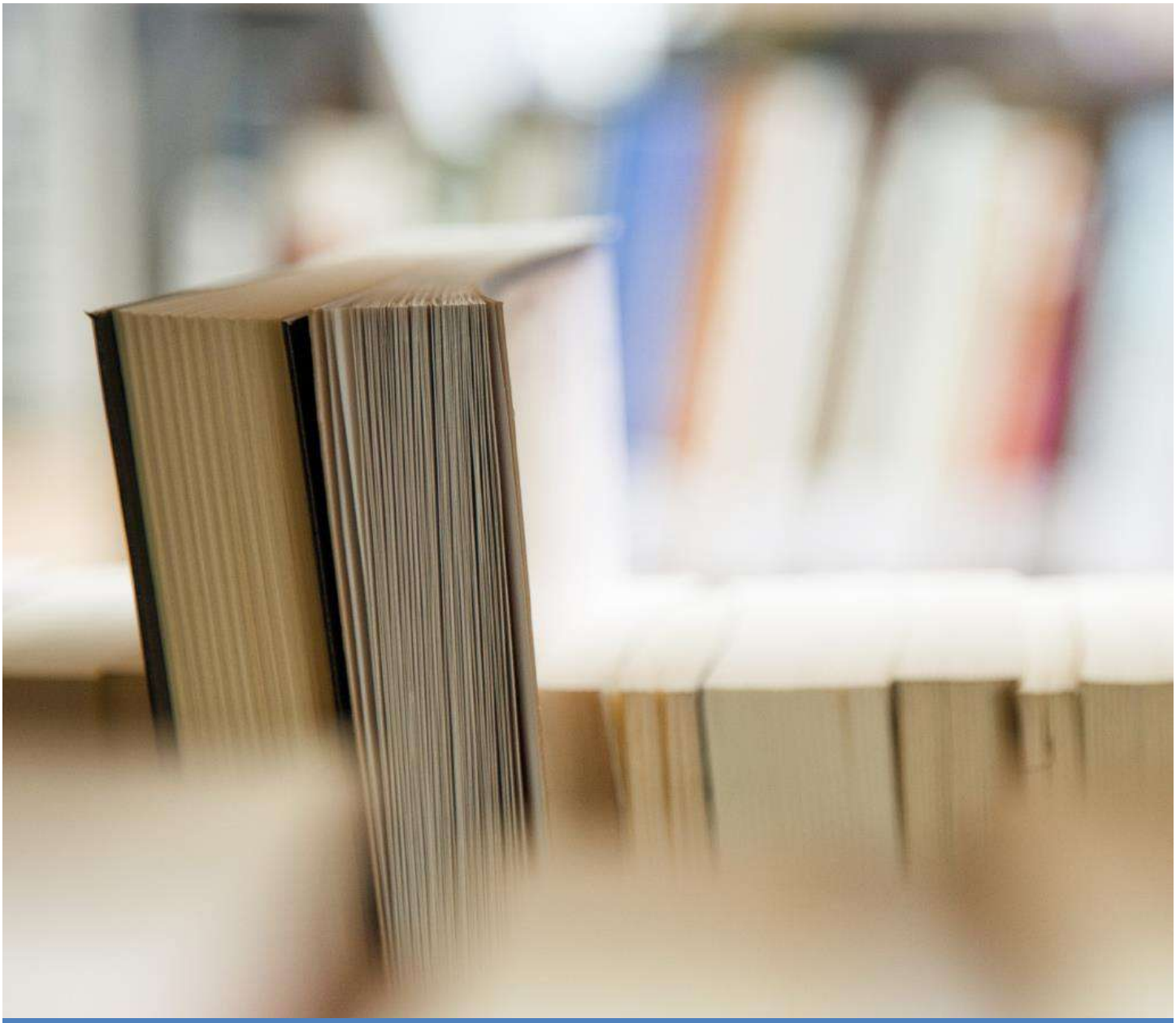

White Paper – Fasoo Data Security Framework

Data-centric Security, People-centric Policy, Multi-layered Approach

197 State Route 18 South
East Brunswick, NJ 08816
tel: +1-732-955-2333 (NA HQ)
web: www.fasoo.com | email: inquiry@fasoo.com

396 World Cup Buk-ro, Mapo-gu
Seoul 121-795, Korea
tel: +82-2-300-9000 (Global HQ)

197 State Route 18 South
East Brunswick, NJ 08816
tel: +1-732-955-2333 (NA HQ)
web: www.fasoo.com | email: inquiry@fasoo.com

396 World Cup Buk-ro, Mapo-gu
Seoul 121-795, Korea
tel: +82-2-300-9000 (Global HQ)

Contents

197 State Route 18 South
East Brunswick, NJ 08816
tel: +1-732-955-2333 (NA HQ)
web: www.fasoo.com | email: inquiry@fasoo.com

396 World Cup Buk-ro, Mapo-gu
Seoul 121-795, Korea
tel: +82-2-300-9000 (Global HQ)

Introduction and Executive Summary

Security officers of organizations face a new set of challenges in today's world – particularly those that result from advanced persistent threats (APTs). APTs are able to thwart traditional perimeter security schemes by working patiently over long periods of time to compromise defenses and to manipulate employees to click on familiar looking but malicious websites and emails. Attackers infiltrate corporate networks and discover areas where sensitive data is located, vulnerable areas where confidential data is easiest to steal, which employees are most likely to handle such data, and how sensitive data routinely moves about the organization. For example, attackers can employ "low and slow" techniques of copying a few sensitive files per day over a long period of time once they discover a level of activity that keeps them below the organization's monitoring thresholds.

In the past it was sufficient to guard the organization's IT perimeter with tools such as firewalls, intrusion detection, and data loss prevention (DLP), these techniques are no longer effective by themselves against APTs, other sophisticated attacks and insider threats.

The solution is to add *data-centric security* to traditional perimeter security. Data-centric security includes techniques that protect data as it travels both within the organizational perimeter and beyond, by limiting access to sensitive data according to policies that cover both users and activities. It also includes techniques for determining where sensitive data exists throughout the enterprise, monitoring such data, and analyzing the ways in which users copy, move, and access it over time. It incorporates identity management systems to correlate specific users with activity on sensitive data. By using such techniques on a continuous basis, security officers can not only prevent unauthorized activity automatically but also detect suspicious behavior patterns that suggest APTs and take action before it's too late.

A particular set of data-centric security techniques focuses on unstructured data – on files that are stored in PCs, file servers, and other repositories as well as on the mobile devices that more and more people are using to access enterprise networks – as it is stored, accessed, moved, and used over time.

Data-centric security should also allow users to work without undue interruptions as they pass information among multiple devices. A *people-centric policy* allows for flexibility and dynamic enforceability based on the contexts of content, users, devices, time of day, location, and so on, acknowledging the need for exceptions to predefined policies based on the unpredictable nature of legitimate data creation and usage while relying on advanced analytics to catch excessive deviations from the norm.

This white paper discusses the Data Security Framework, Fasoo's multi-level architecture for combating APTs through data-centric security for unstructured data and people-centric policies. The Data Security Framework consists of three Fasoo solutions, each of which has value on their own but together comprise a comprehensive approach to data-centric security.

The three components of the Data Security Framework are shown in Figure 1. They are:

- **eData Manager**: a data governance solution for **discovering** and **classifying** the constantly changing set of unstructured data based on its association with people and other characteristics, showing the data's security vulnerability and dynamically applying security policies on a continuous basis.
- **Fasoo Enterprise DRM (FED)**: a persistent data security solution for **protecting**, **controlling** and **tracing** data throughout the enterprise – including data at rest, data in use, and data in motion – according to predefined policies based on user, group or role, or dynamically binding existing access control lists of information systems to enable file-level permissions at all times.
- **RiskView**: a risk assessment solution for **monitoring** and **analyzing** users and their activities in using both protected and unprotected files, determining normal levels of activity, and using sophisticated data analysis techniques to discover deviations that may indicate security risks.

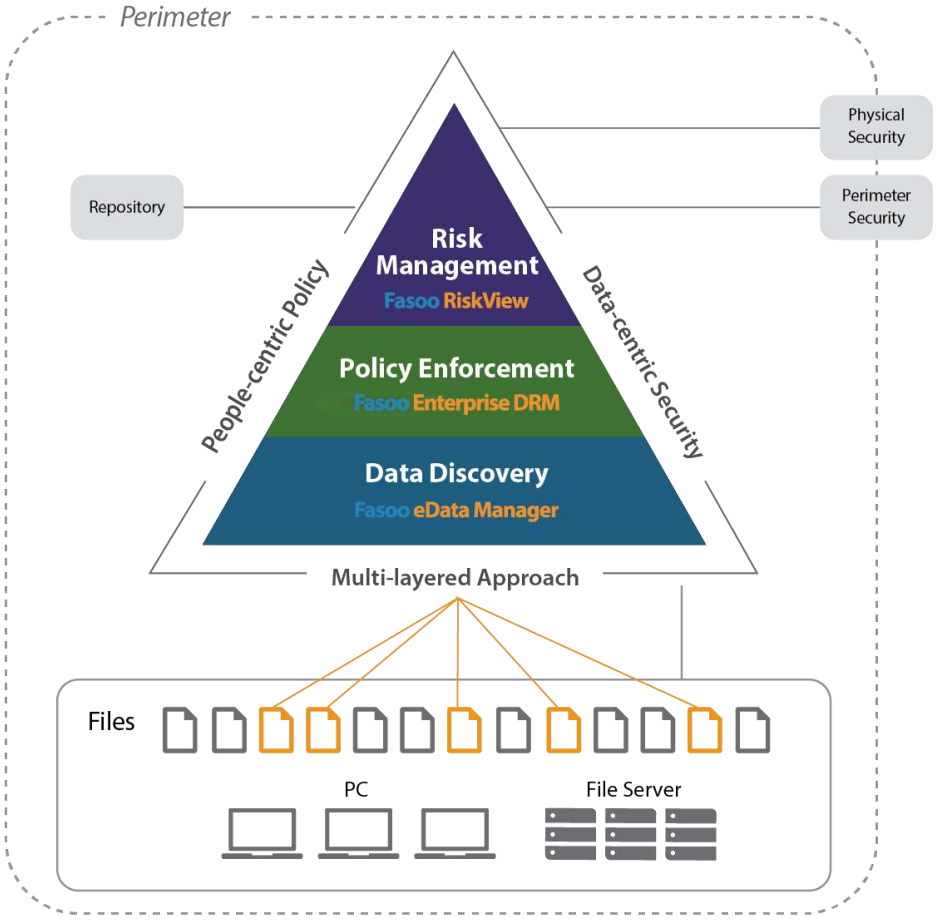

Figure 1: Fasoo Enterprise DRM, eData Manager, and RiskView combine to help organizations achieve data-centric and people-centric security.

Traditional enterprise security includes three common components:

- **Perimeter Security**: techniques to inspect data as it moves across enterprise network boundaries. The most common perimeter security techniques include firewalls, intrusion detection and prevention, and Data Loss Prevention (DLP).
- **Physical Security**: systems that control physical access to a facility and log legitimate entries (and sometimes exits), via keycards, biometrics, or other means.
- **Repositories**: databases, content management systems, and other types of information repositories that have their own data-centric security schemes for information that resides in the repositories.

The Data Security Framework complements these components by providing data-centric security on unstructured data. In the remainder of this white paper, we will discuss each of the components of the Data Security Framework and how they complement one another.

Fasoo Enterprise DRM

The core layer of data-centric security for unstructured data in an enterprise is Enterprise Digital Rights Management (EDRM), also known as Enterprise Rights Management (ERM) or Information Rights Management (IRM).

Fasoo EDRM (FED) enables security officers to set policies that dictate which users can access data on what device, when, and in what context, and enforces those policies through file encryption. FED also allows organizations to track both authorized and unauthorized access to data, send alerts where necessary, and respond to data security triggers to prevent a possible data breach.

Fasoo has been a leader in EDRM since 2000, with more than 1,200 customers globally.

With EDRM, files are *packaged*, meaning they are encrypted along with metadata. Users create, access, and modify them within applications that have been EDRM-enabled, but only if they have the rights to do so. Users or administrators set policies that determine which users can perform which operations on protected files, and under what conditions.

Table 1 lists the rights that FED grants or limits through policies. Policies can apply to specific users, groups of users, locations, time ranges, or any combination of these. They can also be limited to a maximum number of devices per user if desired. FED also enables classes to be defined on files, such as “Confidential” or “Top Secret,” so that policies can be defined on files of each class (e.g., User X has view and print permission on Confidential documents and no permission on Top Secret documents). In addition, it is possible to revoke access rights when required.

Right	Description
View	View or read only
Secure_Save	Save with policies inherited, regardless of file format or name
Secure_Extract	Copy to clipboard for pasting into another protected file
Edit	Edit (includes Secure_Save and Secure_Extract)
Secure_Print	Print with visible watermark (requires Fasoo Secure Print)
Print	Print without visible watermark
Print_Screen	Screen capture (e.g., using PrtSc key or capture tools on a PC)
Extract	Copy to clipboard without protection
Save	Save as un-packaged (decrypted) file

Table 1: Enterprise DRM rights options.

FED is implemented with a combination of server functionality and client software that integrates with common desktop content authoring/viewing applications and makes them EDRM-enabled. When a user opens an EDRM-protected file in an EDRM-enabled application, the DRM functionality within the application sends details of the user, device, location, time, and other information to an FED server. The server checks to see if the user's device has access permissions on the file. If so, the server returns a small encrypted file called a *license* to the EDRM-enabled application. The license contains keys for decrypting the file and a description of the rights to be granted. The application unpacks the license, determines the rights, extracts the keys, and decrypts portions of the file only as necessary to grant the rights.

FED works with a wide variety of applications, including Microsoft Office (Word, Excel, PowerPoint, Project, Visio), Notepad, WordPad, Paint, Adobe Acrobat, Adobe Reader, Adobe Photoshop, Adobe Illustrator, various CAD/CAM applications, and several others. FED enables cross-platform and multi-device support: it runs on iOS and Android as well as Windows operating systems (Fasoo provides view and print access for Mac operating systems; a full OS X version of Fasoo EDRM is under development).

FED integrates with LDAP-based identity management systems, including Microsoft Active Directory, for authenticating user identities; it can also integrate with a wide variety of other authentication schemes. FED can also authenticate users outside of the organization by their email addresses, by means of a patent-pending scheme called Fasoo Email Based Authentication (FEBA).

FED can also integrate with enterprise content management systems (ECM) and other types of repositories that control access to data via access control lists (ACLs) or similar mechanisms. When a user checks a file out of a repository, FED can automatically package the file and set a policy on it that emulates the security policy of the file while in the repository.

While it is possible to define policies for files one at a time, this is not a scalable technique for large enterprises: it takes a significant effort and invites inconsistency as different users apply

different policies, fail to take organization-wide security policies into account, or simply neglect to apply EDRM when necessary.

To get around this limitation, FED includes various tools for applying policies automatically or centrally. For example, an administrator can assign default policies to users, so that whenever a given user creates a file in a supported application, it gets that user's default policy unless the user (or an administrator) overrides it. Default policies can also be defined for user groups or job titles.

As discussed below, eData Manager complements these with additional tools for applying security policies to large numbers of files automatically.

Overcoming Limitations of EDRM

EDRM is an essential component for data-centric security within the enterprise, but it has limitations. It is sometimes not practical to implement or may not fill certain security needs. For example, EDRM is not always a good fit for people-centric security:

- There may be legitimate reasons to grant individual users exceptions to EDRM-enforced security under certain circumstances.
- Conversely, it may be more effort than it is worth to apply persistent security policies to documents that may only need protection in certain limited cases
- Or it may be too restrictive to impose policies that require all documents created by certain users to be protected.

EDRM has additional limitations, such as:

- An organization may have files whose native applications are not EDRM-enabled.
- EDRM by itself is not capable of foreclosing certain types of security risks related to APTs, such as actions by credentialed insiders.

FED has features that overcome some of these limitations, while others are addressed by other components of the Data Security Framework, as explained below.

An FED feature that overcomes the first of these limitations is exceptional policy setting, which lets users request one-time rights on files. The user makes the request with a message to an administrator, who can decide whether to grant the rights. Any such rights are granted on a one-time basis: for example, a user who has view-only rights to a file can request edit/save rights. Once she edits and saves the file, she can no longer do so, unless she requests an exceptional policy again and that is granted.

For applications that are not EDRM-enabled, Fasoo makes an API available for EDRM integration. For example, an organization may have a legacy financial application that generates reports in a proprietary format, and the CISO may decide to plug potential security leaks by controlling access to reports so that only certain types of users can view or print them and that a

smaller group of users can modify them (e.g., for Board of Directors presentations). In that case, integrating FED with the legacy application may be the most reasonable solution.

eData Manager

Fasoo eData Manager is an enterprise classification and security policy management tool that is complementary to EDRM as well as valuable by itself. It scans files throughout the enterprise to find content that is confidential or of high value. It can scan files located within folders and logical drives on PCs – that is, it can scan files on file servers, cloud storage servers, repositories, and anything else that can be mounted as a logical drive or shared folder.

The files that eData Manager scans are those that match templates which specify criteria for files to be scanned. These include:

- Storage devices (fixed or portable), folders, or individual files.
- Filename extensions (file types, e.g. Word document, Excel spreadsheet, PDF).
- Pattern matching within file names or file content, as defined by keywords or regular expression matches. Common uses for this include detection of personally identifiable information (PII) such as credit card numbers, keywords such as “Proprietary,” and names of confidential projects, products, etc.
- FED document classes (see above).
- Users and user groups; this information can be added manually or imported from LDAP identity management systems such as Microsoft Active Directory.

Scans can be set up to take place periodically, such as daily. eData Manager displays statistics on file characteristics that it gathers from scans, which include:

- Files that are unprotected, protected by FED, or protected by eData Manager encryption (see below).
- Sensitive item: files whose names or contents contain matches to regular expressions or keywords, such as PII.
- File extensions (types) of interest, such as Excel spreadsheets or PDFs.
- Files that have been distributed throughout the organization.
- Day-to-day variations in these statistics.

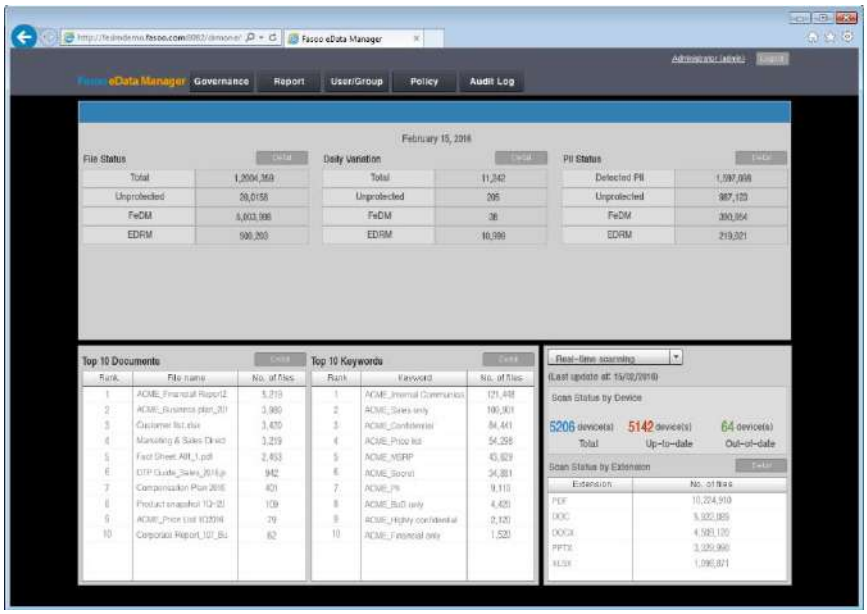

Figure 2: eData Manager view of statistics from scan, showing files that contain PII.

This view is useful to CISOs to determine the type, location, and owners of files of interest throughout the organization. The statistics can be used to help determine security policies, such as files to protect with FED, applications to integrate with FED, locations of files that contain sensitive information, and the time and location of concentrated activity on files with sensitive information.

eData Manager can also be configured to enforce security policies on files that it scans. Policy enforcement methods include:

- Apply FED (if it is installed).
- Assign an FED document class (see above).
- Apply eData Manager encryption (see below).

eData Manager has its own simple encryption scheme, which can be used whether or not the organization uses FED. With eData Manager encryption, files are encrypted, using the same strong AES-256 symmetric-key encryption scheme as FED normally uses, while they are at rest on a user's device or external storage device. When the user opens an eData Manager encrypted file, eData Manager automatically decrypts it for that user through functionality integrated at the operating system (Windows) level. The file remains unencrypted until the next eData Manager scan takes place, when the same rule is invoked and the file is encrypted again.

Even if an organization uses FED, eData Manager encryption can be useful in certain cases, such as if the file is associated with an application that is not integrated with FED (as explained above). In such a case, at least the file is protected most of the time while at rest.

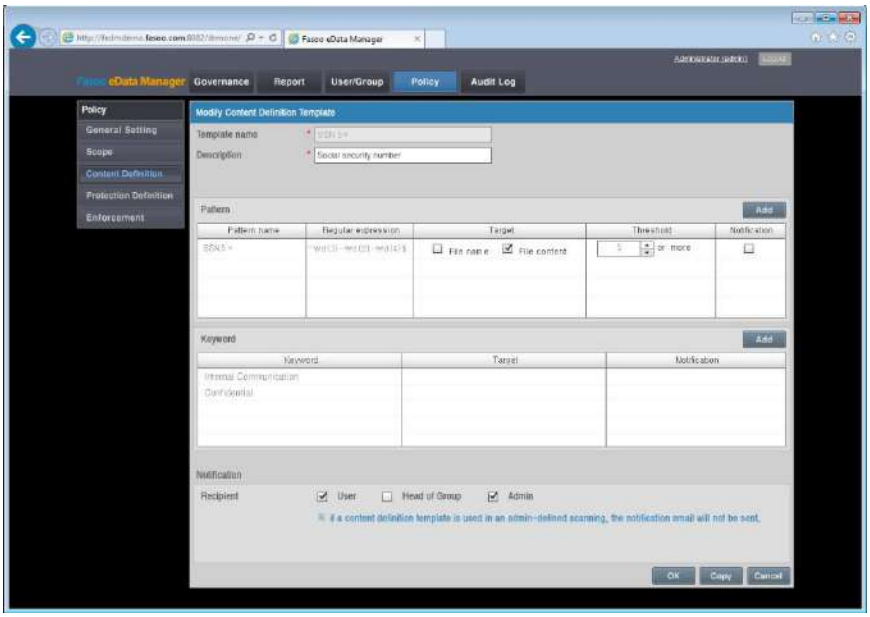

Figure 3: eData Manager can apply file protection automatically to files that meet certain criteria.

RiskView

RiskView is a tool for security administrators that monitors activity related to unstructured data and user activities with confidential data. It gathers information from Fasoo Usage Tracer (the log analysis utility for FED) and eData Manager, and it has APIs that can be configured to import log data from other security technology components, including firewalls, DLP, databases, and even physical security (e.g., entry/exit data from keycard or biometric systems) and employee attendance records.

RiskView includes a decision making framework that security administrators as well as business managers can use to review risky activities and after suitable investigation, decide whether or not to take action to address them.

RiskView applies sophisticated rule-based modeling to the data sources mentioned above, to establish normal patterns of behavior and flag suspicious activities that indicate enough risk to merit concern and potential intervention by business management. The types of activities that RiskView tracks include:

- **Event Anomalies**, such as logins with user IDs of resigned employees, a given user logging in from multiple locations simultaneously, or unauthorized users owning excessive numbers of files containing sensitive data.
- **File Risks**, such as unauthorized users' attempts to decrypt classified files.
- **User Risks**, such as users decrypting dormant files more frequently than usual, printing more files than usual after regular business hours, or sending files to external recipients that are of different types or formats than usual.

As shown in Figure 4, RiskView displays a dashboard showing these risks, their sources and magnitudes, and steps being taken to analyze and act on them.

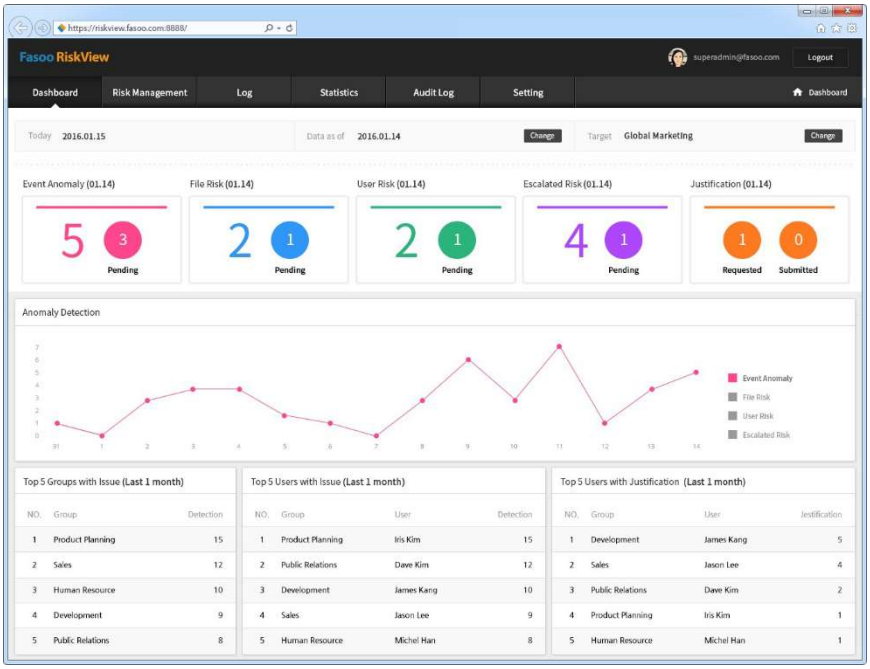

Figure 4: the RiskView Dashboard tracks three types of suspicious activities and steps taken to address them.

RiskView enables business security administrators to drill down on suspicious activities and send messages to business managers asking them to either justify the activity or recommend remedial actions. For example, Figure 5 shows that a particular user has been decrypting dormant files more frequently than usual. Figure 6 shows detailed data about the suspicious activity and recommended remediation steps. Finally, Figure 7 shows that the security administrator has chosen to send a request for justification to the user.

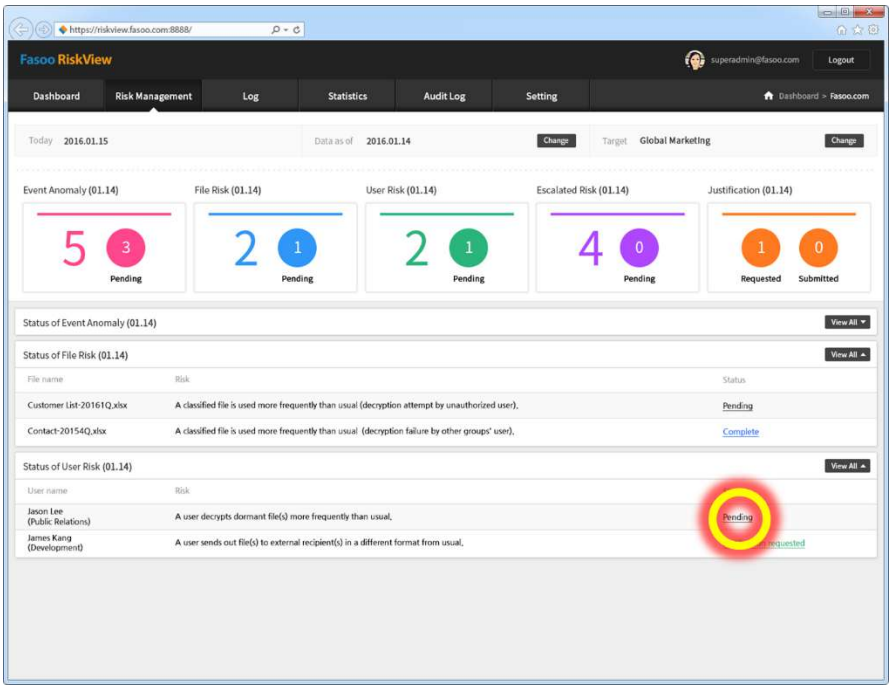

Figure 5: Detailed view of User Risks showing a user who has been decrypting dormant files more frequently than usual.

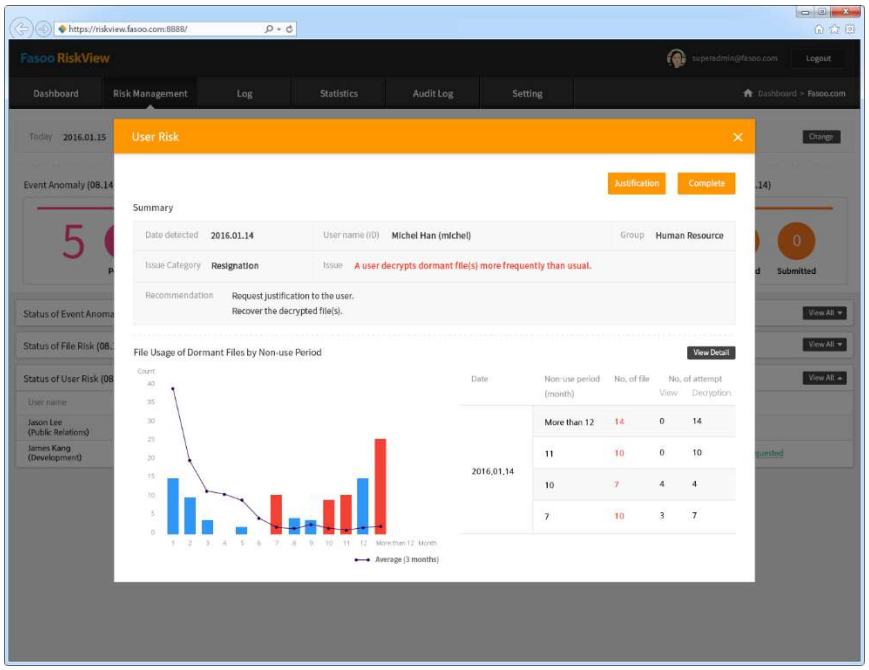

Figure 6: Detail view of a particular source of User Risk, with recommendations for steps to be taken in remediation.

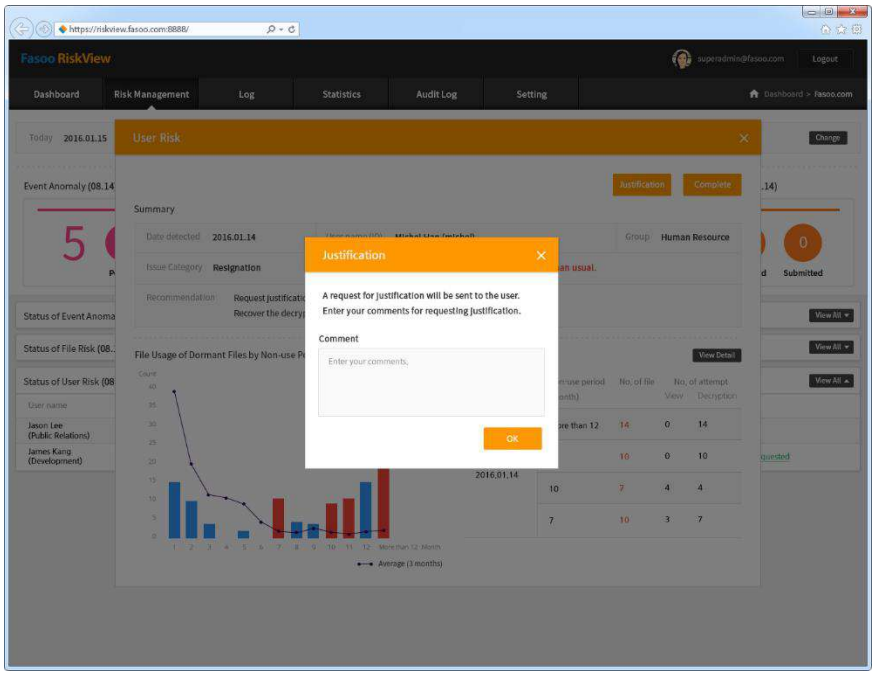

Figure 7 : a security administrator sends a request for justification to the user whose activity RiskView has determined to be suspicious.

RiskView also lets security administrators set up rules for escalating issues automatically whenever they come up or on a case-by-case basis. As an example, Figure 8 shows a User Risk detected from suspicious activity by an employee who has resigned. Figure 9 shows that the user printed out excessive numbers of documents after hours and decrypted files containing sensitive data through self-approval. The employee's manager decides to escalate the issue (Figure 10), which will result in appropriate action being taken against the employee.

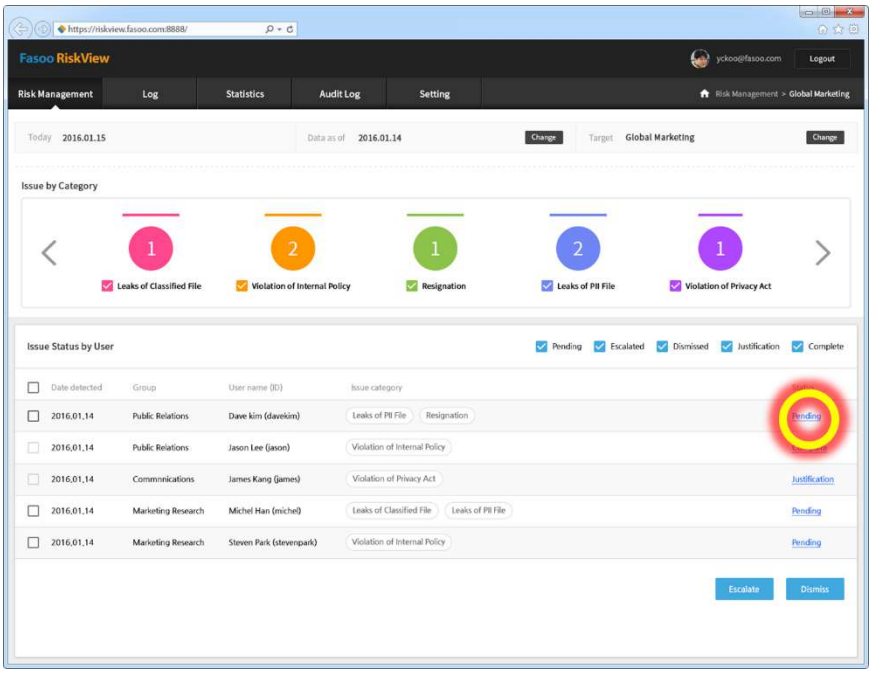

Figure 8: RiskView detects suspicious activity by an employee who has resigned.

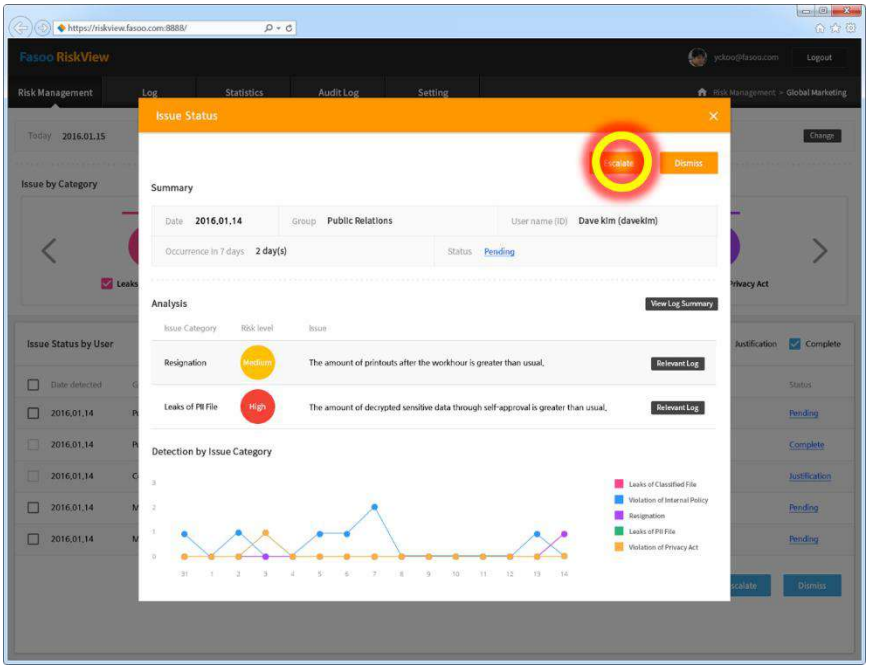

Figure 9: detailed view of activities that caused RiskView to raise a User Risk: an employee resigns, then prints documents after hours and decrypts files containing sensitive information.

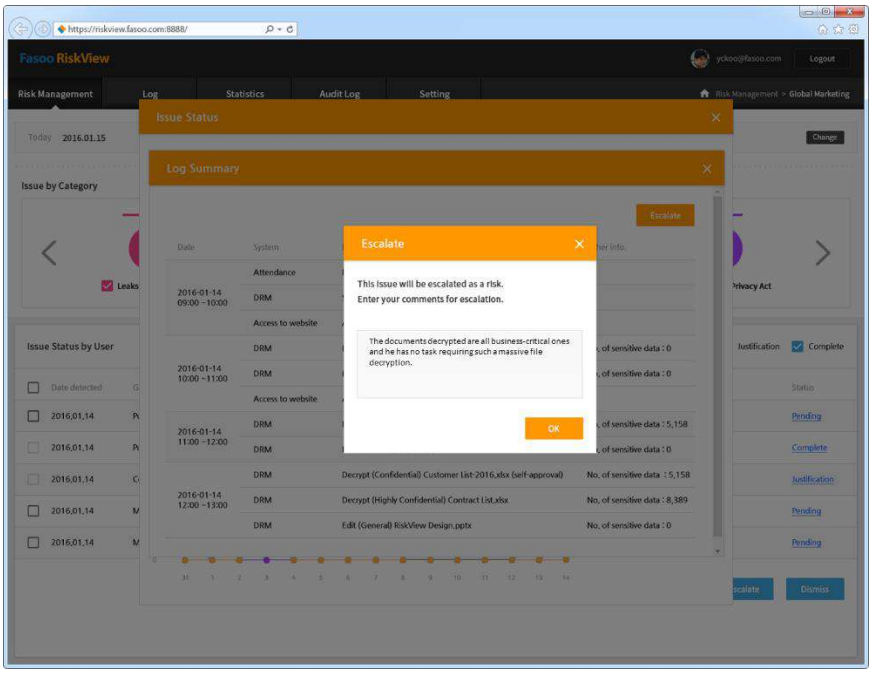

Figure 10: the business manager decides to escalate the incident, which will cause action to be taken against the employee.

All of these notifications and actions relate to activity on unstructured data, most of which takes place inside the technical and physical enterprise perimeters. In other words, actions enabled by RiskView are part of addressing APTs through data-centric security with people-centric policies.

Examples

Here are some examples of how the three components of the Fasoo Data Security Framework interact to implement data-centric security with people-centric policies.

Emailed File Attachment

A user receives an email message with sensitive information contained in a file attachment and saves the attachment to a folder on her PC. Under normal circumstances, nothing would happen to protect this file or monitor access to it. If the organization used EDRM, the user would have to open the file in an EDRM-enabled application and save it as a protected file, applying the appropriate set of rights to it. It is not practical to rely on all employees to follow this process.

With the Data Security Framework, eData Manager can detect the presence of this file in the location where the user saved it. By analyzing the contents of the file and applying rules, eData Manager can determine whether the file should be packaged with FED or simply encrypted with eData Manager encryption. At that point, the file is protected if required by policy. eData

Manager can be configured to recognize files sent from certain outside organizations as email attachments and control them in a consistent manner.

Whether or not eData Manager decides to encrypt the file, RiskView will monitor its usage – the number of times it is moved or copied and to which other users, devices, or locations. It will compare the usage patterns for this file against typical usage patterns for files with similar types of content and flag any anomalies. In any case, the Data Security Framework takes all these possible actions automatically without any user intervention.

Ad Hoc Third-Party Access to Sensitive Information

A salesperson prepares a confidential price quote and wants to send it to a prospective customer. Under normal circumstances, the salesperson would send the file through email as a plain, unprotected PDF. It would obviously be inappropriate for a data loss prevention (DLP) scheme to prevent this file from exiting the enterprise perimeter, yet the information in it should be protected.

The Data Security Framework can automatically determine the sensitivity of this document from pattern-matching that suggests the price quote is confidential. It can be configured to encrypt the document and set a temporary usage policy. Instructions on how to open the document (and any necessary tools) can be sent to the customer. That way, the customer can view and possibly print the price quote during its validity period (e.g., 30 days) but not thereafter.

Automated Policy Exceptions

A product team leader has a PC with EDRM-enabled applications, but because many of the documents he creates are not confidential, his PC is not configured to protect every file with EDRM. The team leader creates a datasheet for a new product before it is released. The datasheet is shared with team members and certain other employees, but the information is to be treated as confidential until the product goes on the market.

In a case like this, an exception has to be made for the established policy of allowing the team leader to create unencrypted documents. This can be done automatically by eData Manager, which can find the document in a daily scan because it contains language that matches a list of keywords that imply sensitive information. For such documents, eData Manager is configured to package the file with FED.

In this situation, in addition to the protection afforded by FED, RiskView can detect suspicious activities on the file, such as copies being made to external storage devices. (Here, a DLP solution is complementarily useful for ensuring that the datasheet can’t be sent outside of the perimeter via email or uploaded to cloud storage.) Such activity on files containing sensitive information can imply an insider threat that requires management attention.

Conclusion

To implement data-centric security with unstructured data and address APTs, security officers need to perform several tasks in relation to files that contain sensitive information, wherever it may be throughout the enterprise. Table 2 shows these required tasks; it also shows how each of the components of the Fasoo Data Security Framework enable them. Note once again that while all of these contribute to information security, traditional perimeter and repository security techniques apply to them only in very limited ways.

Data-centric Security Requirements	EDRM	eData Manager	RiskView
Determining that a file contains confidential information		☑	
Classifying a file as confidential reactively		☑	
Classifying a file as confidential proactively	☑		
Setting normal security policies on a confidential file	☑		
Setting security policy exceptions on files containing confidential information		☑	
Ensuring that only certain users can perform certain operations on a confidential file	☑		
Identifying a user who legitimately needs to access a confidential file on an ad hoc basis	☑		
Determining highest-risk areas of the company regarding concentrations of sensitive information		☑	
Identifying risky activities related to files			☑
Reviewing risky activities to determine whether action is necessary			☑
Setting up rules to take action on risky activities automatically			☑

Table 2: Data Security Framework components' applicability to data-centric security.

The result of applying these tasks is data-centric security, implemented through people-centric policies, which are sufficient to address the challenges posed by advanced persistent threats (APT). The components of the Fasoo Data Security Framework – eData Manager, Fasoo EDRM, and RiskView each enable a subset of data-centric security, but together they enable the highest level of protection against APT.

To learn more, please contact Fasoo at inquiry@fasoo.com.