

Information Leak Prevention Accuracy and Security Tests

Comparative Accuracy Test Findings of PortAuthority Technologies PrecisID™ 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.

Table of Contents

Introduction	4
Information Leak Prevention Technologies	5
Testing Methodology	6
Measuring Success	8
Tested Products	9
Policy Configuration	9
Protected Content Used for Testing	9
Test Results	10
1. Testing for False Positives	10
2. Records Management	13
3. Partial Data Recognition.....	14
4. Data Flooding	15
5. File Type Manipulation	16
6. Information Contained in E-mail Body	17
7. File Format Manipulation	18
8. Additional Malicious Testing	19
Conclusions	20

List of Tables

Table 1: Test results for false positives.....	10
Table 2: Test results for records management of customer data.....	13
Table 3: Test for partial data recognition.....	14
Table 4: Test results for data flooding.....	15
Table 5: Test results for file manipulation (keyword in files).....	16
Table 6: Test results for file manipulation (no keyword in files).....	17
Table 7: Test results for confidential information in e-mail body	17
Table 8: Test results for file format manipulation	18

List of Figures

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

Introduction

Information Leak Prevention. Although this is not a common phrase, it refers to breaches of sensitive data outside and within a business and organization and the increasing requirements to control such incidents from occurring. Most companies have confidential data that is not properly protected and can easily be leaked via outbound protocols such as e-mail, FTP or HTTP. Different companies have unique data to protect. Whether the company is a bank protecting account numbers and Social Security Numbers, a government organization protecting sensitive data, or an engineering firm protecting its intellectual property, each organization requires an Information Leak Prevention solution.

Since 2005, more than 110 information leaks were publicly reported, affecting more than 54,000,000 Americans and costing billions of dollars. Studies shows that the number of information leaks is increasing and recent State and Federal legislations demonstrate the urgency of this subject.

Information leak prevention devices function by examining outbound communications such as e-mail, web communications, file transfers, instant messaging etc. When examining e-mails, they receive the message, open, 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 leak prevention technologies, the most critical factor to examine is accuracy. A lack of accuracy in identifying sensitive information can result in False Positives and False Negatives. False Positives create false alarms, falsely blocking legitimate e-mails, messages and business critical applications and can have negative consequences such as:

- Organizations spend too many resources reviewing safe messages and e-mails, resulting in reduced productivity.
- Productivity is reduced due to the blocking of important business communications.
- Employee privacy is at risk if e-mail is falsely blocked and reviewed by an administrator.

On the other hand, False Negatives would create a wrong sense of security leading an organization to believe that there are no policy violations while in fact they are occurring frequently. False negatives can compromise the brand, reputation, competitive advantage of a company leading to significant financial and business costs.

Information leaks may consist of loss of customer or private data or confidential information. Potential confidential data which leaks out of a company may include:

- New product details or specifications
- New project information
- Confidential client information
- Customer information (social security numbers, credit cards, etc.)
- Other proprietary information that should not be viewed by outsiders

In short, an effective Leak Prevention technology should balance between False Positives and False Negatives, being capable of preventing information leaks and data security breaches without interrupting the daily business of an organization, or necessitating additional resources to manually examine messages.

Percept Technology Labs, Inc., an independent testing laboratory, worked with PortAuthority Technologies to establish an open industry testing and evaluation standard for information leak prevention and competitively analyze PortAuthority's PreciseID™ technology and information leak prevention product, **PortAuthority MX** with the 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 can prevent information leaks for multiple protocols, we have focused on email 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 occurs when users communicate from the "inside out", using a variety of different protocols such as e-mail, HTTP, FTP, Instant Messaging or even when printing confidential data. Product requirements to prevent leaks should include protocol agnostic capabilities (in other words, information leak prevention solution should prevent leaks for different outgoing communication protocols)

There are several technologies used by for content identification which Percept Technology Labs, Inc. tested. The three technologies tested by Percept Technology Labs for identifying sensitive information are:

- Keyword Content Filtering
- Regular Expression Content Filtering
- PreciseID™ Fingerprinting

When using keywords for identification, the 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 technology is used by different vendors including PortAuthority Technologies, Symantec and CipherTrust.

Regular expressions are used to detect a specific order of digits and characters. For example, it can look for numbers in certain sequence (such as 9-digits for Social Security Numbers or 5-digits for ZIP codes). This technology is used by different vendors including PortAuthority Technologies, Symantec and CipherTrust products.

PreciseID™, invented by PortAuthority Technologies, identifies actual data rather than the presence of a keyword, or sequence of numbers inside a document. With PreciseID™, the content of a protected document is 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™ is designed to identify documents which are not exact match of the original document 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 the detection capabilities of PreciseID™ with other detection technologies such as regular expressions and keywords. Percept compared these technologies by testing the 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.

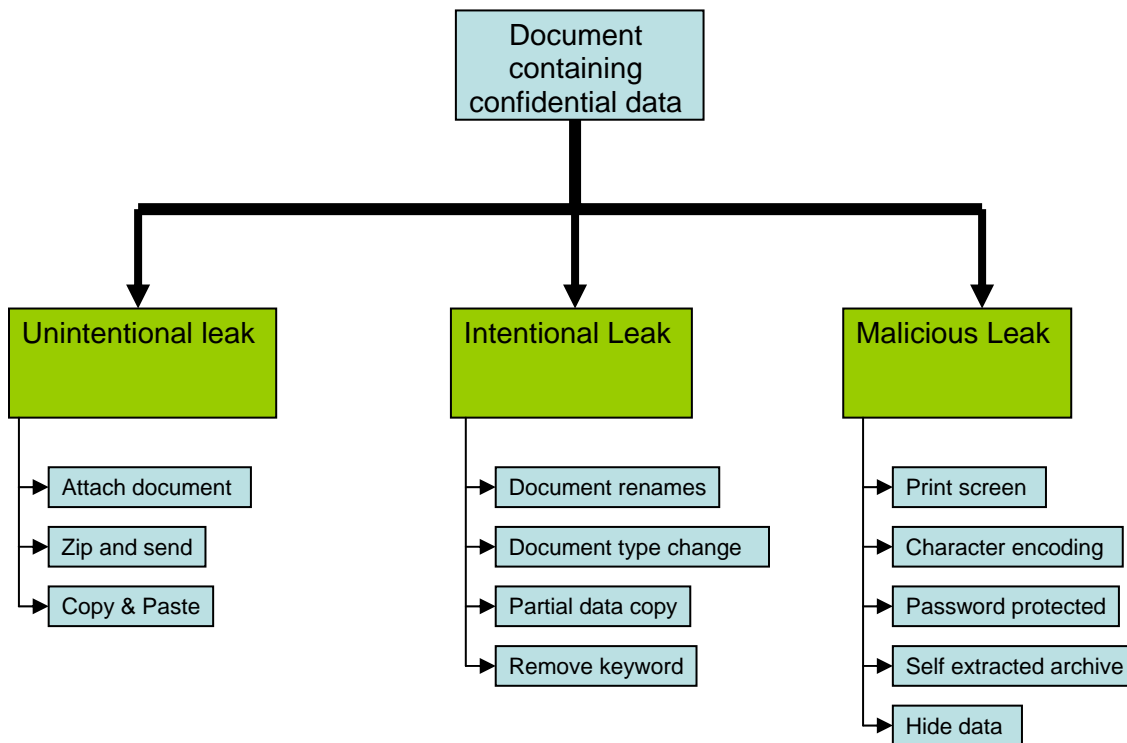
Using a testing standard provided by PortAuthority Technologies as our basis, Percept created nine sections of testing in order to fully test the capabilities of each product.

The nine sections are as follows:

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. This is 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) – Leaking of data in which the person sending an e-mail did not intend to send the confidential data. Unintentional leaks can occur when a person is mistakenly attaching the wrong document to the email message or when Microsoft's Outlook auto completes the email address and the message is sent to the wrong recipient.

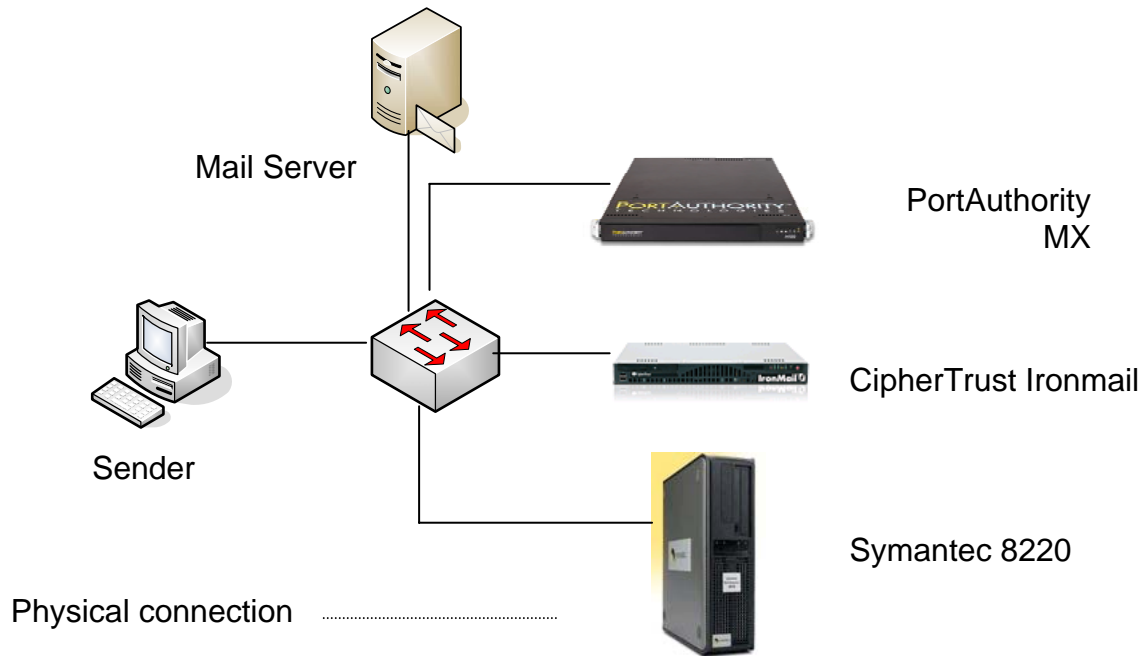
Intentional Leak (I) – Leaking of information in which the person sending the e-mail is aware of his or her company policy but decides to try and send the confidential information anyway. Intentional leaks occur when the sender is aware of the policies and is bypassing security devices without trying to gain personal benefits. For example, when changing a document name or converting it to zipped archive

Malicious Leak (M) – Leaking of information in which the person sending the e-mail is deliberately trying to sneak information past the security product. Malicious leaks are very rare.

Percept's goal was to measure PreciselD™ technology accuracy by comparing it with 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 as well each of the test products. All e-mails originated from one test station, were then directed through the product being tested, and finally arrived at the second test station. E-mails were then evaluated for detection accuracy.

Figure 2: Map of Test Network



The software used for testing includes *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 for a large number of e-mails to be sent at one time.

Measuring Success

Percept Technology Labs, Inc. based its test findings on 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 *

* All products were installed using the latest software releases as of April 10, 2006

Policy Configuration

Product configurations for the three competitively analyzed products are as follows.

- PortAuthority MX: PortAuthority was tested using only Precise ID fingerprints. Other product capabilities were not used. A single document containing the data that needs to be protected 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 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 may be incorrectly blocked by the test products. PortAuthority, using PreciseID™ was capable to accurately identify a leak without causing any False Positive, comparing with other technologies that 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 B220
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. The tests that it passed are due to the fact that it cannot scan for the contents e-mail attachments. 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 will not allow for non-confidential Word documents to be sent. In an office environment that is sending hundreds to thousands of documents 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 was enabled. As a result this test created a false positive result. In Test 5.30 the e-mail was designed to be an 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.

Ironmail S-10 had mixed results. In test 5.11 Percept enabled the filter for attachment type and this as a result CipherTrust failed this test like the Symantec product. Due to the fact that Ironmail S-10 can scan the contents of attachments, it incorrectly blocked test e-mail 5.20, which is a public document containing a marked keyword. Ironmail S-10 also shows a limitation in its inability to scan an attachment footer. In test 5.40, a document which contains a keyword in the footer, Ironmail S-10 successfully blocked it once, but on a retest (with all of the same settings) failed to block it. 5.41 showed two

different results as well. Therefore Percept deemed these results inconclusive for Ironmail S-10.

PortAuthority MX using PrecisID™ excelled in this category. It passed all six tests and demonstrates the ability of fingerprinting technology to reduce or eliminate false positives. Test 5.41 was particularly designed to create a false positive in PortAuthority MX. 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. However, PortAuthority MX has a negative fingerprinting feature, which will correctly ignore common data that may be shared by both public and confidential documents. Percept enabled this feature for Test 5.41 and it correctly let this e-mail pass.

Figure 3: False Positive detection rate

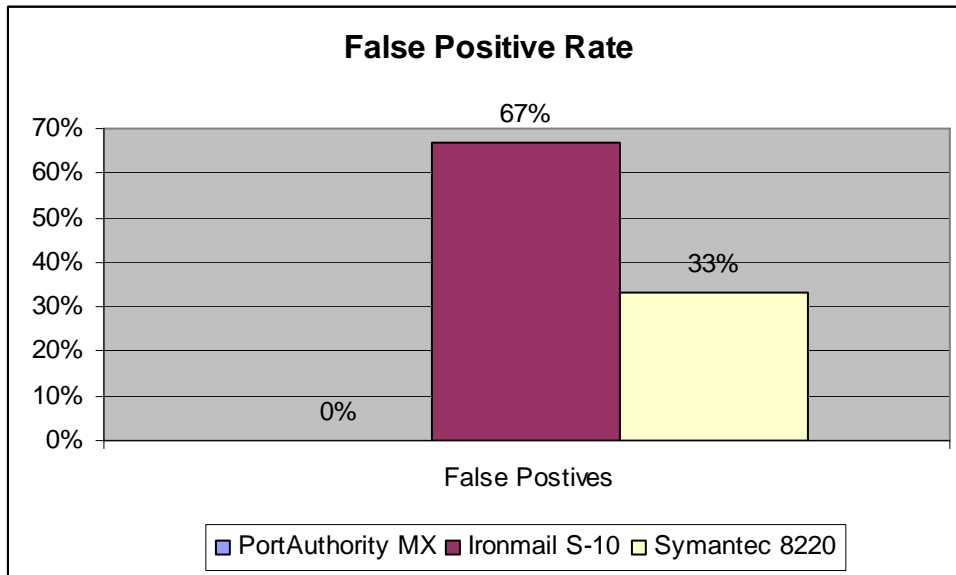
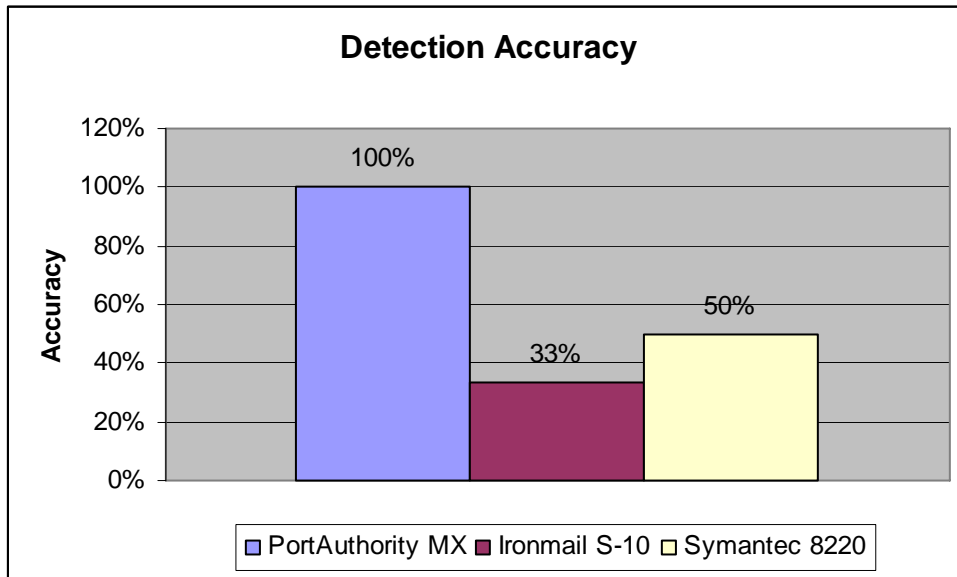


Figure 4: Accuracy Results



2. Records Management

This section of testing focused on the ability of each product to identify confidential customer data that should not be leaked versus data that can be sent via e-mail. Data files did not included the exact records and special attention was given to both False Positives and False Negatives scenarios.

Table 2: Test results for records management of customer data

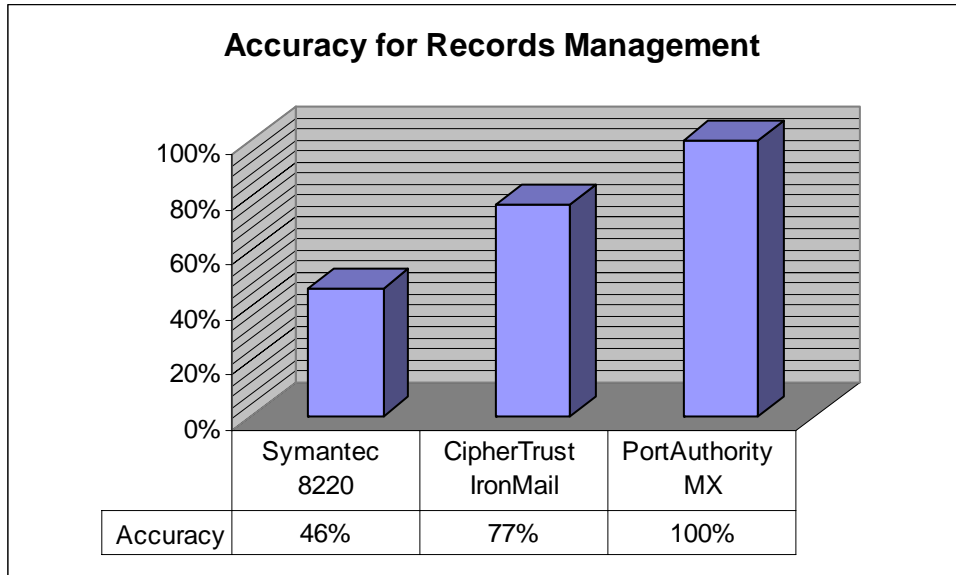
Records Management – Customer Data Tests		Final Results			
Test #	Purpose of test	Class	PortAuthority MX	Ironmail S-10	Symantec 8220
1	Can the products identify original list?	U	TP	TP	FN
2	Do the products block a single ssn in doc?	U	TN	TN	TN
3	Can the products block a .pdf containing blocked info 1?	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 was testing the how well each product could protect confidential customer records. This test was not applicable to Mail Security Gateway 8220, which was using keyword technology only, and was not able to scan the contents of attachments. However, Percept published the results just to illustrate that this product could not successfully filter any of this information. It could only let emails through that were not supposed to be blocked.

Ironmail S-10, which uses regular expressions filtering, in addition to keyword filtering, was able to successfully block several of the test emails that contained 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. Also, it is unclear why Ironmail S-10 had no false positives, because it seems that a regular expressions filter would catch any regular expression whether it was confidential or not. However, Ironmail S-10 successfully identified all of the True Negatives in this section.

PortAuthority MX, demonstrated its best results with a perfect score in this section of testing. PrecisID™, when extracting confidential data in this format, matches names with the relevant account numbers. If these names and numbers appear together in an e-mail or attachment then the e-mail is blocked. If the names and numbers do not match, the message is let through. Protection of this type of data is the highlight of the PrecisID™ technology.

Figure 5: Accuracy Results for Record Management



3. Partial Data Recognition

This section of testing focused on partial data recognition. Section 4 is an extension of Section 2 tests 2.70, 2.80, and 2.90. Instead of a portion of the confidential document being added to the e-mail body, it has been added into a Word document and attached to the e-mail. PortAuthority, using PreciselD™ was capable to detect all leaks.

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

Mail Security Gateway 8220 fails all three tests due to its inability to scan the contents of e-mail attachments.

Ironmail S-10 displays the same results as tests 2.70 – 2.90. If the keyword is not present, then this product cannot block the data.


PortAuthority MX excels in this category. It successfully identified attempts to leak documents even if only 15% of the original document were sent.


4. Data Flooding

This section of testing focused on testing the ability of each product to identify confidential data that has been inserted into both a document and an e-mail body that contains 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 keyword and failed the tests that did not contain a keyword. Once again this demonstrates the limits of content filtering technology.

PortAuthority MX excelled in this section of testing and was able to detect small sections of confidential data that were flooded with other meaningless data.

5. File Type Manipulation

The first section of testing was focused on file type manipulation. Percept created a series of files that contained the exact content of an original confidential document, but modified the format. The tests that Percept ran 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 is 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. Symantec failed all of these tests because this product is incapable of scanning e-mail attachments. It can only scan the subject and body of an e-mail.

***NOTE:** Regarding Ironmail's results in this test. 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 8220
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 identify 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 do contain other confidential data from the original confidential document. The Symantec product, which bases its compliance policy solely on keywords, fails to identify every

confidential e-mail which contains no keywords. Once again, this demonstrates the limits of content filtering based on keywords. Ironmail, also using keyword technology, had the same results as the Symantec product.

PortAuthority MX performed better than the other two products with information contained in an e-mail body. It can block small percentages of the original data, with or without keywords. However, PortAuthority failed to identify 2 of the 6 malicious e-mails.

7. File Format Manipulation

This section of testing focused on file format manipulation. The goal was to test if these security products can correctly block e-mails that have attachments, which contain confidential data but in a different format than 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 c0n 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 0 in entire doc)?	M	FN	FN	FN
11	Can the products block original with no zip code and letter changed (all o to 0)?	M	FN	FN	FN

= Test documents that do not contain a keyword.

Detailed Analysis

This section of testing is similar to Section 2. However, this section tested for changes made in the attached documents rather than the e-mail body.

Once again Mail Security Gateway 8220 fails to recognize any of this confidential data because it cannot scan the contents of e-mail attachments.

Ironmail S-10 is able to recognize documents which contain a marked keyword, despite a font type change or font color change. Test 3.50 also contains a keyword and therefore is blocked by Ironmail S-10.

PortAuthority MX performed the best in this section of testing. It is 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, as an independent test lab, created two additional tests to see how these products handled malicious attempts to leak data.

The first test involved maliciously hiding confidential data in the following areas of a document:

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

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

Detailed Analysis

Mail Security Gateway 8220 again lacks the ability to scan the contents of attachment and therefore hidden data makes no difference in results. Ironmail S-10 has the ability 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, but was unable to block all cases of maliciously hidden content in this test case.

For the second test, Percept took Confidential Information in Document 2 and created several images files containing the original confidential data. This was Percept's most malicious attempt to sneak data past these security products. All three products were unable to detect confidential information in this test case.

NOTE: PortAuthority Technologies has advised Percept Technology Labs, Inc. that they are developing functionality to address these areas and Percept has been slated to test this functionality in the near future.

Conclusions

PortAuthority's PreciseID™ technology greatly excels at data leak prevention, when compared to other technologies such as keywords, dictionaries and regular expressions used by CipherTrust and Symantec. The PortAuthority solution was capable to detect 100% of all unintentional and intentional leaks and without a single False Positive or False Negative event performing two to three times better than other technologies.

The tables below summarizes the overall accuracy of PortAuthority Technologies: A perfect 100% score comparing with other technologies:

Figure 6: Detection Accuracy – Unintentional Information Leaks

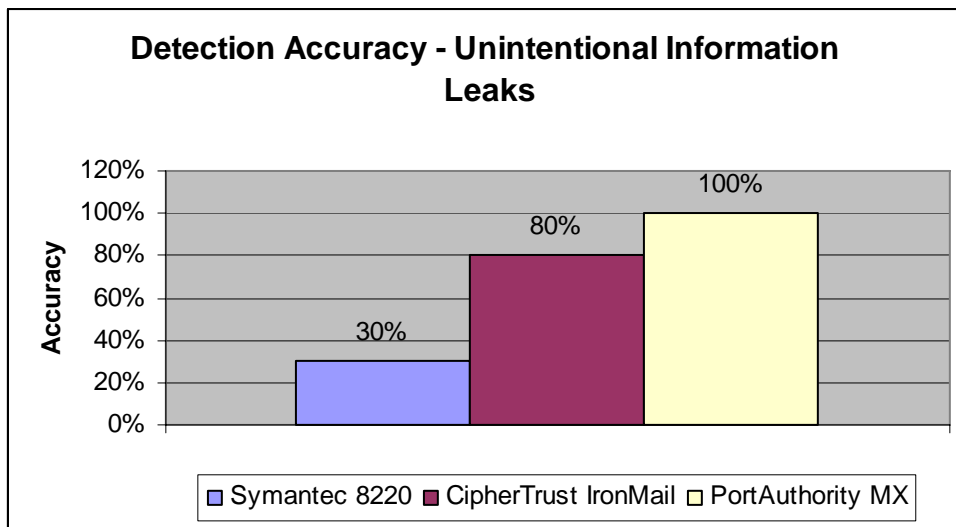
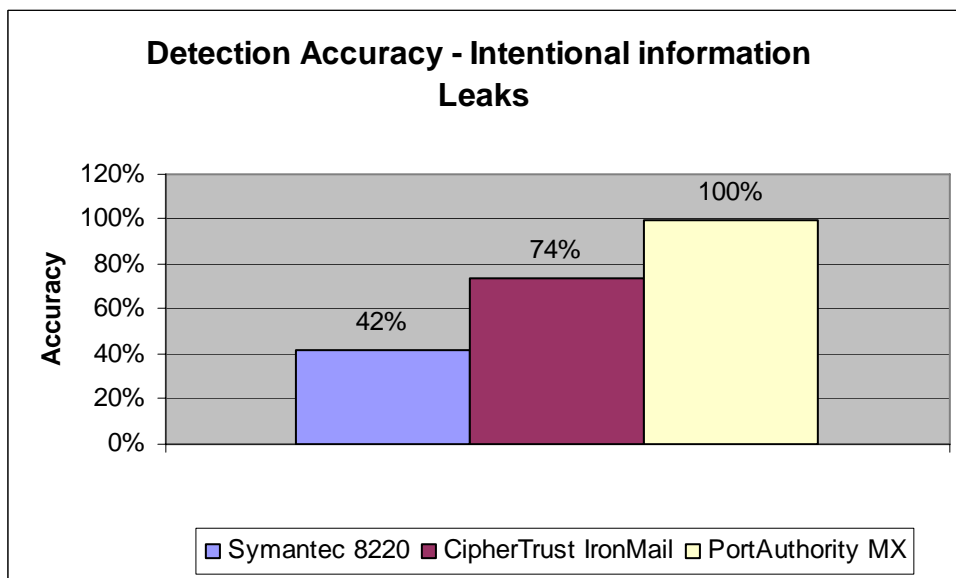


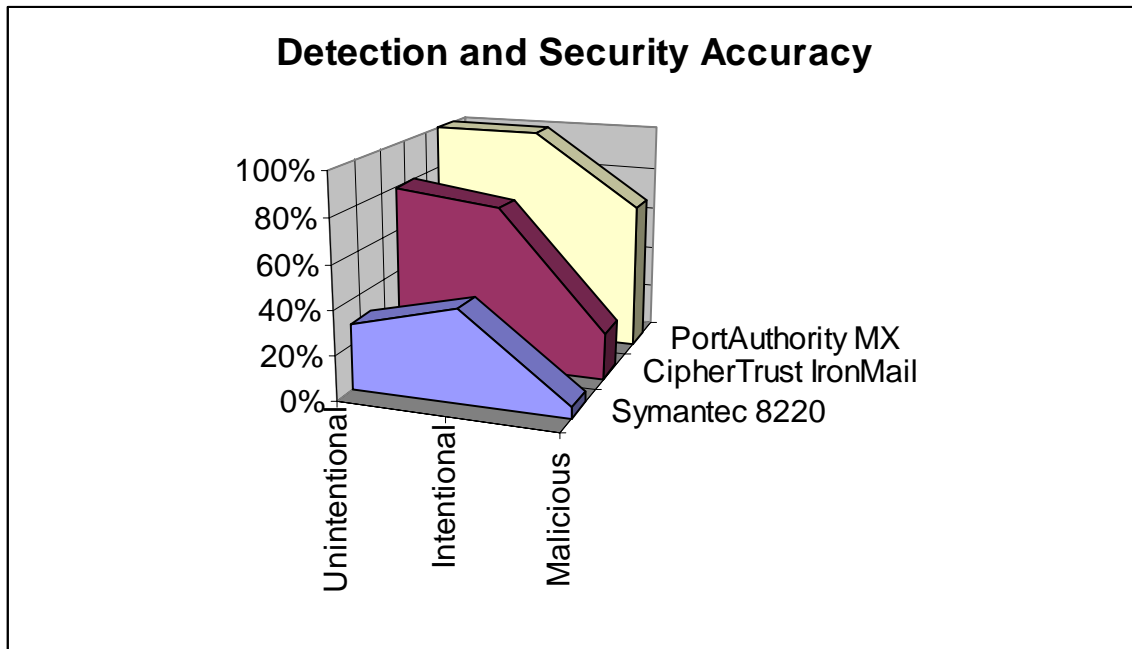
Figure 7: Detection Accuracy – Intentional Information Leaks



Despite our attempts to bypass the system with different malicious attempts, PortAuthority was capable of identifying and preventing the majority of leak attempts while compared to nearly zero detection rates of the other technologies. For companies that are concerned with data leaks, PreciselD™ technology offers the security of knowing that sensitive and confidential information is protected from leaks. However, further testing in malicious attempts for leaking data will be performed with an updated version of PortAuthority's product.

Below is a summary of the accuracy of the 3 different types of technology tested by Percept Technology Labs, Inc. PortAuthority's ability to catch confidential information using the PreciselD™ technology is clearly identified.

Figure7: Accuracy Measurement



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.