SPIRION

Spirion Extensions

Finding Unsecured Videoconference Recordings on Workstations

Introduction

In March 2020, the global workforce began a large-scale migration from offices to home, and many organizations used video conference services like Zoom, GoToMeeting, and Cisco WebEx to conduct virtual meetings. In fact, according to litigation involving Zoom Communications, Inc., "the number of daily meeting participants across Zoom's services has increased from 10 million at the end of 2019 to 200 million" by mid-April 2020.[1]

These meetings, which are often recorded, can contain sensitive data: healthcare, financials, or intellectual property discussions, for example. It's not always clear where these recordings are housed, and people may forget that they exist. These recordings create a new threat vector that Spirion can help manage.

The Problem That Spirion Solves

Using Spirion to locate and protect conference recordings:

- **Advances compliance with a range of data protection laws**
- **Assists in protecting intellectual propertyl such as trade secrets and privileged or confidential communications**
- **Minimizes the prospect of having to report losing these recordings as part of a sensitive data breach.**

Using Spirion to manage virtual meeting recordings also helps you maintain compliance with contractual obligations regarding sensitive data protection.

United States' Data Protection Laws Implicated

While there is no generally-applicable federal data protection law, multiple sectoral privacy laws protect a wide (and growing) range of personal data. All of these laws apply to virtual conferencing:

HIPAA (healthcare) HIPAA protects 18 categories of personal information, called Protected Health Information or PHI. The U.S. Dept. of Health and Human Services' (DHHS) Office of Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy Rule and Security Rule. In March 2020, OCR stated that certain non-public teleconferencing providers would be permitted to be used for tele-medicine.[2] Among those providers are Zoom for Healthcare and GoToMeeting.

GLBA (financial) GLBA protects personal information of a financial nature, referred to as nonpublic information (NPI). Like HIPAA, GLBA has a Privacy Rule and Security Rule prescribing protections for NPI. GLBA is enforced by the U.S. Federal Trade Commission and the states' attorneys general.

FERPA (student) FERPA protects the "education records" of students and is enforced by the U.S. Department of Education. Under that definition, recorded conferences between the student and faculty or administration would likely be included.

COPPA (children) COPPA protects the personal information of children under 13. Persistent online identifiers, geolocation information, and Social Security numbers are included in the definition of personal information. COPPA is enforced by the FTC and "applies to personal information collected online by operators of both websites and online services."[3]

[1] Kondrat et al v. Zoom Communications, Inc., Case 5:20-cv-02520-LHK (April 13, 2020), at 5.
[2] See U.S. Dept. of Health and Human Services, Office of Civil Rights, Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, found at https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.
[3] The Federal Trade Commission, COMPLYING WITH COPPA: FREQUENTLY ASKED QUESTIONS, found at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#:~:text=COPPA%20is%20meant%20to%20give,of%20personal%20information%20from%20children.

State law All individual U.S. states have data protection laws, with some being particularly restrictive, such as California's Consumer Privacy Act of 2018. California also has an equivalent to HIPAA (Confidentiality of Medical Information Act ot CMIA) and one for GLBA (Financial Information Privacy Act or FIPA).

Other U.S. Protections for Sensitive or Personal Data

Uniform Trade Secrets Act The Uniform Trade Secrets Act (UTSA) is a state-level statute that protects certain intellectual property, defined as information that includes "a formula, pattern, compilation, program, device, method, technique, or process" and which has independent economic value and is protected by reasonable efforts on the part of the information owner. Trade secrets are especially brittle, since once a trade secret is improperly revealed, the owner of the secret irrevocably loses protection.

Attorney-client privilege Attorney-client privilege is an Anglo-American legal tradition that protects communications from a client to his/her attorney. This tradition has been codified in state and federal law. Like trade secrets, attorney-client privileged information must be protected by reasonable means and if improperly revealed, the privilege is lost.

Business associate agreements Business associate agreements (BAAs) are contracts between healthcare institutions and those that provide services to them. Such service providers (e.g., cloud service providers), agree to implement technical and other controls to protect PHI and to adhere to mandates set forth in HIPAA and state equivalents.

Other Data Protection Regimes

EU GDPR The EU General Data Protection Regulation (GDPR) protect the personal data of individuals inside the boundaries of the EU, including those of residents and tourists. Under it, even a phone call or video conference from the EU to outside the EU that incorporates personal information is considered a "transfer" of that information (e.g., an HR professional in London discussing the discipline of an employee to a supervisor or colleague in New York). Even the viewing of personal information from outside of the EU qualifies as a transfer. The GDPR restricts the transfer of personal data outside of the EU to those countries with essentially equivalent data protection regimes or via the use of Standard Contract Clauses, the latter of which will list the technical controls employed to protect the transfer of personal information.

Requirements

Spirion version 11.0 or higher
Spirion Agent installed on the workstations you wish to scan
Remote network access so the Spirion Agent can connect to the Spirion web server

NOTE: This guide is meant to be used by a trained Spirion Administrator on a Spirion implementation that uses our Best Practice Policies correctly managed for your environment. Please ensure you test this procedure on a small subset before implementing it in production. If you need help, reach out to our Support team or your Customer Success Manager.

Step 1: Check Default Base System Policy

First, make sure your Default Base System Policy allows Scheduled Task policies to override it.

1. Open your Default base system policy.
2. Check the box next to **Allow settings specified in Scheduled Task policies to take precedence over settings in this policy** (see Figure 1).
3. Save the policy.

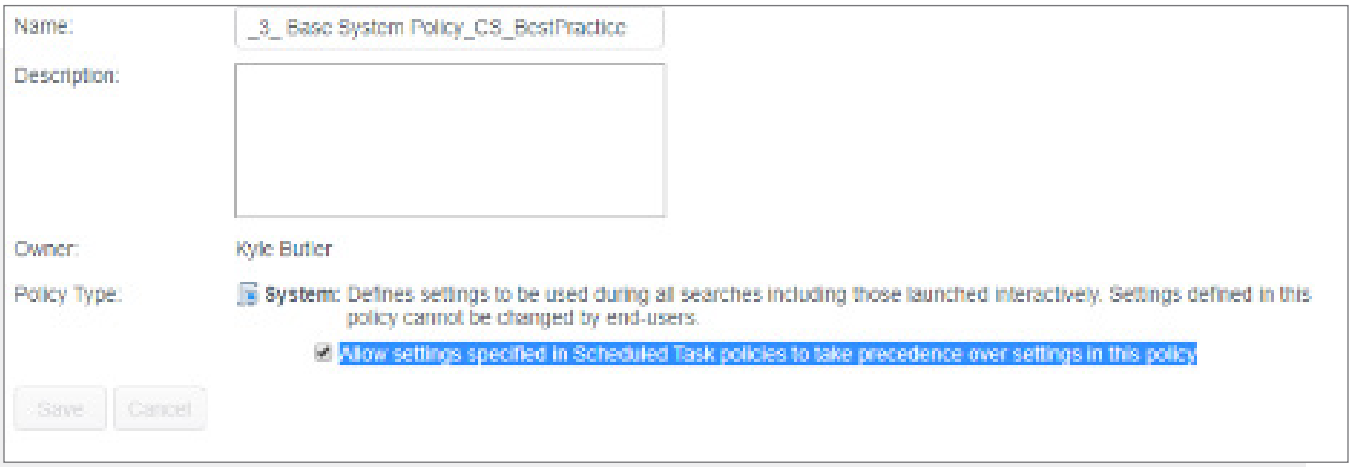

Figure 1: Base System Policy Configuration

Step 2: Create Custom Sensitive Data Types

Next, you need to create a custom Sensitive Data Definition using regular expressions that can identify your video conferencing recordings.

In this example, we create a Definition that identifies Zoom meeting recordings.

1. Navigate to the **Admin** tab in the Console.
2. Select **Sensitive Data Types** on the side menu.
3. Click the **Add** button in the Ribbon bar.
4. Create a Regular Expression sensitive data type that can locate "Zoom" *(see Figure 2).*
5. **Save** the Regular Expression.
6. Repeat the process to create a regular expression as shown in Figure 3, which identifies the .mp4, .mp3, or .m4a file types Zoom uses.

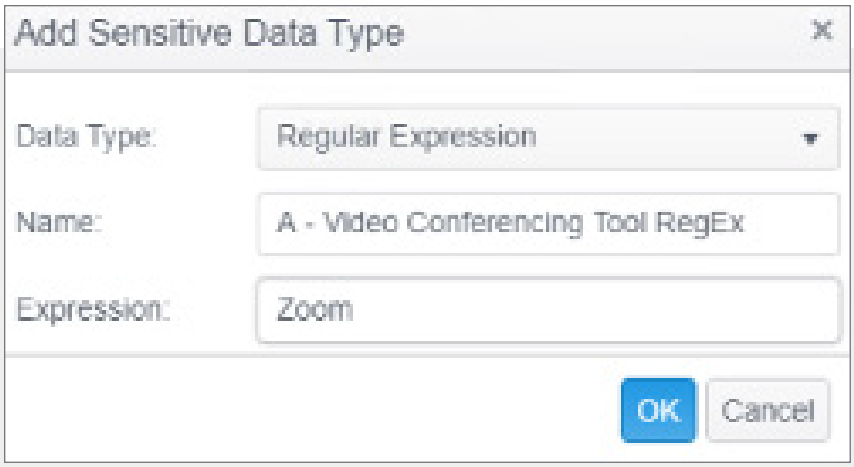

Figure 2: Regular Expression for "Zoom"

Note: Though this Regular Expression could also be created as a Keyword data type, we recommend the Regular Expression because it is not case-sensitive.

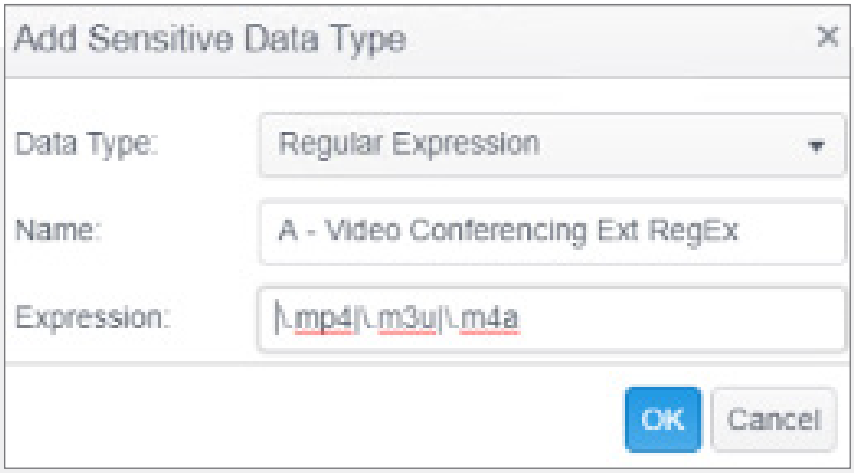

Figure 3: Regular Expression for mp4, mp3, or m4a file types

Note: The Regular Expression above translates to ".mp4 or .m3u or .m4a"

Step 3: Create Custom Sensitive Data Definition

Next, you should combine the two Regular Expressions into a Sensitive Data Definition.

1. Navigate to the **Admin** tab in the Console.
2. Select **Sensitive Data Types** on the side menu.
3. Click the **Add** button in the Ribbon bar.
4. Name the Sensitive Data Definition as shown in *Figure 4* below.

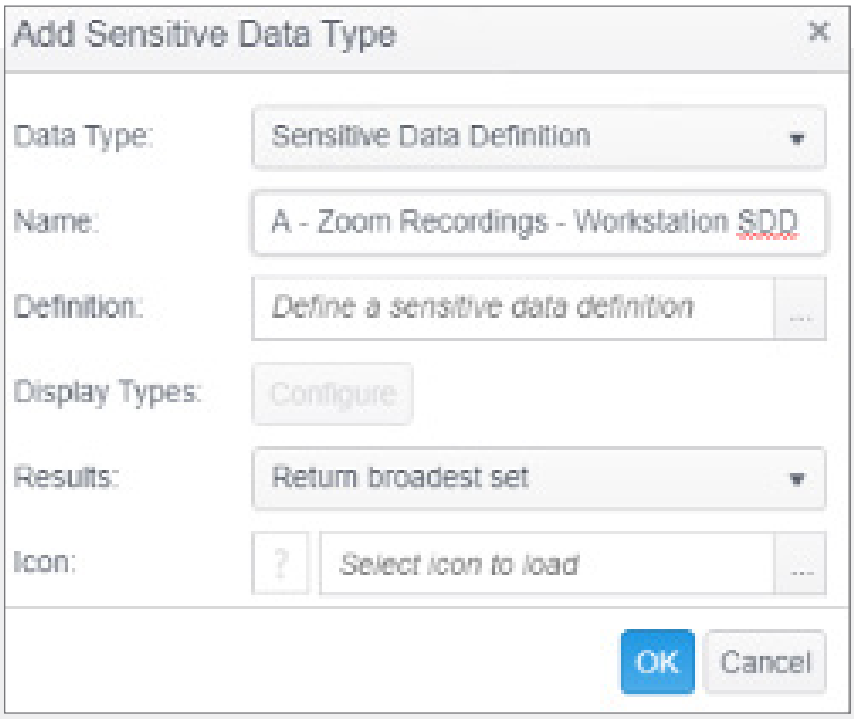

Figure 4: Sensitive Data Type Name and Results

5. Create the definition to use the two Sensitive Data Types you created earlier, as shown in *Figure 5* below.

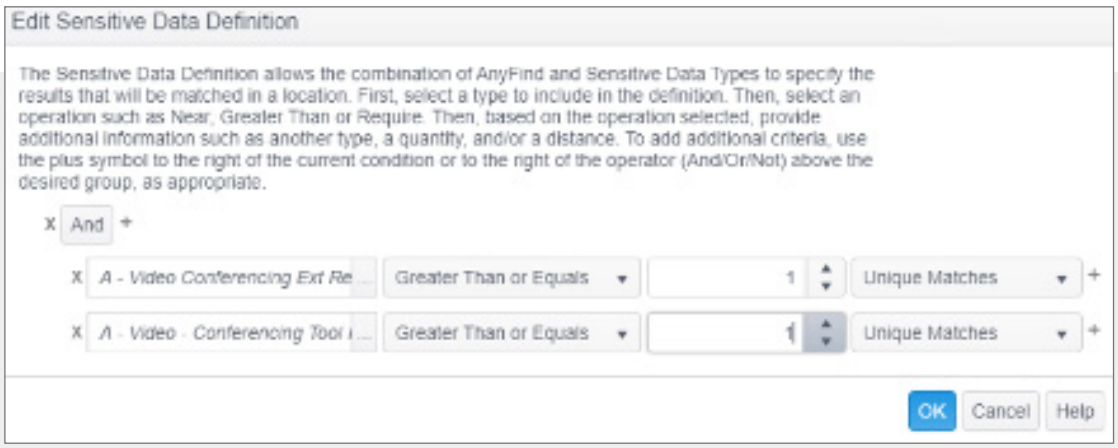

Figure 5: Sensitive Data Definition

Step 4: Create and Configure Scheduled Task Policy

Now that you have a Sensitive Data Definition that can locate Zoom recordings, you should create a scheduled task policy to scan for the recordings.

1. In the Spirion Console, navigate to the **Policies** tab.
2. Click the **Policy** button and select **Create New.**
3. Name the policy in a meaningful way, such as "Local Zoom Recording Workstation Search."
4. Set your policy to be a **Scheduled Task Policy.**
5. Under the **Endpoints** section of the policy, select the endpoints you'd like to search.
6. Under the **Settings** section of policy, set the following under **Locations/Files/:**

   • **EnableCompressedfiles:** set to *Disable*
   • **EnableFiles:** set to *Enable File Search*
   • **FileAnalysisType:** set to *Analyze file name, Analyze file metadata*. Do not select file content
   • **FileLocations:** set to *Custom*
   • **FileTypeSearchOption:** set to *All*
   • **UseAdvancedFileIdenfitication:** set to *All Files*
   • Finally, *Enable* **Locations/Files** itself.

Your Policy settings should have a number of settings under Files that are now green *(see Figure 6)*.

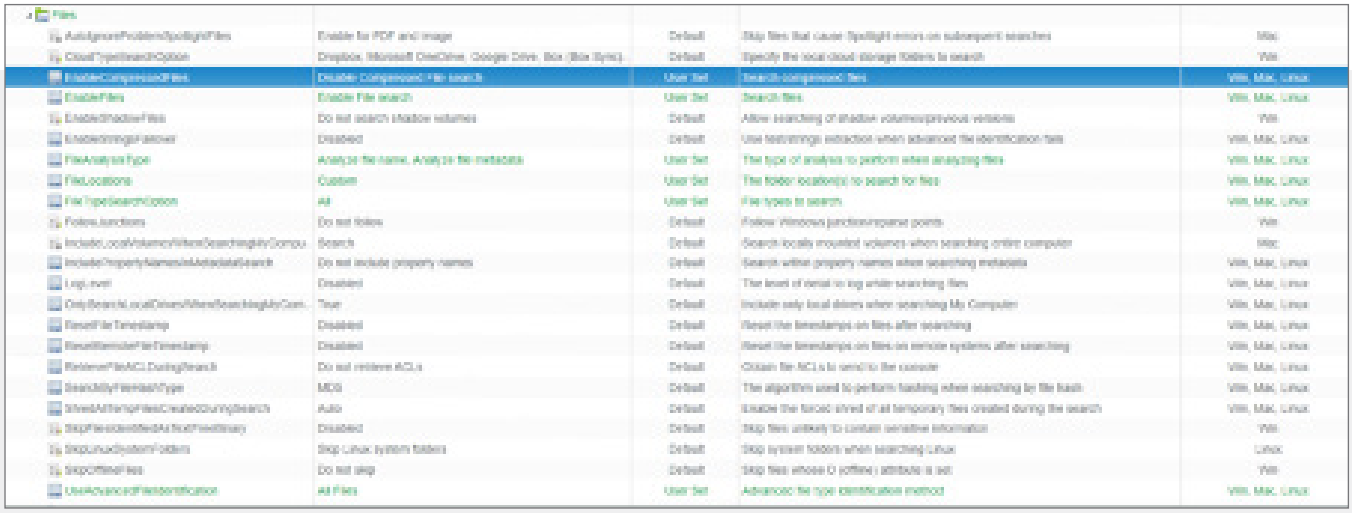

Figure 6: Locations/Files Settings

7. Under the **Settings** section of policy, set the following under **Performance**:

   • **MaxFileSize:** set to *1047527424 (note: Spirion has a hard limit of files under 1 GB)*
   • **(Optional) CreateData/EnableFileRestriction:** set to *Enabled*
   • **(Optional) CreateData/FileRestrictionDataNewerThan:** set to you're your workforce went remote

Date Formatting
YYYYMMDDTHHMM

YYYY: 4 digit year
MM: 2 digit month (01–12)
DD: 2 digit day (01–31)
T: (capital T must be present in this position)
HH: 2 digit hour (00–23)
MM: 2 digit minute (00–59)

Translations
2/4/2018 2:30 PM = 20180204T1430
11/15/2017 6:15 AM = 20171115T0615
8/25/1995 12:00 AM = 19950825T0000

Your Policy settings should have a number of settings under Performance that are now green *(see Figure 7)*.

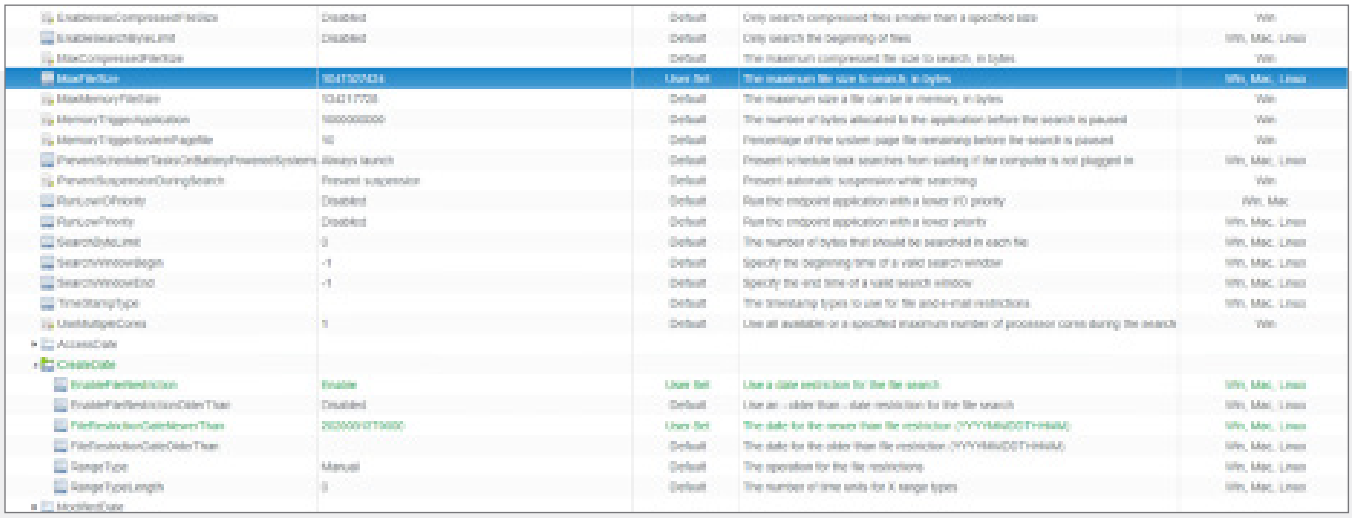

Figure 7: Performance Settings

8. Under the **Settings** section of policy, set the following under **SensitiveDataEngine:**

   • **EnableSensitiveDataDefinitions:** set to Enabled *(see Figure 8)*

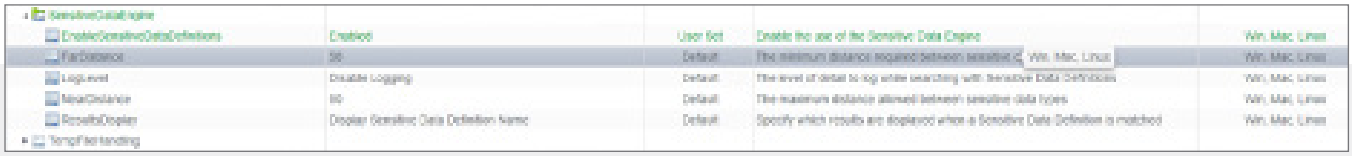

Figure 8: SensitiveDataEngine Settings

9. Under the **Search Locations** section of policy, select Custom Folders and add the following folders:

   • **C:\Users** – Set the Scope to *Include* in Search
   • **C:\Users*\AppData\Local\Temp** – Set the Scope to Exclude from Search

10. Finally, under the Sensitive Data types in the Scheduled Task, find and select the finished SDD you created for this process.

Step 4: Create and Configure Scheduled Task Policy

Finally, you should schedule this scheduled task policy to run and review the results. Be sure to do the following:

- Start with a limited set of endpoints to test the policy
- Set your task to run as soon as possible and to stop any other instances of Spirion
- Once you have tested and configured the policy as needed, roll out to the rest of your workstations

Legal Disclaimer

This solution shown herein is based on a standard system configuration, which may be different from the system in your computing environment. Additional customization of your system may be required. Please contact Spirion Support for assistance.

There is no guarantee or warranty of any kind that this solution will perform as documented herein in your environment.