

Stopping Information Leaks: Why Traditional Content Filtering Is No Longer Enough

By Sharon Besser
Director, Product Marketing
PortAuthority Technologies

PortAuthority Technologies, Inc.

Three Palo Alto Square
3000 El Camino Real, Suite 100
Palo Alto, California 94306-2122
Tel 650-739-0991
Fax 650.739.0992
www.portauthoritytech.com
info@portauthoritytech.com

Executive Summary

Despite the implementation of sophisticated malware detection, firewalls, intrusion detection and intrusion prevention, and content filtering, corporations continue to leak customer data and company information at alarming rates. These defenses are ineffective in the prevention of information leakage for a number of reasons:

- Their focus is on the threat, not the information
- They deal with inbound, not outbound, communications
- They monitor for known threats and standard keywords
- They are prone to inaccuracy and false positives
- They are not context-sensitive

Email filtering is designed primarily to prevent malware and spam from getting into the network, benefiting the organization through improved security, availability, and productivity. Web filtering is intended largely to prevent users from visiting inappropriate websites, benefiting the organization through improved regulatory compliance and productivity. But neither approach is focused on preventing the leakage of corporate information.

In order to effectively prevent information leaks, corporations must not simply monitor outbound communications, but monitor those communications in such a way that confidential information is prevented from escaping under cover of other content. This requires a radical change in thinking, from focusing on the threat — a largely reactive process — to focusing on the information itself, which is under the control of the organization and can thus be proactively protected.

Traditional content filtering goes some way towards controlling the movement of structured data such as database entries, although nowhere near far enough to prevent current levels of leakage. However, 80% of enterprise data is unstructured, its confidentiality dependent on factors such as context and origin. Applying structured data filtering to unstructured data leads to false positives, false negatives, and high degrees of user frustration — which in turn leads to attempts to bypass the system.

This paper examines the risks inherent in relying on traditional content filtering solutions to prevent information leaks and why a different approach is required. It goes on to discuss how PortAuthority Technologies' unique PreciseID™ approach delivers sufficient granularity in filtering to ensure protection of critical data, enforce regulatory compliance, reduce inappropriate user behavior, and seamlessly integrate with existing infrastructure.

Table of Contents

Executive summary	2
What's the problem?	4
The challenges of information protection.....	4
What are organizations doing now?	6
Context is key.....	7
Technology limitations.....	8
The Information-Centric Approach	9
First, identify the information.....	9
Tightening the filter.....	10
The PortAuthority Solution	13
PortAuthority fingerprinting.....	13
Not just accuracy, but manageability.....	15
Flexible, integrated solution.....	15
Why PortAuthority Technologies?	17
Summary and Conclusions	18
About PortAuthority Technologies™	19
About The Author	19
Appendix: Legislative Reference	20

"Sixty-six percent of security experts surveyed cited loss of private customer data as a high or very high level of concern."

- 2004 Ernst & Young Global Information Security Survey

"Eighty-three percent of companies surveyed experienced security breaches of some kind in 2004. Sixty-two percent report attacks from an internal source."

- 2004 Deloitte Global Security Survey

"Although the general trend of losses is down, there were two areas of increase - unauthorized access to information (average loss per respondent up from \$51,545 in 2004 to \$303,234 in 2005) and theft of proprietary information (average loss per respondent up from \$168,529 in 2004 to \$355,552 in 2005)."

- CSI/FBI 2005 Computer Crime and Security Survey

What's the Problem?

Information security is hardly a new topic. The war against viruses and worms began almost two decades ago, and early content filtering efforts were not far behind. Yet despite the millions of man hours and award-winning intellect that's been applied to the problem, and the relatively sophisticated solutions that most organizations now have in place, confidential information continues to leak from corporations at an alarming pace.

Consider the following — just a few of many examples:

- In 2002, Eli Lilly mistakenly sent its Prozac users' e-newsletter to 670 email addresses without masking each address from the others; every recipient could see the identities of all the other people receiving the newsletter. The result: alienated customers and a \$160,000 fine for the company.
- In late 2003, the founder of Valve Software confirmed that hackers had stole the source code to Half-Life 2, the game industry insiders were counting on to help revive the struggling PC gaming business. Release was delayed six months, and the economic effects on the developer, publisher, and industry are unquantifiable.
- In February 2005, a statistician at Palm Beach County Health Department inadvertently emailed a confidential list of 4500 AIDS patients and 2000 HIV positive patients to 800 county employees.

And it seems that every week there's another instance of personnel records or credit card databases being cyberjacked by some unauthorized individual or organization.

It also seems there's a new law every week that corporations must abide by or risk the inevitable public relations fallout and fines. It's not only federal statutes like Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA and state laws like California's SB 1386 and 1950, but also overseas laws that impact US businesses; Canada, New Zealand, Japan, the European Union, as well as individual laws in individual EU nations, such as the UK's Data Protection Act, also impose limitations on the ways organizations handle electronically-stored confidential information.

The challenges of information protection

Let's take a moment to review the challenges facing organizations seeking to protect confidential information against threats, both internal and external:

- Most information leaks are the result of legitimate users performing a legitimate operation that breaches corporate security policies
- To protect customer data and brand reputation, organizations must control the exposure of sensitive private information or risk jeopardizing customer loyalty and tarnishing the brand
- To comply cost-effectively with external policies and regulatory requirements, organizations must manage the ever-increasing costs of ever-broader security solutions
- To enforce corporate information security policies, organizations must improve their insight into policy violations
- To prevent the loss of intellectual property information, corporations must be able to track the source of leaks among thousands of employees and contractors

Compounding the problem is the enormous range of data that must be protected. Personnel records, health records, insurance records, patent filings, product designs, manufacturing schedules, financial transactions, academic records, donor information, sales pipelines — the list is almost endless. The forms in which this data is held render the problem even more complex — server, desktop, mainframe, database, spreadsheet, word-processor, presentation, email, archived storage, weblogs — any or all of which may be onsite or offsite, internally controlled or accessed as a hosted application. Thus far, anti-virus, anti-spyware, or content-filtering programs failed to protect data in all these different forms and formats.

What Are Organizations Doing Now?

As we noted earlier, there are plenty of potential solutions out there. Anti-virus, anti-spam, content filtering — all fill a partial need in the ongoing war to protect against threats to information integrity and confidentiality.

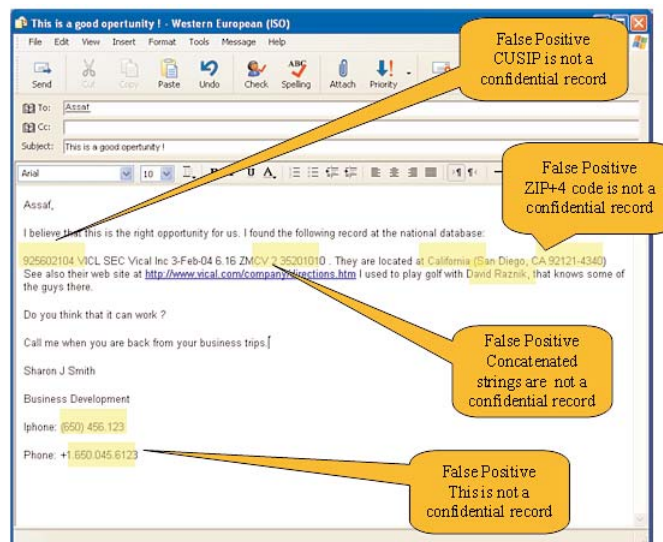
- anti-virus and anti-spyware solutions are effective at detecting known malware threats as well as malware-like behavior
- anti-spam and content-filtering solutions are effective at matching sequences of characters in documents or IP addresses

But these solutions were developed to deal with generalized threats, using known factors and behaviors, and focus their attention on the threats, not the data that needs to be protected:

- the same virus will attack Company A and Company B
- social security numbers have the same structure in Company A's database as in Company B's
- spam for Company A is also spam for Company B

But now, we are recognizing that the relative importance of information is governed by its context - the Cayman Islands, for example, is a vacation destination as well as a tax haven — and whether that information exists in a structured world such as a database — where its context never changes - or an unstructured one, such as Word or Acrobat, where a string of characters representing a specific item of information may appear in many different places and forms.

The result of this new level of understanding is a realization that content filtering needs to function at this contextual level to effectively enforce security policies and prevent information leaks. Current content filtering solutions are not equipped to deal with this level of granularity, as can be seen in the example email message below. This message illustrates the different types of 'noise' that may appear in a single email. Traditional, or Regular Expression based, systems cannot differentiate between noise and data. In this example, there are four different 9-digit sequences, none of which is confidential and all of which may be falsely identified as a breach by a traditional regular-expression-based content filtering system.



Context is key

Let's imagine that we're looking at the information we need to protect on a sonar screen. In a perfect world, it is easy to identify the target; for example, social security numbers are easy to detect, they all look alike, have nine digits, and follow the same general rules.

Unfortunately, it is not a perfect world. CUSIPs (the security identifiers that facilitate the clearing and settlement of stock trades), Social Security numbers, ZIP+4 codes, some state drivers' licenses, national ID numbers, account numbers, and many other records also look like social security numbers — and that's just one example of the 'noise' that can and does confuse traditional content-filtering systems. The challenge for effective information protection in business is precise identification.

Traditional content filtering, like traditional spam filtering, lives in a black and white world. A document is either compliant with policy or it is not. Information is either permitted to be included in a document or transmission or it is not. Information is either in a keyword list or regular expression dictionary or it is not. Without granular knowledge of the information contained in a document, if part of that document is cut and pasted into an email message, a policy breach will not be detected. This approach, while a good starting point, is just that, a starting point. Information in different contexts essentially has different meanings, so that nine digit social security number in an employee database represents a radically different leakage risk than a nine-digit ZIP+4 code in a letter to the local newspaper. The probability of false positives is therefore high — and years of wasting time dealing with false positives from other generalized protection solutions tell us this is not the way of the future.

The issue of context also extends to the portability of information between applications. Many content-filtering solutions can only offer document-level information control — in other words, the software takes a snapshot of the entire sensitive Word document, such as an M&A offer, to protect that information. Unfortunately, if parts of that Word document are cut and pasted into an email, that information will leave the organization unchecked because it's been taken out of the context of the protected document.

Clearly, traditional content filters go a long way towards helping control what information is allowed to enter the organization. But equally clearly, they cannot accurately, precisely and reliably prevent unauthorized information from *leaving* the protected network and leaking to the outside. Universal policies cannot be applied to all corporations and all contexts, because every corporation and every context demands that the information be seen through a different lens. The only way to tackle this quandary effectively is to turn the whole problem on its head; instead of looking at how to prevent threats against data — which is what traditional content filters do — we need to look at how to protect the information from being leaked. The way to a viable and lasting solution lies in focusing on the information, which is a constant, not the threat, which is ever-changing.

"Many content-filtering solutions can only offer document-level information control — in other words, the software takes a snapshot of the entire sensitive Word document, such as an M&A offer, to protect that information."

"...content security vendors that scan email and Web activity are limited by their crude detection capabilities based on keywords and phrases. They are well-suited to enforcing simple policies around inappropriate dialogue or blatant disclosures of privileged information. But attempts to provide more subtle detection are ineffective: Too often they end up blocking legitimate communications and overlooking instances where sensitive information is sent inappropriately.

- Forrester Research, June 2005

"Fifty-two percent of CISOs say they have a "moat and castle" approach to network security, admitting that once the perimeter is penetrated, the inner defenses are soft."

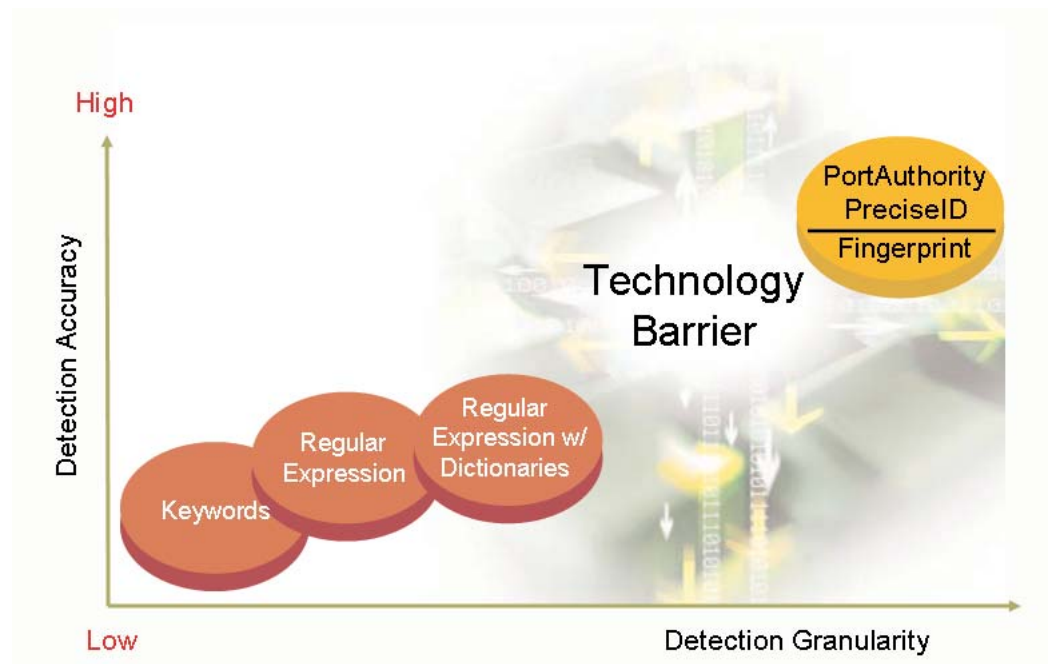
- CSO Magazine, March 2005

Technology limitations

Traditional content filters are self-limiting in that they are looking only at one or more of the following:

- File types
- File-based binary signatures (file hash)
- Text-based binary signatures (exact file index signatures)
- Numbers, patterns, regular expressions and keywords/phrases

By restricting their monitoring to these elements, these filters generate high rates of false positives, as we saw with the example email earlier in this section. Any 'protected' data that has been cut and pasted into another document becomes unprotected, leading to false negatives. Data in non-typical file types such as CAD files are ignored completely. And incorrect data feeds to the policy manager lead to the blocking of legitimate communications. Taken together, these elements can lead to a significant drop in productivity while still leaving major holes through which data can leak. The diagram below shows why information granular filtering to the level of fingerprinting is essential to effective leak prevention and policy enforcement.



The Information-Centric Approach

Information is the lifeblood of every organization, commercial or not-for-profit, private or public. Information is something we can control; the nature of an outside threat is something we cannot control. So it makes sense to approach the protection of information from the perspective of the information, not the threat.

First, identify the information

Information leaks occur, either accidentally or maliciously, because most security approaches are 'outside-in' rather than 'inside-out'. Organizations need an efficient means to correctly and instantly recognize when a communication containing sensitive content is being sent to an unauthorized recipient. But without a high degree of accuracy, content monitoring systems quickly overwhelm IT staff with false positives and cause a dramatic slowdown in employee productivity. Simply blocking messages is not enough; the real challenge lies in identifying whether a message containing sensitive information is being sent to an inappropriate recipient, and then enforcing the appropriate security policy.

The difficulty in identification

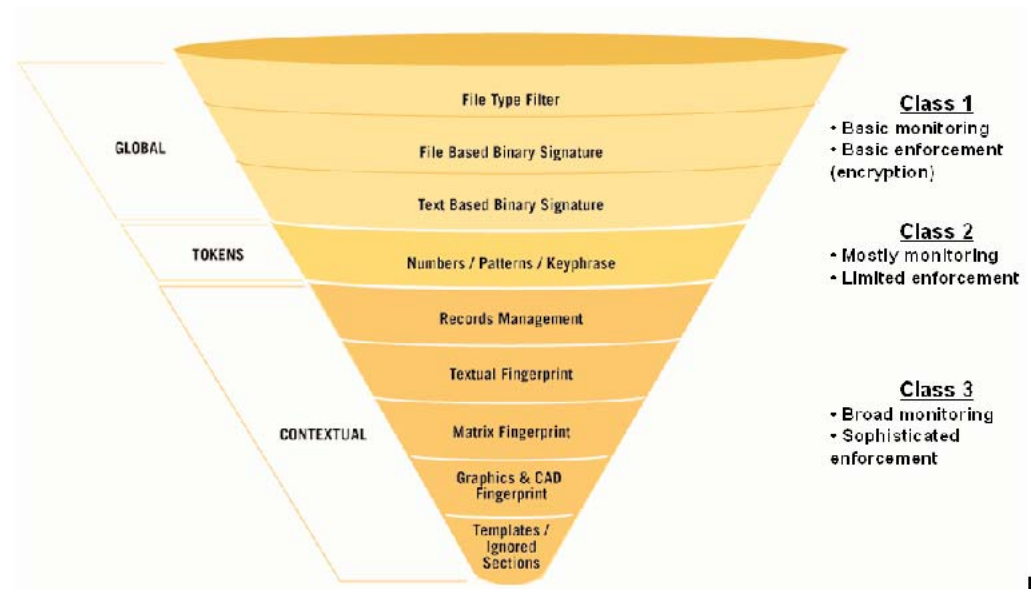
Identifying sensitive content in transit is particularly difficult because:

- Fragments of sensitive content, such as credit card numbers, account numbers, customer records, and phone numbers, can be easily cut and pasted into other documents and messages, or simply posted to web sites — a process which bypasses traditional content filtering.
- Sensitive information like contracts, employee offers, financial filings, and product specifications is often modified from an original document into derivations or excerpts.
- Multiple copies of sensitive information typically exist, and attempts to secure a particular file are thwarted by the reality that employees have access to identical or similar information elsewhere on the network.
- Sensitive information can be kept in multiple unstructured file formats or structured databases with different versions and compatibility issues.
- Sensitive content can be communicated through a variety of channels, including email, web mail, instant messaging, FTP, or simply be printed

To handle the range of information types, formats, and transmission channels, organizations need a set of identification technologies that are robust enough to identify both structured and unstructured content as well as fragments and derivatives of either. These identification technologies must work in real-time or they risk paralyzing business communications. Finally, these identification algorithms must account for the context of the content to accurately and correctly recognize which messages must be handled by which policies. Without a complete set of identification technologies, real-time policy enforcement can not be applied with a high degree of precision and accuracy.

Tightening the filter

Let's take a look at how taking an increasingly granular approach to content filtering radically improves both the accuracy and the reliability of information protection.



The illustration above shows how increasing the granularity of the filtering delivers the highest degree of accuracy. We looked earlier at the limitations of Class 1 (file types, file-based binary signatures, and text-based binary signatures) and Class 2 (numbers, patterns, and keywords/phrases). Most traditional content-filtering products provide good coverage for Class 1 filtering and fair coverage for Class 2; as noted earlier, some will also handle elements of contextual filtering (at the document level). But it's when we get down to fingerprinting of the information within a document that the potential for truly granular and context-sensitive content identification becomes apparent.

Let's take a closer look at how Class 3 contextual filtering impacts the process of smart information leak prevention. Each contextual filter is optimized to detect certain types of information, achieving extremely accurate information identification. These contextual filters can be organized into five major categories:

Records Management Fingerprinting Filter allows the application of Boolean logic to various fields within an individual record, for example to identify a potential information leak if a customer's account number and date of birth are found in a single message or if the person's name and social security number appear in the same message. This significantly reduces false positives and false negatives by applying multiple criteria within a record.

"Content monitoring and filtering tools detect malicious or accidental misuse of private data and intellectual property. 80 percent or more of the violations detected by content monitoring and filtering tools are part of an established business process, such as data exchange over FTP or e-mailing unencrypted account numbers. Another 10 percent or more of violations are accidental, with less than 10 percent being malicious activity."

- Gartner Group

Textual Fingerprint allows extremely robust identification of content, including fragments or derivatives, by converting unstructured text into a series of mathematical representations, or "information fingerprints." This ensures that any attempt to cut and paste, reformat, or retype designated protected information is detected.

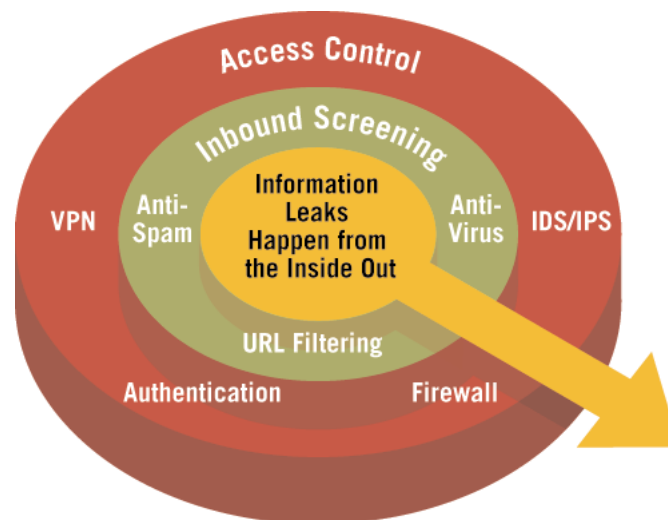
Matrix Fingerprint converts content from a tabular or spreadsheet format into a series of mathematical representations, while capturing its many idiosyncrasies. Proportionality checks ensure accurate identification of protected content, thus resisting content manipulation such as the global conversion of currency from US dollars to Euros.

CAD/CAM Fingerprint interprets the value associated with a diagram regardless of changes to its outward appearance, such as rotation or inversion.

Template/Boilerplate Fingerprint improves the accuracy of detection by accounting for false similarity and screens out commonly recurring text in similar documents, including boiler plates, disclaimers, template descriptions, forms, and contract terms. This technique dramatically reduces the false positives associated with basic identification techniques.

Additionally, fingerprinting should be derived from a unidirectional process to ensure that original content cannot be reverse engineered from an existing fingerprint.

By adding this layer of identification on top of existing content filtering solutions, organizations can significantly decrease the potential for information leakage.



Information is controlled from inside the organization, so placing filters at the perimeter of the organization can only go so far in managing access to privileged content. Information control needs to be embedded inside the organization, where it's contained and manageable.

In the same way that a firewall protects against threats by looking for source, destination and protocol and intrusion prevention systems look for source, destination, protocol and application, effective information leak prevention should look for source, destination, protocol, application, and the actual data.

What's needed, therefore, is a new type of solution — one that transparently monitors and controls outgoing and internal communications and is custom-built for your data.

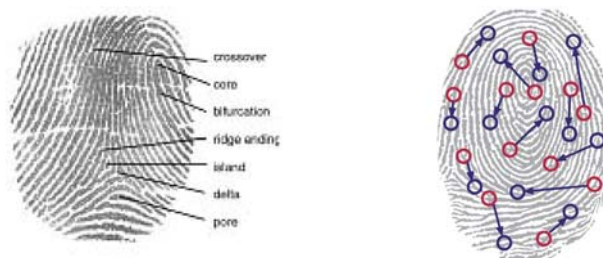
The PortAuthority Solution

Drawing on years of experience in policy-based enforcement, PortAuthority uses PreciseID™ fingerprinting technology to detect and prevent the unauthorized communication of all types of sensitive information via outgoing mail, web, internal mail and other channels. By adding this extra layer of granularity, PortAuthority's technology enables organizations to not only protect their information but also gain insight into their insider risk vulnerabilities and effectively enforce internal policies in real time.

PortAuthority fingerprinting

PortAuthority's PreciseID™ information fingerprints are mathematical representations of groups of sentences, words and characters taken from the content of a document, publication or message, which may serve to identify the document, publication or message uniquely. In mathematical terms, each fingerprint is a set of quasi-random function clusters that are used to describe the content. Unlike MD5 file hashes that work on the file level and create a checksum for the entire document, PortAuthority fingerprints work at the content level, providing the ability to find content similarity between different documents regardless of source or context and the ability to perform standard content filtering processes.

PreciseID™ allows for extremely reliable and accurate identification of information. Just as human fingerprints include different elements that can be used to identify a person with great accuracy, information files can be threaded with the same concept as seen in the diagram below.



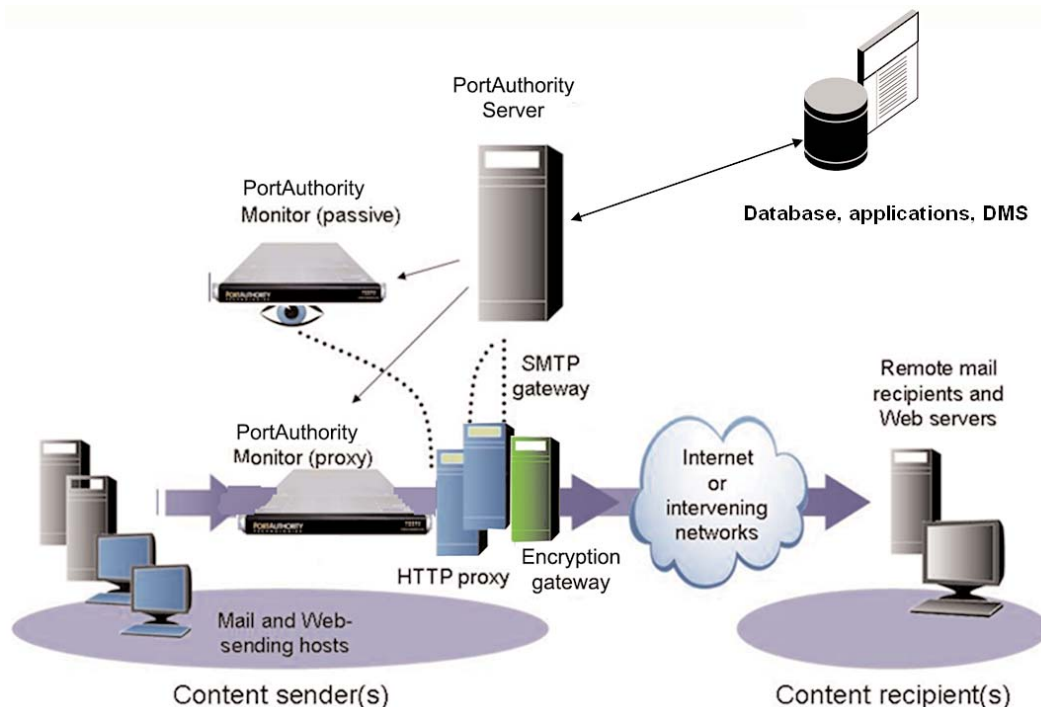
PortAuthority's proprietary fingerprinting technology delivers robust, contextual information identification. Using a unidirectional process, PreciseID™ examines the content of documents or raw data and extracts a set of mathematical descriptors or "information fingerprints". These fingerprints are compact and faithfully describe the underlying content. By assigning unique identities to each information asset, PreciseID™ can track information in motion with great precision. Original content cannot be recreated or reverse engineered from an information fingerprint.

The power of the PreciseID™ fingerprinting technique is its ability to detect sensitive information despite manipulation, reformatting, or other modification. Fingerprints enable the protection of whole or partial documents, antecedents, and derivative versions of the protected information, as well as snippets of the protected information whether cut and pasted or retyped.

Beginning the process of fingerprinting an organization's confidential information is simply a matter of targeting directories with sensitive or confidential information and assigning the required policies to these directories. PortAuthority's file-system agent then recursively fingerprints all the information in these directories and stores the fingerprints together with the corresponding policies in a secure database. The process is automatic, and enforcement is operative from the start.

From this point, the information is protected. All monitored traffic is compared with the stored fingerprint and, if a match is found, the corresponding policy (block, quarantine, encrypt, audit, or notify) is applied. The policy is assigned to information, not individual files.

For example, suppose that an employee cuts and pastes information from a Word document containing a sensitive meeting record into a PowerPoint slide for onward transmission to an editor or analyst. A fingerprint of the original Word document is already stored in the database, so when a different file containing some of the information already fingerprinted is passed through the system, real-time fingerprinting occurs, the similarity is flagged, and the message with the PowerPoint attachment is quarantined or otherwise prevented from leaving the network. PortAuthority's filtering goes beyond traditional content filtering to trap context-sensitive information in multiple formats. This level of precise identification of protected content is the true value of PreciseID™ technology.



"PortAuthority, when used in conjunction with proper network architectures and tight configuration controls, can prevent the majority of protected data from leaking to unauthorized parties."

- Information Security magazine

Not just accuracy, but manageability

PortAuthority technology has been built from the ground up to meet all key requirements for an effective information leak prevention system. Forrester Research has determined that the following criteria should be met by any viable information leak prevention solution:

- Accuracy
- Identification and classification
- Comprehensiveness
- Enforcement location and actions
- Configurability
- Management, reporting and forensics
- Low cost of ownership

To meet the **accuracy** requirements, PortAuthority delivers real-time detection and blocking of privileged information throughout Class 3, regardless of whether that information is structured or unstructured, textual or graphical, in its original or a derived format — even if it's buried in multiple layers of file compression.

To meet the **comprehensiveness** requirement, PortAuthority monitors multiple communications protocols — HTTP, generic SMTP, Microsoft Exchange, Lotus Notes — and over 300 file types, including CAD files.

To meet the **enforcement** requirements, PortAuthority prevents information leaks at the network level, filtering content through its own embedded ecosystem to avoid the need for client software deployment or changes to the network infrastructure. Policy options for action include block, allow, quarantine, monitor, encrypt, and archive.

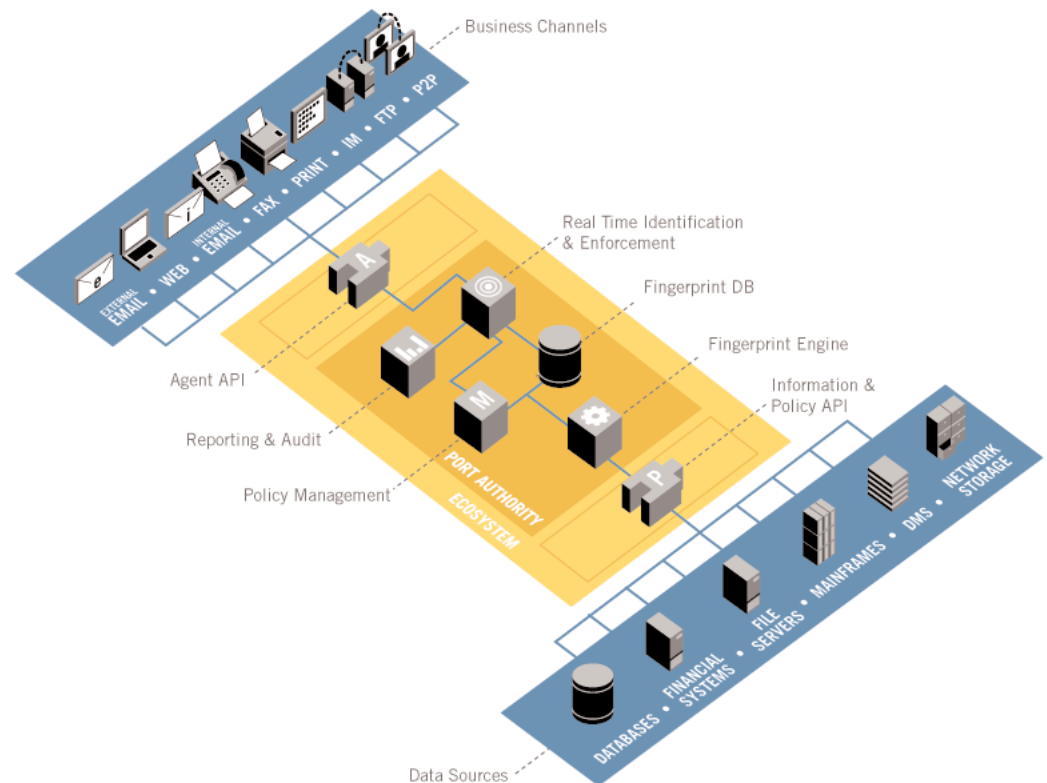
To meet the **configurability** requirements, PortAuthority ships with predefined policy templates for regulation violation reporting, a wizard-based tool for creating policy rules, real-time policy engine, the ability to automatically build a custom content base, and an open API for integration with third-party systems.

To meet the **management, reporting and forensics** requirements, PortAuthority supports delegate and hierarchical administration, remediation, and reporting as well as directory-enabled group policy, delivering reports in real-time and on an ad-hoc basis. Detailed log histories provide violation forensics information and trend analysis.

To meet the **low cost of ownership** requirements, PortAuthority deploys seamlessly into existing business processes and IT environments. Users do not have to change the way they work nor do they need training. The fingerprinting process does not demand excessive overheads in time or resources: a million records can be fingerprinted in less than ten minutes. And PortAuthority's open architecture minimizes the cost of integration with data sources, policy enforcement options, and communication channels.

Flexible, integrated solution

PortAuthority delivers open, flexible architecture to allow for integration with application servers, database management, customer relationship management, enterprise resource planning and other key business infrastructure systems.



Protecting sensitive information using PortAuthority's information leak prevention solutions is a simple, three-step process:

1. **Learn.** Security and compliance staff define and map confidential data sources and create distribution policies
2. **Monitor.** The PortAuthority server processes outbound and internal communications and determines any matches against the fingerprint library
3. **Enforce.** Deliver content to authorized recipients, quarantine suspicious messages, and create an audit trail to substantiate compliance

Why PortAuthority Technologies?

PortAuthority Technologies in 2002 delivered the first Information Leak Prevention (ILP) solution to both monitor and prevent the unauthorized distribution of all types of sensitive information in transit through enterprise communication channels.

Unlike traditional content-filtering companies, PortAuthority takes an information-centric view of the business world, focusing on managing enterprise information assets and reducing the exposure of information distribution.

With more than three years of active customer deployments and 27 patents filed, PortAuthority Technologies provides a proven, best-of-breed information leak prevention solution available to help enterprises:

- Protect customer data and confidential information
- Achieve true regulatory and corporate compliance
- Quantify risk and control sensitive information
- Reduce inappropriate employee behavior
- Secure data with low cost of ownership

PortAuthority Technologies is led by a seasoned executive team with deep roots in information security and with strong track records of rapidly building successful software firms. Our customers include leaders in the financial services, health-care, technology, and government sectors.

Summary and Conclusions

PortAuthority solutions provide proven, reliable and accurate leak prevention for sensitive data. The company's patent-pending algorithms deliver precise, contextual matching with minimal false positives; concurrently, resilience to data manipulation delivers a low rate of false negatives. All types of sensitive information can be protected, from structured databases to CAD diagrams, through most web and email communications channels.

Simple, flexible policy management by user, department, group, domain, content type and threshold ensures low-maintenance enforcement of security and compliance policies, with a wide range of containment options. PortAuthority technology can be transparently integrated into existing network infrastructures, with no workflow or process changes or user training. The open architecture ensures that integration with data sources, communication channels, and policy enforcement options is seamless.

Why not start out on the road to information leak prevention today? To help you identify your information risk vulnerability, PortAuthority Technologies offers a free risk assessment to quickly identify security vulnerabilities, at-risk business processes, and ineffective policies. The assessment will provide your organization with an executive summary, including:

- Detailed reports of information assets distribution
- Highlights of key vulnerabilities
- Actionable recommendations

The visibility you gain from the information risk assessment will provide you with a measurable and actionable insight to address information leak vulnerabilities before they become a problem.

Complete the form at http://www.portauthoritytech.com/services/serv_ra.html and start protecting your information today.

About PortAuthority Technologies™

PortAuthority Technologies (www.portauthoritytech.com) 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. Using patented PreciseIDTM technology, only PortAuthority stops information leaks 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 Act (GLBA), HIPAA, CA CC1798, PIPEDA and Sarbanes-Oxley by closing the gap between employee behavior and corporate and legal policies.

PortAuthority Technologies™
www.portauthoritytech.com
877.843.4879 Toll-Free

WP0102-1205

Appendix: Legislative Reference

Gramm-Leach-Bliley

The security provisions of the GLB Act are implemented in a Safeguards Rule adopted by numerous federal financial regulators, including the Federal Trade Commission (Federal Register: May 23, 2002, Vol. 67, No. 100, page 36484.). The Rule has teeth, as evidenced by recent enforcement by the FTC. See "FTC Enforces Gramm-Leach-Bliley Act's Safeguards Rule Against Mortgage Companies: Agency Alleges Companies Failed to Protect Customers' Personal Information," Press Release, Nov. 16, 2004, <http://www.ftc.gov/opa/2004/11/ns.htm>.

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. Among other things, the Rule mandates that financial institutions:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and assess the sufficiency of safeguards in place to control risks;
- Design and implement safeguards to address risks and monitor the effectiveness of these safeguards.

16 CFR §314.4

Although the Rule gives little detail, and does not specify any particular technology, many financial institutions logically interpret it as requiring the encryption and tracking of email containing customer information. See The Norcross Group, "Security Law Compliance," <http://norcrossgroup.com/securitylaws.html>.

HIPAA

The Health Insurance Portability and Accountability Act ("HIPAA") requires that covered entities such as health plans, health care clearinghouses, and health care providers safeguard electronic patient information.

Under HIPAA, the Department of Health and Human Services publishes a Security Rule mandating that each covered entity develop policies, procedures and contingency plans for securing information. See <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>.

PortAuthority makes it easy to meet the specific goals of HIPAA's Security Rule. See the section-by-section analysis of the Rule's requirements for user authentication and data tracking, published at <http://www.certifiedmail.com/industries/Healthcare/hipaa-cm.aspx>.

California AB 1950

California Assembly Bill 1950 is new legislation requiring that the holders of sensitive information about California residents use "reasonable security procedures" to protect that information. Failure to use such procedures could expose the holders to liability under class action lawsuits.

California's privacy legislation is setting national standards because California is so populous, and it is almost impossible for an enterprise possessing private information to know for sure whether the subject of the information is or is not a California resident.

California SB 1386

California's Senate Bill 1386 requires enterprises to notify California residents when the security of private data about them is compromised. This law has triggered a wave of embarrassing public announcements by brand name companies such as Wells Fargo (pertaining to customer information) and Time Warner (pertaining to employee information). SB 1386 is codified as California Civil Code Sections 1798.29, 1798.82 and 1798.84.

Professional Ethics

Lawyers, investment professionals, and certified public accountants are subject to ethical duties to maintain the confidentiality of client information. Schools and colleges are subject to the Family Educational Rights and Privacy Act, which requires them to protect the confidentiality of education records.

Sarbanes-Oxley

The Sarbanes-Oxley Act motivates public companies to tighten internal controls so as to deter fraud and protect assets. This requirement naturally includes protection for sensitive financial information, so as to prevent eavesdroppers (company employees and otherwise) from seeing financial information before it is released to the public. Premature access to information leads to insider trading.

Example: The Securities and Exchange Commission charged James Adelt, AmeriCredit's senior vice president for information technology, for exceeding his authority in the company's information system, and then trading on the non-public financial information he accessed. SEC Litigation Release. Complaint: James M. Adelt, et al., November 3, 2003
<http://www.sec.gov/litigation/complaints/comp18442a.htm>.

Data Privacy Laws Outside the US

Many jurisdictions outside the US have adopted strict data privacy laws requiring that electronic data containing personal information be secured against unauthorized access.

Article 17 of the European Commission's Directive on Data Protection calls for holders of personal data to use technical methods to protect the data from unauthorized access. This requirement applies "in particular where the processing involves the transmission of data over a network." (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995)
http://europa.eu.int/comm/internal_market/privacy/index_en.htm

Consistent with the European Data Directive, many countries in the European Union have adopted local data protection legislation. The United Kingdom, for example, enacted the Data Protection Act 1998 <http://www.hms.gov.uk/acts/acts1998/19980029.htm#aofs>. It requires anyone processing personal information to follow certain principles of good information handling practice. Principle number 7 requires that personal data be kept secure. The principle states, "Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA) requires the use of technical safeguards to protect personal information. See "A Guide for Businesses and Organizations: Your Privacy Responsibilities," http://www.privcom.gc.ca/information/guide_e.asp.

Australia enacted the national Privacy Act 1988, which includes National Privacy Principles applicable to the private sector. Principle 4.1 states, "An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure." See <http://www.privacy.gov.au/act/index.html>.

Section 20 of Japan's Personal Information Protection Act (2003 Law No. 57) states: "A Business must take steps to prevent the unauthorized disclosure, loss or destruction of Personal Data. And it must protect Personal Data security." Translation at http://www.proskauer.com/hc_images/JapanPersonalInformationProtectionAct.pdf