

Complete Data Loss Prevention with Blue Coat

Key Benefits

- Gain visibility and control over Webmail communication
- Provide automatic policy enforcement to prevent accidental data disclosure
- Prevent data loss via Web 2.0 applications including wikis, blogs, and other web postings
- Detect and eliminate backdoor information transfer over email and FTP
- Address regulatory compliance requirements for electronic communication (HIPAA, GLBA, SOX)
- Accelerate acceptable content and applications
- Manage Web applications and content
- Inspect SSL-encrypted sessions
- TrueDLP™ content inspection for highest accuracy
- Apply network based DLP across all network channels

Overview

Today enterprises must safeguard confidential customer data and intellectual property from unauthorized disclosure. Outbound Internet communication channels, if not properly controlled, represent a significant risk for sensitive information, either inadvertently or intentionally, leaking outside the corporate walls.

Code Green's TrueDLP™ is a centralized, comprehensive, and easy to deploy and manage data loss prevention solution. Code Green's Content Inspection Appliances combine sophisticated content inspection and detection capabilities with complete network inspection to ensure data leaks are accurately detected and prevented.

Blue Coat solutions provide a layered approach for inbound and outbound Internet gateway protection from spyware, malware, mobile malicious code, viruses, trojans, botnets, phishing and Web 2.0 threats. Blue Coat ProxySG appliances enable enterprises and organizations to manage Web applications and content, enforce acceptable usage policies and comply with laws and regulations.

Together, the Code Green Networks' TrueDLP™ solution and Blue Coat® Systems ProxySG® appliances provide organizations with a highly integrated solution to stop the loss or theft of confidential or proprietary information over Web and FTP channels, including data carried over SSL-encrypted sessions.

Common Data Loss Concerns

Many organizations monitor and control standard SMTP email traffic, watching for sensitive information contained in outbound messages with rudimentary pattern matching methods. Web and FTP access, however, is often provided to users in an unrestricted and unmonitored fashion.

Some of the common data loss concerns companies are experiencing:

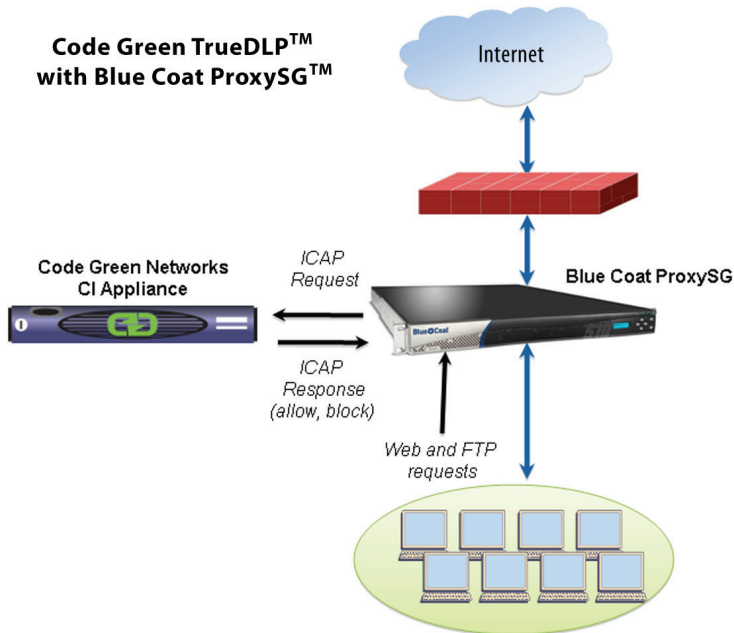
- An employee sends sensitive files to his/her Yahoo, Gmail, or other Webmail account, so he/she can access the information from a home/remote computer-- such behavior puts sensitive data into a risky, unsecured environment and may violate policy or regulatory requirements for data security.
- A disgruntled employee steals company secrets, using Webmail or FTP as a means of moving/copying sensitive data to external locations, often without a trace.
- Users are posting sensitive company information to external unsecured websites using Web 2.0 applications such as blog postings, wikis or other web applications.
- Unknown FTP transfers of information are silently initiated by backdoor
- programs previously installed by a Trojan or virus.

Most data loss events are unintentional policy violations; employees are typically unaware that they are violating data security policies. Less frequently, Web and FTP may be used in a deliberate attempt to sneak data out of the organization over unmonitored channels. Whether preventing an accidental violation, a deliberate insider theft, or a backdoor penetration, IT organizations require a DLP solution that can monitor and control sensitive data flowing over any communication channel.

The Code Green Networks and Blue Coat Solution

Code Green Networks and Blue Coat offer organizations a highly integrated, standards-based data loss prevention solution for monitoring and controlling Web and FTP traffic, including control over SSL-encrypted sessions.

Blue Coat ProxySG appliances share information and access to Web and FTP sessions with Code Green Content Inspection Appliances using an enterprise-class implementation of the Internet Content Adaptation Protocol (ICAP). The Content Inspection Appliances inspect the traffic for sensitive content and apply the appropriate DLP policy. Based on policy, the Content Inspection Appliance instructs the Blue Coat ProxySG to allow or block the session.



This complete DLP solution examines all forms of Web communication between internal employees and external sources, even those with SSL encryption. In addition it has the ability to control or block multiple types of Web communications to remove backdoors for information transfer.

Conclusion

Outbound Internet communication channels, if not properly controlled, represent a significant risk for sensitive information to leave the corporate network. Code Green Networks' TrueDLP™ solution combined with Blue Coat® Systems ProxySG® appliances form an integrated solution to stop the loss or theft of confidential or proprietary information over all communication channels, even for data carried over SSL-encrypted sessions.

Code Green Networks provides enterprise class data loss prevention solutions that are centralized, comprehensive, and easy to deploy and manage, helping you replace guesswork with the tools, roadmaps, and recommendations necessary to address risks, establish management policy, allowing you to deploy a robust approach to securing one of your corporation's most valuable assets — your data.

Blue Coat®

About Blue Coat Systems

Blue Coat secures Web communications and accelerates business applications across the distributed enterprise. Blue Coat's family of appliances and client-based solutions - deployed in branch offices, Internet gateways, end points, and data centers - provide intelligent points of policy-based control enabling IT organizations to optimize security and accelerate performance between users and applications. Blue Coat has installed more than 40,000 appliances worldwide. Blue Coat is headquartered in Sunnyvale, California.

For more information visit:
www.bluecoat.com

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 a loss of revenue, financial penalties and irreparable damage to a corporation's image, brand and customer loyalty.



Corporate Headquarters

Code Green Networks, Inc.
385 Moffett Park Drive, Suite 105
Sunnyvale, CA 94089

Phone: +1 (408) 716-4200
Fax: +1 (408) 716-4201
E-mail: info@codegreennetworks.com
www.codegreennetworks.com