



IBM Proventia Content Analyzer

Safeguarding critical data is becoming more difficult. While the theft of laptops, data cassettes and hard drives accounts for the majority of data loss incidents, network information leaks involving sensitive data are occurring more often than in recent years, and are more difficult to detect and prevent.

Confidential corporate data poses a substantial risk when transmitted outside an organization's security safeguards. The risk involves both the possibility of interception and theft, and the potential for penalties levied against organizations not complying with today's privacy regulations.

IBM Proventia® Content Analyzer comprises a collection of new data inspection capabilities designed to monitor and identify unencrypted personally identifiable information (PII) such as credit card information, social security numbers, telephone numbers, monetary amounts and other potentially confidential information. Proventia Content Analyzer technology is available on IBM Proventia product family of network appliances that include an IBM Internet Security Systems (ISS) Intrusion Prevention System (IPS), including IBM Proventia Network Multi-Function Security and IBM Proventia Network Intrusion Prevention System (IPS).

Data awareness

Many organizations are concerned about protecting not only PII, but also confidential information such as project names, product release dates and financial information. Proventia Content Analyzer offers organizations the ability to use eight defined detection signatures geared towards PII, and to create up to eight additional custom signatures defined by the user using the library of Deterministic Finite Automata (DFA) regular expressions.

The defined signatures built into Proventia Content Analyzer can identify the following types of information:

1. *Credit card numbers*
2. *Name*
3. *Date*
4. *U.S. Dollar amounts*
5. *E-mail address*
6. *Social Security number*
7. *U.S. telephone numbers*
8. *U.S. postal addresses*
9. -- 16. *Custom signatures defined by the user*

Proventia Content Analyzer focuses on content detection and does not recognize context. Network IPS will act on any potentially confidential information that matches defined and custom signatures rather than overburdening the network IPS with additional policy-based rule verification that can add increased network latency. Context-based detection and validation should be addressed separately as part of a holistic data security framework.

With the ability to create compound data-set inspection criteria (e.g., User Name **AND** SSN), and the extensibility to create custom inspection signatures, Proventia Content Analyzer gives users a truly flexible and broad search criteria catalog in order to inspect network traffic for confidential information.

Leveraging market-leading technology

Proventia Content Analyzer leverages the robust capabilities of the protocol analysis module (PAM) to identify sensitive data in various protocol and content delivery types. PAM is the intrusion prevention technology behind many IBM Proventia products, including the IBM Proventia Network Intrusion Prevention System and IBM Proventia Network Multi-function Security.

PAM performs deep packet inspection of network traffic across 177 network and application layer protocols and file formats to stop a number of today's worst threats including:

- *Worms*
- *Spyware*
- *P2P*
- *DoS/DDoS*
- *Cross-site scripting*
- *SQL Injection*
- *Buffer Overflow*
- *Web Directory Traversal*

Protocol Analysis Module (PAM)	
Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

Incorporating more than 20 different inspection technologies, PAM works in conjunction with Proventia Content Analyzer to inspect unencrypted data across multiple content types and file formats (including zip and gzip).

Updates to PAM and Proventia Content Analyzer are made through content updates automatically, ensuring that the most current research intelligence from the IBM Internet Security Systems™ X-Force® Research and Development team is available at all times.

Proventia Content Analyzer inspection at a glance

Proventia Content Analyzer can inspect and identify data in a number of Application Layer Protocols:

- *AIM™ (OSCAR, TOC/TOC2)*
- *Microsoft® Messenger (MSNP9, MSNCL, MSNP10)*
- *Yahoo!® Messenger (YSMG)*
- *IRC*
- *HTTP*
- *FTP*
- *SMB*
- *SMTP*
- *IMAP*
- *POP3*

Along with deep packet inspection of the data transmitted via these protocols, Proventia Content Analyzer can also inspect attachments for any data content that violates one of the content enforcement signatures. The content types and markup languages that Proventia Content Analyzer can inspect include:

- *Microsoft Office documents*
- *Adobe PDF*
- *Rich text format (RTF)*
- *Text*
- *XML*
- *HTML*
- *GZIP (compressed)*
- *ZIP (compressed)*

Two modes of operation for use depending on the level of intervention desired

To help prevent the loss of sensitive data, Proventia Content Analyzer can operate in inline or passive mode, while inspecting traffic in both directions.

In passive mode, Proventia Content Analyzer can generate an alert in the management console, send a TCP Reset to the remote user's system*, or both.

In inline mode, recommended on segments where confidential information should be encrypted at all times, Proventia Content Analyzer can block the transmission of data.

As with any inspection technology, the performance impact depends highly upon the level of inspection required, as well as the number of inspection parameters in use. With all Proventia Content Analyzer signatures and protocols turned on, network performance may be impacted as specific needs are defined and baselines measured. The performance impact should improve dramatically as the use of defined and custom signatures is tuned and as the number of protocols inspected is adjusted to fit the organization's particular needs.

Compound search string capability

Differing types of sensitive information require a solution that is flexible and customizable. For example, telephone numbers in the U.S. differ in structure or character length from those in other countries. In these instances, users can copy the syntax and structure from one of the defined signatures, modify it as necessary and save it as a custom signature.

Further strengthening the protection afforded by Proventia Content Analyzer, is the ability to create multiple search strings using both the preconfigured signatures and any customized signatures defined by the user.

For example, administrators can create search criteria to look for content in any number of circumstances and to respond differently depending on the content detected.

For instance, the search string, **“name”+“credit_card_number”** will detect an individual's name and credit card number.

With this search string, when a person's name and a character string matching a defined credit card structure are detected, Proventia Content Analyzer can be configured to simply generate an alert. To take this search a step further, a separate search string can be created using a customized signature—in this case looking for a credit card's three-digit verification number, or, “CV_number” in addition to the “name” and “credit card number” values: **“name”+“credit_card_number”+“CV_number.”**

When these three criteria are detected in the data, Proventia Content Analyzer can generate an alert, block the traffic from continuing, or both.

This search string gives administrators a host of search criteria and detection possibilities to match a variety of situations or geographically-specific needs to support audit requirements.

Proventia Content Analyzer Key Benefits

Proventia Content Analyzer offers several benefits to customers seeking to gain control of data in their network environment.

Provides visibility into internal risk areas

Confidential data disclosure is the cornerstone of nearly every major IT security regulation. Proventia Content Analyzer can help identify confidential information moving in and out of a network. As a result, administrators may be more aware to potential areas of security risk in the organization.

Provides flexibility and scalability to inspect for confidential information

Content awareness efforts need not just concern personal information. Proventia Content Analyzer can help organizations track nearly any type of confidential information such as project names, organizational

financial dealings and more. This extends Proventia Content Analyzer's functionality to help administrators understand what confidential data is allowed to traverse their network. Complimentary to Proventia Content Analyzer are the data leakage prevention (DLP) solutions offered by IBM Data Security Services. Data leakage prevention solutions are designed to help control and prevent data leakage in critical areas identified by Proventia Content Analyzer.

Utilizes existing PAM technology

Many IBM Internet Security Systems products already include the PAM module's advanced detection capabilities. Proventia Content Analyzer leverages PAM's capabilities to extrapolate data from the data stream, bringing a new level of functionality to existing hardware and software.

Leverages market leading IPS technology

Proventia Content Analyzer installs on existing Proventia product family appliances as part of an IBM X-Press Update product enhancement and remains shut off until activated by the network administrator. Upon activation, Proventia Content Analyzer increases the value of your IBM ISS IPS solution and extends its usefulness as part of an overall threat detection and mitigation solution.

For more information about IBM Proventia Content Analyzer, contact your IBM representative, IBM Business Partner or visit:www.iss.net

Footnote:

**Not all protocols support TCP reset*



© Copyright IBM Corporation 2008.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

02-08

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia, SiteProtector, and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc., in the United States, other countries, or both. Internet Security Systems, Inc., is a wholly-owned subsidiary of International Business Machines Corporation.

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.