TRIAGE TRAINING group

X-Tra Secure: HIPAA/ISO17799 Enforcer Internal Security Software

Perimeter Defense is not enough!

Internal Security: Why is it important?

Internal Security Programs reflect a growing corporate awareness of the need for management tools that determine and enforce how users are allowed to handle corporate information and data. According to IDC's report on *Policy-Based Information Protection and Data Integrity,*

Dependency on the knowledge, behavior, good-will and discipline of PC-users to safeguard information assets is the weakest spot in each Security method today.

> *When we consider the complexity of objects moved across the Internet, the need to protect intellectual property, the legal necessity of avoiding workplace harassment, and the desire to improve productivity, we realize that content security is an essential component for organizations using the Internet, email and the Web.*

Specifically, companies need tools that actively monitor, log, analyze and enforce security policy in business information systems such as intranets. Activities that attempt to violate those rules (such as unauthorized copying or printing of confidential files, or transmission of unencrypted files) are prevented. Armed with such tools, companies do not have to rely on voluntary employee compliance with information security policy.

In many typical organizations, gateway solutions search e-mail and Web-based content for excessive file size, known viruses, prohibited content, profanities, corrupted data, pornography, and racist or hate material. Thus content security tends to be confined to:

1. the ability to recognize and manage complex objects (e.g. attachments, exe files, malicious code, pornography and spam) transferred over e-mail and the Internet,
2. the ability of an organization to apply flexible and adaptable security policies
3. the control of email and internet related traffic.

Such conventional approaches foster a feeling of security, but they are insufficient to accommodate the dynamic reality of today's business and computing environment. Internal security goes beyond stopping viruses and blocking web sites. Effective content security needs to include all information, file and applications within a standalone or distributed computing environment. And it must address the internal threats posed by authorized users to the integrity of business processes and data.

To do this, it must include the ability to selectively monitor, track, manage and control the use of corporate information and data by those who are authorized to access it.

ENTER HIPAA ENFORCER — Technology Roadmap

HIPAA Enforcer Technology can deploy, monitor, log and enforce pre-defined policy and rules with respect to any type of data. For example, it can identify critical words, sentences and strings (e.g. credit card numbers) before files are opened, saved, read, copied, deleted or sent. This capability can be coupled with **HIPAA Enforcer's** ability to attach security rules to the file content. As a result, certain rules can be invoked if the file content is determined to contain critical pieces of information.

HIPAA Enforcer Framework

HIPAA Enforcer framework occupies a unique, strategic position below the network operating system level. From this position, it is able to monitor and analyze all data before it reaches the operating system. For every operation, **HIPAA Enforcer** poses questions such as: Can this file be copied, moved, or deleted? Can the file be stored locally? Can it be opened by a particular application? Can the contents of a Website be stored locally? If a pre-determined policy rule attached to a file is violated, **HIPAA Enforcer** will immediately stop the request, before it reaches the operating system.

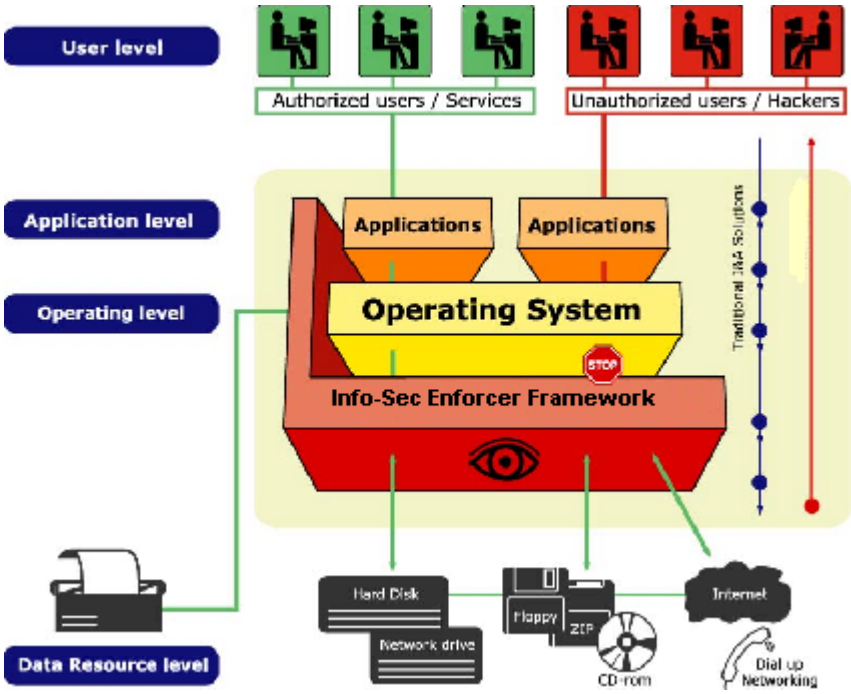

Figure 1: HIPAA Enforcer framework position

For the user, HIPAA Enforcer is invisible, automatic, reliable, always operating and up-to-date.

Based on the nature of content (checked at the internal file format/bit level), the application opening it and the location of the data, HIPAA Enforcerframework can execute one or more actions such as: encrypt, deny access, scan for viruses, move, copy, delete, sign, monitor, or notify.

Contrary to current network control and security systems, HIPAA Enforcer solution keeps efficiency and productivity high. From a central location, it deploys and installs an invisible "Stealth Agent" on each desktop. This agent does not require any training, support, or service to operate. HIPAA Enforcer guarantees active monitoring and enforcement of policies at each workstation. The policies, changes and notifications are always deployed centrally and collected by the HIPAA Manager. This functions

seamlessly in any client-server-based environment. The HIPAA Enforcer Administrator can assist in the creation of additional policy rules for central deployment by the HIPAA Network Manager.

Plugging into HIPAA Enforcer's Framework — Implementable Features

The HIPAA Enforcer Framework supports a host of specialized features and services. These are illustrated in Figure 2 and summarized by functional groups below.

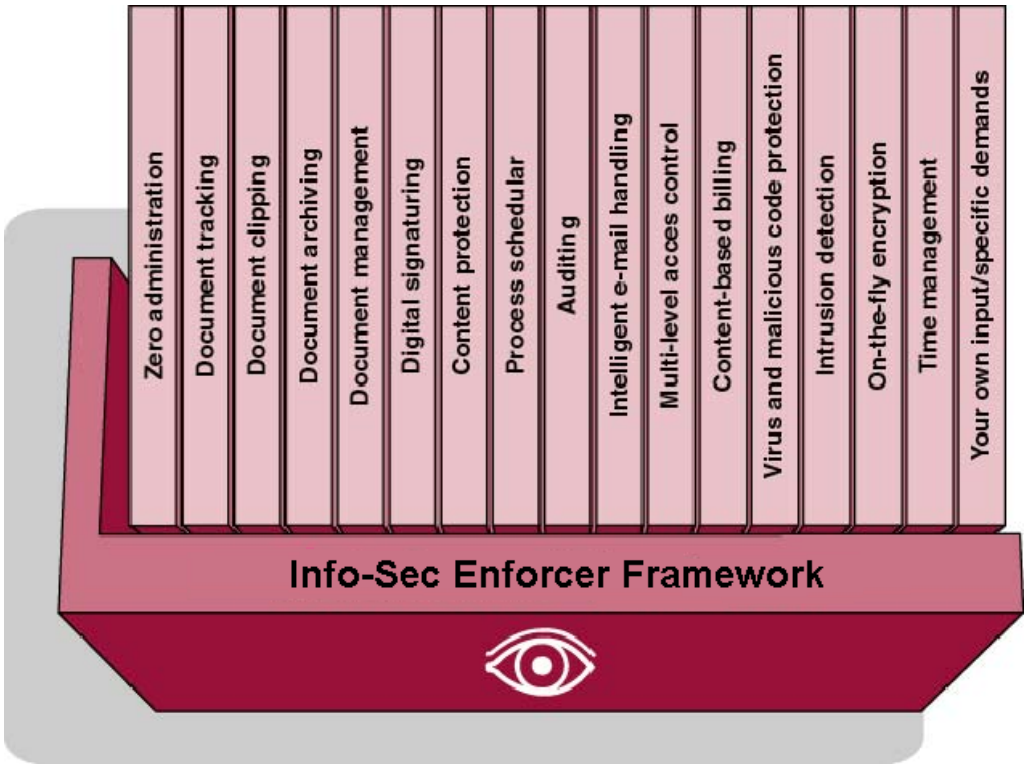

Figure 2: HIPAA Enforcer Features

Armed with HIPAA Enforcer tools, companies do not have to rely on voluntary employee compliance with information security policy

Document management

- Central archiving on the server
- On the fly encryption on any media
- Disabling copying to/from CD-ROM, diskette or other removable media
- Permission to access given only to trusted programs
- Isolation of documents in quarantine prior to processing

Access Control Management

- Prevention of unauthorized tampering or theft of information
- Access controls on all file characteristics (e.g. user, content, size, type, location)
- Execution only by trusted programs
- Monitoring of all company network access performed off-site

Encryption Management

- Enabling automatic file encryption
- Disallowing the use of unauthorized encryption
- Enabling automatic diskette encryption
- Fully centralized key management/password storage

Desktop Security Management

- Preventing unauthorized software installation
- Preventing modification to the control panel settings
- Preventing users from creating, renaming and deleting files
- Preventing deletion of desktop icons
- Preventing downloading and installation of offensive material/illegal software
- Management of oversized files
- Locking of Windows registry
- Denying access to selective programs even through icons and short-cuts regardless of the number of users
- Preventing users getting to DOS
- Preventing users from deleting, or adding printers
- Disabling function keys at boot up
- Setting unique policies for individual users and/or groups
- Allowing only authorized applications to run
- Preventing users from modifying hardware settings
- Denying access to the "Find" command

Content Monitoring and Filtering

- Enabling search on key words, numbers, strings or particular keypunches to safeguard confidentiality.
- Forcing automatic archiving based on key words (e.g. 'contract' or 'date')
- Forcing automatic encryption based on key words (e.g. credit card numbers)
- Controlling access based on file content.

Empowers security managers to build and manage an integrated security infrastructure reaching into all corners of their organization.

Anti Virus Management

HIPAA Enforcer has a twofold approach to virus protection:

1. By automatically activating a company's preferred virus scanner (as predefined in HIPAA Enforcer rules);
2. By blocking the actions executed by viruses through rules defined in HIPAA Enforcerconfiguration. The ability to block the execution of malicious software code is extremely valuable in protecting corporate information against unknown viruses.
    - Prevent execution of certain programs based on type, (such as VBS scripts, JavaScript and ActiveX)
    - Prevent installation of certain file types (e.g. .exe), thus avoiding a possible virus
    - Prevent virus-initiated actions, such as the renaming of files, or the deletion of system files.
    - Automatically invoking a virus scanner when writing data to a diskette or other media.

HIPAA Enforcer Options

Because of its innovative framework approach, HIPAA Enforcer can quickly adapt to incorporate new processes or unique corporate tools that can augment **HIPAA Enforcer** functionality:

- Integration of smart card / other tokens
- Integration with Firewall-1 compatible Firewalls (OPSEC-CVP)
- Integration with other applications by means of HIPAA Enforcer API

Configurable Features

- Blocks files by type, content, size, name, location and extension
- Monitors data on any drive known to the system (e.g. hard disk, diskette, CD-ROM, ZIP drive, network drive)
- Blocks or passes information based on policy definition
- Enables detailed audits of desktop activity
- Automatic report generation reports based on rule violations
- Notification messages in response to rule violations
- Controls for centralized deployment and management
- Offers stealth surveillance by means of Stealth Agents

HIPAA Enforcer Benefits

The HIPAA Enforcer approach to content security offers versatile deployment coupled with a wide range of benefits.

- Overheads are reduced since users are not allowed to delete system files and this minimizes support requests.
- Documents are tracked to create a log of which users transformed what data and when.
- Document clipping supports marking or tagging of data to enforce document management.
- Document archiving ensures that critical files stored locally will be automatically moved/copied to the central archive.
- Content protection through the use of watermarking or signing a template or document is used to support automatic encryption of documents containing information (such as credit card numbers) that are classified as confidential.
- Automated notification allows the system administrator to see which rules are most often being challenged and which users are the most frequent offenders. This can be used to define a need for additional training, either in rules that seem to be giving everyone difficulty, or for particular employees who may not understand aspects of security policy.
- Intelligent e-mail handling allows **HIPAA Enforcer** to accommodate different contexts. For example, **HIPAA Enforcer** will automatically disable a rule (such as no copying of files) to enable a back-up.
- Multi-level access control through which **HIPAA Enforcer** not only controls who accesses data or what they can do with it, but also the applications (or programs) that the user is allowed to employ in accessing it. This feature ensures that a document management system cannot be bypassed through the use of applications external to the system.

HIPAA Enforcer offers significant reductions in the TCO of corporate information systems, with central deployment security

- Intrusion detection is included: **HIPAA Enforcer** monitors all external attempts to access the company network.
- Individual content and specialized needs are provided for. **HIPAA Enforcer** can quickly adapt standardized solutions or develop new ones to address special or customized security needs.

Cost of Ownership: One of the most important benefits of **HIPAA Enforcer** is its impact on the total cost of ownership (TCO) associated with corporate information systems. Recent studies have shown TCO to be much more expensive than originally expected. Indeed, direct management and support costs much more than the annual amortized purchase cost for hardware and software. To reduce these high costs, IT departments must focus on reducing the labour burden associated with both management and support as well as indirect user costs. By using automated systems to enforce security, **HIPAA Enforcer** offers significant reductions in the TCO of corporate information systems.

For more information:

Becky Smith
210.680.8392
bsmith@triagetraining.com

http://www.TriageTraining.com