THETALAKE

2022 Modern Communications Compliance and Security Report

Contents

Executive *Summary*

Modern unified communication (UC) tools have become a critical part of the communications infrastructure in even the most heavily regulated industries. The use of SMS/mobile messaging, collaboration and chat applications like Slack, Zoom, Microsoft Teams, RingCentral and Webex by Cisco as well as consumer apps like WhatsApp to conduct business is the lifeblood powering the work-from-anywhere era.

However, they present complex new challenges for those in the organization tasked with maintaining compliance, security and data privacy. **From recording and retrieving records of communications to protecting sensitive conversations in new channels, there are significant issues to manage in this new paradigm.**

As history has repeatedly shown, mistakes, breaches and data exposure happen when people communicate and share information digitally. The need to effectively mitigate these risks is made all the harder by the limitations of legacy supervision and archiving approaches, which pose real risks and costs to businesses.

At the same time, regulators expect the same robust controls regardless of where staff are working. In financial services, the fines levied this year for failures to capture, retain and supervise communications already exceed $2 billion. This crackdown on non-compliant communications is the clearest indicator yet that regulators have lost patience with firms that still haven't addressed supervision and record-keeping risks that were exacerbated by the pandemic.

The insights shared in the report are based on the views and experience of over 500 compliance and security professionals across global financial services, healthcare, insurance and government sectors who took part in Theta Lake's annual survey.

It provides a snapshot of how communications platforms are being used, details of the issues organizations are specifically struggling with, as well as practical recommendations to address them.

"The time is now to bolster your record retention processes and to fix issues that could result in similar future misconduct by firm personnel"

Sanjay Wadhwa, SEC Deputy Director of Enforcement, Press release SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures, September 2022

5 Key *Findings*

1

Unmonitored communication channels remain the biggest risk.

Two thirds (66%) of respondents say it's likely employees in their companies are using unmonitored communications channels. Another 4% don't even know whether this is happening or not. This presents one of the biggest risks for organizations in light of the intense regulatory scrutiny and enforcement surrounding unmonitored channels like WhatsApp.

2

Existing archiving solutions have blind spots and limitations.

39% of respondents cite gaps in coverage as a top challenge with their current archiving tools, while only 9% report having no issues. Another 45% need to be able to selectively archive written in-meeting communications like chat without having to record the video or audio. A mismatch between legacy tools built for email, and today's workplace where 81% use chat and 63% use video equally or more than email, has created critical gaps in records as well as put a spotlight on dated compliance tools that cannot adequately capture, retain, and supervise dynamic communications data.

3

Chat content remains the biggest risk to privacy and security.

Content shared in chat conversations, including in-meeting, is viewed as the biggest threat to compliance, security and privacy. In line with last year's findings, the transfer of files via chat (52%) and the ability to share links in chat or on screen (41%) are considered the riskiest features. This is driven by the ease of sharing files and links which could contain confidential, sensitive or proprietary information.

4

Video is gaining regulatory attention.

4 out of 5 respondents from financial services businesses anticipate there'll be increased regulatory expectations to monitor video. Not only is the camera functionality the number one feature disabled in organizations, 36% of respondents from all industries believe video conferencing and webcams create the greatest risks in terms of data privacy and employee misconduct.

5

Critical information is hard to search and retrieve.

85% of organizations experience challenges in retrieving records, exposing them to potential fines and sanctions for not being able to provide timely, complete data for investigations, data privacy or other compliance purposes. 52% find it difficult to search modern communication channels outside of traditional email methods. Meanwhile, 33% require significant manual resources to search multiple channels.

About This Research

Building on research first undertaken in 2018, this industry report provides insight into how modern unified communication tools are being used in practice, current approaches to managing security and compliance, as well as the challenges that organizations face.

The report is based on the views and experiences of more than 500 compliance and security professionals who took part in Theta Lake's annual benchmark survey through an independent third party in Q3 2022. Participants held senior roles in compliance, security, technology, and data privacy in heavily-regulated financial services, healthcare and government sectors across the U.S., the U.K. and Canada.

This year, questions were expanded to explore organizations' experiences and expectations of their archiving and e-discovery tools, including gaps or capabilities needed. New questions asked how firms undertake key compliance and security activities today and their expectations about what's on the regulatory horizon.

Theta Lake defines unified communications (UC) as a spectrum of communications including video meetings, mobile messaging, cloud voice, whiteboards, project tools, persistent chat and others such as workstream collaboration.

The findings are intended to help organizations benchmark their own practices, experiences and expectations against the wider industry, and identify any gaps or areas of exposure they may have. Practical steps for mitigating the compliance and security risks raised are also set out.

Anonymized quotes from participants have been included, with permission, which highlight specific issues and findings.

Total respondents: 504

Country of residence	USA 301	UK 152	Canada 51
Responsible for	IT 77%	Compliance 50%	
Size of company	Less than 1999 43%	2001-9999 38%	10000+ 20%
Business sectors (top 3)	Financial Services 60%	Healthcare 20%	Government 20%

The *Compliance And Security* Context

Modern communications like chat, SMS, mobile messaging and video have become integral to post-pandemic workplaces, wherever staff are based. However, their rapid deployment and exponential use has largely been matched with a failure to appreciate the risks and issues around information security and compliance obligations.

The recent fines levied by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CTFC) against 16 banks for unmonitored use of SMS, chat, mobile messaging and WhatsApp are the starkest example yet. These fines serve as an important reminder that obligations to retain, supervise and protect data extend equally to modern communications under global regulatory and compliance regimes like MiFID II, HIPAA, GDPR, CFTC, FCA, SEC, FINRA, IIROC, and other rulebooks.

> *"The term 'electronic communication' covers many categories of communications and includes amongst others video conferencing, fax, email, Bloomberg mail, SMS, business to business devices, chat, instant messaging and mobile device applications. ESMA will not produce an exhaustive list of electronic communications because of the continuing innovation and advancement in technology which would mean the list frequently becomes out of date."*
>
> **ESMA MiFID II FAQs, May 2021**

Fundamentally different to text-based communications like email, modern communications platforms require modern compliance and security tools to ensure the rich, dynamic features can be fully captured, retained and supervised - from video, chat and file links to contextual information like GIFs, emojis and reactions.

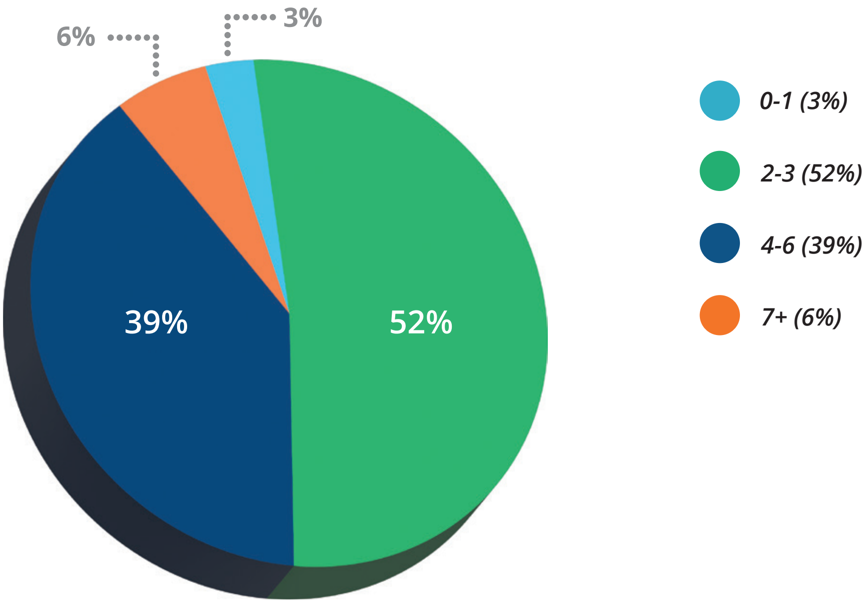
Organizations now face growing challenges to both enable communications across the platforms employees and customers are using while deploying technologies to appropriately capture, retain, and supervise these interactions to meet emerging regulatory obligations.

! Top Concern

"The volume is growing exponentially and it's becoming difficult to keep pace with"

IT Manager - Canada

Q. How many communication tools are you using within your enterprise? Include unified communications like Zoom, Webex, MS Teams, RingCentral, Slack, Symphony, and whiteboarding, mobile messaging and document sharing tools.



With underlying deficiencies in current approaches in the spotlight, pressure from regulators is intensifying, as are requirements to supervise and archive modern communications. According to Gartner's strategic planning assumptions[1], by 2025:

45% of regulated enterprise customers will conduct supervision of audio/video content to meet compliance requirements, up from less than 10% in 2021.

35% of enterprise customers will archive workstream collaboration and meeting solutions for nonregulated requirements, an increase of more than sevenfold from 2021.

The following findings highlight the breadth of complexities and challenges organizations are facing.

> *"...increased reliance on simple, easy-to-access but unauthorized chat and text platforms will pose a significant challenge for many types of entities operating in our markets. Internal compliance programs must adopt internal controls consistent with this new landscape. Firms must inculcate a culture of compliance at all levels of their organization to mitigate the risks associated with using unauthorized chat and text platforms"*
>
> **Kristin N. Johnson, Commissioner, CFTC, September 2022**

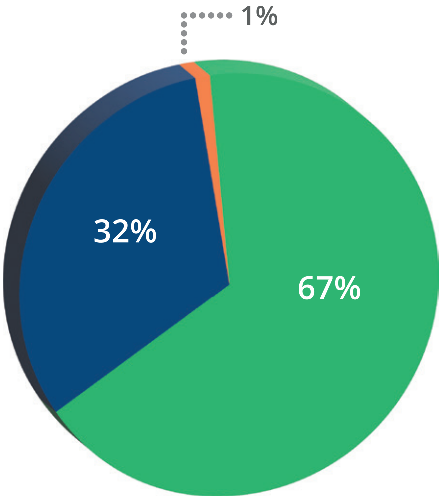
How *Communication At Work* Has Changed

In line with last year's findings, almost all professionals continue to report that their organization deploys multiple communications platforms.

Today, 45% of organizations use four or more tools to communicate, which reflects the growing portfolio of platforms available to teams such as collaborative whiteboards, messaging apps and video tools. All of which create compliance challenges in capturing and retrieving information from multiple sources as well as supervising communications that span multiple platforms.

Two thirds (67%) expect usage of these tools to increase further still.

The tools most frequently used by respondents include Microsoft Teams, Zoom, Webex by Cisco, Slack, RingCentral and Symphony, plus mobile chat tools like WhatsApp and whiteboarding.



Q.

Do you expect the usage of communication tools to increase or decrease in the next 12 months?

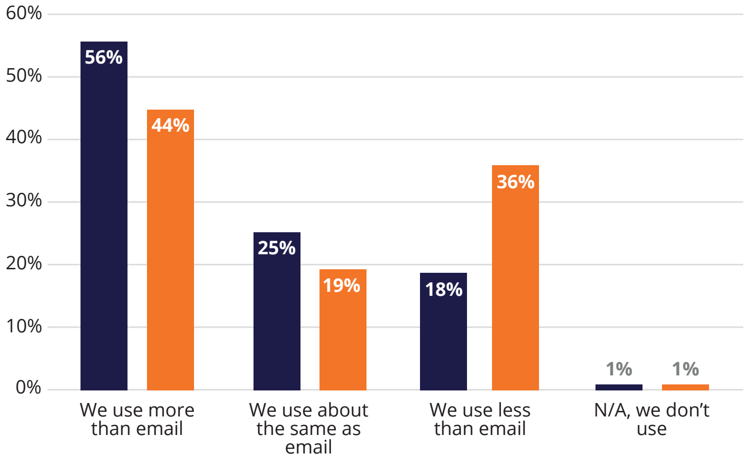
● *Increase* ● *Stay the same*

● *Decrease*

> *"At the start of the pandemic, if your firm moved to an alternative site or a working from home arrangement, we asked you to consider the broader control environment in view of the new circumstances. Given the extensive duration of these arrangements, we now expect you to record all relevant communications (including voice calls) when working outside the office."*
>
> UK FCA, July 2022

At the same time, it's notable that 55% of organizations are now focusing on three communication tools or fewer, which is indicative of consolidation within organizations, as they focus their management and controls on specific platforms.

This year, the most significant shift has been in the actual modes of communications used.



Q.

How are collaboration tools, including video and chat used in your organization compared to a year ago?

● Chat ● Video

Today, 81% of professionals report using chat as much or more than email – with 56% already using it even more than they use email.

Similarly, 63% use video as much or more than email with 44% using it more than email.
In last year's survey, video had been growing more rapidly than chat as a channel, but both have now established themselves as mainstays of the new workplace.

! Top Concern

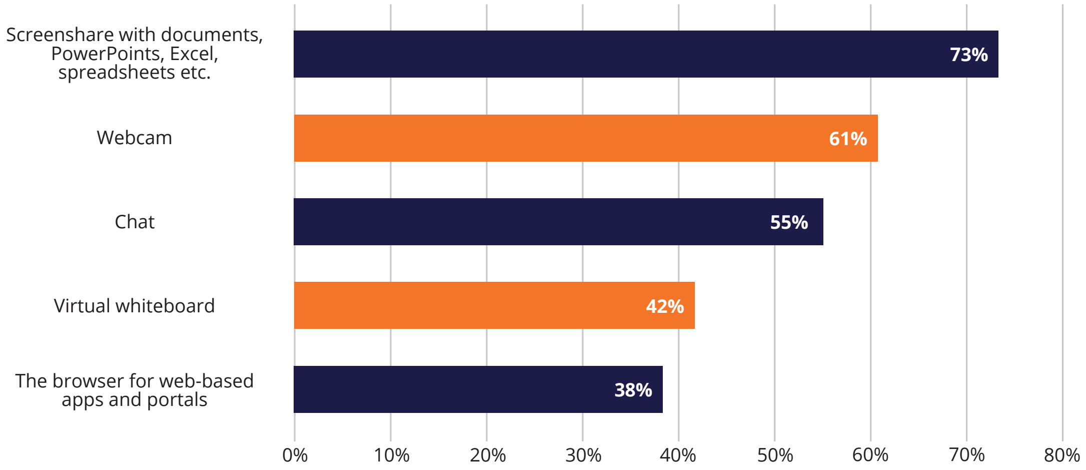
"People viewing the chat as a more informal communication and veering off topic"

Compliance Manager - UK

In terms of productivity, more collaborative features are being used during meetings. Screen sharing remains the most frequently used feature (80% in 2022, 73% in 2021) and there's a growing use of webcam (61% in 2022; 44% in 2021). **The most notable rise is the use of chat during meetings** - 55% in 2022 compared to just 14% in 2021. The use of browsers for web-based apps and portals has declined from 61% (in 2021) to 38%.

Q.

What are the most common items used, shown, or shared during a collaboration meeting?



The evolving behaviors reflect how employees are collaborating through tools and features that enable them to be productive, and that their customers want to use.

Unmonitored Communications

The heightened regulatory scrutiny and enforcement surrounding unmonitored communications in financial services reflects the importance of record-keeping and oversight.

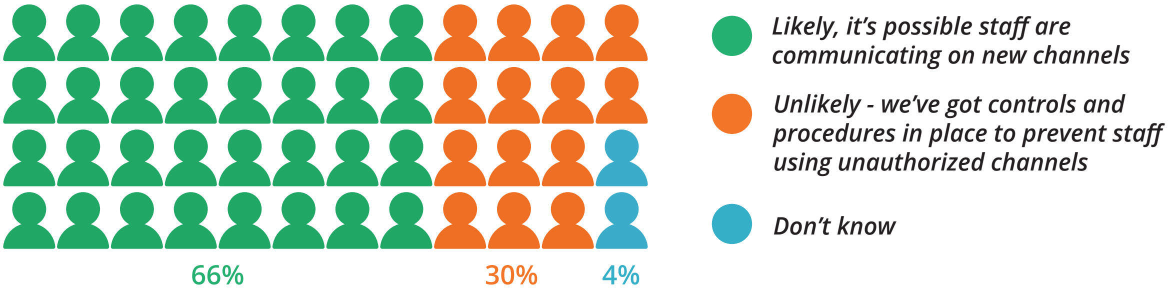
The investigations led by the SEC and the CFTC have already led to fines exceeding $2 billion this year, for failures in monitoring or retaining records of communications via WhatsApp, SMS, chat, and mobile messaging.

This major breach of record-keeping rules prevents regulators from checking whether firms are complying with obligations such as protecting market sensitive or personal data. Organizations themselves are hampered from effectively overseeing staff conduct, or responding to complaints, litigators or information requests under transparency or data privacy laws like the General Data Protection Regulation (GDPR) or Freedom of Information Act requirements.

Being able to capture, and quickly retrieve, a full audit trail of communications across the rich, dynamic features of modern communications including chat, audio, video, and file links as well as contextual information like emojis, GIFs or images is therefore critical.

Concerningly, 2 out of every 3 (66%) leaders surveyed say it's likely staff in their organizations are using unmonitored communications channels.

Q. How likely is it that staff are using unmonitored communications channels - including mobile and messaging tools like Whatsapp and WeChat?



Existing compliance controls and solutions are struggling to keep pace with the new dynamic technologies for communication.

Gaps in coverage is considered to be one of the top three challenges of existing archiving tools by respondents to this survey (39%).

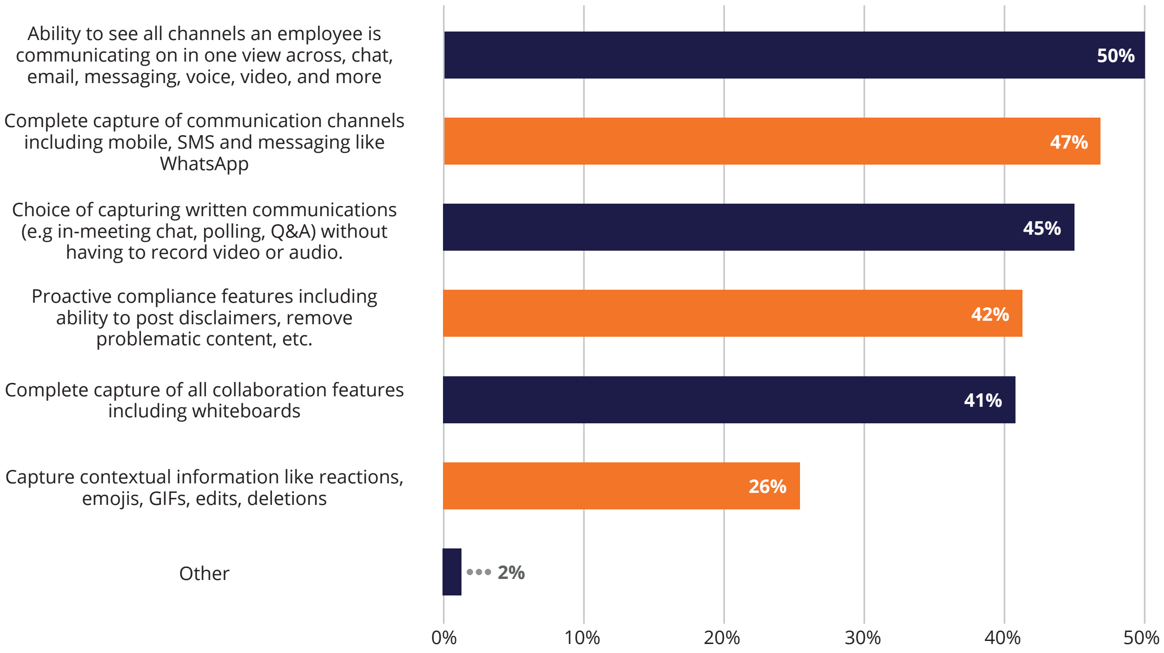
Nearly half (47%) of organizations stated they would like their legacy archiving solution to be able to capture all communications channels including mobile, SMS, and messaging like WhatsApp.

! Top Concern

"I'm afraid technology has fallen behind the ability to capture all the communications necessary"

Technology Director - USA

Q. Are there any capabilities that you would like your legacy archiving solution to provide?



That current weak spot was similarly called out during 1LOD's ecomms Deep Dive[2] which revealed that "62% of surveillance professionals say there are potential gaps in the surveillance of their communications due to the proliferation of channels".

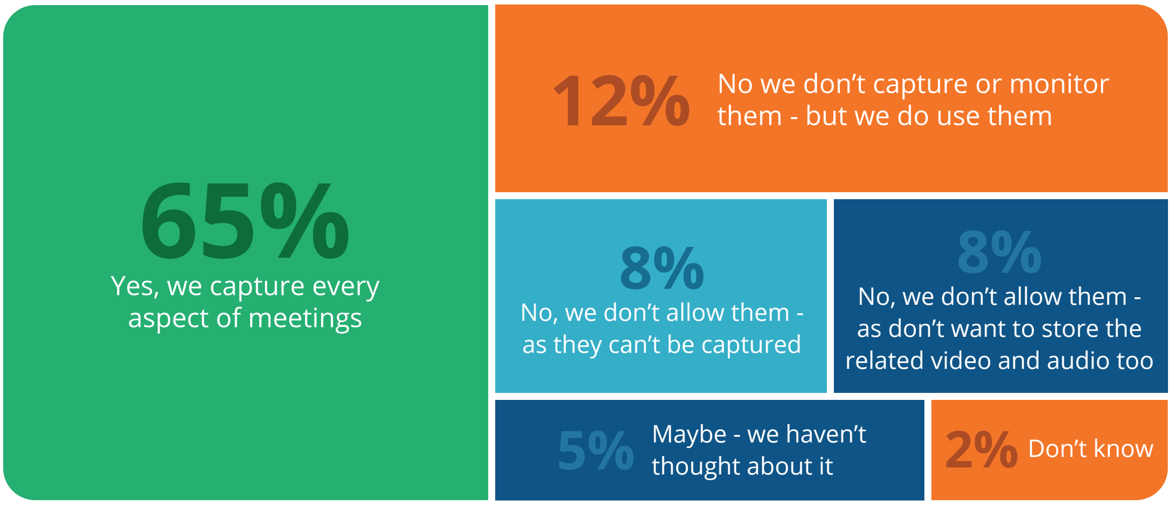
Given the sheer volume and complexity of communications and information in question, businesses can't expect to rely on manual resources and/or legacy tools to meet these requirements in the long term, without the support of modern technology.

> *"[a]s technology changes, it's even more important that registrants ensure that their communications are appropriately recorded and are not conducted outside of official channels in order to avoid market oversight."*
>
> **Gary Gensler, Chair, SEC, December 2021**

In-Meeting Communications

Q. **Are written communications during meetings, like chat, polling, Q&A or whiteboards being captured and monitored?**

Financial Services

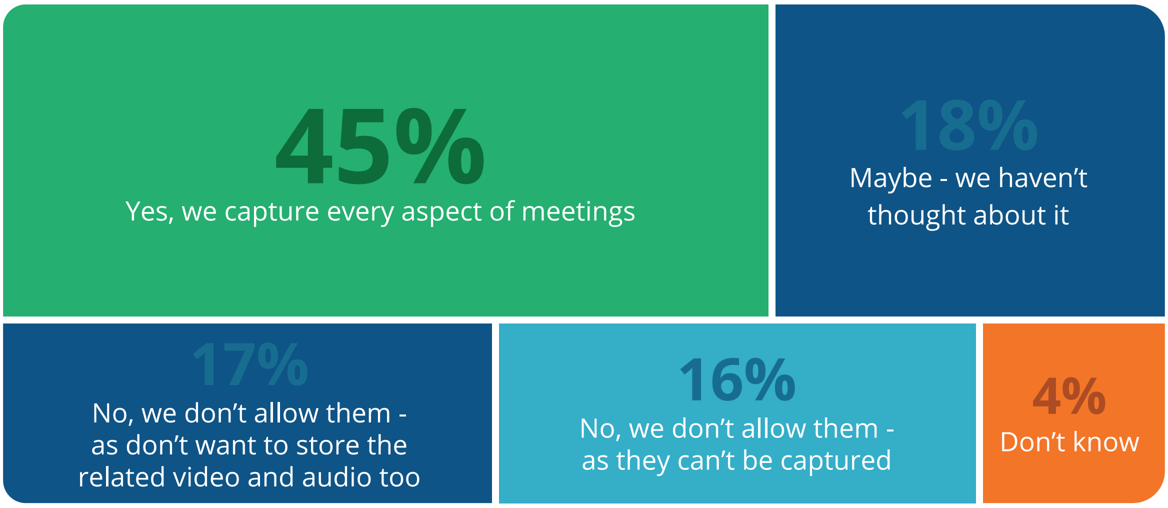


Regulated industries like financial services are required to retain and supervise electronic written communications, including those in collaboration meetings such as in-meeting chat, polling and Q&A.

The related problem for most organizations is that they still face a number of issues when it comes to recording audio and video, from the sheer amount of data that would need to be stored to the capability to navigate all this information. Many simply don't want to capture video and audio, where there is no regulatory or business need.

Q. **Are written communications during meetings, like chat, polling, Q&A or whiteboards being captured?**

Healthcare



But the result is that firms are either failing to capture the information regulators demand or they're disabling in-meeting features so that end-users are prevented from using them, which can lead to dissatisfaction and loss of productivity.

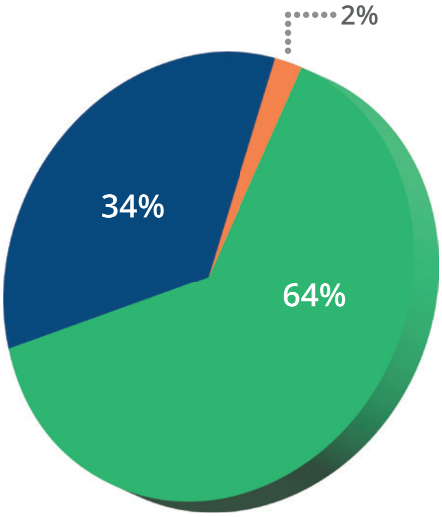
33% of financial services businesses and more than half (55%) of healthcare businesses in this survey face issues with capturing or allowing in-meeting communications. This indicates a significant blindspot given that 55% of organizations overall identified chat as one of the most common features used in meetings.

Across the industries surveyed, 45% of respondents report that they'd like to see their existing archiving vendor be able to capture written communications without having to record the video or audio.

There are solutions to this problem provided by innovative technologies taking a modern approach to compliance.

> *"...the use of these visual aids [whiteboard or dynamic charts, or a chat or instant messaging feature] may be correspondence, retail communications or institutional communications, and the firm must supervise them as such."*
>
> FINRA FAQs, September 2021

Video Communications



Q.

When using video conferencing – how frequently is a screen shared?

● *In most meetings - more than half*

● *Sometimes - less than half of meetings*

● *Never - compliance does not allow screen sharing*

Video has quickly become one of the most dominant communication channels at work. 44% of professionals now use video more than they use email.

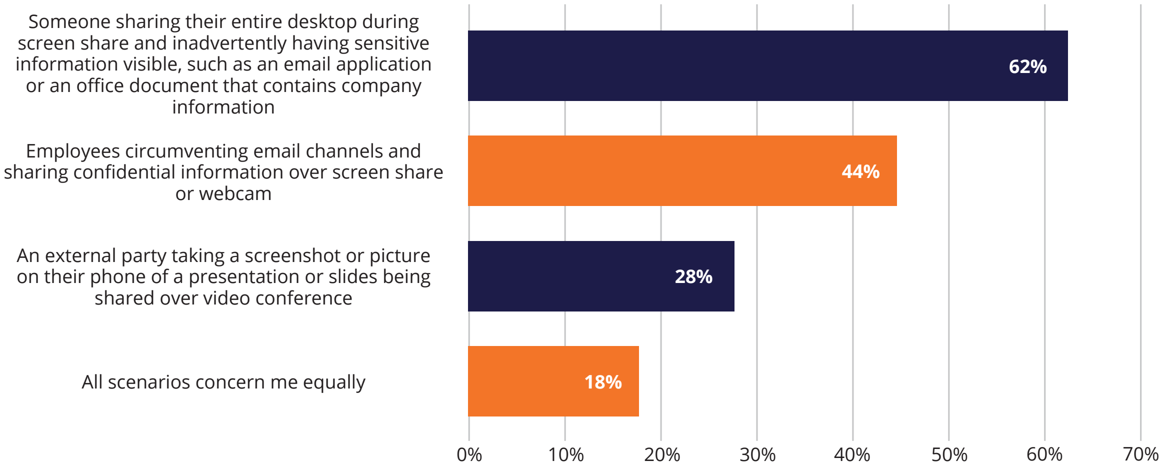
But the same multimedia features of video tools that make it so popular for meetings also make it one of the most concerning channels from a compliance and security point of view.

For instance, 64% of professionals report that they share their screens in more than half of all their meetings. That's in addition to the 73% that report screen-sharing as the most commonly used feature in collaborative settings.

At the same time, 62% of respondents also cite "someone sharing their entire desktop with sensitive information visible" as the scenario they're most worried about occurring, which is completely in line with last year's findings. Another 18% reported desktop sharing as being equally concerning as other scenarios. However, one notable change is the decrease in participants raising 'employees circumventing email channels' as their number one concern, (44% in 2022; from 63% in 2021), which likely reflects the declining use of email in favor of video and chat.

Video remains a double-edged sword.

Q. **When using video conferencing, which of the following scenarios concerns you most?**



36% of those surveyed believe video conferencing and webcams pose the greatest security, compliance and privacy risks. In fact, the camera is the feature most commonly reported as being disabled (by 46% of respondents).

Looking forward, this is only going to become more urgent for organizations to overcome. A point borne out by the 78% of respondents in financial services who anticipate regulators will increasingly expect firms to monitor video communications.

Q. **Regulatory bodies like ESMA have stated that all communication channels including video need to be monitored for MiFID II compliance. Given the recent regulatory enforcement and scrutiny of unmonitored communications do you anticipate the regulatory expectations to monitor to video?**

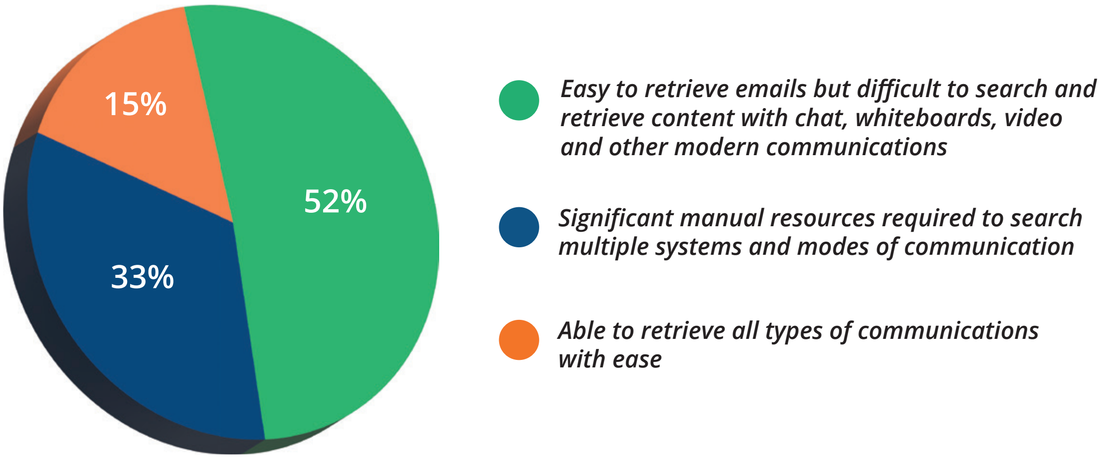
↑ 78% Increase

↓ 3% Decrease

→ 19% Stay the same

Finding And Extracting Records

Q. When retrieving information for FOIA, GDPR/privacy, investigations or complaints purposes, which statement best describes your organization?



Meticulous record-keeping plays a pivotal role in enabling businesses to demonstrate compliance. Organizations must be able to provide comprehensive records and evidence to investigators, regulators or auditors in a timely manner, providing the complete audit trail they need.

The problem with such a diverse collection of dynamic modes and channels is that it becomes extremely cumbersome to retrieve information.

85% of all businesses in this survey report facing difficulties in retrieving information, for a variety of reasons.

52% of businesses struggle with searching modern communication channels beyond email, while 33% of businesses report having to use significant manual resources to search multiple systems and platforms.

In fact, the number one challenge with existing archiving tools (cited by 41% of all professionals) is finding and extracting data.

! Top Concern

"Receiving FOI and not being able to provide it all"

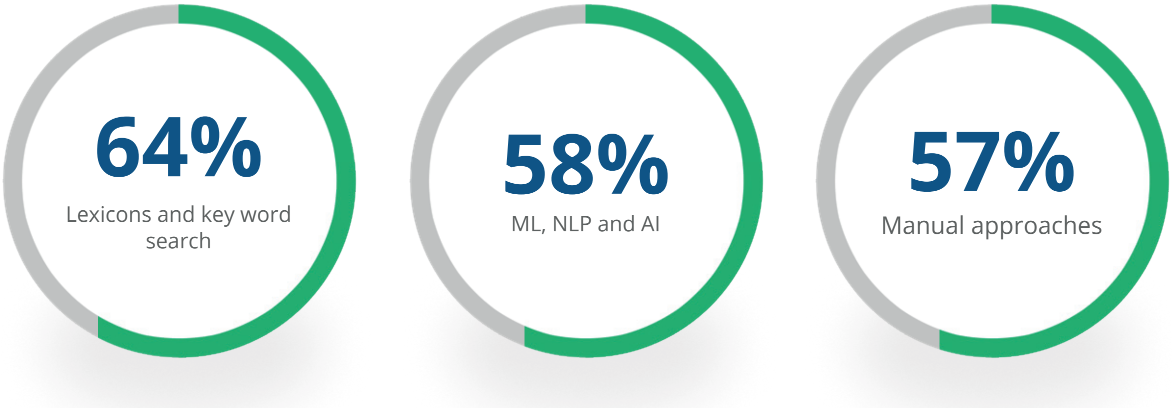
Monitoring Manager - UK

Supervising Modern Communications

In addition to the more specific issues with retention and oversight of individual communication channels, businesses also need to ensure they are able to supervise the high volume of rich, dynamic communications. A challenge that is expected to grow according to practitioners at 1LOD's e-comms Deep Dive, where **"70% believe that communications surveillance will encompass the majority of a bank's employees within the next 5 years".**

Today, 64% of businesses rely on lexicons and keyword search for the purposes of supervision. Concerningly, 57% of respondents indicate their business still relies heavily on more manual approaches.

Q. **How are you approaching the supervision of communications today?**



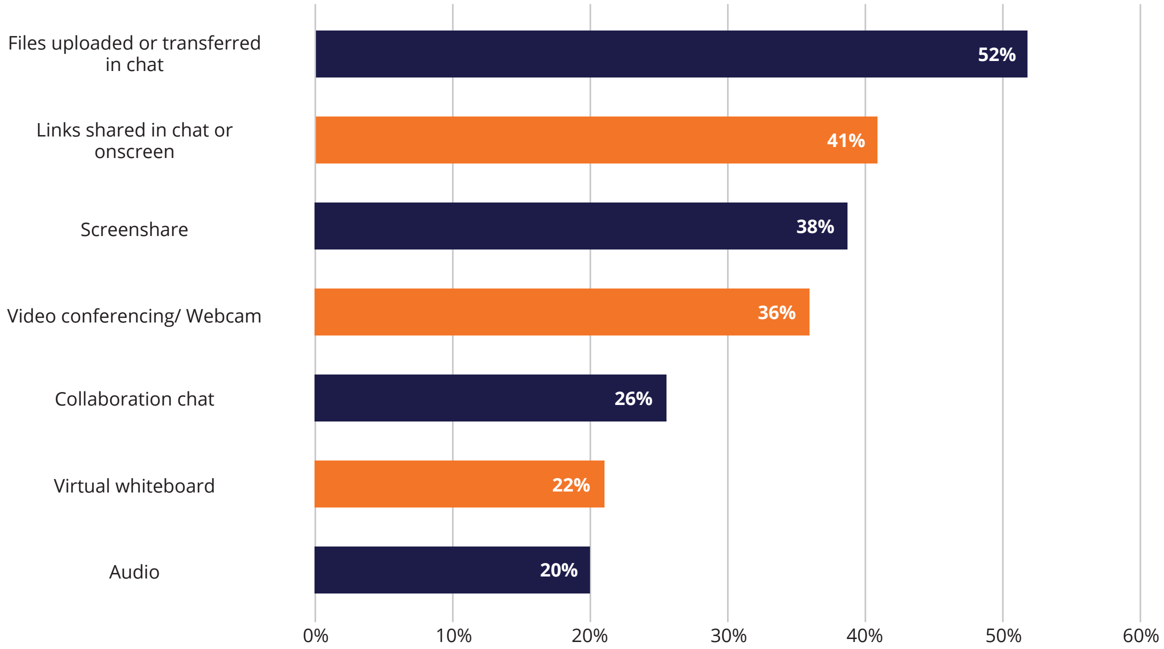
Notably, nearly the same amount of businesses are also working with new technologies to try and overcome the issue. 58% are using machine learning, natural language processing and artificial intelligence for more scalable supervision - evidence that AI/ML/NLP have moved to mainstream use for supervision, rather than a future event out on the horizon.

In parallel, the capability that professionals identified as most needed from their existing archiving vendors is the ability to see all employee communication channels in a single, unified view.

This number one compliance capability, required by 50% of respondents, clearly reflects the scale and complexity of tools and channels that need to be supervised, and the need for archiving vendors to have contemporary approaches to compliance to meet the demands of modern communication tools.

Security And Privacy

Q. Which modern communications features create the greatest risk when it comes to privacy, security or compliance risks like employee misconduct or data leakage?



Underlying all the challenges with the usage of modern communication tools is a fundamental concern about the security of sensitive information.

The top three features that are considered the greatest risk to compliance, security and privacy issues like employee misconduct are the transfer of files via chat (52%), the ability to share links in chat or on screen (41%) and the risks of screenshare (38%). Notably, the findings are completely in line with professionals' views reported last year.

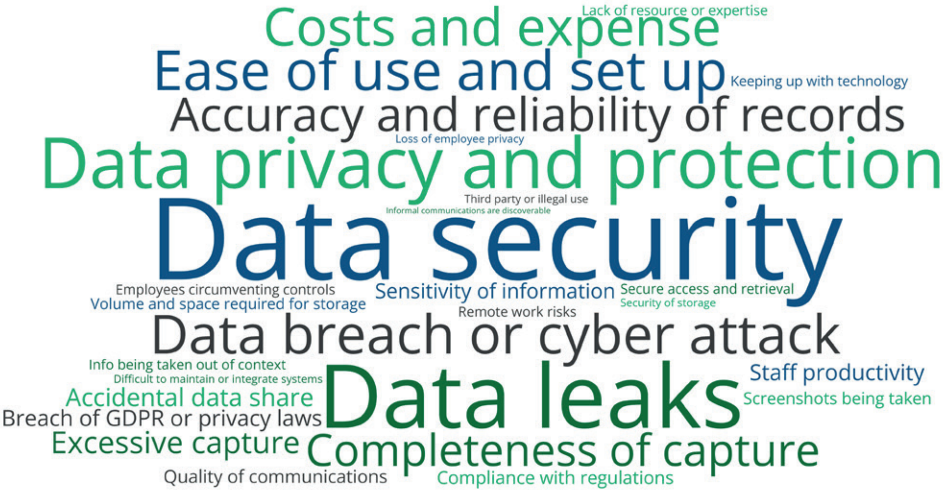
The senior leaders that took part in the research were specifically asked about any concerns they have relating to capturing and monitoring communications. A vast array of issues surrounding security and privacy were highlighted, with respondents repeatedly citing the risk of content being hacked, leaked or shared externally.

Top Concern

"My number one concern would be confidential information that is shared during meetings will be breached through staff taking pictures or screen shots of information that is shared."

Compliance Director - Canada

Q. What is your number one concern relating to capturing and monitoring modern communications?



Concerns were also raised about screenshots and information being recorded on mobile devices – recognizing the ease with which any participant can capture content during a virtual meeting.

The potential risk of information being leaked externally further reinforces the need for an organization to undertake proactive supervision and maintain complete records so they are firmly ahead of the curve if they need to respond.

Far from abating, these concerns around security and privacy have grown alongside organizations' increased use of communications tools since last year.

> *"sharing your screen without making the proper checks can change everything in an instant. Once scammers gain [access] to your screen, they have complete control. That means access to your sensitive banking and investment information, the freedom to browse at their leisure, and the ability to take whatever details they want"*
>
> ***Mark Steward, Executive Director of Enforcement and Market Oversight, UK FCA, May 2022***

Compliance Controls Need To Anticipate Change

The views and experiences of participants have uncovered numerous challenges organizations need to overcome to stay safe and compliant in an increasingly complex communications environment.

There are specific capabilities that organizations are seeking in modern compliance tools. These include capturing contextual information such as reactions, emojis, GIFs, edits or deletions and features like whiteboards, as well as proactive compliance functionality including being able to automatically post disclaimers and remove problematic content.

! Top Concern

"Not enough resources to accurately capture and monitor."

Monitoring Manager - USA

! Top Concern

"Time required to do this sufficiently and comprehensively."

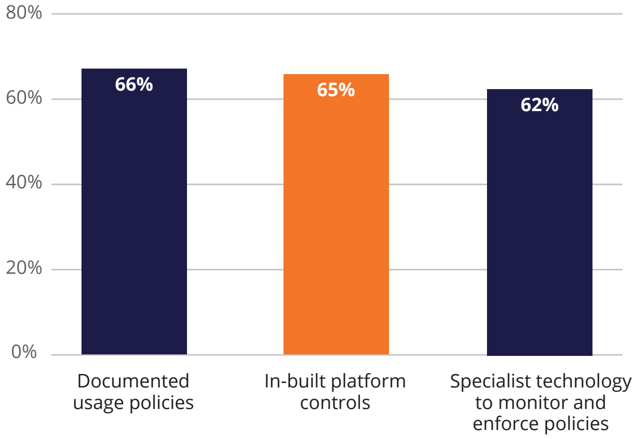
IT Manager - UK

In an environment where compliance resources are stretched and costs are rising, continually adding resources to manage growing communications isn't sustainable. According to this year's Cost of Compliance report[3] from Thomson Reuters:

"The emerging challenge is that the tightening of compliance budgets and possible shortage of skilled staff will make it more difficult for the compliance function to deliver successfully on the broadening range of activities now being asked of them."

Given 57% of businesses still rely too heavily on manual approaches to supervision, there's a real pressing need for technological solutions to solve this growing problem of complexity.

Unsurprisingly, the control environment across all organizations is varied and complex as approaches evolve to meet the rapid and constantly changing nature of communications and regulatory expectations.



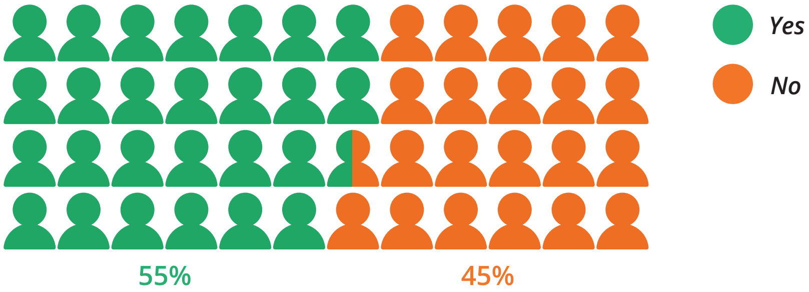
Q.

Which controls are you relying on to manage privacy, security and regulatory risks?

Currently, 66% of survey respondents in the financial services industry are using documented usage policies as controls, with 65% using in-built platform controls and 62% using specialist software to enforce policies.

However, 45% of organizations take a more draconian approach - disabling features in an attempt to limit the risk of new channels. Most frequently, the camera functionality, file sharing and screen sharing are disabled.

Q. **Are you disabling features within your communication tools (such as screen sharing, file uploads, camera usage) because of compliance, security or privacy challenges?**



In the short term, bans and blocks may work as a control. But given the features being disabled are as essential as camera functionality, file sharing and screen sharing, it's only a matter of time before employees circumvent such policies - an observation reinforced by the recent regulatory enforcement relating to the use of non-approved communication platforms and features.

Ultimately, organizations need to have the confidence and assurance to be able to unlock the value of the platforms they've invested in and staff and customers want to use.

Top Concern

"The volume of communications that are taking place now that there is less working in office meaning more is done via other channels making more work"

Surveillance Manager - UK

Final *Thoughts*

Organizations remain exposed to significant risks, even though the compliance and security requirements, as well as the regulatory costs of failing to have complete oversight and records of communications have become clear.

The legacy archiving, compliance and security tools such as Data Loss Prevention are inadequate and result in end-users not being able to use the communication channels they need.

Ever-increasing data volumes, regulatory scrutiny and cyber risk continue to drive the need for modern solutions. In parallel, the growing regulatory and public demand for accountability makes assurance over conduct, data privacy and security controls more important than ever.

Organizations need modern compliance and security technology to tackle today's challenges. It is evident that the legacy approaches have inherent gaps and are not able to capture, retain, supervise, search and retrieve across all communications platforms. These gaps result in compliance teams disabling key features that users want and need in their UC tools. That in turn exacerbates the risk of employees adopting unmonitored channels with the increased danger of substantial enforcement action. Modern solutions provide a seamless approach to compliance enabling the full use of UC tools together with increased levels of employee engagement and reduced risk.

The effectiveness of controls is determining the extent to which organizations are able to turn compliance and security challenges into competitive advantages, embrace new ways of working and navigate heightened regulatory attention. With banks expected to increase investment in surveillance over the next three years, according to 4 out of 5 (81%) practitioners in 1LOD's e-comms Deep Dive, the implementation of modern security and compliance tools will be one of the best investments a firm can make.

! Top Concern

"Utilizing all features of the communication without any data breach."

Data Privacy Director - USA

"Let me be clear here: I am talking about more than putting together a stock policy and giving a check-the-box training. This requires proactive compliance, and this type of approach has never been more important than today - a time of rapid and profound technological change."

Gurbir S. Grewal, Director, SEC Division of Enforcement, October 2021

Recommendations

Practical, incremental steps can be taken to address any gaps in current coverage and capabilities. These are recommended steps to get started:

- ☐ **Adopt UC platforms that have the capabilities end users want,** but that also support compliance capabilities through robust APIs and integration partnerships.
- ☐ **Undertake a risk assessment** of all communications channels to determine potential gaps in record keeping, oversight or information security. Check that all new communication modes like in-meeting chat, video, mobile, WhatsApp, file links, images and more are captured and searchable.
- ☐ **Ensure policies reflect the new working reality** and are understood by staff. That includes training and guidance on data security, record keeping requirements and acceptable use of channels. Spot checks, internal audits, reviews and updates of existing policies should also be part of the mix. Ensure that accountability and tone from the top reflects the importance of security and compliance.
- ☐ **Adopt AI-assisted compliance processes** that align with your readiness. Seek technologies that will assist in making processes like compliance review more scalable as opposed to custom made, complex solutions.
- ☐ **Don't disrupt existing compliance processes, and do leverage existing infrastructure.** Theta Lake's chat connector for collaboration platforms like Microsoft Teams, Cisco Messaging, Slack and RingCentral is an excellent starting point for turning on important disabled features without introducing coverage gaps, all while sending captured content to existing archive infrastructure, and without disrupting existing compliance processes and tools.
- ☐ **Take an incremental, risk-based approach.** Start with addressing capture, archiving and supervision gaps in areas where the risk is highest, such as SMS, WhatsApp and other consumer messaging apps under regulatory scrutiny.
- ☐ **Choose compliance platforms designed to support and integrate with modern communications** so that users will benefit from better communication tools with all features enabled rather than less productive tools which are hampered by legacy compliance approaches.
- ☐ **Use compliance platforms with meaningful UC relationships and investment.** Specifically scrutinizing vendor claims about the depth of integrations, and solutions created through multiple product acquisitions is a key part of the assessment process. Organizations should also seek more compliance coverage by using UC tools with compliance API and the certified recommended compliance tool providers that support the API and its features.
- ☐ **Ensure effective security settings** are in place on your meeting platforms.

Key Takeaways Across The Three Lines Of Defense

1

First line governance and security functions

Check whether effective compliance and security controls are in place across all collaboration platforms, enabling communications to be utilized safely and compliantly, and mitigating the need for employees to circumvent channels or use non-approved modes.

2

Second line functions including compliance and risk

Check there are no gaps in compliance with obligations - keeping up with regulatory guidance and learning lessons from industry weaknesses is key. That includes complete capture of communications, being able to retrieve them in a timely manner to meet regulatory or data privacy requests, and oversight to identify and address conduct, privacy or security risks.

3

Third line including internal audit

Ensure the oversight of security and compliance of today's modern communications is part of the annual audit plan. Assess the completeness and effectiveness of archiving and supervision controls as part of that review.

The evolution of the three lines of defense:

Proactive investment in targeted areas can strengthen the traditional three lines of defense, making it more suitable for today's remote/hybrid digital workplace. For example, identification and enablement of collaboration features that users want, such as in-meeting chat, while implementing compliance controls like selective archiving for them at the outset. Or recognition that the second line of defense cannot overcome the volume and variety of evolving e-comms and leaning into the adoption of more assistive AI-based approaches for supervision.

About Theta Lake

Backed by the investment arms of Cisco, RingCentral, Salesforce, and Zoom, Theta Lake's multi-award winning product suite provides patented compliance and security for modern collaboration platforms, utilizing hundreds of frictionless partner integrations including RingCentral, Webex by Cisco, Microsoft Teams, Slack, Zoom, Movius and more.

Theta Lake captures, compliantly archives, and acts as an archive connector for existing archives of record across video, voice, and chat collaboration systems. In addition to comprehensive capture and archiving, Theta Lake uses patented AI to detect and surface regulatory, privacy, and security risks in an AI assisted review workflow across what is shared, shown, spoken, and typed. Theta Lake enables organizations to safely, compliantly, and cost-effectively expand their use of unified communication platforms.

Visit us at :

ThetaLake.com | LinkedIn | Twitter at @thetalake

If you'd like to see how Theta Lake can help, request a demo today from our friendly team.

> *"The findings show just how integral modern communication platforms have become in today's workplace, but there's a lot of catching up to do when it comes to the compliance and security tools currently being used. The more than $2bn in fines is the biggest wake up call yet that Compliance and Unified Communications teams need to be in lockstep to ensure a comprehensive approach to record-keeping and supervision."*
>
> **Stacey English, Director of Regulatory Intelligence, Theta Lake**

References

1. Gartner, Magic Quadrant for Enterprise Information Archiving, 2022, Michael Hoeck, Jeff Vogel, 24 January 2022

Gartner Disclaimer: Gartner and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2. 1LOD Ecomms, May 2022 https://online.flippingbook.com/view/427926701/

3. https://legal.thomsonreuters.com/en/insights/reports/cost-of-compliance-2022-competing-priorities