globalscape™
securely connected

Data Sheet

Content Integrity Control™ (CIC) Module

Control what gets through

Key Benefits:

> Ensures transfers are free of viruses/malware.

> Ensures employees are not sharing confidential/ proprietary information.

> 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.

Fully Integrated Content Control

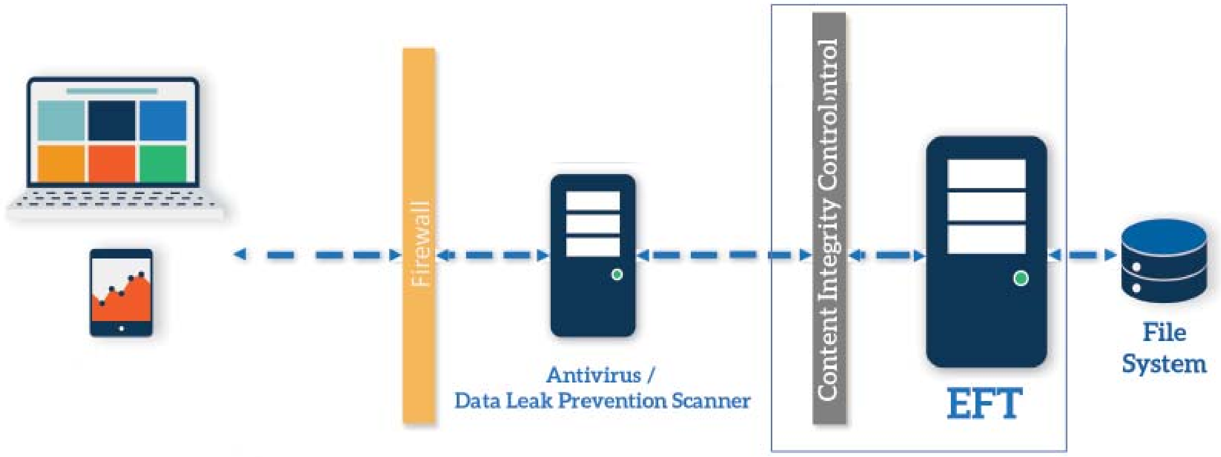
Enhanced File Transfer (EFT) is Globalscape's best-in-class, customizable managed file transfer software and a leader in Gartner's Magic Quadrant for MFT. Companies of all sizes (including the US Army) use EFT, trusting its unmatched simplicity and top-notch security. EFT's Content Integrity Control™ (CIC) module supports integration with virus scanners and DLP (Data Loss Prevention) tools, so you can permit or prevent transfers based on policies. With CIC, employees won't inadvertently share confidential or proprietary information, or receive files that contain malware.

EFT's Content Integrity Control module is used to send files to an antivirus scanner or DLP solution for processing. When the Content Integrity Control Action is added, any file that triggers the Event Rule is sent to a content inspection server for scanning.

> If the file passes the scan, other actions can occur, such as moving the file to another location.

> If the file fails the scan, Event Rule processing can stop, or other Actions can occur, such as sending an email notification and moving the file to a quarantine folder.

Multiple Content Integrity Control profiles can be created to send files to different solutions, or to look for different ICAP status codes or text in the ICAP header or body. The results can be captured in the Auditing and Reporting module database to generate reports.



Consolidate Costs with EFT Integration

Having an agent on every desktop is expensive to license, deploy, and maintain. Stopping the file before it gets to the desktop saves IT's time in hunting down and eliminating the spread of a virus. In the case of DLP, EFT can identify files that have proprietary or protected information before they leave the organization, instead of after the fact.

Integrating the task of processing into EFT allows you to audit these occurrences and ensure files are properly handled before being visible to the rest of the organization. The Content Integrity Control module is fully integrated into EFT's Event Rule system. Configure the connection to the antivirus or DLP server in reusable "profiles" one time, and then insert the profile in any Event Rule that can trigger upon inspection of files uploaded to or downloaded from EFT. Subsequent actions can occur based on inspection results, including sending email notifications, moving the file to a quarantine folder, or allowing the file to continue to its destination.

Many antivirus and DLP servers offer reporting, but they are often weak on details. In EFT, all actions are tracked in a log file and in the database, allowing you to generate reports of all transfers and CIC activity. A predefined CIC report is installed with the module, and you can customize it with other information that is captured in the database. Additionally, EFT's Status Viewer allows you to view transfers in real time.

Unlike other MFT providers, EFT's integrated CIC module can replace all of the agents installed on desktops. No more multi-seat licensing fees or pushing antivirus updates to every desktop in your organization.

Supported Antivirus and DLP Servers

EFT's CIC module uses the ICAP protocol, the industry standard for antivirus and DLP servers. Any third-party content inspection product that supports ICAP can communicate with our CIC module. Globalscape's testers have verified that the CIC module works with the following antivirus and DLP servers:

Antivirus:

> Kaspersky

> Sophos

> Symantec

> Trend Micro

> And others

DLP:

> Symantec

> Websense

> McAfee

> RSA

> And others