

48-hour Content Risk Assessment Overview

The Code Green Networks' 48-hour Content Risk Assessment provides powerful insight about your outbound traffic flows and network vulnerabilities. The assessment reveals the magnitude of risk from inappropriate disclosure that might put you into jeopardy with compliance regulations as well as damage your reputation and operations. It's a rapid way to discover potential insider threats, fix poor business processes and justify the implementation of an enterprise-wide content protection solution. If you aren't taking action, you may be unduly increasing your risk – reputation risk, compliance risk and operational risk. To mitigate these risks and guard against unauthorized disclosure of your sensitive information, we invite you to take Code Green Networks' 48-hour Content Risk Assessment. It requires minimal commitment of your staff and resources and can be performed without obligation on your part.

Code Green Networks' 48-hour Content Risk Assessment enables you to take the first step in protecting your sensitive information. As part of the assessment, Code Green Networks provides a Content Inspection Appliance and a default set of policies which monitor the outbound flow of content on your network. These policies, which can be installed and activated in less than one hour, are typically run, off a network tap, for 48 hours.

At the end of the Content Risk Assessment process, you will know the kinds of content flowing out of your organization, who is sending it and where it is being sent. Multiple protocols are monitored including SMTP, FTP, HTTP and web mail. Policies can also include registration of specific sensitive content to see if anyone is sending it outside of the organization. Reports have "drill-down" capability to enable you to more precisely analyze patterns and incidents.

With this information, you can identify content protection "hotspots" within your organization and start implementing more specific policies to protect your sensitive content and demonstrate your conformance with compliance initiatives such as SOX, GLBA, HIPAA, CA 1386 and others.

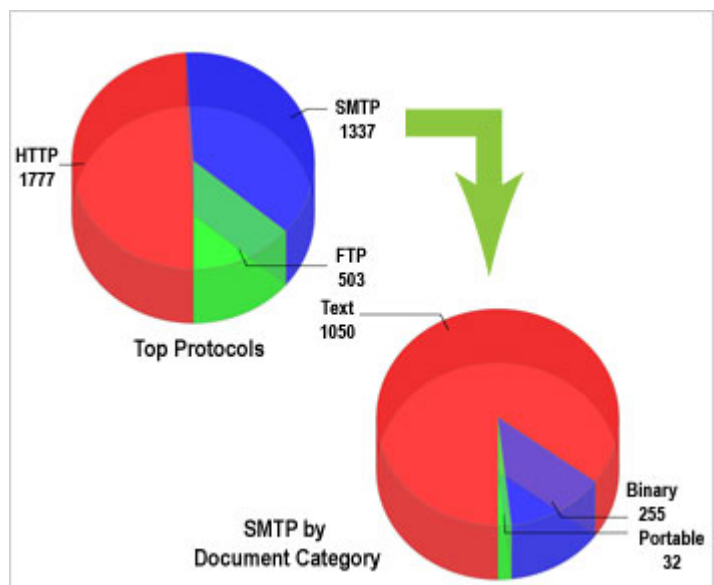
What you will learn:

- How much and what type of content is being sent to unauthorized external recipients?
- Who is transmitting the content outside the company?
- Who is receiving this unauthorized information?

Typical Reports

- Content transmitted by type of file
- Top protocols utilized
- Top destination and source users
- Top acceptable use language violators
- Top credit card and social security violations
- Top encrypted file users
- Top FTP source IP addresses

Sample Report with Drill-down Capability



Steps for Content Risk Assessment

The Content Risk Assessment is designed to help you evaluate and quantify your company's current level of content disclosure risk and accurately detect violation incidents originating from your network environment. The process consists of the following steps and can typically be completed in a 3-5 day period.



1. Install Appliance

Code Green Networks team will work with your team to install the Content Inspection Appliance™ off a tap from your network. This process typically takes one hour or less.

2. Load and Configure Policies

A set of policies is automatically loaded into the appliance. Some of these policies can be customized via the web-based graphical user interface. In addition, selected content from a file system or content management system can be fingerprinted and registered for subsequent detection.

3. Inspect Content Flow

During this step, the Content Inspection appliance is used to monitor the network traffic to evaluate and quantify your current

level of confidential content risk. The monitoring phase clearly identifies and quantifies the content flows by file type, sender, recipient, policy, and network protocol. Analysis of the results will provide best practice recommendations for policy creation and employee education.

4. Analyze and Report

The key decision makers, information security managers and content owners from your company will join representatives from Code Green Networks for a presentation and discussion of the results of the Content Risk Assessment. Recommendations can be made about how to protect sensitive content moving forward.

Get Started

To get started, contact Code Green Networks at:

Code Green Networks
 Email: info@codegreennetworks.com
 Phone: 408-213-2300
 3975 Freedom Circle, Suite 900
 Santa Clara, CA 95054



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

Your Code Green Networks Reseller

About Code Green Networks

Code Green Networks™ offers the only next-generation enterprise solution that identifies and protects 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, 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. For more information about Code Green Networks, visit <http://www.codegreennetworks.com>.