THETALAKE

Data Loss Protection for Your Collaboration Platforms

Modern collaboration tools that enable video, voice, and chat engagement are at the forefront of how employees communicate and share information today. Left unmonitored, they also create an avenue for intentional and unintentional data loss that can lead directly to fines and theft as well as competitive disadvantage while negatively impacting an organization's brand trust and bottom line.

With the inherent rich capabilities and flexibility provided by collaboration platforms, they also introduce a wide range of ways that data loss can occur. During a typical one-hour video conference meeting, a wide range of confidential topics may be discussed, data shared on screen, and files transferred over chat. All of it bypasses a company's traditional data protection tools.

Solution Overview

Theta Lake is a purpose-built solution that protects your organization from unknown confidential information exposure during collaboration sessions across audio, video, and chat communication instances. With Theta Lake, you gain an automated and simple solution to mitigate the depth and breadth of private data exposure risks that can occur in unified collaboration:

- ✓ Captures and detects all content spoken, shown, shared, and typed in chat, video, and voice including analysis of files uploaded and shared
- ✓ Assesses risks based on both the dialogue and the content or files shared or exposed
- ✓ Detects risks of cloud-based or corporate applications shared within meetings as well as the actual risk of content displayed from those apps

With hundreds of detections and search filters for identifying confidential information, private data, and information security risks along with robust workflow, alerting, and remediation features, Theta Lake eliminates this critical data loss blind spot, empowering your organization to fully utilize all features and functionality of modern communication platforms, without the worry.

Solution Capabilities

Data privacy risk detection for every collaboration use case

Powered by advanced deep learning and behavior analysis, Theta Lake detects real and relevant data privacy risks in what is spoken, shown, and shared. This includes sharing data-rich desktop and browser-based apps, speaking about sharing confidential information, sharing or showing documents, uploading or transferring files in chat, as well as exposing personally identifiable information (PII) in audio, video, and chat.

Confidential data can come in many formats during collaboration sessions.

Talking about confidential documents	Sharing sensitive cloud apps, desktop, or documents
Sharing sensitive information	Showing documents or background on camera
Uploading, transferring sensitive files	Using built-in whiteboarding or collaborative workspaces

Experience the Advantages

Eliminates data loss blind spots

Proactively detects private and sensitive data exposure risks in media-rich collaboration platforms

Enables safe adoption of collaboration capabilities

Empowers organizations to adopt collaboration features, without worry

Reduces data security monitoring costs

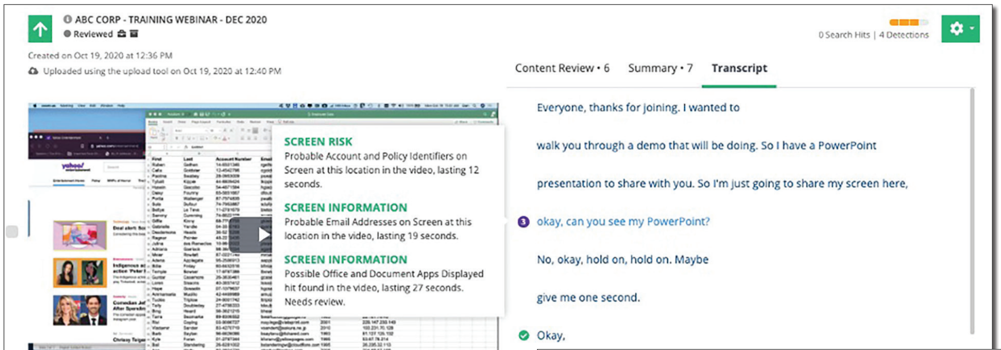
Provides more insights via integration for other security and data privacy tools

Theta Lake provides comprehensive analysis capabilities to address each of these mediums, including natural language processing (NLP), machine learning (ML), image recognition, whiteboard identification, document analysis, text analysis, as well as optical character recognition (OCR), and audio transcription analysis.

Intelligent Risk Detections Across All the Ways Employees Use Collaboration				
AUDIO *“What I am about to show you is confidential”* OR **SHARE** A document is held up to the camera or shared on screen	**CLOUD APPLICATION SHARING** A user shares a cloud-based application like their CRM or development portal to share sensitive data	**AUDIO** An attendee reads a credit card or personal account number out loud	**CHAT** A user pastes a URL to access a personal storage drive, such as Box	**DESKTOP SHARING** A user shares their full desktop on screen with sensitive documents or data shown

Granular private data classifications

Theta Lake’s classifications make it quick and easy to address any and all types of sensitive data, confidential information, PII, and other private data risks, out of the box. The solution detects these data loss risks across collaboration use of video, audio, and chat content, such as data rich applications, financial documents, files with PII, non-public information files, account numbers, social security numbers, national ID numbers, email addresses, credit card numbers, birthdates, and more.



ABC CORP - TRAINING WEBINAR - DEC 2020
Reviewed
Created on Oct 19, 2020 at 12:36 PM
Uploaded using the upload tool on Oct 19, 2020 at 12:40 PM

0 Search Hits | 4 Detections

Content Review • 6 | Summary • 7 | Transcript

SCREEN RISK
Probable Account and Policy Identifiers on Screen at this location in the video, lasting 12 seconds.

SCREEN INFORMATION
Probable Email Addresses on Screen at this location in the video, lasting 19 seconds.

SCREEN INFORMATION
Possible Office and Document Apps Displayed hit found in the video, lasting 27 seconds. Needs review.

Everyone, thanks for joining. I wanted to

walk you through a demo that will be doing. So I have a PowerPoint

presentation to share with you. So I'm just going to share my screen here,

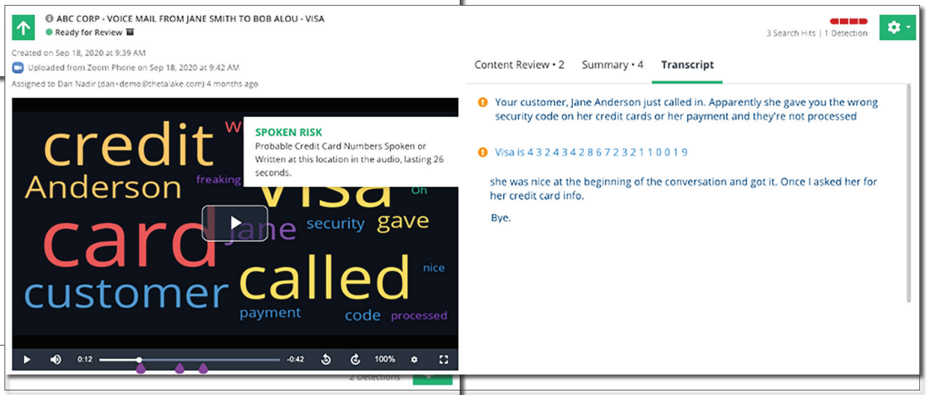
okay, can you see my PowerPoint?

No, okay, hold on, hold on. Maybe

give me one second.

Okay,

Figure 1 Excel detected on screen; PII detected in spreadsheet



ABC CORP - VOICE MAIL FROM JANE SMITH TO BOB ALOU - VISA
Ready for Review
Created on Sep 18, 2020 at 9:39 AM
Uploaded from Zoom Phone on Sep 18, 2020 at 9:42 AM
Assigned to Dan Nadir (dan+demo@thetalake.com) 4 months ago

3 Search Hits | 1 Detection

Content Review • 2 | Summary • 4 | Transcript

SPOKEN RISK
Probable Credit Card Numbers Spoken or Written at this location in the audio, lasting 26 seconds.

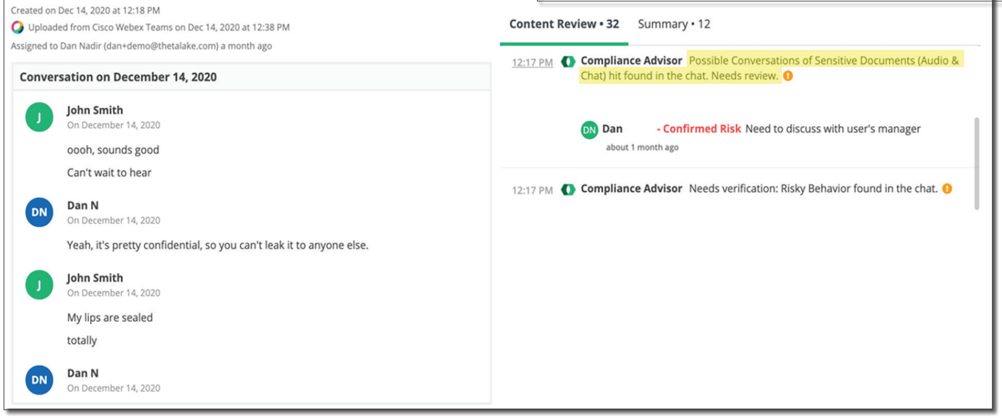
Your customer, Jane Anderson just called in. Apparently she gave you the wrong security code on her credit cards or her payment and they're not processed

Visa is 4 3 2 4 3 4 2 8 6 7 2 3 2 1 1 0 0 1 9

she was nice at the beginning of the conversation and got it. Once I asked her for her credit card info.

Bye.

Figure 2 PII detected in audio



ABC CORP - WEBEX CHAT - DEC 2020 (MULTI DAY)
In Review
Created on Dec 14, 2020 at 12:18 PM
Uploaded from Cisco Webex Teams on Dec 14, 2020 at 12:38 PM
Assigned to Dan Nadir (dan+demo@thetalake.com) a month ago

Conversation on December 14, 2020

John Smith
On December 14, 2020
oooh, sounds good
Can't wait to hear

Dan N
On December 14, 2020
Yeah, it's pretty confidential, so you can't leak it to anyone else.

John Smith
On December 14, 2020
My lips are sealed
totally

Dan N
On December 14, 2020

Content Review • 32 | Summary • 12

12:17 PM **Compliance Advisor** Possible Conversations of Sensitive Documents (Audio & Chat) hit found in the chat. Needs review.

Dan - **Confirmed Risk** Need to discuss with user's manager
about 1 month ago

12:17 PM **Compliance Advisor** Needs verification: Risky Behavior found in the chat.

Figure 3 PII detected and deleted from chat

Theta Lake provides comprehensive detection of privacy risks across content types and communication mediums. Some examples include:

SENSITIVE INFORMATION

- Conversations about sensitive material (audio and chat)
- Documents marked as sensitive
- Risky URLs of shadow IT and personal storage

PRIVATE DATA SPOKEN, WRITTEN, AND ON SCREEN

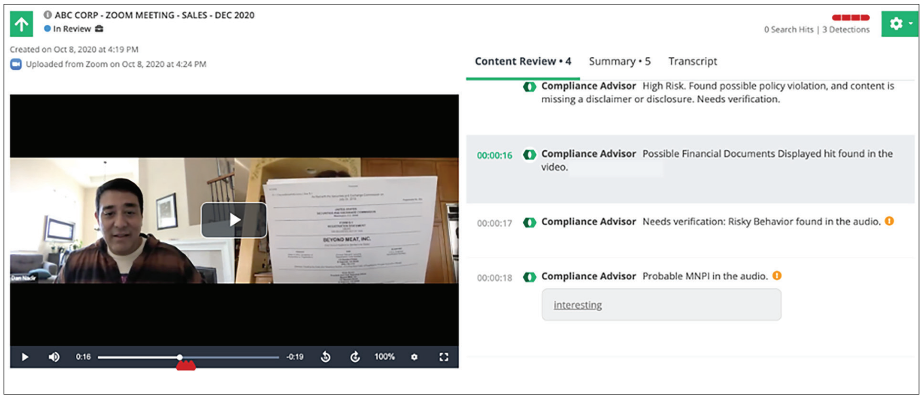
- Account numbers, credit card numbers, and tax ID numbers
- Email addresses and birthdates
- Social security numbers
- Custom data privacy detections

BACKGROUND RISKS

- Documents held up to the screen
- Physical whiteboard that appears in a host or attendee's background
- Built-in collaboration platform whiteboard and annotations

BROWSER-BASED OR DESKTOP VISIBLE APPS

- Office and other document apps
- Email apps and portals
- Financial, CRM, HR apps and portals
- Development and operations apps and portals



ABC CORP - ZOOM MEETING - SALES - DEC 2020

In Review

Created on Oct 8, 2020 at 4:19 PM

Uploaded from Zoom on Oct 8, 2020 at 4:24 PM

0 Search Hits | 3 Detections

Content Review • 4 | Summary • 5 | Transcript

Compliance Advisor High Risk. Found possible policy violation, and content is missing a disclaimer or disclosure. Needs verification.

00:00:16 **Compliance Advisor** Possible Financial Documents Displayed hit found in the video.

00:00:17 **Compliance Advisor** Needs verification: Risky Behavior found in the audio.

00:00:18 **Compliance Advisor** Probable MNPI in the audio.

interesting

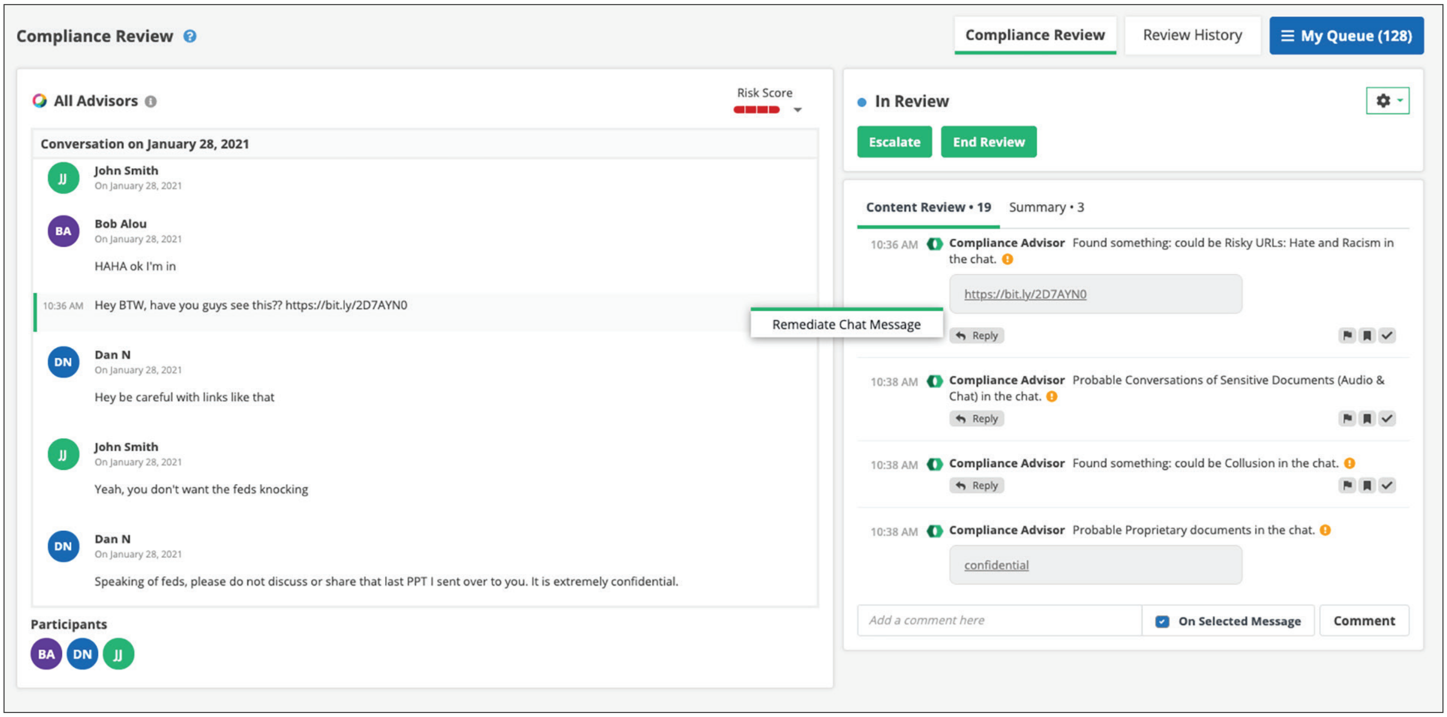
Figure 4 Detection of financial document displayed on screen

Proactive Remediation

A rapidly growing problem for organizations is sensitive data shared in chat. Whether that data is typed, shared as a link, or uploaded in a file, it remains documented in the chat, visible and accessible to all parties in that conversation. The period of exposure to this data could be days, weeks, or months, posting a real data loss threat. Theta Lake solves this issue with powerful remediation capabilities that allow organizations to alert stakeholders, share alerts with other security tools, set automated remediation, and allow compliance reviewers to remediate risks on demand as they search and review detections or conversations for risks. For example, in a chat if a user posts an account number, a file with customer or patient information, or a link to a risky website, that text, file, link, image, and more will be directly removed from the chat conversation in platforms like Slack, Microsoft Teams, Webex Teams, and many others. This comes with full logging and activity reporting for all stakeholders and systems.

Automatic Redaction

One growing challenge around data management, protection, and privacy is stopping the downstream exposure of private data to an organization's compliance and security stakeholders as well as integrated systems of the organization. Organizations with robust security and compliance monitoring routinely, and increasingly, collect private and sensitive data. That data, in nearly every scenario, should not be exposed to employees of the organization or shared and exposed through other integrations in other compliance or security products. Theta Lake solves this with automated, content-aware redaction and robust redaction features for compliance teams. Theta Lake provides built-in risk detection policies that an organizations can set to detect private data and automatically redact it from the audio, chat, video, and transcript. For example, if a video meeting participant shares a credit card number onscreen while potentially reciting the credit card number verbally, when Theta Lake analyzes that recording with PCI detection and redaction policy on, the actual scene in the video with the credit card number will be removed as will the audio track and the transcript section for that audio track. In its place stakeholders that need to review the meeting for risk, as well as any integrated systems consuming risk data from Theta Lake, will see a placeholder noting the type of risk detected and that it was redacted per the organizations data privacy policy. In addition to this automated approach, designated and



Conversation on January 28, 2021

John Smith
On January 28, 2021

Bob Alou
On January 28, 2021
HAHA ok I'm in

10:36 AM Hey BTW, have you guys see this?? https://bit.ly/2D7AYN0

Dan N
On January 28, 2021
Hey be careful with links like that

John Smith
On January 28, 2021
Yeah, you don't want the feds knocking

Dan N
On January 28, 2021
Speaking of feds, please do not discuss or share that last PPT I sent over to you. It is extremely confidential.

10:36 AM Compliance Advisor Found something: could be Risky URLs: Hate and Racism in the chat.
https://bit.ly/2D7AYN0

10:38 AM Compliance Advisor Probable Conversations of Sensitive Documents (Audio & Chat) in the chat.

10:38 AM Compliance Advisor Found something: could be Collusion in the chat.

10:38 AM Compliance Advisor Probable Proprietary documents in the chat.
confidential

Figure 5 Detecting discussion of confidential information

role-permissioned user of the Theta Lake Suite can also search and redact private data with full logging and in compliance with any overriding retention rules configured. As fines mount for breaches as well as improper private data collection and storage, it is more essential than ever to intelligently remove and redact sensitive data.

Unified, seamless platform integrations

Theta Lake provides extensive and quick to implement collaboration integrations across 40+ collaboration tool integrations all to mitigate the data loss risks of using modern collaboration platforms. Your organization can use any combination of collaboration tools that best suit your business and utilize Theta Lake's single pane of glass visibility with unified and consistent security and risk management across those platforms in a heterogenous environment.

To request a free demo, visit: https://thetalake.com/request-a-demo/

Or Visit us our website: https://thetalake.com/solutions/data-loss-protection/

ABOUT THETA LAKE. Theta Lake, Inc., dual winner of UC Today's 2020 Best Compliance Product and Best Security Product, was founded in 2017 by proven entrepreneurs and enterprise technologists with decades of leadership experience and recognition from Global 100 customers and top industry analysts. With a mission to provide modern collaboration security and compliance, Theta Lake's patented and multi-patent pending AI helps security and compliance teams more effectively and quickly scale their risk detection and the workflows for communication security, data loss protection, and supervision of modern video, voice, and unified collaboration systems. The Theta Lake Compliance Suite is SOC 2, Type 2 compliant. Visit us at ThetaLake.com; LinkedIn; or Twitter at @thetalake.