



# Data Loss Prevention 2.0

*Preventing the loss of confidential information via webmail,  
Facebook, wikis and blogs*

## The Web 2.0 Generation

From the very beginning the World Wide Web was designed to make sharing information easier. Webmail sites like Yahoo!, Hotmail and Gmail were the first generation of applications accessible enough that the average user could now publish information to the web. This was one of the first channels of communication outside the enterprise that was not based on traditional email. The Web 2.0 generation of applications has taken this concept even further. Facebook and MySpace are designed to allow you to easily share information with your friends, while Twitter, blogs, and Wikis make it very easy to share information with the world.

According to a poll of US enterprises recently conducted by the Security Executive Council, a risk mitigation research organization, 86% of companies allow staff to use Facebook and other Web 2.0 applications. For most enterprises, widespread use of Web 2.0 applications increase the risk of data breaches, compliance failures, and loss of intellectual property.

## The Web 2.0 Dilemma

### *You can't turn social media off*

The first instinct of many CISOs/CSOs is to block sites like Facebook and Twitter outright. While this will prevent your users from accessing those sites, it will not prevent them from posting information to blogs or wikis elsewhere on the Internet. If you block too much you run the risk of creating contemptuous users. Contemptuous users will actively seek to evade technical controls you put in place because they are perceived to be either draconian or getting in the way of business. A determined and technically savvy user will always be able to get around simple controls such as URL blocking; furthermore their unmonitored actions may be the most dangerous threat to your organization.

### *You don't want to turn social media off*

As companies realize the benefits of Web 2.0 applications most don't want to disable these applications. Management wants to enable people to come together and collaborate--use social media to project the image of a progressive place to work and use the image as a recruiting and employee retention tool. Companies are also finding the applications beneficial in customer and market research as well as interacting with key stakeholders and driving revenue. In the Internet News article, "What Keeps Twitter Chirping Along", Dell claims that Twitter has produced \$1 million in revenues through sales alerts.

## Web 2.0 Posting Concerns

### *Regulatory Compliance*

All the compliance concerns that go along with email also apply to Web 2.0 applications. With Web 2.0 applications the regulatory compliance focus is on risk assessment and implementing security controls that are responsive to the threats your company faces. It is not enough merely to implement impressive-sounding security measures. According to attorney Thomas Smedinghoff, partner at Wildman

***" 86% of companies allow staff to use Facebook and other Web 2.0 applications. "***

The Security Executive Council

Harrold, adopting appropriate security controls in response to risk assessment plays an important role in determining whether liability will be imposed in the event of a breach.

What happens if you are in a regulated industry and, using a Web 2.0 application, one of your employees posts the Personally Identifiable Information (PII) of one of your customers to a public Internet site? For example, what if a nurse or physician uses their Facebook account to discuss options for patient treatment? Do you have any controls over this type of information or any means to remediate it? Without security measures in place is your organization liable?

### **Loss of Intellectual Property**

Would an employee facing a layoff at your company take valuable information with them or post confidential company information on blogs, if they could get away with it? The sobering reality is that 4 out of 5 employees do exactly this and most companies are powerless to stop them. Every organization has confidential documents like business plans, source code or product designs. Loss of this information may not be a regulatory or compliance problem, but it does have the potential to be a large business problem.

For example, what if an employee attaches a product design or confidential source code to a webmail? Do you have any controls that would detect this type of loss? How would you remediate it?

### **What is the Solution?**

Gartner analysts counsel that prohibition of social networking services (such as Facebook, Twitter or social networks in the enterprise) is unlikely to be in the best interest of the company. Instead they believe that properly controlled use of consumer-orientated technologies can have “real business benefits”.

If you open the door to social networking sites, the first step is to make sure you have the policies in place for the appropriate use of external web sites and the appropriate use of social media.

A technical solution can also be used to mitigate much of this risk. The technical solution is composed of two parts:

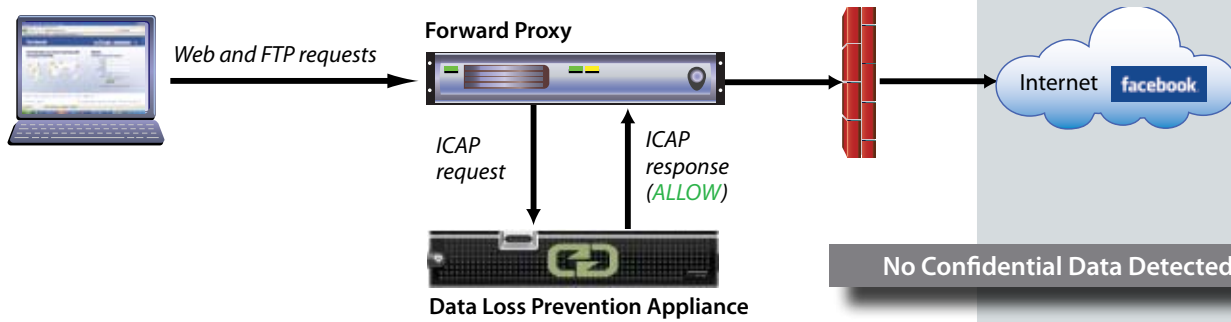
1. A Forward Proxy – a forward proxy accepts all HTTP/HTTPS and FTP connections that are outbound from an organization. The proxy makes connections on to Internet sites on behalf of end users. Prior to sending out any data, the proxy can utilize a DLP solution to ensure no sensitive data is being transmitted.
2. A Data Loss Prevention (DLP) Solution – A data loss prevention solution has the ability to examine outgoing traffic and determine if it contains confidential information. A DLP solution has the ability to fingerprint your confidential data and then examine outbound traffic to determine whether it contains confidential data.

***An estimated  
64 million people  
worldwide use Web 2.0  
technology for both  
social and work  
related purposes.***



### Example internet traffic flow with no confidential data

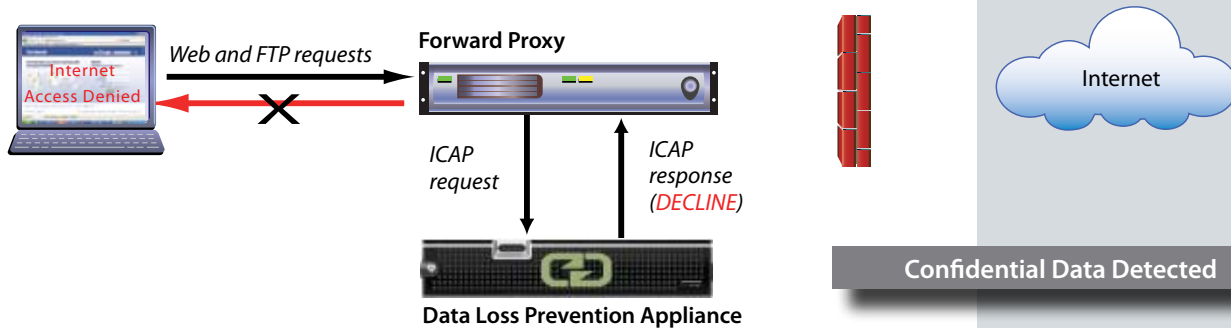
Let's take a look an example of how traffic flows through the solution, showing the inspection process and what happens if no confidential information is detected.



1. User is using facebook.com.
2. The user's web browser is communicating with the forward proxy
3. Forward proxy requests traffic inspection by the DLP solution via the ICAP protocol
4. DLP solution inspects traffic. If no confidential data is detected the transaction is approved.
5. Forward proxy initiates HTTP connection on behalf of the user to facebook.com

### Example internet traffic flow with confidential data

Let's take a look an example of how traffic flows through the solution, showing the inspection process and what happens if confidential information is detected.



1. User is using facebook.com.
2. The user's web browser is communicating with the forward proxy
3. Forward proxy requests traffic inspection by the DLP Solution via the ICAP protocol
4. DLP solution inspects traffic. If confidential data is detected the transaction is declined.
5. Forward proxy returns an error page to the end user.
6. Outbound connection never initiated. Confidential data does not leave the enterprise.

## Conclusion

In today's technology rich environment organizations are finding that employees often post sensitive company information to insecure or public Internet sites using Web 2.0 applications such as webmail, popular social networking, blog postings, Wikis, and other web applications. Security officers must refocus their attention beyond email to ensure regulatory compliance and adequate data privacy protection. New or updated policies to address Web 2.0 use will be needed, and a data loss prevention solution is required to provide adequate controls. Code Green Networks TrueDLP - fully integrated with Blue Coat Systems ProxySG and its Secure Web Gateway solution - provides organizations with a complete data loss prevention solution to stop the loss or theft of confidential or proprietary information over today's social media channels.

### 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.



### 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](mailto:info@codegreennetworks.com)  
[www.codegreennetworks.com](http://www.codegreennetworks.com)