Proofpoint Digital Asset Security Module

As email has become the most important communications channel in today's enterprise, email systems have become the main repository for sensitive, confidential, and mission-critical information. And enterprises are becoming increasingly concerned about this information leaving the company via email. A recent survey by Proofpoint and Forrester Consulting[1] found that more than 70 percent of large companies polled were concerned or very concerned about leaks of valuable intellectual property and trade secrets via email. More than 76 percent were worried about protecting the confidentiality of personal identity and financial information.

overview

Proofpoint Digital Asset Security™ makes it easy to protect your organization's confidential, proprietary, and sensitive information from accidental or malicious leaks.

Protect valuable intellectual property and confidential information

The Proofpoint Digital Asset Security module, an optional component of the Proofpoint Messaging Security Gateway™ and the Proofpoint Protection Server®, keeps valuable corporate assets and confidential information from leaking outside your organization via email. Powerful MLX machine learning technology analyzes and classifies your confidential documents and then continuously monitors for that information in the outbound message stream. Proofpoint Digital Asset Security goes beyond simple monitoring for classified content—content security breaches can be stopped before they happen.

features

Easy training and secure document repository

The Digital Asset Security module employs patent-pending Proofpoint MLX™ machine learning technology to analyze the documents you want to keep confidential. Putting documents into the system "trains" the Digital Asset Security module to recognize that document and portions of its contents.

Documents can be loaded for analysis through Proofpoint's graphical user interface, through file systems or document repositories (via Proofpoint Enterprise Data Connectors) or by emailing them as attachments to a special mailbox. MLX technology then analyzes the information and stores it in a secure form in Proofpoint's document repository. Negative cases can also be loaded to train the system to ignore common, non-confidential content such as company boilerplate information.

Access controls let you grant certain business users access to the training module and control which users can add documents to the system for training.

Multiple category document protection

A graphical user interface lets you define categories for different types of documents to secure, each with different access controls and properties. For example, you can create separate categories for internal memos, draft press releases, organizational charts, price lists, and so on. Each category can have its own properties, such as default time, after which documents expire, and document similarity matching thresholds.

Flexible policy definition and management

A graphical user interface lets you quickly define policies for handling confidential information that is detected in outgoing messages. Any number of policies can be created to handle specific cases, with a great degree of control. Each policy can trigger based on specific document type and a customizable document similarity score. Route-based definitions allow you to create different policies for protecting digital assets depending on whether they are found in the inbound or outbound messaging stream.

Enterprise Content Security

Beyond the inbound messaging threats of spam, viruses, and phishing attacks, corporations, universities, and government organizations are looking for messaging security solutions that help them enforce outbound email policies, protect the privacy of customer and employee information, defend against leaks of confidential information, and help them comply with email-related regulations. Proofpoint provides a complete suite of easy-to-configure modules that solve these problems.

Proofpoint's Content Compliance™, Digital Asset Security™, and Regulatory Compliance™ modules for the Proofpoint Messaging Security Gateway and Proofpoint Protection Server represent a complete content security solution for today's enterprise.

Content security modules

○ Proofpoint Content Compliance allows enterprises to define and enforce acceptable-use policies (based on keywords, regular expressions and dictionaries) for message content and attachments.

○ Proofpoint Digital Asset Security keeps valuable assets and confidential information from leaking outside your organization via email and other network protocols.

○ Proofpoint Regulatory Compliance protects your organization from liabilities associated with privacy regulations such as HIPAA and GLBA.

[1] *Outbound Email Security and Content Compliance in Today's Enterprise*, June 2007.

Proofpoint Digital Asset Security Module

features

Flexible policy definition and management (continued)

Messages that are deemed to contain confidential information can be handled using any of Proofpoint's standard message dispositions, including quarantine, reject, annotate, redirect, reply to sender, discard, and many others. For example, an outbound message containing portions of a confidential memo can be quarantined and flagged for review by the appropriate manager.

Enhanced digital asset quarantine

A dual-pane quarantine view allows administrators with the proper permissions to view quarantined suspect messages side-by-side with the original training document. Portions of the message that caused the message to be quarantined are highlighted along with the matching regions in the "original" document—making it clear which portions Proofpoint identified as a breach. Workflow features such as automatic incident status tracking enable administrators to comment on, track and search violations in quarantine and export matching messages.

Reports

The Digital Asset Security module has built-in graphical reporting capabilities, including the ability to display trendlines showing which policies have triggered over a certain period of time—making it easy to see which types of assets are most at risk.

Supported document types

Proofpoint Digital Asset Security can be used to secure more than 300 unique document types, including:

- Plain text and email, such as the contents of a confidential email memo
- Microsoft Word and other word processing formats
- Microsoft Excel and other spreadsheet formats
- Microsoft PowerPoint and other presentation formats
- Adobe PDF documents
- CAD drawings including DWG, DWF, DXF and other formats
- Documents included in archives, including ZIP, GZIP, TAR, and TNEF (Windows email archive) formats

Support for custom and proprietary document types

In addition to the hundreds of built-in document types that Proofpoint's outbound email security modules natively understand, administrators can use Proofpoint's File Type Profiler to easily extend support to new, custom or proprietary file types (e.g., proprietary CAD/CAM formats).

Outstanding extensibility

Proofpoint Enterprise Data Connector™ technology allows the Proofpoint Digital Asset Security module to easily integrate with filesystems, databases, content management (including EMC Documentum systems), version control systems and other external applications to enable automatic indexing of new or modified confidential information. Access control and policy information can be automatically imported by the system, greatly reducing initial setup time and ongoing maintenance.

Protection beyond email

By adding the Proofpoint Network Content Sentry™ appliance, Proofpoint Digital Asset Security can also defend against intellectual property leakage via HTTP and FTP protocols, ensuring that confidential materials are not posted to blogs and other message boards, web-based email systems or FTP sites.

Proofpoint MLX Technology

Secures your digital assets

The Proofpoint Digital Asset Security module uses patent-pending Proofpoint MLX machine learning technology to analyze confidential documents and keep them from leaving your organization via email. Digital Asset Security leverages some of the same advanced statistical techniques used in Proofpoint's industry-leading anti-spam engine—widely acknowledged as one of the most accurate systems available.

In the same way that Proofpoint scientists and engineers train Proofpoint's MLX Anti-spam Engine by presenting it with examples of spam and valid email, Proofpoint Digital Asset Security works by analyzing specific documents that you present to the system. Both "positive" cases (documents that you want to keep secure) and "negative" cases (documents that contain common, non confidential content such as company boilerplates) can be loaded into the system.

Proofpoint MLX technology creates a statistical representation of the trained documents and then compares all messages against these statistical representations, looking for matches. This technique allows the Proofpoint Protection Server or Proofpoint Messaging Security Gateway to scan with great speed and accuracy. Scanning for breaches of confidential information is efficiently performed in parallel with other forms of processing, such as virus scanning.

The resulting system is a content security solution that is highly accurate, high performance, easy to train, and easy to maintain. Proofpoint is the only vendor who has applied these advanced statistical techniques to both inbound spam detection and outbound content filtering. Scientists at the Proofpoint Attack Response Center continue to conduct primary research into new, advanced statistical techniques and to develop new defenses based on MLX. This ongoing research and development ensures that Proofpoint's solutions are always one step ahead of threats to the security of your messaging infrastructure.

©2008 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Enterprise Data Connector and Proofpoint MLX are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 09/08