DATA SHEET

CONTENT INTEGRITY CONTROL™ (CIC) MODULE

KEY RESULTS

- **Protect:**
  - Confidential/ proprietary company information.
  - PHI (protected health information)
  - PFI (personal financial information)
- **Prevent** spreading of viruses/ malware
- **Consolidate** costs instead of having multi-seat licensing fees or pushing antivirus updates to every desktop in your organization
- **Facilitate** compliance with PCI DSS requirements regarding DLP.

Enhanced File Transfer (EFT) Enterprise secures, manages, and tracks data transferred between people and applications both inside and outside your organization. To help you protect this data, EFT Enterprise offers an integrated Content Integrity Control (CIC) module to replace all of the antivirus/ Data Loss Prevention (DLP) agents installed on desktops. No more multi-seat licensing fees or pushing antivirus updates to every desktop in your organization. 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.

CONTROL WHAT GETS THROUGH

The CIC module integrates with virus scanners and DLP tools to permit or prevent file transfers based on your organization's policies, and supports compliance with PCI DSS. With CIC, you won't expose your network to files containing malware, or share confidential or proprietary information.

When the CIC Action is added to an Event Rule, any file that triggers the Event Rule is sent to a content inspection server (antivirus scanner or DLP solution) 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 CIC profiles can be created on the server to send files to different solutions, or to look for different ICAP status codes or text in the ICAP header or body. Then you can add the predefined profile to one or more Event Rules. The results can be captured in a predefined CIC report or your own custom reports in the Auditing and Reporting module database.

FULLY INTEGRATED CONTENT CONTROL

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. Configure the CIC 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.

EFT

GLOBALSCAPE

ABOUT GLOBALSCAPE

Globalscape is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Founded in 1996, Globalscape's data exchange and integration software and services are trusted by over 13,000 customers in over 150 countries worldwide, including global enterprises, governments, and small and medium enterprises. Headquartered in San Antonio, TX, Globalscape enables companies to increase business agility by unleashing the power of data. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. Globalscape has consistently been named a top workplace by Computerworld, the San Antonio Business Journal, Texas Monthly, and the San Antonio Express-News, among others.

GENERATE REPORTS OF ALL CIC ACTIVITY

Many antivirus and DLP servers offer reporting, but they are often weak on details. In EFT Enterprise, 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.

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. The CIC module is compatible with the following antivirus and DLP servers:

Antivirus:

- Symantec
- Sophos
- McAfee AV
- Kaspersky
- Trend Micro
- Clearswift
- And others

DLP:

- Symantec
- Forcepoint (formerly Websense)
- McAfee
- RSA
- Clearswift
- And others

GLOBALSCAPE

www.globalscape.com
1.800.290.5054

4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249
United States