

# CONTENT INSPECTION APPLIANCE

## Complete Data Loss Prevention for Smaller Organizations & Branch Offices

## CI-750



- Affordable, Enterprise-Class Data Loss Prevention
- Designed for Quick Deployment & Ease of Use
- Protect Customer Data & Personal Information
- Safeguard Intellectual Property

### OVERVIEW

The Code Green CI-750 content inspection appliance brings enterprise-class data loss prevention to smaller organizations and branch offices or remote locations. The CI-750 is designed specifically to meet the challenges of protecting confidential customer information and safeguarding intellectual property for organizations or locations with less than 250 network users.

The CI-750 is a complete, easy-to-deploy and easy-to-manage appliance that enables smaller organizations and branch offices to effectively monitor, enforce and audit the loss of customer data and intellectual property across all popular Internet communications channels – including Email (SMTP), Web (HTTP), File Transfer Protocol (FTP), Secure Sockets Layer (SSL), and online tools such as WebMail, Blogs and Wikis.

The CI-750 has enterprise class throughput that adds no latency to TCP traffic while affording protection for up to 20 million elements of stored data in databases and structured files, and up to 250 GigaBytes (GB) of source data across more than 400 different file formats including Microsoft Office documents, CSV files, CAD drawings, image files, rich media and other industry-specific application formats.

The CI-750 is designed not only for speed and performance, but also for ease-of-use and affordability. Each CI-750 content inspection appliance includes everything you need to locate and register content, inspect TCP traffic and online communications, and manage policies and incidents for compliance. A typical installation takes less than a day..

### MODEL COMPARISON

Product	Organization	Deployment	Key Benefits	Demonstrate Compliance
CI-750	Up to 250 Network Users	<ul style="list-style-type: none"> <li>• Smaller Organizations</li> <li>• Branch Offices</li> </ul>	<ul style="list-style-type: none"> <li>• Protect Customer Data &amp; Personal Information</li> <li>• Safeguard Intellectual Property</li> <li>• Monitor, Enforce &amp; Audit All Popular Internet Communications Channels</li> </ul>	<ul style="list-style-type: none"> <li>• CA SB 1386 and Similar Data Privacy Laws in 35 Other States &amp; Around the World</li> <li>• Federal Trade Commission (FTC) Guidelines for Protecting Personal Information</li> <li>• Health Insurance Portability &amp; Accountability Act (HIPAA)</li> </ul>
CI-1500	Up to 5,000 Network Users	<ul style="list-style-type: none"> <li>• Medium-Sized Organizations</li> <li>• Organizations With High Data Loss Prevention Requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Automatically Encrypt Email Messages According to Policy</li> <li>• Quick Deployment &amp; Ease of Use</li> <li>• Predefined Policy Templates</li> </ul>	<ul style="list-style-type: none"> <li>• Gramm-Leach-Bliley Act (GLBA)</li> <li>• Sarbanes Oxley (SOX)</li> <li>• Federal Rules of Civil Procedure (FRCP) Requiring Auditing &amp; Discovery of Electronic Communications</li> </ul>

## FEATURES

### Protect Customer Data and Safeguard Intellectual Property

The CI-750 automates compliance with data privacy laws and recent FTC guidance for protecting personal information by registering high-risk data elements directly from databases or structured files, such as spreadsheets and CSV files.

If these elements, such as name, account number and social security number, are detected in an electronic communications, the messages or transactions can be blocked and key details such as source, destination and protocol recorded as part of the incident record.

Similar capabilities are provided to register confidential content or intellectual property that resides in more than 400 file types across the network and prevent transmission of a full document or any derivative content.

#### Data Element Fingerprinting™

Patent-pending technology registers up to 20 million data elements for protection from flat files or directly from Oracle RDBMS and Microsoft SQL Server databases.

#### Deep Content Fingerprinting™

Patent-pending technology registers up to 250 GB of confidential content for protection across more than 400 unique document types including Microsoft Office, software source code, engineering drawings, image files, rich media and industry-specific formats.

#### Automated Database and Repository Crawling

Efficiently registers content from file shares, Oracle RDBMS, Microsoft SQL Server and content management systems including Microsoft SharePoint, EMC Documentum and Oracle Stellent.

#### Smart Crawl

Powerful, user-defined pattern matching during crawling automates locating of sensitive data and intellectual property.

#### Language Independence

Ability to fingerprint, protect and accurately detect content written in any language and character set (including non-Roman character sets such as Japanese).

#### Derivative Work Detection

Fragments of registered content are accurately detected, as well as the complete content itself.

### Monitor, Enforce and Audit Internet Communications

To detect sensitive information or confidential content, the CI-750 monitors content across Internet communications channels, including SMTP, HTTP, HTTPS, FTP and consumer WebMail services, Blogs and Wikis. Communications can be monitored, inspected, blocked and copies retained for electronic discovery and auditing purposes.

By monitoring and retaining messages sent in and out of the organization through consumer WebMail accounts, the CI-750 closes a key "loophole" in corporate email archiving systems and facilitates electronic discovery and auditing in accordance with recent amendments to the Federal Rules of Civil Procedures (FRCP).

#### Content Inspection

Real-time inspection of content streams across SMTP, HTTP, HTTPS, FTP and other TCP communication protocols at the network gateway.

#### WebMail Inspection

Parses, decodes, inspects and optionally retains copies of all popular WebMail services including Gmail, AOL Mail, Hotmail, Windows Live Mail and Yahoo Mail.

#### Web Proxy Interface

Enables WebMail, HTTP, HTTPS and FTP blocking when used in conjunction with an ICAP proxy server.

#### SMTP and WebMail Email Blocking

Policy action prohibits messages from being sent. An incident is recorded and routed to appropriate content authority. Optionally, email can be retained and/or the sender notified of policy violation.

#### SMTP Email Quarantine

Policy action prohibits the message from being sent and places it in a quarantine queue. An incident is recorded and routed to the appropriate content authority. The content authority can resend the message or delete it as a means of closing the incident. Optionally, the email sender can be notified that their email violated policy.

#### Flexible Policy Constraints and Exceptions

Enables policies to be easily constrained by protocol, document type, source address, destination address, number of occurrences and other criteria. On-Board Mail Transfer Agent(MTA) – Included to support SMTP blocking, quarantine, encryption and re-routing capabilities.

### Encrypt Email Messages According to Policy

In recently published guidelines for protecting personal information, the Federal Trade Commission (FTC) calls for businesses to adopt data loss prevention technology and encrypt email messages that contain sensitive information.

The CI-750 provides integrated policy-based email encryption capabilities with data loss prevention. The CI-750 allows organizations to establish policies that detect the transmission of personal information and encrypt it before it leaves the network, automating compliance with FTC guidelines.

#### Integrated Email Encryption

Policy-based email encryption comes integrated with data loss prevention and policy management.

#### Identity-Based Encryption (IBE)

Code Green Networks has partnered with Voltage Security to leverage their Voltage Security Network (VSN). VSN uses identities as public keys, eliminating the complexity of certificates, Certificate Revocation Lists and other mechanisms. IBE is easy to manage, with no burden on the end user to decrypt the message once their identity is established.

#### Inspect Client-Encrypted Email

If users encrypt email using the Voltage client software, it is then decrypted, and if sensitive information detected, appropriate policy actions are taken and then re-encrypted for transmission.

#### SMTP Email Re-Route

Policy action prohibits the message from being sent directly and re-routes it to another Mail Transfer Agent (MTA) which can then process the message and send it. This enables organizations to easily utilize existing email encryption solutions such as PGP and Voltage.

### Demonstrate and Manage Compliance

Data privacy compliance is a continuous process of assessing risk, managing policies, detecting incidents, determining root causes, remediating violations and tracking trends over time. Code Green Networks provides robust incident management functions that allow content authorities and administrators to customize data security policies for demonstrating and managing compliance.

#### Productive Incident Management

Enables content authorities to analyze incidents and take corrective action. Comments can be recorded at each step and saved to provide a defensible audit trail. Incidents can be routed to managers for approval.

#### Workflow with Role-Based Queues

Automatically route incidents to content authorities designated to receive them. Enables incident processing to be easily aligned with organizational structure.

#### Status Tracking

Workflow processing can be tracked by incident status, approval status and transmission status.

#### Flexible Filtering and Reporting

Color-coded incidents can be sorted and filtered by assignee, status and severity. Enables content authorities to focus first on the most severe incidents.

#### SYSLOG

Generates SYSLOG messages to facilitate integration with integrated security event and threat management systems.

### Deploy Quickly with Predefined Policy Templates

The CI-750 is designed to be easily configured and deployed quickly – typically within hours. To make the initial setup process easy, a robust set of predefined policy templates are included that can be easily activated and customized to meet organizational requirements.

#### Predefined Policy Templates

Preloaded policy templates allow for quick setup and deployment - typically within hours.

#### Intelligent Pattern Matching

Powerful, user-defined pattern matching supplemented by predefined patterns for many common identity numbers.

#### European National ID Numbers

Intelligent detection of British, Danish, Finnish, German, Norwegian and Swedish identity numbers.

#### Web-Based Policy Definition

Flexible wizard interface enables data policies to be easily defined and modified using detection criteria, actions and constraints.

**SPECIFICATIONS**

Content Inspection Appliance		
	CI-750	CI-1500
Form Factor	1U Rack-Mountable Chassis	2U Rack-Mountable Chassis
Dimensions	30.4" D x 16.7" W x 1.67" H	29.31" D x 17.5" W x 3.4" H
CPU	Single Dual Core Intel Xeon Processor	Twin Dual Core Intel Xeon Processors
Memory	4GB RAM	8GB RAM
Storage	1 Terabyte	1.2 Terabytes
RAID	RAID 1 Configuration	RAID 5 Configuration
Drives	Two 500GB 7200 RPM SATA Drives	Four 300GB 10000 RPM SAS Drives
Ethernet	Five Gigabit Ethernet Ports	Five Gigabit Ethernet Ports

**STRUCTURED CONTENT**

	CI-750	CI-1500
Capacity	20 Million Data Elements	20 Million Data Elements
Sources	Database (MS SQL, Oracle RDMBC), Flat File (Spreadsheet, CSV)	

**UNSTRUCTURED CONTENT**

	CI-750	CI-1500
Capacity	250 Gigabytes	1 Terabyte
Sources	File Shares (CIFS, NFS), Web Upload, Enterprise Content Management Systems (SharePoint, Documentum, Oracle)	
Document Types	400+ Document Formats, Including MS Office, Software Source Code, CAD Drawings, Images, Rich Media, and Other Industry-Specific Formats	

**CONTENT INSPECTION**

TCP Protocols	SMTp, HTTP, HTTPS, SSL, FTP and Other TCP Protocols
Web-Based Tools	Consumer WebMail Services, Blogs and Wikis
WebMail Clients	Google Gmail, AOL Mail, MSN Hotmail, Microsoft Windows Live Mail, Yahoo! Mail
Web Proxy Interface	ICAP
MTA Throughput	500,000 Messages per Hour

**CODE GREEN NETWORKS**

Code Green Networks delivers data loss prevention solutions that protect private employee and customer information and safeguard intellectual property across all electronic communications channels. The company's easy-to-deploy, easy-to-manage content inspection appliances rapidly detect and prevent potential data leaks, helping organizations automate compliance and mitigate risks from internal breaches that can result in loss of revenue, financial penalties and irreparable damage to a corporation's image, brand and customer loyalty.

For more information about Code Green Networks, visit <http://www.codegreennetworks.com>