

# **Data-Centric Security for Enterprise WANs**

*Combining Secure Web Gateways and Data Leak Prevention Products to Protect Enterprise Data and Networks*

A Blue Coat White Paper



## Executive Summary

Enterprises of all kinds need to protect valuable data, whether to comply with industry regulations or to guard intellectual capital. Unfortunately, it's all too easy—and common—for users to leak this data to outside parties, either accidentally or with malicious intent.

Secure Web Gateways are network and application security products that provide a variety of security measures, including URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications. Data Leak Prevention or Data Loss Prevention (DLP) systems identify and protect confidential data, including both structured and unstructured data. By combining a Secure Web Gateway with a Data Leak Protection solution, enterprises can monitor network activity and data usage and prevent users from transmitting or copying data in violation of company policies or industry regulations.

Blue Coat ProxySG is an industry-leading Secure Web Gateway solution that blocks malware, accelerates business-critical applications, and enforces network usage policies for WANs. Using an industry standard protocol, ProxySG integrates with leading Data Leak Prevention (DLP) products from vendors such as Reconnex, Vericept, Vontu (now Symantec Vontu), and WebSense. Because it also works as an SSL termination point, ProxySG is able to pass all encrypted and unencrypted traffic to one of these DLP solutions for monitoring and enforcement. A best-of-breed approach to data security, combining Blue Coat ProxySG and any of these DLP solutions, offers the comprehensive data security enterprises need, enabling them to protect data in motion, data at rest, and data in use, while optimizing application performance for all their users.

## Introduction: The Challenge of Protecting Data in a Highly Networked World

In this hyper-connected world of enterprise networks, information security involves more than keeping malware off internal networks and end user computing devices. Information security also entails protecting valuable data, wherever it may be in an organization's IT infrastructure, and ensuring that valuable data is not accidentally or maliciously divulged to outside parties.

Some data is valuable because it is personal. Customer records, financial records bank and brokerage accounts, or personal health information (PHI) fall into this category. The protection of personal data is mandated by industry regulations and laws, such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley, and HIPAA in the United States; the Privacy Directive in the European Union; and the Personal Data Protection Act in Japan.

Other data is valuable because it constitutes business knowledge and other types of intellectual capital. Product designs, business plans, and research reports belong in this category. In a growing number of industries, ideas and information, rather than manufacturing prowess and distribution capability, determine who will win and who will lose. Data leaks—whether through carelessness or malicious acts of industrial espionage—can cost a company not only profits in the short term but also market leadership in the long term. Businesses are increasingly aware of the need to protect their intellectual capital. Paul Proctor, vice president of research at Gartner, notes: "We've seen a minor shift from regulatory concern around breach notification and identify theft to intellectual property protection."<sup>1</sup>

For IT departments, the need to protect data only increases the scope and complexity of their work. IT departments need to maintain current systems and provision new ones. They need to keep data centers and daily operations running. They need to deploy new mobile services to keep up with user demand and to accommodate new workplaces designed for mobility and collaboration. They need to bring new Web applications online, possibly using new technologies such as AJAX, while supporting legacy systems and services. They need to optimize application performance at headquarters, branch offices, and home offices to boost productivity.

And throughout their new hyper-connected, multi-domain environments, they need to protect valuable data. They need to track confidential data and prevent users from disseminating it to the wrong people, either accidentally or knowingly. To prevent data loss, they need to monitor and secure all communications channels, including email, Web mail, and IM. They need to stop users from cutting and pasting data to get around security controls. They need to stop users from copying data to removable media, such as external hard drives and USB sticks. They need to advance online communications and make it easier for users to communicate, while ensuring that these same users never communicate the wrong data.

---

<sup>1</sup> [http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_qci1256804,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_qci1256804,00.html)

It's a lot to manage, and the stakes are high. Consider the following:

- A 2006 survey found that 81% of companies had lost sensitive data in the last year.<sup>2</sup>
- A 2007 survey by the Ponemon Institute found that 85% of companies had suffered the loss or theft of customer, consumer, or employee data in the past 24 months.<sup>3</sup>
- Over thirty states have passed laws requiring companies to notify the public about security breaches and data loss.<sup>4</sup>
- Forrester Research estimates that the business costs and financial penalties of lost customer data amount to between \$90 and \$305 per record.
- Data breaches can cost companies millions of dollars in fines and legal penalties. For example, several years ago, weak WLAN encryption led to a security breach at a TJ Maxx store. Over a two year period, hackers intercepted in-store credit card information, then broke into servers at the company's data center. Using this access, the hackers eventually stole over 45 million customer records. The company has already paid \$118 million to address this security breach and will likely pay more before the matter is settled.<sup>5</sup>

## Two Technologies Aimed at Data Security

Two security technologies, when combined, promise to provide a coordinated defense against malware, unauthorized intrusions, and data loss like that suffered by TJ Maxx. These technologies are Secure Web Gateways and Data Leak Prevention systems.

Secure Web Gateways, as defined by Gartner, are network and application security products that provide a variety of security measures, including URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Secure Web Gateway products filter traffic in real time, ensuring that devices surfing the Web do not become infected. The gateways also enforce company security and compliance policies, such as preventing users from accessing inappropriate Web content using company equipment.<sup>6</sup>

Data Leak Prevention or Data Loss Prevention (DLP) systems identify and protect confidential data, including both structured and unstructured data. These systems monitor networks and user endpoints to ensure that confidential information is not distributed surreptitiously through any means, including email, IM, or offline storage.

The combination of Secure Web Gateway products and DLP products offers enterprises a potent solution for protecting networks and data.

---

<sup>2</sup> <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002493>

<sup>3</sup> Source: WebSense.

<sup>4</sup> [http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185\\_qci1294447\\_00.html](http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_qci1294447_00.html)

<sup>5</sup> <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=198701100>

<sup>6</sup> For more information about the characteristics of Secure Web Gateways, see Gartner's report, "Magic Quadrant for Secure Web Gateway, 2007," GAS Core Research Note G00148895.

This white paper provides an overview of several Secure Web Gateway and DLP products that have been identified as market leaders by Gartner and Forrester. The products are:

- Secure Web Gateway:
  - Blue Coat ProxySG
- Data Leak Prevention:
  - Reconnex iGuard
  - Vericept Network Monitor/Protection
  - Vontu Prevent
  - WebSense Data Protection

The paper also discusses how these products can be integrated and the benefits they deliver for enterprise security.

## The Blue Coat ProxySG Solution

Blue Coat provides intelligent appliances and software solutions that secure and accelerate application delivery to all users connected over private WANs or the public Internet. Whether an application is hosted internally or externally, Blue Coat can accelerate its performance up to 100 times, while protecting the application's users from malware such as viruses and worms. Blue Coat also provides granular policy-based controls and helps restore IT control of all distributed users – even those with unmanaged endpoint devices.

Blue Coat's Secure Web Gateway solution is called ProxySG. Blue Coat ProxySG appliances establish points of control that accelerate and secure business applications for users across the distributed organization. The ProxySG gateway solution addresses these network needs:

- **Performance** – Blue Coat's patented MACH5 acceleration technology optimizes application performance and helps IT ensure delivery of business-critical applications. Through an optimal use of application-level performance optimization, caching, and parallelization, MACH5 improves the user experience no matter where the application is located, internally or externally on the Internet.
- **Security** – The Blue Coat ProxySG security architecture addresses a wide range of requirements for network and data security, including filtering Web requests and content, preventing malware and other malicious mobile code, validating content and certificates, inspecting encrypted SSL traffic, and controlling IM, P2P, and streaming traffic.
- **Control** – Blue Coat's patented Policy Processing Engine empowers IT to make intelligent decisions about network security, application delivery, and data access. Using a wide range of attributes such as user, application, location, destination, content and others, organizations can effectively align security and performance policies with corporate priorities.

Both Gartner and Forrester recognize ProxySG as an industry-leading product.<sup>7</sup>

---

<sup>7</sup> For example, see Gartner's report, "Magic Quadrant for Secure Web Gateway, 2007," cited earlier.

Because it is a true proxy and SSL termination point, Blue Coat ProxySG offers several architectural advantages over other approaches to network security and application performance optimization.

ProxySG greatly expands the visibility of DLP solutions into traffic. It ensures that valuable data assets never leave the WAN surreptitiously through encrypted connections. Without a ProxySG to terminate SSL connections, DLP solutions have no way of monitoring SSL-encrypted traffic—and SSL-encrypted traffic constitutes a large portion of any enterprise's traffic, especially in industries such as financial services and healthcare. By making encrypted traffic visible to DLP solutions, ProxySG broadens the coverage of DLP security to *all* encrypted and unencrypted traffic. *No DLP solution can be considered truly comprehensive without visibility into encrypted traffic—and ProxySG is the only Secure Web Gateway that provides that visibility in a reliable, scalable way.*

Other security advantages of ProxySG include:

- ProxySG can stop malware including trojans, viruses, worms, spyware, and phishing attempts at the network edge, preventing them from reaching user endpoints, consuming WAN bandwidth, and threatening internal resources such as servers and storage systems.
- ProxySG acts as a policy enforcement point for application usage, managing the “who, what, where, when, and how” of user/application interaction.
- ProxySG provides controls for blocking and managing a broad range of IM and P2P user agents and network types, including many agents and network types ignored by other Web gateway products. Leaving a P2P back door open weakens any DLP deployment. By controlling or blocking IM and P2P back doors, ProxySG makes any DLP solution more rigorous and comprehensive.
- ProxySG can improve network and application performance by caching, optimizing, and prioritizing traffic.

## ***Integration with DLP Solutions***

In addition to providing the network security and application acceleration described above, Blue Coat ProxySG supports data leak prevention through integration with leading DLP products.<sup>8</sup> ProxySG integrates with these products through the Internet Content Adaptation Protocol (ICAP). ICAP (RFC 3507) is a lightweight, HTTP-based protocol designed to enable proxies, such as ProxySG, to delegate specific types of content-scanning to dedicated servers, such as appliances running anti-virus or DLP software. By handing this work off to dedicated servers, proxy servers can take advantage of the advanced features of specialized security products, without the proxies themselves becoming overburdened with additional software and computing requirements.

---

<sup>8</sup> Like ProxySG, these products have been identified as market leaders by Gartner and Forrester. See Thomas Raschke, “The Forrester Wave: Data Leak Prevention, Q2 2008,” June 6, 2008. Also see Eric Quellet, Paul E. Proctor, “Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention,” Gartner Research Report G00157450, 17 June 2008.

This two-pronged, best-of-breed approach to network security and DLP enforcement offers several advantages:

- Customers enjoy the flexibility to deploy whichever ICAP-compliant DLP products they like.
- Customers benefit from the scalability of their security solutions, since off-loading DLP scanning to dedicated servers frees resources on the ProxySG.
- Customers benefit from the synergistic effects of combining a leading Secure Web Gateway with a leading DLP product.
  - The ProxySG can serve as a DLP enforcement point, blocking sensitive data from leaving the WAN.
  - The ProxySG can cache data that the DLP product has approved for syndication, improving network performance in compliance with DLP policies.

## Four Leading DLP Solutions

Blue Coat ProxySG integrates with leading DLP solutions from the following vendors.

- Reconnex
- Vericept
- Vontu (now Symantec Vontu)
- WebSense

These vendors offer DLP products with various approaches to protecting:

- data traveling over a network (called data in motion or DIM)
- data stored on computers but currently being accessed by applications (called data at rest or DAR)
- data in memory for reading or updating (called data in use or DIU)

### **Reconnex**

Reconnex iGuard is an appliance-based solution that protects data in motion (DIM) and data at rest (DAR). The company also offers a desktop agent for protecting data in use (DIU). IT engineers and security officers can define security policies, track policy enforcement, and generate reports across all three data domains—DIM, DAR, and DIU—through the Reconnex inSight Console. A distinguishing feature of the Reconnex solution is its ability to discover and classify sensitive data automatically. Reconnex products perform this analysis by searching for content signatures (e.g., patterns such as Social Security numbers or bank account numbers) and grammar patterns that signify specific types of content, such as FDA approval documents or financial statements. The Reconnex solution also makes use of “document biometrics,” which recognize content-rich elements in files even if file contents have been re-arranged and file names have been changed.

## **Symantec Vontu**

Symantec Vontu DLP 8 is an integrated suite of DLP products that protects DAR, DIM, and DIU. Vontu Enforce Platform is a central platform for defining DLP policies and workflow and for reporting on DLP activities. Other products in the Vontu suite address specific different contexts for data. Vontu Storage Data Loss Prevention discovers and protects confidential data on file servers, web servers, databases, and other types of data repositories, including portal products such as Microsoft SharePoint and content management systems such as Documentum. Network Data Loss Prevention monitors network traffic and prevents data loss through email, IM, HTTP, HTTPS, FTP, P2P, and generic TCP. Endpoint Data Loss Prevention discovers confidential data on laptops and desktops and prevents it being copied to removable media, burned to CDs or DVDs, or downloaded to local drives.

## **Vericept**

The Vericept Data Loss Prevention Solution protects DAR, DIM, and DIU through the deployment of several specialized DLP products. All the protects make use of Vericept's advanced content analysis, which, in addition to matching full or partial documents, analyzes semantic patterns and linguistic constructs, and models abstract concepts.

Vericept Discover detects and classifies data stored on services, desktops, and other edge devices. Vericept Protect scans email for data loss. Based on policies, it can block or quarantine email carrying sensitive data. Vericept Monitor works with a proxy such as Blue Coat ProxySG to prevent data loss over HTTP, HTTPS, and FTP. Vericept Edge prevents data leakage on desktops and endpoints. It continuously inventories data that is sensitive and blocks the unauthorized copying of sensitive data to removable media. The Vericept Management Console provides a central point of monitoring and control for the complete Vericept DLP solution.

## **WebSense**

The WebSense Data Security Suite discovers where data is located in a network, monitors who is using the data and how they are using it, and protects the data to comply with company policies and prevent data loss through accidents or malicious intent. The company's original offering was a network appliance to protect data in motion, but the new Data Security Suite protects data in motion, data in use, and data at rest. WebSense's PreciseID™ "fingerprinting" technology discovers networks hosts and endpoints and classifies the data stored on them. WebSense's Deep Content Control™ protects confidential information, regardless of file type. The Data Security Suite includes a policy wizard featuring over 250 pre-defined policies for DLP.

## Benefits of the Combined Blue Coat-DLP Solution

By integrating Blue Coat ProxySG with DLP products from any of these vendors, customers can achieve these benefits:

- Application acceleration and traffic optimization
- Improved security and regulatory compliance
- Protection of intellectual capital and confidential records
- Filtering of Web, email, and IM traffic for security and policy compliance
- Data loss protection for data in motion (networks), data at rest (servers and endpoints), and data in use (endpoints and media)
- Expanded DLP security through the use of ProxySG as an enforcement point for DLP policies

## Conclusion

Today's enterprise networks reach farther than ever before, creating new opportunities for business collaboration and business agility. But these same networks, spanning corporate domains and comprising a variety of wired and wireless network technologies, increasingly jeopardize data security. A careless keystroke or the machinations of a crafty hacker can irretrievably expose confidential data, abetting identify theft and putting companies at risk of regulatory censure and financial loss.

A best-of-breed approach to data security, combining Blue Coat ProxySG and any of several leading DLP solutions—such as those offered by Reconnex, Vericept, Symantec Vontu, WebSense—offers the comprehensive data security enterprises need, enabling them to protect data in motion, data at rest, and data in use. Through this combined solution, data security increases, while users benefit from other ProxySG features, such as application acceleration and more comprehensive policy enforcement.



Blue Coat Systems, Inc. 1.866.30.BCOAT • 408.220.2200

Direct • 408.220.2250 Fax [www.bluecoat.com](http://www.bluecoat.com)