

Solutions for Monitoring and Controlling WebMail Use

It's a fact of life that WebMail usage by employees continues to grow as both a security and data leakage issue for organizations. Simply blocking WebMail access while employees are on the network is not an option. So for complete information security, organizations must seek to apply the same policy enforcement strategies they have in place for corporate email and online communications to employee WebMail usage on the corporate network.

Recent amendments to the Federal Rules of Civil Procedure (FRCP) clearly point to the need for organizations to ready themselves for providing a wider range of electronic communications for auditing and discovery purposes – including messages sent via WebMail accounts by employees.

The Risk is Real

WebMail today can completely bypass an organization's corporate email servers and unmonitored WebMail traffic can add significant risk in several ways:

- WebMail (including attachments) may contain unauthorized nonpublic personal information (NPI) that violates laws and regulations, or sensitive intellectual property that should not be disclosed.
- WebMail is not inspected by SMTP-based email inspection software.
- WebMail is not archived by your corporate archiving solution, placing you at potential risk for auditing or electronic discovery in legal proceedings.

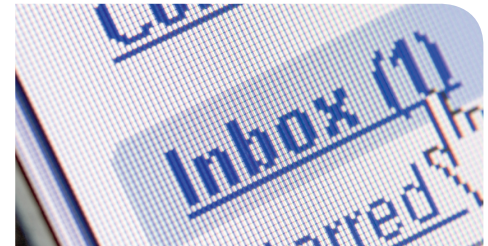
Best Practices for Identifying and Controlling WebMail Use

The Content Inspection Appliance from Code Green Networks enables you to easily define a single policy to prevent sensitive information from leaving your organization over all Internet messaging channels – WebMail, SMTP email, blogging and Instant Messaging. Working in conjunction with an ICAP proxy (such as Bluecoat), the Content Inspection Appliance can inspect encrypted SSL traffic and block HTTP, HTTPS and FTP traffic if it contains sensitive information.

Installed in a day or less, the Content Appliance enables you to quickly assess your WebMail risk profile, identify the issues and take corrective action. We recommend an initiative consisting of three phases:

Identify and analyze WebMail usage by monitoring all WebMail traffic for a fixed period of time – say, several days. This will enable you to understand:

- Who is using WebMail?
- How frequently are they using it?
- Who are they sending messages to?
- What content are they sending?



- **Monitor & Control WebMail Usage Across the Organization**
- **Retain Copies of WebMail Communications for Future Auditing & E-Discovery Purposes**
- **Audit & Enforce Corporate Data Policies**

Get Started

For more information on Code Green Networks solutions, visit our Web site at:

<http://www.codegreennetworks.com>

Assess your WebMail risk by implementing default policies to:

- Detect the transmission of NPI (account numbers, social security numbers, etc.) and sensitive intellectual property such as source code.
- Retain copies of all detected transmissions for analysis.
- Identify particular users who are violating corporate policies.

Educate and enforce for compliance by informing employees of corporate WebMail policies. Implement specific policies to detect, retain and block high-risk transmissions of private data and intellectual property.

Inspecting and Blocking WebMail Communications

The Content Inspection Appliance from Code Green Networks is installed at a company's Internet gateway so that it can inspect all outgoing content flows, including WebMail. When it detects a WebMail transmission with sensitive information, it can invoke management-defined policy actions, which can include blocking the transmission. The blocking is performed by a proxy server (such as the Bluecoat SG proxy server) using the Internet Content Adaptation Protocol (ICAP).

The Content Inspection Appliance monitors traffic by means of your organization's policies and compliance requirements which can define sensitive content such as nonpublic personal information (NPI) and specify an action (allow, allow and notify, block and notify, and other configurable options). Once defined (and Code Green has templates to speed this process along), an organization's policies are easy to set up via a web interface that employs comprehensive wizards.

A typical policy can monitor all WebMail transmissions for a fixed period of time (typically 3-5 days) to identify and understand who is using WebMail and for what purpose. You can also define additional policies to; for example, block all WebMail (and other HTTP and HTTPS) transmissions if the content contains nonpublic personal information.

Identify and Analyze WebMail Usage

Policies can also be created to identify and analyze WebMail usage. Source/destination and other information (including the email body) can be viewed for each transmission and a rich array of detailed reports can easily be generated to analyze the transmissions in various ways.

That means you can monitor all outbound HTTP and HTTPS traffic to mark incidents, with data analysis of those incidents from various angles including number of files inspected, file types sent, top sources, and top destinations. Code Green also allows you to see all of the details about individual WebMail transmissions for review, with a retained copy that can be opened to see the exact WebMail content.

Educate and Enforce for Compliance

Policies are easily configured to educate and enforce for compliance. This is especially important for financial services or healthcare organizations companies needing to comply with PCI, GLBA, SOX, HIPAA or Federal or state data privacy and notification laws such as CA 1386. The Content Inspection Appliance records when employees have sent, copied or downloaded confidential information to support auditing requirements.



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

Your Code Green Networks Reseller

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.

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



Corporate Headquarters

Code Green Networks, Inc.
3975 Freedom Circle, Suite 900
Santa Clara, CA 95054

Phone: +1 (408) 213-2300

Fax: +1 (408) 213-2301

E-mail: info@codegreennetworks.com