

# The Code Green Networks Content Security Solution Protecting Confidential Information in the Digital Age

---

Solution Overview White Paper



*Track. Analyze. Protect.*

# Table of Contents

---

Introduction . . . . .	1
Situation Overview . . . . .	1
The Insider Threat . . . . .	2
How to Respond to the Insider Threat . . . . .	3
CGN Content Security Solution Overview . . . . .	4
Content Inspection Appliance . . . . .	5
Network Management System Appliance . . . . .	9
Content Inspection Agents . . . . .	9
Use Case Scenarios . . . . .	10
Summary . . . . .	12

## INTRODUCTION

*"According to a survey conducted by the Chamber of Commerce, PricewaterhouseCoopers, and ASIS International, businesses lost between \$53 billion and \$59 billion between July 1, 2000 and June 30, 2001 due to the theft of their intellectual property."*

- Net Security, August 2005

*"Studies from the Computer Security Institute/FBI, U.S. Congress, Gartner, and others estimate that as much as 75 percent of the \$200 billion in measured annual security losses comes from within organizations."*

- InfoWorld, June 2005

Companies are challenged to protect their intellectual property and customer information from internal malicious use and accidental mishandling. Unauthorized disclosure of confidential information can result in loss of revenue, financial penalties and irreparable damage to a corporation's image, brand and customer loyalty. In addition, government regulations require corporations to strictly monitor their confidential information and report confidential data leaks. Since corporations are mandated to report confidential data leaks, one cannot read the global news without seeing another article outlining how a sensitive data leak caused substantial corporate financial losses and directly affected the general consumer. The content security issue today is more acute than ever because corporations and government agencies manage far more confidential digital content than they did two years ago. Globalization and increased Internet usage have enabled organizations to extend beyond their internal corporate network. Governments, corporations and consumers have a heightened awareness of the risks of unprotected confidential information, leading to a growing demand for a robust content security solution that goes beyond today's traditional authentication and intrusion prevention security solutions.

Code Green Networks Inc.<sup>TM</sup> (CGN) addresses this demand by providing enterprises real-time comprehensive content monitoring and protection from insider threats, resulting in global data policy compliance and peace of mind. This white paper discusses the essential elements of content security and introduces the CGN content security solution to track, analyze and protect confidential data.

## SITUATION OVERVIEW

For years, companies have focused on protecting their data against external security threats posed by the growing exposure to the Internet. They have spent millions of dollars deploying traditional intrusion detection and prevention security solutions such as firewalls, antivirus, anti-spam and anti-spyware. Most have done a good job building a wall to protect their perimeter. However, over the past several years corporations and government agencies are realizing these defenses cannot protect them from their greatest threat – their own trusted insider. "According to the San Diego based Privacy Rights Clearinghouse, there have been 45 data security breaches -- both internal and external -- made public since February 2004."<sup>1</sup> These data security breaches have negatively impacted the company involved, outraged consumers and raised awareness about the lack of corporate data security. Even though research shows that the vast majority of data leaks originate internally, whether as the result of insiders' accidental mishandling or malicious intent, corporations have neglected to implement adequate data security measures to protect themselves from the insider threat. Consumers and governments are concerned that corporations do not respect or quantify the value of sensitive information (for example personal health information and Social Security Numbers) they collect, store and distribute.

The issue of content security is now visible in the executive suite as a result of recent laws such as Sarbanes-Oxley Act of 2002 (SOX), Gramm-Leach-Bliley Act (GLBA), California SB 1386 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. These laws mandate public disclosure of unauthorized dissemination or loss of confidential information, and these losses may constitute material events affecting the company's reputation, risk profile and market capitalization. Corporations are demanding an automated content security solu-

<sup>1</sup> *Information theft fast becoming big business, Justin Rubner, American City Business Journals Inc., 2005*

tion that will help them mitigate these risks and comply with government regulations.

As companies assess their corporate data security, they usually discover the security problem and solution are quite complex. They can no longer rely solely on written data policies, identity management and other traditional network security solutions to ensure compliance with government regulations. Adding to the complexity of the insider threat is the ever-increasing use and availability of information communication channels including email and mobile and portable storage devices (USB flash drives and iPods). As the amount of dynamic data grows, corporations must enforce corporate data policies across the entire network - both at the network egress points and individual client PC. Content security is now, more than ever, a strategic business imperative. By implementing a solution that combines content security technology and a set of configurable and comprehensive data policies, corporations can prevent confidential data leaks, ensure government compliance and restore customer confidence.

## THE INSIDER THREAT

Data leaks can be accidental, as was the case when a Cisco employee emailed quarterly earnings to unauthorized employees prior to the scheduled financial press release<sup>2</sup>, or malicious, as in the case when a call center engineer attempted to sell customer information to willing buyers. When interviewed, the Cisco employee replied,

*"I don't know if you've ever pressed your email button wrong, it was an honest mistake".<sup>3</sup>*

Whether intentional or inadvertent, internal data leaks present the greatest risk of compromising or exposing confidential information. According to the Gartner Group, 70 percent of security incidents that occur are committed by the trusted insider who has access to confidential information. Insiders know where the confidential information is stored, have authorization to access the data, and have the means of distributing that data. Most companies have instituted data policies to educate employees on the appropriate use and communication of confidential information. However, data policies are not enough to prevent human error or malicious intent. To add to the threat, the trusted insider can assimilate and forward data outside the network using a variety of methods, such as file sharing, iPods, USB flash drives, CD burners, printers, email, web-blogs (blogs), webmail and instant messaging (IM) (Figure 1)<sup>4</sup>. Traditional network security measures such as firewalls, identity management, Virtual Private Networks (VPNs) and intrusion detection systems form an effective barrier against the vast majority of external threats, however they cannot stop data leaks by employees who have access to secure information and numerous ways to disclose that information.

2, 3 Partial Cisco financial results leak early, George A Chidi Jr., *The Edge*, February 2002

4 Information Security Breaches Survey 2004, PricewaterhouseCoopers, April 2004

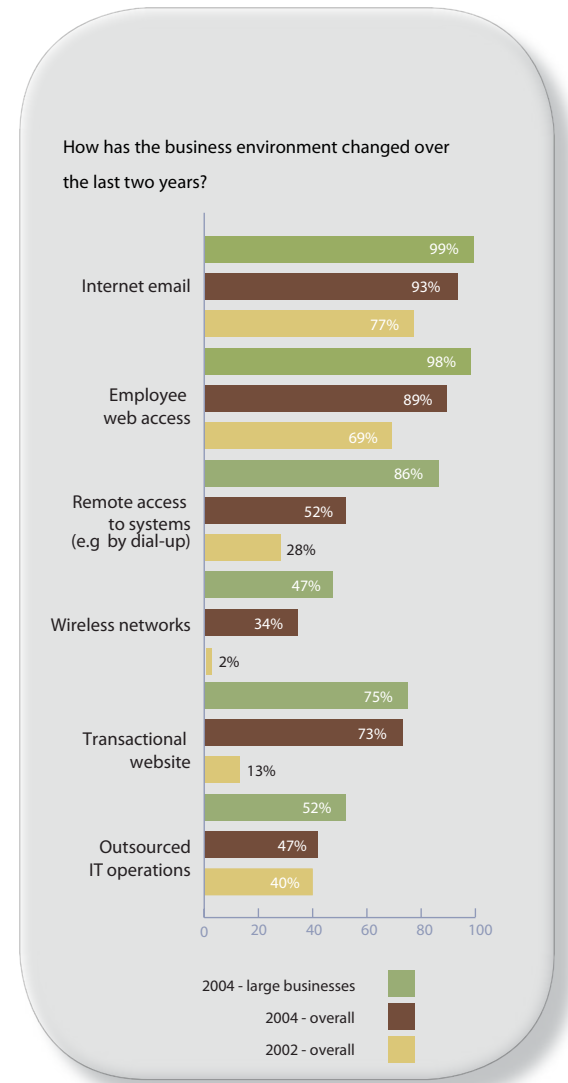


Figure 1: How the business environment has changed from 2002 to 2004.

## Examples of Content Security Threats

- Unauthorized hackers who illegally obtain access to an enterprise's, internal corporate data repository can transfer information out of the secure network, as was the case with a 2004 Cisco source code theft.<sup>5</sup> The hackers' actions posed a serious threat to Cisco's competitive edge when they posted critical Cisco Intellectual Property (IP) on a public website.
- An employee at a recruitment company plugged an iPod into the USB port of a computer and copied the company's client database onto the hard disk of the iPod, presumably with the intent of benefiting from this stolen information.<sup>6</sup>
- Confidential product details and pictures of a pre-release product were posted to a blog by an employee of the company.<sup>7</sup>

## HOW TO RESPOND TO THE INSIDER THREAT

While government regulations dictate strict reporting protocols when a security breach has occurred, the challenge is to prevent the trusted insider from sending confidential information outside the company in the first place. Security products are available that address particular components of content security, such as messaging security, email encryption and access management. However, none of these solutions provide a comprehensive content security solution across multiple file formats and protocols. In order to prevent confidential information from leaving the company, one must implement a robust content security solution that recognizes a wide variety of structured (data residing in structured databases) and unstructured data (for example source code, ZIP files and PDF files). In addition, the solution must be able to uniquely register confidential content, track and analyze that content, and prevent its unauthorized disclosure. In summary, the optimum enterprise content security solution must meet the following requirements:

- Register confidential structured and unstructured data by identifying and efficiently encoding data into a unique signature for accurate and high-performance detection.
- Support multiple protocols and file formats to ensure complete protection.
- Prevent data leaks at the client PC level and network egress points in real-time.
- Provide audit reports and forensic analysis capabilities for audit trail requirements and regulatory compliance.
- Ensure the solution has negligible impact to network performance through high throughput and high speed algorithms.
- Provide easy administration and complete integration with the corporate environment.

Monitoring and enforcing content security is essentially a two-step process. First, organizations must define their confidential content and data security policies to the content security system. Then, the system must monitor and analyze all network and client PC level traffic (any file format or protocol) and detect an attempted disclosure of confidential content. Once the attempted disclosure is detected, the security solution applies the appropriate data security policy.

The effectiveness of any content security system is determined by its ability to successfully detect, monitor and prevent the attempted unauthorized disclosure of confidential information – regardless of the file format or method of disclosure (for example file transfer protocol (FTP), Instant Messaging (IM) or email). This requires a scalable and robust content security system to identify confidential information and to successfully detect unauthorized disclosure attempts. Content security effectiveness is also measured by speed – the system must perform transparently and at a high rate of throughput so the security solution does not negatively affect the efficiency and productivity of the organization.

The following sections describe the Code Green Networks Content Security Solution and how it provides maximum effectiveness for implementing content security for the enterprise.

<sup>5</sup> *British police arrest suspect in Cisco code theft, Marguerite Reardon, CNET News.com, September 2004*

<sup>6</sup> *Fraudsters use iPods to steal company information, Phillip Inman, The Guardian, June 2005*

<sup>7</sup> *Warning: Your clever little blog could get you fired, Stephanie Armour, USA Today, June 2005*

# CGN CONTENT SECURITY SOLUTION OVERVIEW

Through the use of proprietary technology and dedicated hardware, the CGN content security solution provides management with the visibility and control necessary to track, analyze and protect a company's confidential data in real-time, resulting in compliance with privacy legislation and peace of mind.

## Track and Analyze

It is difficult for companies to track confidential data. Most companies lack standard or adequate methods to classify data as confidential or non-confidential. As a result, non-confidential data is over-protected and confidential data is under-protected, resulting in confidential data leaks and multiple false alarms.

To prevent confidential data leaks and reduce false alarms, the confidential data (which can reside in a wide range of application data formats such as Microsoft Office documents, source code and PDF files) must first be identified, then either automatically or manually registered, and finally stored in a content database.

The CGN content security solution registers confidential content by efficiently encoding data into a unique signature – Content Fingerprinting. Content Fingerprinting creates a representative signature database of unique fingerprints. Since content fingerprints are a unique and accurate representation of the original confidential content, they can later be used to track and identify confidential content even if it has been cut and pasted into another document, compressed or modified. CGN Content Fingerprinting is an accurate and precise method for tracking and detecting confidential content. In addition to Content Fingerprinting, content can also be registered using content description rules expressed by regular expressions (regexs) or exact keyword pattern matches.

Once the confidential content is identified, fingerprinted and registered and a trusted insider attempts to disclose the confidential information, several fundamental steps occur: (1) the transmitted data is fingerprinted “on-the-fly”, (2) that fingerprint is compared to registered fingerprints in the Content Fingerprint database and (3) regex and exact keyword pattern comparisons are performed. By combining regex and exact pattern matches and accurate fingerprinting comparisons over a variety of TCP/IP based protocols from all sources, enterprises can accurately and effectively detect the disclosure of confidential information, while reducing the rate of false alarms.

## Protect

The main objective of the CGN content security solution is to prevent the disclosure of confidential information in real-time at the source of leakage while providing audit trail capabilities. Once the CGN content security solution detects the transmission of confidential data, at either the network egress point or client PC level, it can apply data polices and workflow procedures (such as quarantine, prevent and notify) to the data and prevent a damaging data leak. Many data polices and workflow procedures are pre-defined based on industry regulations and acceptable use rules. In addition, the CGN solution allows corporations to define custom data polices based on their particular business needs. Enterprises can have peace of mind knowing their data is secure as a result of applying data policies and workflow procedures and preventing data leaks before they occur.

## Performance

As with any technology solution implementation, the functional benefits must be weighed against the overall impact to a company's infrastructure and budget. Monitoring outbound enterprise network traffic requires real-time analysis of immense volumes of confidential data. The CGN solution has a negligible impact on network traffic flow, without compromising flexibility, scalability and performance, while providing a low total cost of ownership. The CGN solution is also extensible, so as additional information types and protocols emerge, the solution quickly adapts. As companies grow and develop, they may add additional network egress points, new campuses in remote locations, servers, laptops and desktops. The CGN content security solution has a central management system that can easily integrate these distributed network components. Since most government regulations, such as SOX, require audit capabilities, the CGN content security solution is available 24 hours a day, seven days a week.

Code Green Networks provides a powerful, comprehensive and flexible content security solution that consists of three components:

- Content Inspection (CI) Appliance™
- Network Management System (NMS) Appliance™
- CI Agent client software™

The CI Appliance is the heart of the solution. Used by itself, it can detect, monitor and prevent confidential content from leaving an organization's network at the network egress point. However, if only the CI Appliance is deployed, insiders can still download confidential information to their client PC and attached devices without being detected. The CI Agents, when deployed in combination with the CI Appliance, provide enforcement of content security at both the network and client PC level. The third component, the NMS Appliance, provides system management capabilities for the CI Agents as well as for CI Appliances on the network.

The following sections describe, in detail, the functionality, technology and capabilities of the three CGN components.

## CI APPLIANCE

The CGN CI Appliance is a content security appliance that monitors and analyzes content on the corporate network and enforces corporate data security policies. It resides at the network gateway between a company's secure network and the external network. The CI Appliance prevents confidential content from leaving a company's secure network by registering confidential content (content registration) and then comparing content traversing the network with registered content for possible matches (content inspection).

The CI Appliance is comprised of three main functional modules: Content Registration Engine, Content Inspection Engine and Policy Rules and Workflow Engine (Figure 2). Together, the modules comprise a powerful and robust content security appliance that tracks, analyzes and protects a company's confidential information.

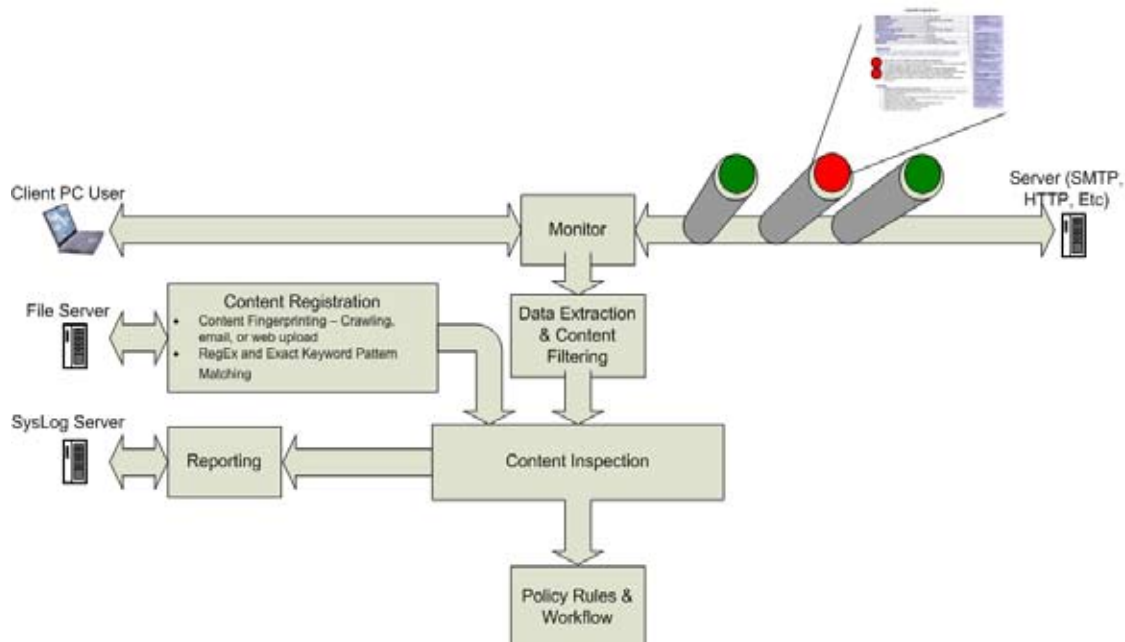
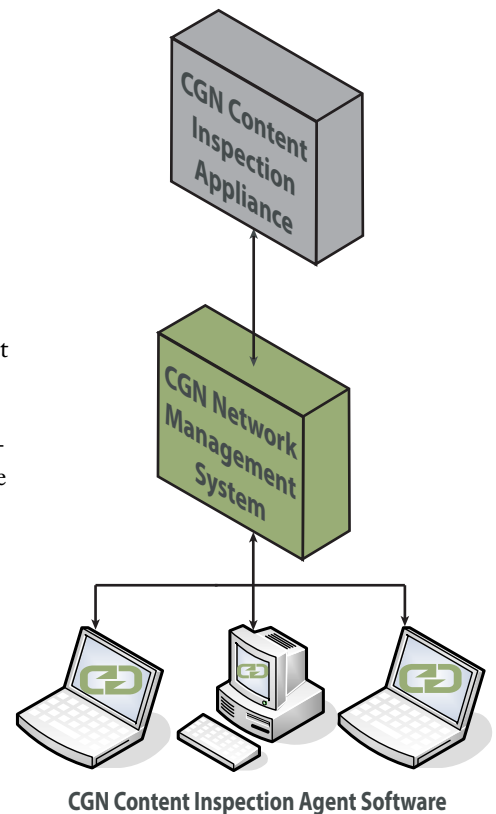


Figure 2: CI Appliance functional modules workflow.

## Content Registration Engine

The CGN Content Registration Engine registers content contained in corporate file system repositories. Content is registered with the CI Appliance in one of two ways:

- By Content Fingerprinting (via file crawling, email or web upload)
- By Regex and Keyword Pattern Matching

### Content Fingerprinting

Content Fingerprinting occurs either automatically, by “crawling” the data repositories, or manually, by email or web upload. Crawling is a key feature of the CI Appliance, providing an efficient and scalable solution to rapidly register confidential content contained in large UNIX and Windows file shares. The content crawling engine recursively traverses file system trees on a UNIX or Windows file share to identify and efficiently encode confidential content into a set of unique digital signatures using a unique patent-pending technique, termed Content Fingerprinting. It does this by opening and inspecting files stored in data repositories and then generating unique signatures, similar to an individual’s fingerprint. These fingerprints are stored in a fingerprint database and are later used to identify confidential content transmitted on the network, even if the content has been cut and pasted into another document, compressed or modified. The confidential fingerprints are stored in the fingerprint database and are termed “RedList” fingerprints (Figure 3). In contrast, the “GreenList” (Figure 3) contains fingerprints of non-confidential content to exclude from any content matching rules. GreenListing improves the efficiency of the CI Appliance by dramatically reducing the incidence of false positives. Authorized users (termed Content Authorities) can perform a RedList crawl to register confidential content, or GreenList crawl to register non-confidential content.

The screenshot shows two tables of content fingerprint data. The top table, titled 'Confidential Content (RedList) · 1 to 5 of 6', lists five entries with columns for Type, Description, Content Authority, Location, Date/Time, Edit, and Delete. The bottom table, titled 'Excluded Content (GreenList) · 3 items', lists three entries with the same columns. To the left of the tables is a sidebar with 'Content Registration' and buttons for 'Submit', 'Matching Rules', and 'Group'.

Confidential Content (RedList) · 1 to 5 of 6						
Type	Description	Content Authority	Location	Date/Time	Edit	Delete
Web Upload	Earnings Doc	admin	Clipboard	5/23/05 3:00pm		
File Crawl	Eng Server	admin	SMB://sbs.codegreennetworks.co...	5/23/05 4:45pm		
File Crawl	pubs confidential	admin	NFS://MSbs\Users\smcintyre\co...	6/29/05 13:42PM		
File Crawl	Pubs foo1	admin	NFS://Sbs\Users\smcintyre\conf...	6/29/05 13:57PM		
File Crawl	Private Server	admin	NFS://private/server	5/23/05 4:40pm		

Excluded Content (GreenList) · 3 items						
Type	Description	Content Authority	Location	Date/Time	Edit	Delete
E-Mail Upload	Footer message	admin	E-Mail Body	5/23/05 2:00pm		
Web Upload	template Doc	admin	File Attachment	5/23/05 3:00pm		
File Crawl	Public Server	admin	SMB://hr/forms	5/23/05 1:00pm		

Figure 3: Sample screen captures of RedList and GreenList content fingerprint data.

CGN Content Fingerprinting differs from other content detection methods in that it is extremely accurate and efficient at inspecting large volumes of data on the network, while ensuring confidential content transmitted on the network is detected. Since content fingerprints are a unique and accurate representation of the original content, they can later be used to identify confidential content even if it has been cut and pasted into another document, compressed or modified. For example, if an employee cut and pasted a section of C++ source code and attempted to email the code outside of the network, the CI Appliance would detect the derivative work.

The unique and efficient encoding scheme used in the CGN Content Fingerprinting can represent as much as 1 TB of source content in as little as 5 GB of content fingerprint signatures. This critical feature allows large volumes of confidential content fingerprints to be stored in a minimum amount of space.

In summary the key differentiating factors and benefits of the CGN Content Fingerprinting technology are:

- Accurate detection of derived content.
- Insensitivity to trivial changes to a content object, such as the amount of white space added or removed.
- Insensitivity to noise in a content object, such as “the” and “and”.
- Insensitivity to changes in positional occurrence of a piece of confidential content within a larger content object. For example, CGN Content Fingerprinting can detect an employee copying a section of a confidential document and pasting it into a non-confidential public document.
- Efficient fingerprint encoding of raw confidential content resulting in a small representative database of a large content set. Up to 1 TB of confidential source content can be represented in a 5 GB fingerprint database.
- Real-time content monitoring, inspection and enforcement at network wire speeds of hundreds of Mbps.
- Flexibility to choose the level of granularity for detection of derivative work.

In addition to crawling data repositories to register and fingerprint confidential content, Content Authorities can manually register content resulting in a RedList fingerprint repository of protected confidential content. Content, such as whole files or snippets of text, can also be uploaded to the CGN Content Registration Engine’s RedList or GreenList through a web form or email.

### ***Regex and Keyword Pattern Matching***

In addition to Content Fingerprinting, Content Authorities can use another method for registering confidential data. This method uses pre-defined or user-defined content description rules expressed by regexs or exact keyword pattern matches. Rules contain regular expressions such as Social Security, Credit Card or bank account routing numbers. By combining Content Fingerprinting, regexs and exact keyword pattern matching, Content Authorities have a comprehensive solution for registering and detecting confidential content on the network.

## **Content Inspection Engine**

The Content Inspection Engine is a core module of the CI Appliance. At the time of network transmission, it inspects the content of more than 370 different application file formats, fingerprints it “on-the-fly”, and then compares the fingerprints of the inspected content with those stored in the RedList or GreenList content fingerprint database. The content inspection engine also performs regex and exact keyword pattern matches based on pre-defined rules. Matching rules can be defined using references to fingerprinted content objects and also by using regexs and keywords for exact matches. The CI Appliance includes a set of pre-defined matching rules, and Content Authorities can modify these or create custom user-defined rules. If there is a RedListed fingerprint match or a regex/keyword match when content is transmitted on the network, then the appropriate defined data policy and workflow rules will be executed (for example quarantine, prevent or notify).

The CI Appliance can detect encrypted network traffic, such as SSL and IPSec. Since the CI Appliance is deployed behind the firewall, it can also inspect site to site VPN encrypted traffic. Content Authorities define data policies, which are executed by the CI Appliance, to handle encrypted content objects, such as documents, engineering drawings and source code files. Flexible policy rules enable a Content Authority to define workflow processing rules for encrypted content objects. In addition, the data policy rules can be defined to handle encrypted content based on users and network destinations. The CI Appliance also protects against unauthorized transmission of encrypted confidential content. An encrypted object is inspected without it being decrypted to determine if its content fingerprints match those in a RedList or GreenList of a previously fingerprinted encrypted object.

## **Policy Rules and Workflow Engine**

The Policy Rules and Workflow Engine enables Content Authorities to define rules for handling confidential content that matches regexs, exact keywords or registered content fingerprints. Workflow rules define how confidential content, which has been intercepted on the network or client PC level, is processed. Policy rules use transport protocols, users, time and actions as variables to form an enforceable data security policy. Content Authorities and administrators can customize data security policies so that acceptable use and confidential content protection policies can be enforced

and violations are appropriately logged and reported. By defining workflow procedures, organizations can apply different levels of policy enforcement - high, medium and low - to confidential content. Actions include work flow notification, copy retention and logging (Figure 4).

Description	Incidence Response				Edit	Delete
	Work Flow Notification	Copy Retention	Logging	Quarantine		
Low Risk	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Medium Risk	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
High Risk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Severe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

**apply**

**Actions** are used when building policies. This table lists the available actions.

Figure 4: Sample screen capture of data workflow procedures.

## CI Appliance Deployment Modes

The CI Appliance can be deployed in either a passive Tap/Mirror Mode (Figure 5) or an active In-line Mode (Figure 6). When deployed in In-line Mode, the CI Appliance audits network traffic and enforces policy rules in real-time to detect outbound network traffic that violates data security policies and optionally enforce data policy rules. The CI Appliance may also be configured for high-availability in a fail-over mode with another CI Appliance placed in standby mode. When deployed in a passive TAP/Mirror Mode, the CI Appliance can be used only for content inspection and monitoring.

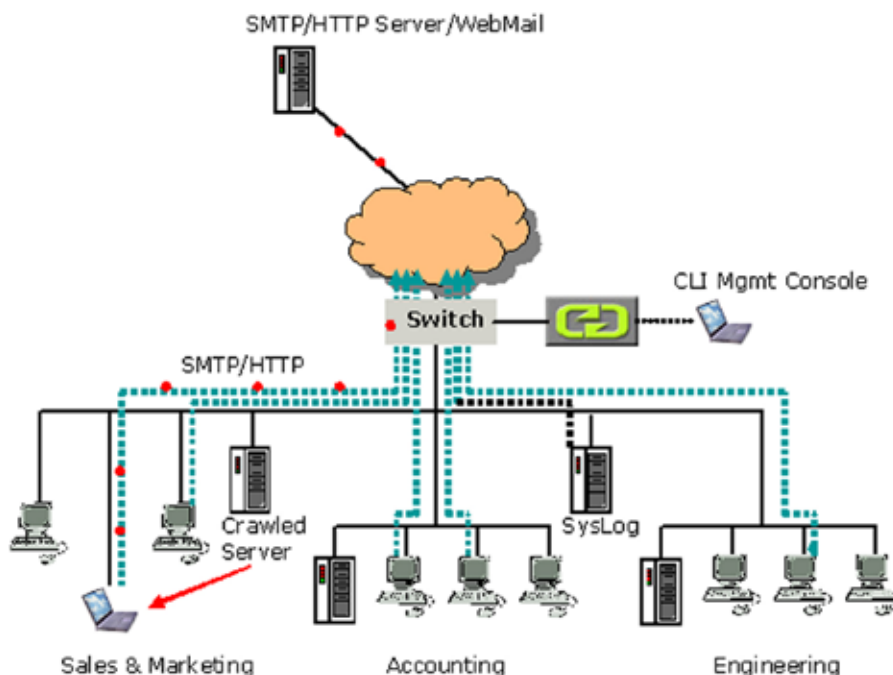


Figure 5: CI Appliance in TAP/Mirror Mode.

*"Apple iPods have become the tool of choice for some fraudsters who use them to download vast quantities of corporate information either to sell to rivals or to support their own start-up operations."*

*- Guardian Unlimited, June 2005*

*"A 2004 FBI/CSI joint study polled 494 companies. Of these, 269 respondents could quantify the losses (information) they suffered from incidents. The total loss among these companies for the categories of Insider Net abuse and Theft of proprietary information totaled over \$22 million dollars. This resulted in an average loss per company due to insider attacks of \$82,000 per company in 2004 alone."*

*- Computer Security Institute Publications, 2004*

SMTP/HTTP Server/WebMail

SMTP/HTTP



Crawled Server



Sales & Marketing

Accounting

Engineering

## NMS APPLIANCE AND CI AGENTS

*Figure 6: CI Appliance in In-line Mode.*

### NMS Appliance

The NMS Appliance and CI Agents are part of the scalable distributed client network management architecture from Code Green Networks. The NMS Appliance is the central management framework for a distributed network of CI Agent clients running on desktop and laptop computers. The CI Agents are configured, updated and managed by the NMS Appliance. The NMS Appliance enables Content Authorities to define and distribute data security rules to the CI Agents. Policy rules apply to such areas as confidential information, acceptable use and regulatory compliance. Extensive logging and reporting capabilities for real-time monitoring, decision analysis and post-event forensics are built-in to the NMS Appliance. The NMS Appliance is configured with pre-defined consolidated activity reports and Content Authorities can create custom reports using a web-based interface.

The NMS Appliance also enables Content Authorities to create and manages offline policies for mobile computers on which CI Agent clients have been installed. Policy updates may be sent to the CI Agents from the NMS Appliance on a scheduled basis at predetermined dates and times.

### CI Agents

CI Agent client software is part of the NMS Appliance architecture. CI Agents are installed on multiple desktops and laptops to monitor and analyze confidential information and enforce data security policies at the client PC level. CI Agents compare client PC level inspected content against the same fingerprint database stored on the CI Appliance. The NMS Appliance provides secure communication between the CI Agents and the CI Appliance for the purpose of exchanging fingerprint information. The CI Agent configuration is resistant to tampering by users or applications, ensuring the integrity of the CGN security solution for PCs. Deployment of the CI Agent is centralized and requires no intervention at the client PC, facilitating ease of deployment.

Content security workflow rules are enforced at the client PC level whether the PC is online and connected to the secure corporate network or offline, as in the case of laptops and other mobile computing devices. The CI Agent monitors Input/Output (I/O) requests made on the client PC. When an application makes an I/O request to the operating system, a comparison is made against

that particular application content using a regex rule. If a match occurs, the appropriate security policy rule is applied and the appropriate workflow is executed. CI Agents support data security policies even when the machine is disconnected from the corporate network.

The CI Agent and the CI Appliance inspect content objects using the same methods and implement data security policies with the same constructs. CI Agents communicate with the NMS to obtain the relevant fingerprint information. By inspecting content at the client PC level, the CI Agent reduces the network load on the CI Appliance, thereby increasing the overall performance of the CGN content security solution.

The CI Agent monitors and prevents the following operations on client PCs:

- Copying confidential data to external devices connected to the client PC, such as USB flash drives, FireWire storage devices, CD/DVD writers and network shares.
- Copying and pasting confidential data to application clipboards.
- Printing confidential data

In addition to the encryption handling capabilities of the CI Appliance, the CI Agents enable Content Authorities to author data security policies and workflow processing rules to handle encrypted content at the client PC level (for example, log event or forward to designated users for approval). CI Agents prevent unauthorized encryption of registered confidential content at the client PC level and protect against unauthorized transmission of encrypted confidential content. An encrypted object can be inspected without it being decrypted to determine if its content fingerprints match those in a RedList or GreenList of a previously fingerprinted encrypted object.

## USE CASE SCENARIOS

This section illustrates how the Code Green Networks Content Security Solution can be configured and deployed to address typical content security threats.

### CORE INTELLECTUAL PROPERTY PROTECTION

**Threat:** Despite the best efforts of a company to prevent unauthorized intrusions, a hacker gains illegal access to the corporate network. The hacker finds a repository with proprietary source code, illegally gains access and emails code for a new product to an email address that the hacker controls. This is a common scenario that is likely to have happened to many companies, including the publicized example of the Cisco source code theft<sup>5</sup>. Regardless of how the hacker gained access to the Cisco repository, he still had to send the information outside of the corporate network through the network egress point. Since there were no content security solutions in place, the confidential information was permitted to leave the network and fall into the hackers' hands.

**Solution:** The Code Green Networks Content Management Solution provides a second layer of security defense against this type of threat (beyond identity management, access controls and intrusion detection already deployed). To prevent the threat, the Content Authority registers all source code repositories for RedList content fingerprinting. When the outside hacker attempts to email the source code outside the network, the CI Appliance detects the attempted transmission and applies the appropriate security policy (Figure 7). In this case, the policy alerts the Content Authority to the attempted transmission, logs the transmission details and blocks the transmission. The hacker does not receive the code and the transmission alert enables security personnel to quickly remove the hacker from the corporate network and begin forensic analysis.

### PREVENTING UNAUTHORIZED COPYING OF CONTENT

**Threat:** Trusted insiders have several methods at their disposal to disclose confidential information. They can download

Policy · 4 items								
Enable	Description	Content	Participants	Action	Transport	Schedule	Edit	Delete
<input checked="" type="checkbox"/>	Intellectual Property Protection Policy	Eng Server	Engineering	Critical	Protects All Channels	2005-07-06 15:39:55		
<input type="checkbox"/>	Notify when HR docs leave	HR Info	Any	Low Risk	Email	2005-06-06 15:48:48		
<input checked="" type="checkbox"/>	Block from emailing	Earnings Doc	Finance	Medium Risk	Any	2005-06-06 15:48:28		
<input checked="" type="checkbox"/>	Acceptable Use Policy	Earnings Doc	IM Users	Critical	Protect All Channels	2005-07-06 15:41:17		

**Policies** define the behavior of the Code Green Networks Appliance. This table lists the available policies.

Figure 7: Sample screen capture of data security policies.

confidential information to their personal PCs and download and/or print the confidential information, from home, to such devices as a USB Flash drive, personal printer or SmartPhone. For example, an engineer who is leaving a company to work for a competitor may copy source code for a new software program onto a USB storage medium and take it with him to use in his new job, compromising the company's competitive edge and accelerating the competition's time to market. USB and FireWire connections are widely utilized by personal consumer electronic devices (such as MP3 players, iPods and Smart Phones) to synchronize information with a personal computer. Most of these personal consumer electronic devices have storage capability in the form of miniaturized magnetic disks or solid state flash memory, typically storing many different application file formats. The internal risk cases cited on page three concerning an employee attempting to copy confidential information (such as a company's client database) to an iPod would have been prevented if the company had implemented the CGN Content Security Solution.

**Solution:** The CGN solution would place the confidential information on the RedList, and Content Authorities would have defined data policies and workflow rules for the content. When the trusted insider attempts to download the RedListed information to the USB flash drive, the CI Agent on the employee's computer communicates with the NMS and CI Appliances to obtain the RedListed fingerprints. The CI Agent then detects a match between the RedListed content and the content attempted to be downloaded, prevents the disclosure of the confidential information and logs the event activity.

## POSTING CONFIDENTIAL INFORMATION TO AN UNAUTHORIZED BLOG (WEB-LOG)

**Threat:** The use of blogs has increased over the past several years and is becoming part of popular culture. ABC News reports that blogs are created at the rate of almost one every second. Blogs are easy to implement, use and maintain, thus they are popular with the general public. Many users feel little inhibition about posting detailed information about their personal and work lives to a public blog. With the increased use of blogs comes the threat of trusted employees intentionally or unintentionally posting confidential corporate information on an external blog. Trusted insiders can post company confidential information to a public blog. A Google employee was recently dismissed for posting unauthorized corporate information to his personal blog<sup>7</sup>.

**Solution:** The Code Green Networks CI Appliance can automatically detect and (if desired) prevent the posting of confidential information to blogs. To prevent this threat, the Content Authority registers critical confidential information for RedList content fingerprinting. In addition, the Content Authority defines business rules and patterns for common types of sensitive information. When the trusted insider attempts to post the confidential information to a blog outside the corporate network (even if they just try to post a few sentences or key words cut from a larger document) the CI Appliance detects the attempted transmission and applies the appropriate security policy. In this case, the data security policy alerts the Content Authority to the attempted transmission, logs the activity and if desired, blocks the transmission. The audit trail enables corporate security and human resources personnel to understand who is blogging with unauthorized information and to properly enforce relevant corporate policies.

## SUMMARY

The Code Green Networks Content Security Solution is the only complete solution for tracking and analyzing all traffic leaving the corporate network and client PC machines. It protects confidential information by creating unique content fingerprints, of confidential information and using this information to prevent unauthorized transmission of confidential content. By monitoring operations on client PC machines, organizations are assured that confidential content cannot be copied to external storage devices or printed; preventing leaks at the source – the trusted insider’s computer.

The CGN patent-pending Content Fingerprinting technology accurately identifies registered confidential content. Uniquely tunable parameters reduce the incidence of false positives and false negatives, and storage-efficient encoding scheme allows 1 TB of raw confidential data results to be represented by a 5 GB fingerprint database. By applying workflow procedures, logging network and client activity, and preventing data leaks before they occur in real-time at the source, enterprises can have peace of mind knowing their data is secure and data forensic details are always available.

Through the use of proprietary technology and dedicated hardware, the CGN Security Solution provides management with the visibility and control necessary to track, analyze and protect a company’s confidential data.

For additional information,  
please contact Code Green Networks at:

3975 Freedom Circle, Suite 900  
Santa Clara, CA 95054  
408.213.2300  
408.213.2301 (fax)  
info@codegreennetworks.com  
www.codegreennetworks.com



www.altaware.com  
sales@altaware.com  
(866) 833-4070  
Your Code Green Networks Reseller

*The Code Green Networks name, logo and products are trademarks of Code Green Networks, Inc. All other company and product names, brands or service names are trademarks of their respective owners.*

*Notice: This document is for information purposes only and does not set forth any warranty, expressed or implied, concerning product, product feature or service offered or to be offered by Code Green Networks Inc. All information is subject to change.*