

# StegAlyzerRTS

## BENEFITS

- Prevent leakage of sensitive information and intellectual property outside the enterprise network through insider use of steganography
- Detect insider use of steganography to conceal evidence of criminal activity
- Real-time detection of files associated with over 800 steganography applications
- Real-time detection of signatures of over 50 steganography applications
- Real-time alerts to network security administrators
- Enforce organizational policy prohibiting insiders from having or using steganography or other data-hiding applications on the enterprise network



## Steganography Analyzer Real-Time Scanner

Sensitive data leakage is an issue of utmost concern to corporate management. Data Leak Prevention (DLP) solution providers offer products with a wide range of functionality and capability. However, none of these products detect insider use of steganography.

Steganography applications are widely available on the Internet—as freeware, shareware, or as commercially licensed software. The threat from insider use of steganography is significant because the applications are easy to find, download, install, and use—many with the familiar “drag-and-drop” or “wizard” functionality available in nearly all popular software applications.

StegAlyzerRTS is the world’s first commercially available network security appliance capable of detecting digital steganography applications and the use of those applications in real-time.

StegAlyzerRTS detects insiders downloading steganography applications by comparing the file fingerprints, or hash values, to a database of known file, or artifact, hash values associated with over 800 steganography applications.

StegAlyzerRTS also detects insiders using of steganography applications by scanning files entering and leaving the network for known signatures of over 50 steganography applications. Using an exclusive signature scanning approach developed in Backbone Security’s Steganography Analysis and Research Center (SARC), StegAlyzerRTS detects insider theft of sensitive information hidden inside other seemingly innocuous files which are then sent to an external recipient as an e-mail attachment or posted on a publicly accessible web site.

### Product highlights in StegAlyzerRTS:

- Detect fingerprints of over 800 steganography applications
- Detect signatures of over 50 steganography applications
- Send real-time alerts to network security administrators
- Retain copies of suspect files for further analysis
- Does not impact network performance

StegAlyzerRTS offers a “drop-in, turn-key” capability that will not affect network throughput.

***Deploy StegAlyzerRTS to prevent sensitive data leakage through insider use of steganography!***

**BACK  
BONE**  
SECURITY

### Backbone Security Steganography Analysis and Research Center

42 Mountain Park Drive  
Fairmont, WV 26554  
877-560-SARC or 304-333-SARC  
Fax 304-366-9163

RR 5, Box 5282  
Upper Cherry Valley Road  
Saylorsburg, PA 18353  
888-805-4331 or 570-234-0635

[www.sarc-wv.com](http://www.sarc-wv.com) • [www.backbonesecurity.com](http://www.backbonesecurity.com)

© 2004 - 2010 Backbone Security.Com, Inc. All rights reserved.  
StegAlyzer and Certified Steganography Examiner are registered trademarks of Backbone Security.Com, Inc.

