Prevent the Transfer of Sensitive Data

Globalscape® EFT™ Scans File Transfers for Sensitive Data

Some of the biggest threats to organizations today are their own employees. Employees often transfer files outside of their organization when doing business, to partners and clients, to coworkers who are working at home, or to themselves at their personal email addresses. Occasionally, they might transfer a file that contains sensitive information about the company, its employees, its partners, or its customers.

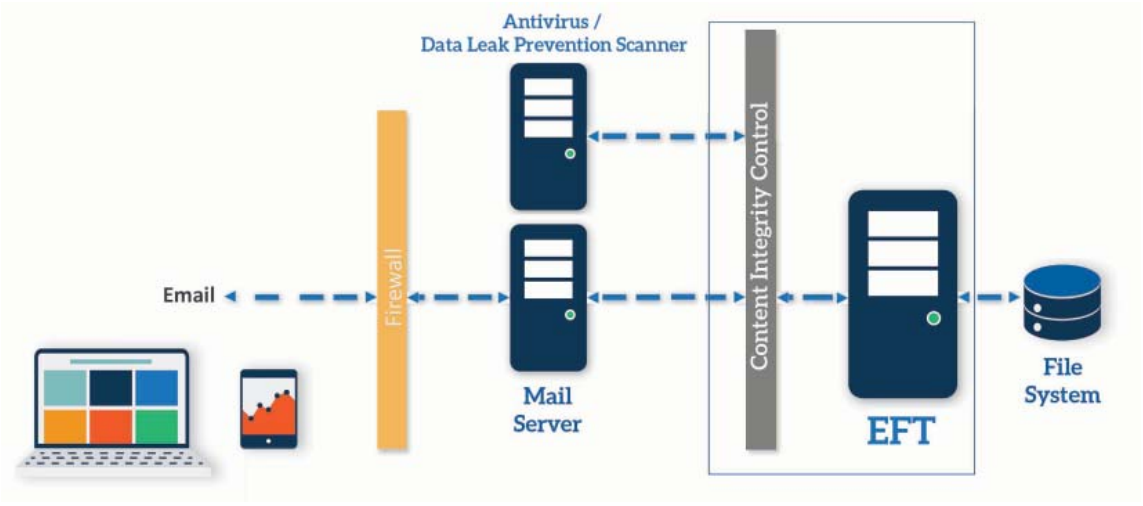
Companies often label documents as protected information, or limit access to those documents, yet information that should have been kept confidential is still shared with competitors, reporters, or customers. Many government and industry regulations (e.g., HIPAA, SOX, PCI DSS) require that a company protect such information to stay compliant.

Receiving documents from outside the organization is often a routine part of doing business, and is fraught with the risk of introducing viruses and other malware to the internal network. Usually, by the time you know a file contained a virus, it has already spread throughout and infected the network.

The best away to stop the leak of information from your company is to scan the documents automatically as they are being sent or received, and then block the transfer if a document contains sensitive information.

Globalscape® EFT™ with Content Integrity Control™ Stops the Leaks

Globalscape EFT™ with Content Integrity Control™ (CIC) integrates with data leak prevention (DLP) solutions to ensure that transferred files do not contain sensitive data. EFT can also send transfers to anti-malware scanners before allowing them to reach their intended destination. Transfers are then permitted or blocked based on policies set in EFT Event Rules.



4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

With CIC, You Control What Gets Through

The EFT administrator can specify how EFT should react to items flagged by the DLP and antivirus solutions, and whether EFT should automatically apply the relevant compliance requirements to your data transfers. Implementing EFT with CIC in your network:

- Ensures transfers are free of viruses/malware.
- Ensures employees are not sharing confidential/ proprietary info.
- Ensures no transfers contain nonpublic information, such as PHI (protected health information) and PFI (personal financial information).
- Helps you maintain compliance with PCI DSS requirements regarding DLP.

Contact Globalscape today to learn more about EFT with Content Integrity Control.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)