

# CI-750

## Content Inspection Appliance



### Why Code Green Networks CI-750

- Designed for smaller companies and branch offices
- Affordable, Easy to Use -- Data Loss Prevention
- Demonstrate regulatory compliance
- Safeguard Intellectual Property
- Secure communications with partners and customers
- Comply with regulations regarding PII and PHI data
- Enforces policy regarding handling of sensitive data

### Key Features

- **Monitors and inspects all TCP protocols**  
SMTP, HTTP/S, FTP/S, IM, P2P, and other TCP
- **Built-in mail transfer agent (MTA)**  
Quarantine, block, reroute, or encrypt
- **ICAP integration with Web proxy servers**  
Allows inspection and control over Web and FTP content, even over SSL-encrypted sessions
- **On-board email encryption**  
Integrates with Cisco, Zix, and Voltage encryption services
- **Centralized administration**  
CI Appliances and CI Agents

### TrueDLP Products from Code Green Networks

- CI-750 - Designed for smaller companies and branch offices
- CI-1500 - Designed for mid-size and enterprise organizations
- CI Agent - Designed for endpoint protection

### TrueDLP Solution

Code Green Networks TrueDLP is a complete data loss prevention (DLP) solution that allows companies to effectively discover, monitor, control, and secure sensitive data, on the network, as it is used on desktops or laptops, or residing on end user systems and network servers. The TrueDLP solution is comprised of Code Green Networks Content Inspection Appliance, Content Inspection Agent, and the Content Inspection Management platform.

### CI-750 Overview

The CI-750 Content Inspection Appliance, designed for smaller companies and branch offices, detects sensitive content, monitors its use on the network, and enforces policies to ensure protection. Policy based actions include: allow, block, encrypt, reroute, quarantine. The CI-750 monitors and controls all communications channels – including email (SMTP), Web (HTTP/HTTPS), File Transfer Protocol (FTP), Secure Sockets Layer (SSL), and Web 2.0 applications such as webmail, blogs, and wikis.

The CI-750 protects up to 20 million elements of stored data in databases and up to 400 gigabytes 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.

### Key Benefits

- Prevents data loss via the network regardless of protocol
- Webmail and FTP visibility and control, including SSL-enabled sessions
- Policy based monitoring and blocking of Web 2.0 applications, including wikis, blogs, and other applications
- Content based email monitoring and message encryption prevents the most common source of data loss
- Simple deployment, installation and management reduces administrative overhead

### Easy To Implement, Easy To Manage

The CI-750 appliance based solution simplifies deployment, providing the fastest time to protection of any DLP solution on the market. The easy to use web based management console reduces administration overhead.

### Enterprise Scalability

Suitable for small business or branch offices, the CI-750 may be deployed stand alone or centrally managed by a CI-1500 to support multiple site deployments.

## CI-750 Content Inspection Appliance Key Facts and Specifications

System Capacity	
Deployment Size	250 users
Structured Data Capacity	20 million data elements
Unstructured Data Capacity	400 gigabytes of source content

Content Registration Sources	
Databases	MS SQL, Oracle or file upload
Network File Systems	CIFS, SMB, NFS, or file upload
Content Management Systems	Microsoft SharePoint, EMC Documentum, Oracle CMS

Content Detection Methods	
Data Element Fingerprinting	Row and column database element matching
Deep Content Fingerprint	Exact and partial document matching
Pattern	100+ predefined patterns including Social Security numbers, credit cards, and driver's license numbers
Regular Expression	User defined regular expressions
Lexicons and Dictionaries	Predefined industry specific dictionaries
Automatic File Classification	Predefined file classifications including technology source code, resumes, earnings press releases, US Patent applications and US Tax Forms

Content Inspection Methods	
<b>Network Inspection</b>	<b>Monitors all TCP-based communication via network tap or SPAN port</b>
Protocols	All TCP protocols
Policy Actions	Log, notify
<b>Email Inspection</b>	<b>Monitors and controls standard email (SMTP) via onboard MTA</b>
Protocols	SMTP
Policy Actions	Log, notify, block, quarantine, reroute, encrypt
Performance	500,000 messages per hour
Email Encryption Integration	Cisco RES, Voltage IBE, ZixCorp
<b>Web and FTP Inspection</b>	<b>Monitors and controls web-based and FTP channels via ICAP interface to web proxy server</b>
Protocols	HTTP, HTTPS, FTP, FTPS
Policy Actions	Log, notify, block, retain
Web-based Communications	Consumer webmail services, blogs, wikis, Web 2.0
WebMail Services	Google Gmail, AOL Mail, MSN Hotmail, Microsoft Windows Live Mail, Yahoo! Mail

### About 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.



### Corporate Headquarters

**Code Green Networks, Inc.**  
385 Moffett Park Drive, Suite 105  
Sunnyvale, CA 94089

Phone: +1 (408) 716-4200  
Fax: +1 (408) 716-4201  
E-mail: [info@codegreennetworks.com](mailto:info@codegreennetworks.com)  
[www.codegreennetworks.com](http://www.codegreennetworks.com)