



Technology and Manufacturing: Monitor Conduct, Protect Sensitive Information, and Preserve Data Privacy During Online Video & Collaboration Interactions

For technology and manufacturing companies, managing a remote and traveling workforce has been a trend for some time. However, with new social distancing protocols, the usage of collaboration platforms like Zoom, Webex, GoToMeeting, Microsoft Teams, and RingCentral has rapidly surged as tech and manufacturing organizations move large portions of their workforce to remote operations.

Executive leadership and employees need to continue to manage the day-to-day activity and meet, plan, and collaborate while working from home, so video is now embedded in the most important aspects of the daily work routine.

At the same time, opening the floodgates of collaboration across video conference, voice, and chat tools can also present risks if they're left unmanaged. It's critical that all collaboration channels are appropriately monitored and supervised to maintain the organization's conduct standards and safeguard against data loss.

The likelihood of accidentally sharing confidential items, such as sensitive product plans, sales information, and employee information increases exponentially with the feature-rich capabilities of a camera, file transfer, virtual or physical whiteboards, and screen sharing. Offensive behavior and downstream liabilities from intentional or unintentional actions on camera, in chat, or on the microphone are abundant. At the same time most DLP, AUP, and compliance monitoring only fully covers email. The resulting gap and lack of monitoring visibility is simply not safe and introduces new risks.

Collaboration and video-based operations create new challenges:



Organizations must prevent abuse, liability, and risks during video, voice, and chat sessions.



Video introduces additional data risk of what is in the background and what is shown and shared.



Inappropriate and controversial behavior that doesn't align with corporate conduct policies can occur.



Intentional and inadvertent sharing of private personal and sensitive company data must be detected

Protect Private Data and PII in Collaboration Sessions

Theta Lake detects disclosure of sensitive information or use of PII during chat, voice, and video conferencing:

- 1 Pre-built policies automatically detect information like SSN, birth date, email address, and phone numbers.
- 2 Find any company-specific confidential or sensitive information intentionally or unintentionally exposed in video, voice or chat.

Bring data protection to your collaboration platforms

Theta Lake makes it easy for technology and manufacturing organizations to protect sensitive business information, preserve data privacy, and mitigate the risks of inappropriate behavior during collaboration sessions.

Theta Lake is a purpose-built risk and data privacy solution that provides automatic detection of conduct, data exposure, and data privacy risks across collaboration platforms, including coverage for what is shared, shown, spoken or written in chat, voice, and collaboration content.

The Theta Lake platform seamlessly integrates with videoconferencing platforms to ingest content and detect risk in what was spoken, shown or shared during a video conference session.

Proactively detect data privacy risks

Video conferencing features, such as document sharing, chat, and whiteboarding provide effective ways to interact during video sessions. However, these features also open up avenues for inappropriate inadvertent sharing of confidential corporate data or personally identifiable information (PII).

Theta Lake empowers organizations to supervise communications and identify privacy and data loss risks to keep data safe. With over 20 detections for acceptable use, privacy, and information security along with redaction features and support for custom detections, Theta Lake enables tech and manufacturing organizations to proactively identify and act on risks.

Safeguard against risky behavior

Potentially inappropriate behavior, such as failure to abide by ethics and conduct guidelines during video conference sessions must be flagged to ensure adherence to the company's policies. Without appropriate monitoring in place, these issues can persist and proliferate, resulting in downstream legal liabilities.

Theta Lake helps technology and manufacturing organizations identify conduct risks, such as abusive and controversial behavior, making it easy to identify and remediate code of conduct issues, as well as mitigate the potential human resource and legal liability risks.

Automatically pre-screen training, webinar, and meeting recordings for risk

With the increasing demand for more video content in the form of training and recorded meetings, technology and manufacturing organizations need to ramp up production in an efficient and safe manner. However, pressures to quickly create and publish online videos of those webinars, training, and other video content can drain review resources. Since time is of the essence, it is impractical to manually review videos for risky content as this approach significantly delays distribution.

Theta Lake makes it easy to accelerate SLAs on video production by automatically ensuring the recording doesn't include any private or sensitive data nor any risky content before it is distributed. The solution runs a risk-detection analysis on the video and can automatically reject videos with too much risk while prioritizing videos that are safe for reviewers to distribute more quickly.

Seamless collaboration platform integrations

Theta Lake provides an enterprise-ready solution with seamless integrations for dozens of platforms, including video conferencing, online video, and chat platforms.

Learn More

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

