SANGFOR | SANGFOR SECURITY | Sangfor IAG

THE SANGFOR APPROACH TO DATA LOSS PREVENTION

SANGFOR

CONTENT

1 Introduction

Sangfor Data Leak Prevention Solution using Internet Access Gateway audits all user file transmission behavior while intercepting and blocking unauthorized file transfers. This whitepaper discusses the IAG DLP Audit module for auditing file transmission activity and the Data Loss Prevention Management and Control module that interdicts unauthorized file transmission.

2 Data Loss Prevention Audit

Employees may intentionally or unintentionally send confidential information out of the organization/to the Internet during their work, resulting in data leaks. To detect, prevent, and trace such incidents, it is crucial to audit and record the file transmission behavior of employees and the content of transmitted files. This is done in the Sangfor Internet Access Gateway (IAG) Data Loss Prevention (DLP) Audit module.

2.1 Capability Introduction

The Sangfor Internet Access Gateway (IAG) Data Loss Prevention (DLP) Audit module monitors various transmission channels used to transmit files out of the organization from endpoint devices. These channels include applications, browsers, peripherals, and printers. In addition to recording outbound file transmission behavior, Sangfor IAG also saves outgoing files to facilitate future evidence collection and traceability.

Flexible DLP audit policies can be configured according to specific needs. Customization options include time, user objects, and file types. Sangfor IAG also supports capturing screenshots of outgoing file transmissions. When a user is detected sending a file out of the network, Sangfor IAG automatically takes a screenshot of the user's screen. To ensure a more complete evidence chain, Sangfor IAG takes three screenshots at certain intervals to provide context for the outgoing file.

By default, audit policies become inactive after an endpoint goes offline. However, an option is available allowing policies to remain active even when an endpoint is offline, enabling stricter management.

2.2 Capability Coverage

The DLP Audit module supports a wide variety of file types and outgoing transmission channels (applications) to minimize the risk of data leaks.

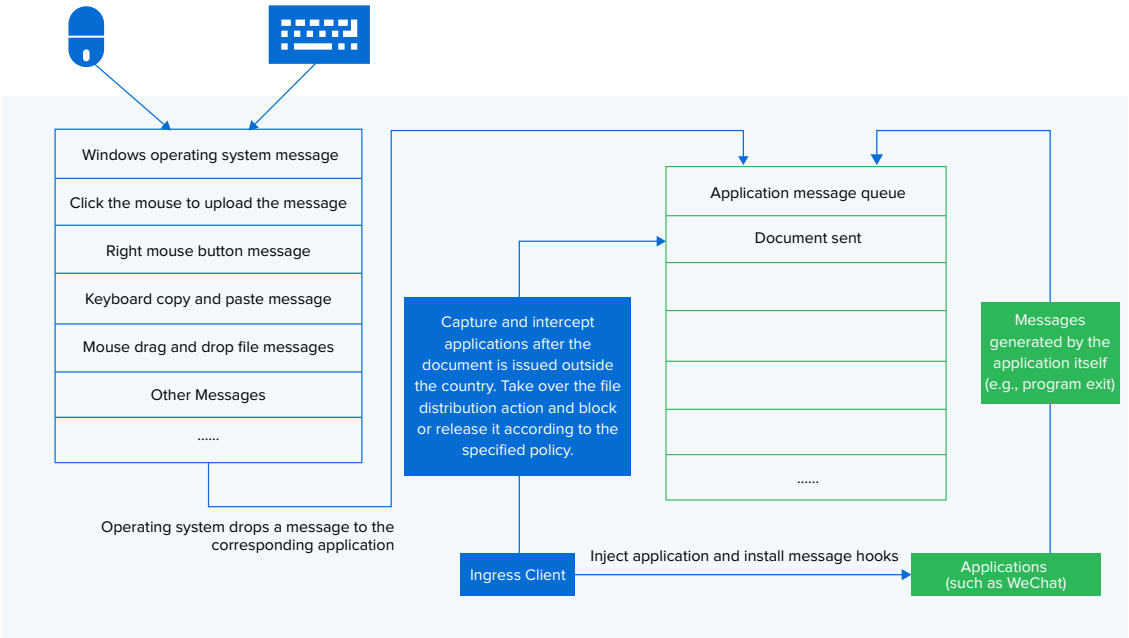
File Types: Supported file types include video, audio, image, text files, compressed files, application files, Office documents, and engineering and manufacturing documents.

Outgoing Channels: Supported channels include browsers, instant messaging applications, email clients, note-taking applications, cloud storage services, remote access tools, video conferencing applications, and file transfer tools.

Instant messaging applications	WeChat, WeCom, QQ, DingTalk, Feishu, etc.
Email clients	Outlook, NetEase Mail Master, Foxmail, etc.
Note-taking applications	Evernote, OneNote, Youdao Cloud Notes, etc.
Cloud storage services	Baidu Netdisk, 360Secure cloud disk, Alibaba Cloud Drive, etc.
Browsers	Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Sogou Browser, etc.
Remote access tools	TeamViewer, SunLogin, etc.
Video conferencing applications	Zoom, Tencent Meeting, etc.
File transfer tools	WinSCP, XFTP, FileZilla, etc.
Decryption behavior	IP-guard, Huatu, etc.
Peripheral behavior	USB drives, external hard drives, etc.

Sangfor IAG continuously updates its application database with new signatures of applications and file types. Users can access this database using the "Application Signature Database" module. Additionally, users can use the "Custom Desktop Apps" feature to add custom applications not included in the database. Refer to the Sangfor IAG user manual for more information.

2.3 Technical Principles



Users typically transmit files from their endpoints through the following actions:

Upload: Users click an upload button, which opens a local Windows folder path or a file selection box in a Windows application or browser, and select the file to send.

Copy and Paste: Users copy a file from a local Windows folder and then paste it into the sending or editing interface of a Windows application to edit the file or send it.

Drag and Drop: Users select a file from a local Windows folder and drag it to a specific location to send.

Right-Click and Send: Some Windows applications add a "Send to" option in the right-click context menu. Users can send a file by right-clicking and selecting this option.

When users perform these file transmission actions in Windows applications, the operating system generates corresponding Windows messages, i.e., file upload messages, file copy-and-paste messages, etc. These messages are processed by the Windows Message Driver and are essential for the proper functioning of Windows applications.

Using Windows message interception technology (service hook), Sangfor IAG installs message hooks on designated applications (such as WeChat) at the application layer of the Windows operating system.

When a hooked application sends a file, Sangfor IAG intercepts the corresponding Windows message and processes it according to data loss prevention audit policies.

3 Data Loss Prevention Management and Control

While auditing outbound file transmissions provides a fundamental layer of data security, it is not sufficient for organizations with stricter data management requirements. For these entities, more proactive measures, like intercepting and blocking unauthorized file transfers, are essential to ensure that sensitive files are not leaked.

3.1 Capability Introduction

Sangfor IAG DLP Management and Control policies can be configured according to specific needs. Customization options include time, user objects, file size, file name, file type, and file characteristics. A DLP dialog box will appear in the Windows client to notify users when actions are denied. As with DLP auditing, files can be automatically archived when sent out, and policies can be configured to remain active when endpoints are offline.

Capabilities are divided into two levels: Channel Level and File Level
01 The channel level controls outgoing communication channels. When users send files out through specific channels, such as Viber, the behavior messages of outgoing files are intercepted when a policy is triggered. This control measure does not affect the normal use of the channel. In the case of Viber, users can still chat and make video calls normally.
02 The file level provides a more granular level of control, allowing the configuration of policies based on file attributes. Supported attributes include file size, file name, and file type.

3.2 Capability Coverage

Supported file types and outgoing channels of the DLP Management and Control module are the same as those of the DLP Audit module (refer to Section 2.2 for details). The following are the unique capabilities of the DLP Management and Control module:

- **File size matching:** Identifies the size of outgoing files.
- **File name matching:** Identifies the name of outgoing files.
- **File type matching:** Identifies the type of outgoing files. File type identification is based on both file extensions and file characteristics.

Control actions are executed once a policy is triggered. Common actions include:

- **Allow:** Users can send files out normally. To record this behavior and the file content, an audit policy must be configured.
- **Block:** The file transfer is blocked, and users are not able to send files.
- Endpoint Notification: A notification pops up in the bottom right corner of the user's screen. The content of the notification can be customized by the administrator.

As with the DLP Audit module, the DLP Management and Control Module has access to both the Application Signature Database Module and Custom Desktop Apps feature (refer to Section 2.2 for details).

3.3 Technical Principles

The technical principles of DLP Management and Control are similar to those of DLP Audit. Windows messages for file transmission actions, including upload, drag and drop, copy and paste, and right-click and send, are intercepted using Windows message interception technology (service hook). After the interception, Sangfor IAG processes the messages according to data loss prevention control policies.

FTID (File Type Identification): The endpoint DLP rule base contains an FTID fingerprint database. The characteristics of each file type are unique and are matched against the FTID fingerprint database for identification, including:

Name	The type of file.
Pos	The key in "pos" represents the offset position from the beginning of the file. Its value represents the characteristic string to be matched for each file type starting from the offset position.
Patt	The attributes of the file type. Each file type must contain an attribute string when matching, and the position of the string is not fixed.

To create the FTID fingerprint database, we collect samples of various file types, read the content of the hard disk sector from the sample file header, and use algorithms like prefix tree, KMP (Knuth-Morris-Pratt), and multi-pattern matching to construct fingerprints of various file types according to the FTID fingerprint database structure.

By extracting features from outgoing files and matching them against specific fields and parameters in the FITD fingerprint database, the Sangfor IAG DLP Management and Control module determines the true file type of outgoing files. This means that changing the extension of a file does not allow it to bypass this method of detection.

File Size and File Name Recognition: Sangfor IAG reads the file size and file name by calling the Windows system API interface. It then compares them with the file sizes and file names configured in the sensitive file identification rules. If a rule is met, the outgoing file will either be blocked from transmission or allowed according to the configured control policy.

SANGFOR

Make Your Digital Transformation Simpler and Secure

Website: www.sangfor.com

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com