

Challenge

- Core business is focused on sensitive data that has to be protected to maintain business continuity
- Better-educated customers are driving data loss protection for compliance
- Keep cost and complexity low

Solution

- Code Green Networks TrueDLP™ solution enables network monitoring to prevent data from leaving the corporation
- The solution was deployed in one day and requires minimal support time
- Code Green Networks supports long-term roadmap for server maintenance and replacement

LCS Financial Services Corporation Ensures Financial and Personal Data Stays Confidential

LCS Financial Services Corporation (LCSF) is a full-service consumer debt collection agency. LCSF specializes in the collection of mortgage, auto, credit card, student loan and medical debt. Its customers include Fortune 500 companies, including the nation's largest investment banks and consumer finance organizations, and small businesses for recovery of debt.

Adding TrueDLP to the Security Arsenal

ESecurity has been a cornerstone of LCS Financial Services for years, which has stringent IT and physical security policies already in place. USB and CD-ROM ports are locked, staff email access via the web is denied, Internet access and social sites are restricted, and those few employees requiring remote access must use two-factor authentication with a token. The company has similarly strict physical access policies as well to protect data and systems.

Increasingly, potential customers were asking about data loss protection (DLP) and including it as a checkbox on requests for proposals from the firm. "We first learned about DLP several years ago in a vendor seminar and in the last year, we've noticed potential customers requiring it in their security arsenal," said Daniel Groves, Chief Technology Officer, LCS Financial.

The company checked out several vendors but ruled them out due to cost and complexity of their offerings. In one case they were amazed to discover that it took four of the vendor's appliances to do what one Code Green Networks appliance could do.

Groves learned of Code Green Networks TrueDLP when doing some additional research. The solution's single-appliance approach and price appealed to him. Groves got in touch with Code Green Networks and started a two-week "try and buy" program. To Groves' surprise, TrueDLP was installed in a few hours one morning in the first quarter 2010 and running at full functionality by mid-afternoon that same day. "I was really a bit uncertain about how quickly we could get this product installed and really working and was blown away by how quickly it happened," he recalls.

One big requirement Groves had for any DLP solution was to complement and support his existing server upgrade and replacement roadmap. Code Green Networks' staff worked with him to develop a longer-term plan to ensure that the DLP aspect of his infrastructure would be in sync with his plan for future hardware.

The Business Case for DLP

Groves emphasizes the business case for any new technology before choosing and deploying it, and DLP was no exception. "The business case is as important to us as the available technology and policies. A solution has to meet business needs. You can have all the hardware and software in the world, but if it does not support your business case, there's no reason to have it."

The company also prefers to deploy what Groves calls "industry standard," or widely used, proven technologies that he knows have been well-tested and supported and support other widely used systems and infrastructure.

At LCS, the increasing amount of highly confidential data, such as Social Security Numbers, credit information, and the like handled by the company, along with demand from customers to see DLP in place resulted in a clear-cut business case for Groves.

“The way we see it, the value in a solution like TrueDLP is avoiding issues later. Many companies don’t see it like this, but we have operated like this for a long time and believe it most effective.”

Catching Data Before It Leaves

LCS Financial Services Corporation now uses TrueDLP primarily for networking monitoring. “We will add endpoint capability in the future, but the network monitoring was our big focus,” explains Groves.

The security officer at the company receives the alerts from TrueDLP via email and cell phone. According to Groves, “It basically manages itself – there is little additional time required now.”

Even with its stringent existing IT security policies, the TrueDLP solution has identified several incidents of potential data loss, as employees hastily reply to clients requests unintentionally releasing confidential information.

Groves observes, “DLP prevents unintentional incidents, which most are, where people don’t realize they’re putting data out there that is confidential.”

LCS will add additional DLP capabilities in the near future. These include integration with proxy servers. Groves says that he also is considering implementing the email encryption capability of TrueDLP. “Many of our clients use various proprietary or lesser-known encryption tools, but we would like to standardize on something that’s enterprise-ready, and TrueDLP offers several options including ZixCorp, Voltage, and Cisco.”

As he considered the deployment time and effort, long-term cost and product features and roadmap of TrueDLP, Groves believes that LCS Financial Services Corporation made the right choice. TrueDLP fits well into the company’s overall infrastructure and philosophy. As Groves says, “Nobody cares about your security except you.” And TrueDLP met not only his customers’ checkboxes but his as well.

“The business case is as important to us as the available technology and policies. A solution has to meet business needs. You can have all the hardware and software in the world, but if it does not support your business case, there’s no reason to have it.”

Daniel Groves, CTO
LCS Financial Services

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
www.codegreennetworks.com