

Protecting Customer Data at Rest and in Motion

The vast majority of banks and their employees have the best interests of their customers at heart, but with bank operations now completely intertwined with the Internet it has become much more challenging to safeguard sensitive data. In their efforts to provide excellent customer service, for example, employees may be using unsecured e-mail to communicate with customers where bank account numbers, online usernames / passwords, or other personally identifiable information may be transmitted. In other instances, bank employees may be copying sensitive data to laptop hard drives or USB drives to take work home, or even exposing very sensitive data through outbound webmail or "Web 2.0" applications such as social networking sites.

In most cases, these activities occur inadvertently, but in some instances there is malicious intent involved. Either way, unauthorized use of sensitive data poses a daunting security risk. Laptops or thumb drives can be lost or stolen and non-secure e-mail or instant messages can fall into malicious hands. Beyond employee activity, there are ever-growing threats from spyware and Trojan Horses, which are becoming more sophisticated and effective at cloaking their existence and their outbound communications... which are often filled with sensitive data.

Along with these fundamental security issues, misuse of sensitive data can also create legal problems for the bank. This is particularly true in states such as Nevada, which have enacted strict privacy laws that can leave banks open to unlimited liabilities in the event of any kind of data loss or theft.

To prevent these occurrences, bank IT managers must be able to know how and where sensitive data is being stored (data at rest) or used on the desktop (data in use) or sent over the network (data in motion), and then have the means to block or restrict activities that could transfer data to non-secure places. TrueDLP for Code Green Networks is a data loss prevention (DLP) solution that allows banks to identify and monitor the use of sensitive data, prevent unauthorized transfers, and encrypt e-mail.

Once installed, the TrueDLP appliance and endpoint agents work transparently and automatically, applying the bank's security policies to data transfer operations, alerting end users and the IT staff when security policies are violated, and taking preventive action such as blocking transfers or encrypting data. TrueDLP is easy to install and manage, and provides a full complement of DLP features (including flexible data classification, continuous monitoring, built-in e-mail encryption, and full logging and reporting) at a fraction of the cost of other products.

True DLP cost-effectively scales from small banks (under 50 users) to the largest institutions. TrueDLP takes the worry out of potential data loss simply, automatically, and cost-effectively.



Rod Murchison
Vice President

Rod Murchison is the Vice President of Marketing & Strategic Alliances at Code Green Networks. Prior to joining Code Green, Rod was the Vice President of Marketing at Vernier Networks, a leading provider of Network Access Control products designed to ensure network security and compliance. Rod has more than 17 years of experience building industry-leading security and networking solutions for Juniper Networks / NetScreen Technologies (NASDAQ: JNPR), Ingrian Networks, Blue Coat Systems (NASDAQ: BCSI) and Newbridge Networks (NYSE: ALA). Rod holds a Bachelor of Science degree in Industrial Engineering from Penn State University.



Contact Info:

www.codegreennetworks.com