

CONTENT INSPECTION AGENT



CI AGENT

Protect Your Sensitive Data and Confidential Content at the Endpoint

- Prevents transferring of files to unauthorized devices
- Automatically encrypts data copied to approved devices
- Provides complete visibility of device and file access

OVERVIEW

With the increased popularity of small data storage devices such as USB flash drives, CD/DVD ROMs, MP3 players and PDAs, it is extremely easy today for end users to accidentally or maliciously move confidential data out of the network without the organization's knowledge.

The Code Green Networks Content Inspection Agent (CI Agent) is installed at each endpoint and enables organizations to protect data and safeguard intellectual property at the endpoint – both on and off the network.

BENEFITS

Maintain Network Integrity

Whether it's an opportunist taking documents to a competitor or a well-meaning employee copying an infected file to the network, leaving portable device use unchecked is an invitation to disaster.

The CI Agent prevents the unwanted transfer of data to or from portable devices by automatically enforcing security policies based on a user's legitimate need to access specific device types. User access can be blocked, limited to read-only or left unrestricted according to the individual's security privileges and device type in use.

Secure Data in Transit

Nearly two-thirds of all USB drives are lost by their owners. Without the right protection, what's to stop that data from ending up in the wrong hands?

The CI Agent can automatically encrypt all data copied to authorized storage devices such as USB flash drives. Using the latest Blowfish and AES 256-bit ciphers, the CI Agent ensures that even if data is lost in transit, it won't result in a costly and embarrassing security breach.

Gain Total Visibility

You can't manage security if you can't see what's being connected to the network, what files are being accessed and how the security policy is being applied.

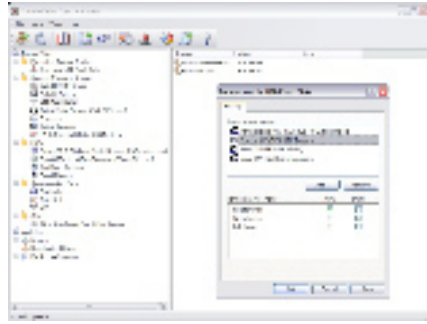
The CI Agent provides complete visibility of all user and administrator actions, recording everything from individual device connections to the most popular files read from or copied to portable devices. Content awareness ensures that you know the type of information being accessed or copied as well as the file name and type.

Regardless of whether the device is connected locally or wirelessly, if the PC is on the corporate network or offline, the CI Agent constantly manages device connections to ensure the integrity of your network is not compromised. Through its combination of strong security and flexible management capabilities, the CI Agent prevents both malicious and accidental security breaches, keeping data safe, both on and off the network.

FEATURES

Single-screen admin

All administration, including creating, modifying and deploying security policies can be done in the CI Agent's single-screen Policy Control Center. There is no need to repeatedly switch back and forth between multiple windows.



Content awareness

Scans content to determine true file type for use in both policies and reporting.

One-click deployment

Client agents can be deployed and updated across Active Directory and NT domains from within the CI Agent Control Center, without third-party software distribution tools.

Advanced device granularity

The CI Agent can manage both entire device classes as well as specific devices. Using the Policy Customizer, it is easy to create white lists of corporate approved devices.

User centric policies

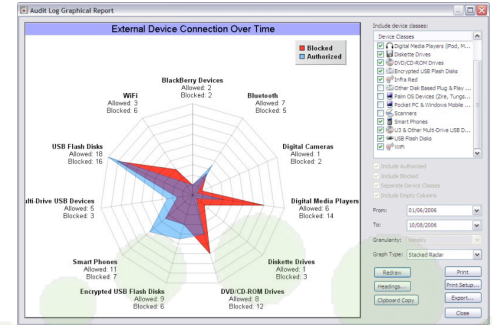
In addition to devices and device classes, policies can be specified and reporting/analysis conducted for specific users and groups of users.

Total visibility

The CI Agent automatically records device connections, file accesses and policy changes. These forensics can be viewed directly from the main Control Center in tabular or in graphical form, or can be exported into CSV format.

Intuitive processes & wizards

Wizards enable you to easily create and deploy security policies faster than ever. Intuitive processes make changing permissions or updating policies an easy task for any authorized user without the need for special training.



Super-strength encryption

256-bit AES and Blowfish ciphers are the strongest available, ensuring that any data carried offsite is protected against misuse by unauthorized third parties. Global or personal keys give maximum flexibility for security management.

User education

The CI Agent's configurable dialogs help organizations ensure that employees are informed about security policies, reducing help desk calls and improving user acceptance.

SYSTEM REQUIREMENTS

Supported Clients

Microsoft Windows 2000/2003/XP/Vista

Policy Control Center

Microsoft Windows 2000/2003/XP

Apache Web Server* or IIS

CI Agent requires a domain-based Windows network.

Database

CI Agent is shipped with a default installation of MDSE which is the recommended database. SQL is supported for customers who prefer this format.

**Shipped with product*

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>