

CONTENT INSPECTION APPLIANCE



Protect Your Sensitive Information, Minimize Your Investment

Code Green Networks™ Content Inspection Appliance 1500 (CI-1500) protects your sensitive information, such as customer data and intellectual property, against unauthorized disclosure over the Internet. Using patent-pending technology and residing at a company's Internet gateway, it monitors and analyzes content on the corporate network and automatically enforces content protection policies. If it detects the unauthorized transmission of sensitive information, it invokes a management-defined policy which may consist of logging, alerting and/or blocking the transmission.

The CI-1500 enables you to easily automate compliance with data privacy laws and the content control provisions of Sarbanes-Oxley. Key benefits include:

- Educating trusted employees to prevent accidental disclosures
- Identifying and fixing poor business processes that expose sensitive data
- Preventing industrial espionage
- Preserving your firm's reputation by preventing costly compliance incidents

Complete Protection in a Cost Effective Appliance

The CI-1500 is designed to provide complete protection in a cost-effective, easy-to-use appliance. Installing in about an hour, you can quickly begin defining protection policies for your business or agency using a simple, web-based interface. Monitoring begins immediately and incidents are visually logged according to their severity – so you can instantly identify high risk transmissions and resolve them. The appliance includes all the capabilities you need to protect your sensitive information:

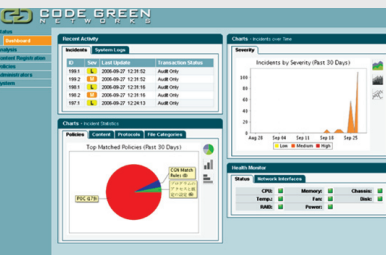
- **Comprehensive Data and Content Protection** – Protects structured data and unstructured content in over 390 different file formats including Microsoft Office documents, engineering drawings, image files, rich media and industry-specific application formats. Protects information from all storage locations and repositories including file systems, EMC Documentum repositories and Stellent repositories.
- **Flexible Policy Definition** – Ability to easily define policies that meet the organization's business needs. Pre-defined policy components and web-based wizards facilitate policy definition.

- **Multi-Protocol Inspection and Enforcement** – Inspects content flows and enforces policies in the most widely used TCP protocols including SMTP, FTP, HTTP and webmail. Enforcement options include blocking and quarantining of email.

- **Powerful Incident Management and Workflow** - Enables the content authority to analyze an incident, take corrective action and close it. Comments can be recorded at each step and are saved to provide a defensible audit trail. Incidents can be routed to managers for approval.

From the Founders of SonicWall

Code Green Networks was founded by Sreekanth Ravi and Sudhakar Ravi, who previously founded SonicWall, to develop easy-to-use, cost-effective solutions for identifying and protecting sensitive information in business and government.



Content Protection Dashboard

- Simple to use Web GUI
- Create and generate custom alerts and reports
- View graphical trends of incidents and responses
- Measure risk metrics
- Forensics and audit trail capabilities

Inspection and Enforcement Features

Inspection – High-speed, instant inspection of content streams in SMTP, FTP, HTTP and other TCP protocols at the network gateway.

Deep Content Fingerprinting™ – Patent-pending technology registers up to 1 TB of confidential content for protection and can fingerprint over 390 unique content formats including Microsoft Office documents, engineering drawings, image files, rich media and industry-specific application formats.

RedListing™ and **GreenListing™** – Highly accurate detection of confidential content transmission while reducing false positives.

Derivative Work Detection – Fragments of registered content are accurately detected, as well as the complete content itself.

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).

Intelligent Pattern Matching– Powerful, user-defined pattern matching supplemented by pre-defined patterns for many common identity numbers.

Automated Repository Crawling – Efficiently registers content from file shares or content management system repositories including EMC Documentum & Stellent.

Email Blocking – Policy action prohibits the message from ever being sent. An incident is recorded and routed to the appropriate content authority. Optionally, the email can be retained and/or the email sender can be notified that their email violated policy.

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.

Email Re-route – Policy action prohibits the message from being sent directly and re-routes it to another Mail Transfer Agent (MTA) server which can then process the message and send it. This enables business process automation of encryption, digital rights management (DRM) and other services. Optionally, the email sender can be notified.

European National ID Numbers – Intelligent detection of British, Danish, Finnish, German, Norwegian and Swedish national identity numbers.

Code Green Networks, Inc.

Code Green Networks offers next-generation content protection solutions that identify and protect all content — in all formats and languages — against unauthorized disclosure across all leakage points. The company's flagship product, Content Inspection (CI) Appliance, rapidly detects and prevents potential leaks of content, such as internal memos, customer lists, contracts, CAD drawings, financial documents, source code, product plans, and other confidential information. Code Green Networks' solutions enable enterprises to 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. The Code Green Networks solutions are sold and supported through a global network of business partners in North America, Asia and Europe.

Policy and Incident Management Features

Component-Based Policy Management – Provides wide flexibility and fine-grained control in defining content protection policies through reusable components.

Productive Incident Management– Enables a content authority to analyze an incident, take corrective action and close it. Comments can be recorded at each step and are saved to provide a defensible audit trail. Incidents can be routed to managers for approval.

Workflow with role-based queues - Automatically routes incidents to a content authority designated to receive them. Enables incident processing to be easily aligned with organizational structure (e.g. incidents involving financial information leakage can be routed to a content authority in the finance department).

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 most severe incidents.

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

Appliance Features

High Performance Appliance – Dual Intel Xeon CPUs, 1.2 TB local disk storage, 8 GB RAM, RAID-5 storage, 2U rackmount.

Field-Upgradeable – Ensures fast installation, low cost of ownership and easy upgrades to more advanced capabilities.

Mail Transfer Agent – Included to support SMTP blocking and quarantine capabilities.

Three Models and Price Points – To support organizations of varying sizes. (250 users, 1000 users and unlimited users)



www.altaware.com
sales@altaware.com
(866) 833-4070

Your Code Green Networks Reseller