	TP	FN	FN

 = Test documents that do not contain a keyword.

 = Inconclusive test results.

Detailed Analysis

Mail Security Gateway 8220 failed the first two tests again because of its inability to scan the contents of e-mail attachments. It passed 8.30 because a keyword was present, and it failed 8.40 because there was not a keyword in the e-mail body. Ironmail S-10 passed the tests that contained a keyword and failed the tests that did not contain a keyword, demonstrating the limits of content filtering technology.

PortAuthority MX demonstrated its ability to detect small sections of confidential data that were flooded with other meaningless data.

5. File Type Manipulation

The first section of this testing focused on file type manipulation. Percept created a series of files that contained the exact contents of an original confidential document, but in a modified format. The testing simulated different scenarios of intentional, unintentional and malicious information leaks. The table below lists the results of this testing category:

Table 5: Test results for file manipulation (keyword in files)

U = Unintentional **I** = Intentional **M** = Malicious

File Manipulation Tests		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products block original confidential file?	U	TP	TP	FN
2	Can the products block original converted to pdf?	U	TP	TP	FN
3	Can the products block renamed original file?	I	TP	TP	FN
4	Can the products block original converted to power point presentation?	I	TP	FN	FN
5	Can the products block original converted to text file?	I	TP	TP	FN
6	Can the products block original converted to rtf?	I	TP	TP	FN
7	Can the products block original converted to zip file?	I	TP	TP	FN
8	Can the products block original converted to html?	I	TP	TP	FN
9	Can the products block original converted to xls?	M	TP	TP	FN
10	Can the products block original converted to protected xls?	M	TP	FN	FN
11	Can the products block original inserted into power point editor's notes?	M	TP	FN	FN
12	Can the products block a self extracting zip file?	M	TP	FN	FN
13	Can the products block original fully copied and pasted into power point?	M	FN	FN	FN
14	Can the products block original partially inserted into power point?	M	FN	FN	FN
15	Can the products block original partially inserted into power point?	M	FN	FN	FN


Detailed Analysis

In this section of testing, PortAuthority MX performed better than the other two products. PortAuthority MX was able to detect all of the leaks categorized as intentional or unintentional and two of the malicious leaks. It was able to detect confidential data in a password-protected .xls file and in a self-extracting zip file, two files which Ironmail S-10 failed to identify. Mail Security Gateway 8220 again failed all of these tests because of its inability to scan e-mail attachments.

***NOTE:** Regarding Ironmail's results in this testing: In all of these tests, the documents contained the keyword "confidential." If this one word was moved from the documents, Ironmail did not pass any of these tests. This clearly demonstrates the limits of keyword technology.

Table 6: Test results for file manipulation (no keyword in files)

File Manipulation Tests - removing keywords		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec B220
1	Can the products block original confidential file?	M	TP	FN	FN
2	Can the products block original converted to pdf?	M	TP	FN	FN
3	Can the products block renamed original file?	M	TP	FN	FN
4	Can the products block original converted to power point presentation?	M	TP	FN	FN
5	Can the products block original converted to text file?	M	TP	FN	FN
6	Can the products block original converted to rtf?	M	TP	FN	FN
7	Can the products block original converted to zip file?	M	TP	FN	FN
8	Can the products block original converted to html?	M	TP	FN	FN
9	Can the products block original converted to xls?	M	TP	FN	FN
10	Can the products block original converted to protected xls?	M	TP	FN	FN
11	Can the products block a self extracting zip file?	M	TP	FN	FN
12	Can the products block original converted to html?	M	TP	FN	FN
13	Can the products block original fully copied and pasted into power point?	M	FN	FN	FN
14	Can the products block original partially inserted into power point?	M	FN	FN	FN
15	Can the products block original partially inserted into power point?	M	FN	FN	FN


 = Test documents that do not contain a keyword.

6. Information Contained in E-mail Body

In this section Percept tested how well the security products identified confidential data that is contained within the body of an e-mail. The table below lists the results of this testing category:

Table 7: Test results for confidential information in e-mail body

Information Contained in E-mail Body		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products block original copied to e-mail body?	U	TP	TP	TP
2	Can they block copy of 90%	U	TP	FN	FN
3	Can the products block original modified and copied to body? (double spacing)	I	TP	TP	TP
4	Can they block copy of 50%	I	TP	TP	TP
5	Can the products block original minus keywords in the body?	M	TP	FN	FN
6	Can the products block original modified and copied to body? (Wingding font)	M	TP	TP	TP
7	Can the products block original modified and copied to body? (single letter change)	M	TP	FN	FN
8	Can they block copy of 15%	M	TP	FN	FN
9	Can the products block original modified and copied to body? (single letter change)	M	FN	FN	FN
10	Can the products block original modified and copied to body? (single letter change)	M	FN	FN	FN

 = Test documents that do not contain a keyword.

Detailed Analysis

The areas highlighted in blue indicate e-mails that contained no keyword in them, but did contain other confidential data from the original confidential document. Mail Security Gateway 8220 product, which bases its compliance policy solely on keywords, failed to identify every confidential e-mail which did not contain keywords. Ironmail S-10, also using keyword technology, showed the same results.


PortAuthority MX performed better than the other two products with information contained in an e-mail body. It blocked small percentages of the original data, with or without keywords, and was able to identify four of the six malicious e-mails.

7. File Format Manipulation

This section of testing focused on file format manipulation. The goal was to test how well the security products can correctly block e-mails attachments containing confidential data that had been reformatted from the original document. The table below lists the results of this testing category:

Table 8: Test results for file format manipulation

File Format Manipulation Tests		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec #220
1	Can the products block original without keywords?	M	TP	FN	FN
2	Can the products block original with changed keywords?	M	TP	FN	FN
3	Can the products block original with new fonts (wingding)?	M	TP	TP	FN
4	Can the products block original with new font color (white)?	M	TP	TP	FN
5	Can the products block original with spacing change (single to double)?	M	TP	TP	FN
6	Can the products block original with one letter changed (all l to z in part of doc)?	M	TP	FN	FN
7	Can the products block original with one letter changed (all l to z in entire doc)?	M	TP	FN	FN
8	Can the products block original with one letter changed (all con to cOn in entire doc)?	M	TP	FN	FN
9	Can the products block original with one letter changed (all n to z in entire doc)?	M	FN	FN	FN
10	Can they block original with one letter changed (all letter o to O in entire doc)?	M	FN	FN	FN
11	Can the products block original with no zip code and letter changed (all o to O)?	M	FN	FN	FN

 = Test documents that do not contain a keyword.

Detailed Analysis

This section tested for changes made in the attached documents rather than the e-mail body.

Once again Mail Security Gateway 8220 failed to recognize any of this confidential data because it cannot scan the contents of e-mail attachments. Ironmail S-10 was able to recognize documents which contained a marked keyword, despite a font type change or font color change. Test 3.50 also contained a keyword and therefore was blocked by Ironmail S-10.

PortAuthority MX was able to recognize data with or without keywords. However, PortAuthority MX failed some of the letter change manipulation tests.

8. Additional Malicious Testing

Percept Technology Labs, Inc, created two additional independent tests to analyze how well these products detected and prevented malicious attempts to leak data. The first test involved purposely hiding confidential data in the following areas of a document:

- White space
- Comments
- Properties field
- Field code
- Tracking fields

The second test involved converting confidential data into image files and focused on the ability of the test products to block these image files . None of the tested products claim to have this capability at this time.

Detailed Analysis

Mail Security Gateway 8220 again lacked the ability to scan the contents of attachments and therefore hidden data makes no difference in results. Ironmail S-10 was able to scan the content of attachments but demonstrated an inability to scan for hidden data.

PortAuthority MX was able to block two of the six test e-mails. For the second test, Percept used the confidential information in Document 2 to create several images files containing the original confidential data. This was Percept's most sophisticated attempt to sneak data past these security products. All three products were unable to detect confidential information in this test case.

Conclusions

As companies look to implement the most effective Information Leak Prevention solution for their enterprises, it is essential for them to understand the accuracy and capabilities of the major technologies and products available on the market today.

Through a series of rigorous and extensive tests performed by independent testing lab, Percept Technology Labs, comparing three key Information Leak Prevention technologies – PreciselD Fingerprinting, Keyword Content Filtering and Regular Expression Content Filtering – the following results were found:

- PortAuthority's PreciselD fingerprinting technology demonstrates a significant performance advantage in preventing all types of data leaks – unintentional, intentional and malicious.
 - The PortAuthority product detected 100% of all unintentional and intentional leaks without a single false positive or false negative event.
 - The PortAuthority product also identified and prevented 66% of the malicious leaks attempted (four of six were prevented)**, while the other two products demonstrated less than a 1% detection rate.
 - Overall, the PortAuthority product performed two to three times better than other technologies in the series of tests.
- A comprehensive summary of results is located in Appendix A.

****NOTE:** The PortAuthority product demonstrated superior malicious leak detection in this round of tests, even though this version of the product does not claim this capability. PortAuthority Technologies is currently developing increased functionality in this area to increase accuracy even more.

About PortAuthority Technologies

PortAuthority Technologies is the leading provider of Information Leak Prevention security solutions that reliably and accurately control the unauthorized distribution of sensitive information for data privacy, confidential information protection and true compliance. PortAuthority stops information leaks of customer data and confidential information by monitoring internal and outbound enterprise communications and delivering policy enforcement in real-time. PortAuthority Technologies ensures compliance with regulations such as Gramm-Leach-Bliley, HIPAA, CA CC1798, PIPEDA and Sarbanes-Oxley by closing the gap between employee behavior and corporate and legal policies. PortAuthority Technologies is headquartered in Palo Alto, California. For more information on PortAuthority Technologies, visit www.portauthoritytech.com or call 877- 843-4879.

About Percept Technology Labs

Percept Technology Labs is an established, independent product test and consulting company with a proven track record of helping customers test and improve their products since 1996. Specializing in data storage, ITE and consumer electronics products, Percept does more than simply test products in its 5,000 square foot real world

and environmentally controlled lab spaces. With years of specialized technology testing experience and absolute commitment to customer care, the Percept team manages the entire product testing, improvement and certification process from start to finish. Percept provides everything clients need to launch and deliver their products around the world – on time and within budget. Customers include leading information technology equipment (ITE), data storage, consumer electronics, scientific instrumentation, and telecommunications firms. To learn about Percept's full line of testing and consulting services, visit www.percept.com or call 303-444-7480.

Appendix A

The tables below summarize the overall accuracy of the PortAuthority product:

Figure 6: Detection Accuracy – Unintentional Information Leaks

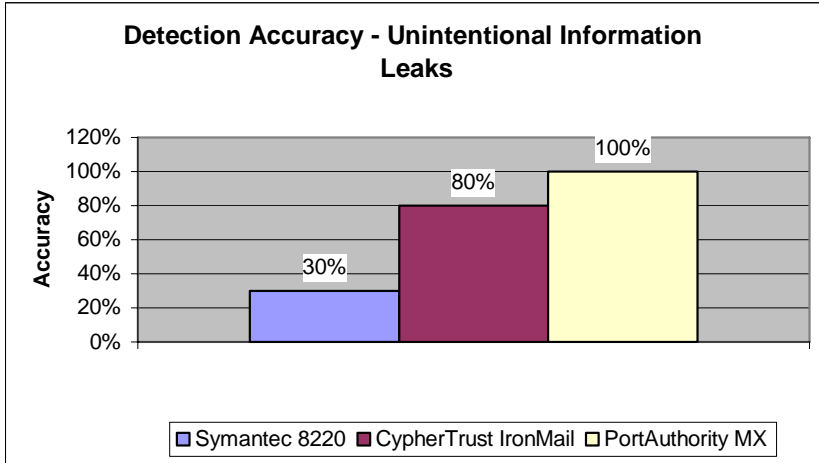


Figure 7: Detection Accuracy – Intentional Information Leaks

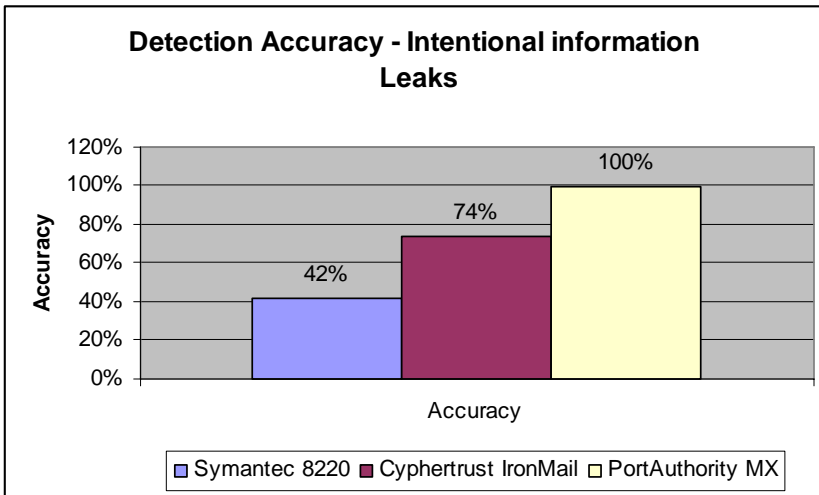


Figure7: Accuracy Measurement

