

Perimeter, Host and Endpoint Security – Finding the Right Mix

There has been a gradual transition from worrying exclusively about outside threats to realizing the importance of protecting against inside threats. While firewalls are certainly a necessity, unfortunately they provide no visibility whatsoever into content. Increasingly, banks are starting to focus on content security – protecting their customer account numbers, Social Security numbers, credit/debit card numbers, etc. In addition to this type of structured data, they also need to protect unstructured information that may be contained within Word documents, PowerPoint files, and other documents.

Without a data leak prevention system in place, it is virtually impossible for banks to know if they are properly protecting their customer data. That is because there are so many avenues for this data to leave the bank: email, WebMail, Instant Messaging, blogs, and more. This unauthorized disclosure of sensitive information can have catastrophic consequences from lawsuits to problems with government regulators to irreparable damage to a bank's image, brand and customer loyalty.

Without a doubt, the vast majority of bank employees are honest and hardworking. However, they can still make mistakes that lead to inadvertent data loss. In fact, our experiences show that over ninety five percent of data loss leaving an organization is completely unintentional and not malicious in nature. Most of our clients are quite surprised by this data leakage and admit that they never would have known about it without using our platform that permits them to gain complete visibility and control of their data.

When a bank installs one of our Content Inspection Appliances, we provide them with pre-defined best practice and compliance templates specifically designed to help banks protect their sensitive customer data and organizational intellectual property. Our system features an easy to use interface and relieves their IT Department from having to spend many hours configuring the system – with typical deployments taking less than a day. And within each data policy, banks have the flexibility to determine the appropriate actions for policy violations: alert, quarantine, block, reroute or encrypt.

Because data leak prevention and data encryption go hand in hand, we have built encryption right into our appliances. Banks receive a fully integrated data protection solution and email encryption package in one easily managed device. Plus, our Content Inspection Agent protects data, both on and off the network by preventing the transfer of files to or from unauthorized portable devices, and automatically encrypting data copied to approved devices.

Every bank is concerned with doing well on their audits and our systems provide a complete audit trail and show that the bank's policies are being enforced across all departments and employees. At Code Green Networks we have developed the next generation of content protection systems that help banks meet compliance guidelines, and are easy to deploy and above all affordable.



Brian Czarny
Vice President

Brian Czarny is the Vice President of Marketing at Code Green Networks. Prior to Code Green, Brian was the Vice President of Marketing and Product Management at MessageLabs, a leading provider of messaging and Web security services to organizations around the world. Brian has more than 12 years experience building technology brands and has been regularly quoted as an industry expert on a range of security and messaging topics in media and broadcast outlets around the world including The New York Times, Wall Street Journal, Business Week, Information Week, eWeek, CNN, ABC 20/20, and CNBC. Brian holds Bachelor of Arts degrees in Journalism and Political Science from The Pennsylvania State University.