GUIDE

# The Benefits of SaaS

Addressing compliance complexity
with cloud-native infrastructure

smarsh® | aws

# Introduction

The world thrives on technology, but today's financial services organizations face a common problem when managing their business communications: exponential data growth.

Global data creation is predicted to reach over 180 zettabytes by 2025. Large organizations are dealing with multiple petabytes of data, driven by an increasing volume of communications and a variety of channels – from multi-modal chats to voice and video. This rapid data growth was further accelerated by the shift to hybrid work.

Organizations are obligated to meet regulatory requirements around the globe regardless of the channels those communications take place on. It's critical to find a scalable solution with an agile infrastructure that allows for retention and analysis regardless of the size, frequency and types of tools used by staff.

However, choosing the right solution is not as simple as saying, "Okay, we pick this one," even if the choice reflects your needs. While data has grown unabated, budgets have largely remained the same. Abundant data and tight budgets mean many organizations' legacy systems and staff are overwhelmed. Organizations need a scalable solution that doesn't incur linear increases in software and staffing costs.

In this guide, you'll learn:

- Which priorities global financial institutions are setting for their data
- What a future-focused archive looks like and why it involves cloud technology
- How secure and compliant workloads can be built using cloud-native services on AWS

# Table of Contents

# Battling regulatory pressures

In addition to data challenges, financial institutions face unique risk and regulatory challenges:

Constantly evolving regulatory requirements

Requirements that vary significantly across regions

Highly dynamic security threat landscape

Stringent reporting & documentation requirements

Limited cloud security & compliance specialists

When the pandemic hit in 2020, regulators understandably gave firms the time and space to care for their employees and create resiliency. However, as the pandemic subsided, regulators refocused on their objectives to ensure that hybrid work received the same level of regulatory oversight as in-person settings.

This renewed scrutiny led to new and larger fines initially targeting mobile applications like WhatsApp and WeChat. Undoubtedly, others will soon follow suit. A sharp increase in regulatory enforcement actions and fine amounts make it more critical than ever for compliance and IT leaders to work together to update compliance strategies and infrastructure.

While the majority of these fines were handed down in the US, global organizations must anticipate that international regulators will soon come with their own penalties.

## Understand your industry regulations

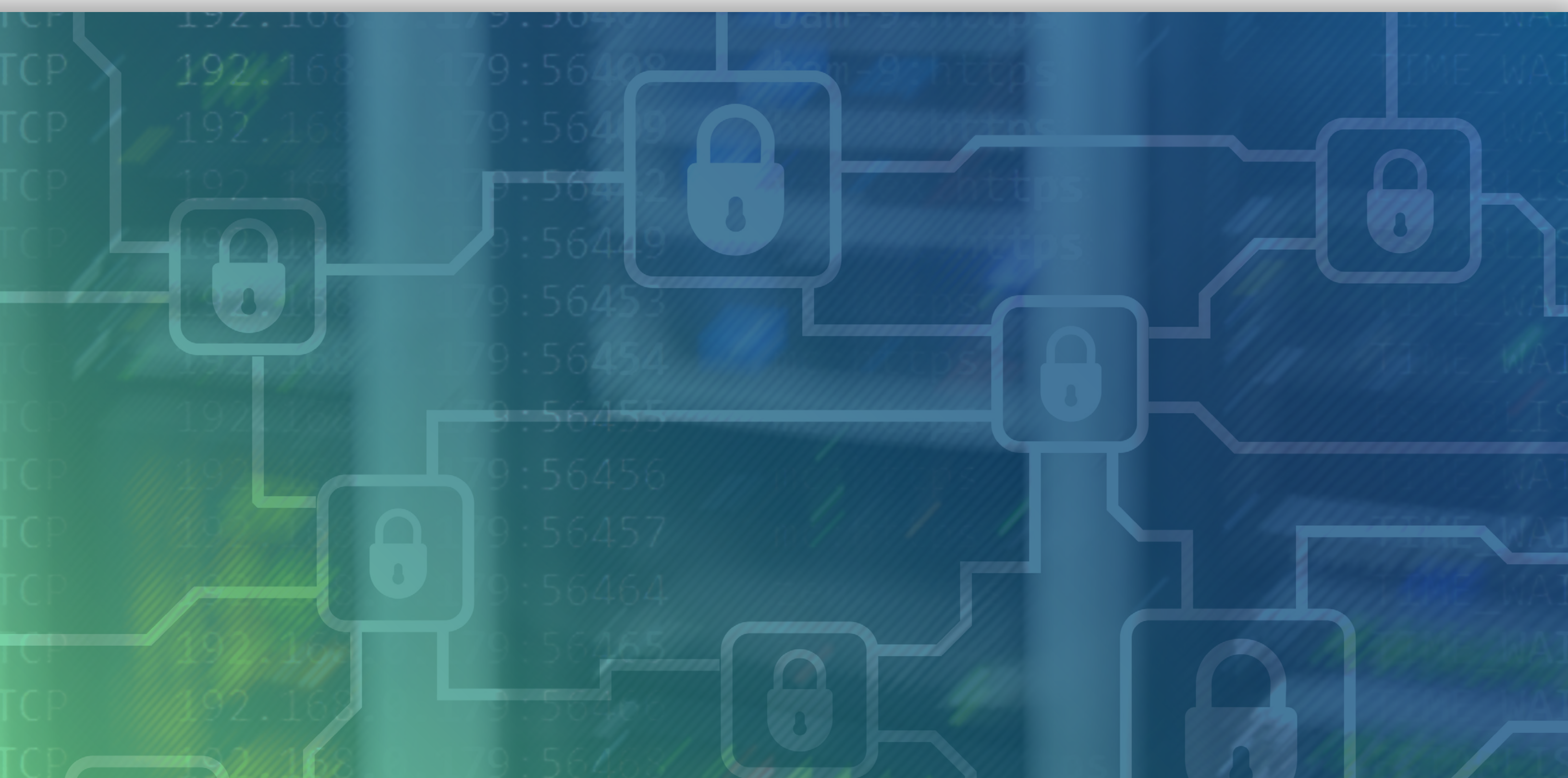
To make the right decision for your organization, you must understand your needs, budget and, most importantly, your regulatory requirements.

In Europe, Article 16(7) of MiFID II states "… an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm."

Similarly, for financial services firms in the U.S., both the SEC and FINRA have recordkeeping requirements and guidelines:

- SEC Advisers Act Rule 204-2
- SEC Rule 17a-3 and 17a-4
- FINRA Rule 3110(b)(4)
- FINRA Rule 2010
- FINRA Rule 4511

If third-party vendors are involved, additional considerations regarding data control and security are necessary. Banks must engage in proper risk management and ongoing oversight when using third-party solutions or collaborating with vendors for AI applications to ensure compliance, consumer protection, and privacy.



# The data hangover

We are far removed from the days when email was the only electronic communication channel requiring supervision. Over time and as they adopted new communication channels, many firms acquired multiple tools to handle data capture, storage, and surveillance. As technology advanced, new communication and collaboration tools became the standard, making data – and data management – more complex.

With hybrid and remote work surging, regulated industries now face what we have termed a "data hangover." The incorporation of new productivity, collaboration and communication tools have become an ongoing struggle when dealing with supervision and surveillance and maintaining regulatory compliance. As organizations integrated new data sources, data volumes surged while hybrid work increased firms' surface area of risk. The result is a complex, inefficient infrastructure that would give any compliance or IT team a headache.

## Setting priorities for global financial organizations

For many financial organizations, technology and regulatory changes have created a short list of key priorities for the year ahead. Organizations are looking to solve one or more of the following challenges:

**Scale alert review efforts**

- Current processes overwhelm compliance teams with false alerts, which require manual and time-consuming reviews

**Expand risk coverage**

- The surface area of risk has expanded greatly with hybrid work; firms require new tools to address this new work model

**Adapt to new geographies**

- Doing business in different countries means knowing and abiding by the data capture and collection regulations of those regions, as well as adhering to global data privacy laws

**Cover new modalities like voice**

- New communication tools mean new requirements when it comes to how financial firms manage data from voice and other tools generating large file sizes that must be captured and archived

# What does tomorrow’s “archive” look like?

As we look to the future, the concept of an "archive" as we know it today will transform into the central hub for an organization’s communications. Soon it will become a "communications data warehouse," enabling the deployment of advanced technologies like ChatGPT to optimize worker efficiency.

As a business grows, compliance requirements evolve. A fully integrated, cloud-native solution is needed that can adapt and grow along with the organization's needs. The solution must also enable businesses to collect, retain and analyze communications to meet global regulatory requirements while controlling operational costs and risks.

## Integrating public cloud technology unlocks significant benefits:

1. An end-to-end integrated solution minimizes downstream changes — centralizing administration and allowing IT teams to focus on adding value elsewhere.
2. An integrated platform offers incredible speed at petabyte scale, making data growth a problem of the past. Deploy system-wide updates within hours across global regions. Searches are returned in seconds and minutes vs. days. Data lifecycle management enables organizations to balance specific economic and performance needs.
3. Public cloud offers ongoing agility, innovation and security updates.
4. As the regulatory backbone of a company's communications, proper controls, auditability, and change management while maintaining responsiveness to external risks is a must. Features such as explainable AI, versioning, rollback, and reconciliation support success.
5. "Triple Active" architecture deploys to a minimum of 3 Availability Zones in every region, ensuring resilience against cloud provider outages.

# Building secure and compliant workloads on cloud-native architecture

In its shift to the cloud, the financial services industry is confronting a range of familiar and emerging issues. Using SaaS built on AWS, businesses gain control and confidence to securely run with the most flexible and protected cloud computing environment available today.

Customers can improve their ability to meet core security and compliance requirements, such as data locality, protection and confidentiality with AWS' comprehensive services and features. Customers should also look to work with a service provider that cooperates directly with financial services customers and regulators to enable the secure and compliant adoption of services.

**Cloud-native services like AWS offer customers tools and guidance to enable compliance**

Terms & conditions

Transparency

Agreements and third-party audit reports to support financial services compliance objectives

Compliance, security tools & services

Industry frameworks & assets

Services and assets to automate controls, collect evidence and manage audit demands

Deep industry expertise

Regulatory engagement

Mechanisms to advocate for and share best practices with customers

## Ensuring data privacy and confidentiality with AWS

As data growth accelerates along with data privacy concerns, security is a top priority for AWS.

Enterprise firms and organizations work with AWS to provide the necessary security and data management abilities to ensure confidentiality while maintaining data compliance.

| | |
|---|---|
| **Storage** | You choose the AWS region(s) in which your content is stored and the type of storage. Replicate and back up your content in more than one AWS region. Your content will not be moved or replicated outside of your chosen regions without your consent. |
| **Security** | You choose how your content is secured. AWS offers strong encryption for content in transit and at rest. These data protection features include data encryption capabilities available in over 100 AWS services.<br>Flexible key management options allow you to choose whether to have AWS manage your encryption keys or enable you to keep complete control over your keys. |
| **Access** | Maintain full control of your content and responsibility for configuring access to AWS services and resources. AWS provides multiple  set of access, encryption and logging tools to help you do this.<br>AWS provides APIs to configure access control permissions for any of the services you develop or deploy in an AWS environment. |
| **Disclosure of Customer Content** | AWS will not disclose customer content unless required to do so to comply with the law or a binding order of a government body. If a governmental body sends AWS a demand for customer content, they will attempt to redirect the governmental body to request that data directly from the customer.<br>If compelled to disclose customer content to a government body, AWS will give customers reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so. |
| **Security Assurance** | AWS has security assurance services that use best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of the security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. |

# AWS and Smarsh: Compliance and collaboration

Pairing AWS and Smarsh provides regulated businesses with the agility and scale needed to thrive financially and remain compliant with evolving communications data regulations.

Smarsh solutions are specifically designed for today’s digital communications and position your business for the future. Using modern web-scale technologies built on AWS, we can ingest, search, protect and export your content orders of magnitude faster than legacy archives.

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated agencies of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. federal, state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions.
You must consult your legal team regarding your compliance with applicable laws and regulations.

Guide - 08/23

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh