DATA SHEET

ADVANCED SECURITY MODULE FOR EFT™ ENTERPRISE

KEY RESULTS

- **Comply with requirements**
  - Achieve or exceed industry, government, and corporate security standards
  - Actively monitor compliance with security warnings
- **Secure sensitive data**
  - Protect data at rest with EFS
  - Protect data in transit with industry-standard, secure protocols, strong ciphers/ encryption keys, and strict password policies
  - Prevent sharing of confidential or proprietary information, PHI, or PFI, or files that contain malware
  - Prevent spreading of viruses/ malware
- **Authenticate securely**
  - Provide smart card, single sign-on, and multi-factor authentication options
  - Enforce existing security policies in edge applications
  - Support for SAML SSO, RADIUS, RSA SecurID®,, CAC, SMS

The Enhanced File Transfer™ (EFT™) Enterprise Advanced Security module (ASM) secures sensitive data, provides secure authentication options, achieves or exceeds security practices mandated by the most rigorous standards. Whether your business is obligated to comply with certain regulations or you simply desire the utmost in security standards, the ASM is your solution for securing data transfer, access, and storage.

SECURE SENSITIVE DATA

Securing sensitive company data requires continuous monitoring and validation of security policies and controls. Globalscape makes it easy for an administrator to create and maintain file-transfer services that meet or exceed these standards with a simple set-up wizard. EFT's integrated antivirus/data loss protection can protect private and confidential data. No more multi-seat licensing fees or pushing antivirus updates to every desktop in your organization. Stopping the file before it gets to the desktop saves time 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

Once enabled, the ASM is an ever-vigilant security tool that disallows low-security options, captures compensating controls, and generates reports for auditing the system's compliance status.

With support for multiple secure protocols, including FIPS 140-2 certified protocols, the ASM thoroughly protects data in transit, enforces the use of secure protocols, strong ciphers, encryption keys, and password policies, and ensures data transfers strictly follow all security guidelines.

MONITOR COMPLIANCE

Whether you have to comply with GDPR, PCI DSS, FIPS 140-2, HIPAA, HITECH, SOX, GLBA/FFEIC, DIACAP, and many others, a setup wizard provides you with an easy, step-by-step method to configuring a security-enabled site, with each page describing the requirement and what you need to do to meet that requirement, or to provide a compensating control (workaround).

The ASM, in concert with EFT and DMZ Gateway®, helps organizations comply with data storage requirements—including not storing data in the network DMZ. EFT uses repository encryption and securely sanitizes (wipes) deleted data so that it cannot be reconstituted.

The ASM actively monitors settings by alerting when less secure options are chosen, identifying the cause of non-compliance, allowing reverting of security controls, and implementing mitigation/workaround techniques.

A predefined "PCI DSS Compliance" report is installed with the module, and you can customize it with other information that is captured in the database.

EFT

GLOBALSCAPE

ABOUT GLOBALSCAPE

Globalscape, Inc. (NYSE MKT: GSB) 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. 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.

For more information, visit www.globalscape.com or follow the blog and Twitter updates.

AUTOMATICALLY ENFORCE POLICY

Event Rules allow you to automate processes to prevent human error and enforce policies, using file system events, Workspace events, user events, and connection events, in addition to server, site, timer, and folder monitor events. When these events occur, actions can occur, such as writing to logs, emailing administrators, copy/move a transferred file, execute advanced workflows, or scanning the file with antivirus/DLP solutions.

Through Event Rules, EFT with the ASM 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 regarding DLP. Any file that triggers the Event Rule is sent to a content inspection server (antivirus scanner or DLP solution) for scanning. 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.

The ASM is compatible with a variety of antivirus and DLP servers, such as:

Antivirus:

- Symantec
- Sophos
- McAfee AV
- Kaspersky
- Trend Micro

DLP:

- Symantec
- Forcepoint (formerly Websense)
- McAfee
- RSA

SECURE AUTHENTICATION OPTIONS

EFT Enterprise with ASM eliminates the need to create and track built-in, user and administrator accounts, by using your existing Active Directory infrastructure for account creation, helping you maintain security of accounts in one location. Additionally, the ASM provides support for easy-to-use authentication methods, including smart card (CAC), single sign-on, and multi-factor authentication options. ASM with EFT Enterprise can be your single source of authentication across the IT resources you use, including EFT. For user authentication, you can use an AD, NTLM, LDAP, or ODBC-compatible database, or EFT's built-in authentication manager.

The ASM enforces account access policy controls such as the automatic lock out of accounts after a set amount of incorrect login attempts and the removal of inactive accounts after a certain period of inactivity. Additional security controls can be set to expire passwords automatically on certain dates, and notifications such as emails and banners can be configured accordingly.

GENERATE REPORTS OF ALL EFT AND ASM ACTIVITY

With the addition of the Auditing and Reporting module, all transfers. event rules, and user/admin/system activity are tracked in a log file and in the database, allowing you to generate reports of that data. A predefined "PCI DSS Compliance" report, "Content Integrity Control" report, and many other reports of activity, traffic, and security are installed with the module, and you can customize them with other information that is captured in the database.

Contact Globalscape to find out more about EFT™ Enterprise and the Advanced Security Module.

GLOBALSCAPE

www.globalscape.com
1.800.290.5054

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