

Credit Unions Find Protection in Data Loss Prevention Technology

By Rod Murchison

Although perimeter security systems have been preventing network attacks from the outside for decades, credit unions are now focusing on innovative new security solutions which add another layer of critical protection. Instead of thwarting attacks from the outside in, Data Loss Prevention (DLP) systems prevent sensitive data from leaving the company, whether by inadvertent means or through deliberate theft.

In their ongoing drive to provide better member services, credit unions now operate external web sites and use both corporate e-mail (i.e., Outlook) and occasionally webmail to respond to member inquiries. In addition, key employees may take work home from the office using laptop computers or via external flash drives. The problem is that the security and confidentiality of this sensitive corporate data can be significantly compromised when it is transmitted out over the Internet or transported on portable devices that can be lost or stolen. DLP solutions protect this sensitive internal data by constantly examining network transmissions, files stored on removable media, and data existing on servers to ensure it can't be exposed to unauthorized parties.

How DLP Works

DLP products use various means of identifying sensitive data, including exact document matching, pattern matching (social security number formats, for example), regular expressions, and most importantly, database and file fingerprinting. Once sensitive data is identified in your organization, IT administrators define policies that govern what should be done when it is detected that this sensitive data is being used. The system then monitors activity on network servers and desktop systems and then acts appropriately based on the policies set. Today's DLP solutions can monitor and alert, reroute, encrypt, and block sensitive data in real time before it leaves over the Internet – or even before it is copied off a computer via a flash drive or other removable media.

DLP solutions on the market today can take the form of software on user desktops, hardware systems that perform network monitoring, hardware or server software that allows for policy creation and management, and encryption engines that can encrypt sensitive corporate e-mail messages. Since the market is in a highly innovative phase, it's easy to find many diverse product approaches to implementing DLP, but this can also make it hard to choose what is best for your organization. Some solutions are designed for very large installations and offer a high degree of customization while others are tightly packaged but geared more towards small to mid-sized deployments.

The TrueDLP solution from Code Green Networks is a good example of a tightly packaged and purpose-built solution for Credit Union customers. It uses a network appliance to handle policy creation and network DLP enforcement, ongoing data inspection, and encryption of corporate e-mail. In many cases, the Code Green solution can be deployed within a day or two, and its support for all commonly-used methods of data inspection and discovery gives credit unions the flexibility to identify data and define policies in the way that best suits their operations. The system is priced by the number of employees protected.

Data Classification, Inspection, and Blocking

The accuracy of data classification and policy creation are keys to successful implementation because general data definitions based on data formats or pattern matching can create a high number of “false positive” alerts that take up valuable IT time. Each credit union is unique, and therefore it is a common practice to import and “fingerprint” member data and sensitive documents, and then look for this exact data as it leaves your network or is copied off to a removable device.

At First Technology Credit Union in Portland, Oregon, system administrators used the Code Green system’s own industry-specific document libraries and templates to speed data classification and policy creation. As a major supplier of DLP solutions to the credit union industry, Code Green offers a series of templates and libraries that simplify identification of data formats commonly found in credit union databases.

At Georgia’s Own Credit Union in Atlanta, on the other hand, administrators used the Code Green system’s database fingerprinting and SQL query capabilities to identify data based on what was actually in use. When the credit union’s own databases use SQL, database fingerprinting is the most accurate method of identifying data since it inspects the network and user desktop systems for the presence of actual database contents and then takes appropriate action if those records are about to be improperly transferred.

With database fingerprinting, the DLP solution simply needs to be shown what data is declared sensitive, such as a credit union member database, and then specific policies can be written that define exactly what data to look for, where to look, and what the solution will do if a data breach in progress is detected.

Once the Code Green DLP system is deployed, the results are often immediate. Credit union technical teams typically test the system by creating and sending out a document containing a social security number, for example, and then see if the system catches the breach. Credit union IT teams are often surprised at the number of initial policy violations found, even if they thought their systems had been quite secure.

Administrators can use the Code Green solution to specifically alert end users, IT staff, department heads, or upper management when the policy violations are detected. For example, a minor policy infraction might alert the end user while more significant issues might trigger alerts to the department head or the IT security staff.

Unlike some other DLP systems, the TrueDLP system includes a corporate e-mail encryption engine and does not require a separate encryption server. The TrueDLP encryption engine integrates with cloud-based encryption key servers from Cisco, Voltage, and ZixCorp – when a sensitive corporate e-mail is sent, the message is automatically encrypted and sent to the recipient with instructions on how to open and view the contents securely. This process is fast and effective and prevents the e-mail from being opened by anyone but the actual designated recipient.

Data Loss Prevention is becoming an essential part of the overall security system for financial services firms, but the DLP system needs to be highly accurate, cost-effective, and easy to manage. Credit unions deploying the Code Green system have found just such a solution.

Challenge

- Prevent accidental data loss via e-mail, WebMail, Web 2.0 applications and removable devices
- Minimize training and disruption for credit union employees
- Avoid adding significant IT overhead

Solution

- Code Green TrueDLP appliances accurately classify, detect, and block unauthorized data transfers on the network and on the endpoint
- Deployments within two days with immediate identification/remediation of security issues
- Customized alerts and low rate of false positives make administration easy and cost effective

Rod Murchison is Vice President of Marketing and Strategic Alliances at Code Green Networks