GUIDE

smarsh®

The Cost of Doing Nothing: **Public Cloud**

Overcoming common obstacles to adopting a cloud archiving solution

Available in AWS Marketplace

Introduction

The financial services industry operates in a dynamic regulatory environment that requires constant focus and adaptation. Against the backdrop of evolving regulations, information security, and privacy laws, new communications tools and devices are contributing to the transformation of legal and regulatory compliance.

Legacy compliance solutions may have once been the shiny new technology. Now, those systems are keeping financial firms stuck in the past. Many compliance and e-discovery tools were made for email and can't provide adequate coverage for the explosion of new data generated by modern communications channels.

However, replacing a critical system that's entrenched in so many key processes and workflows has given some firms pause.

Fortunately, archiving solutions that support regulated industries are transforming, too. Today's cloud-based services are addressing:

- **The ever-growing set of communications and content types (chat, text, social, voice, etc.) that regulated users need to engage with clients**
- **How to keep up with the increasing volume of communications data by adopting artificial intelligence and machine learning to augment supervision processes**
- **The legal and privacy needs of global organizations operating across jurisdictions**

Considering the latest advancements in cloud technology and capabilities, why are so many financial services firms still slow to migrate their compliance and discovery workflows to the public cloud?

In this guide, we outline common obstacles holding back key stakeholders in financial services firms (compliance, IT and legal teams) from moving technology infrastructure to the public cloud. We discuss why reality runs counter to these arguments, how to move forward, and — most importantly — why maintaining the status quo (i.e., "doing nothing") may be the greatest cost of all.

The stakeholder point-of-view

It's important to address concerns that are keeping compliance, IT and legal departments stuck in old patterns. While there is significant overlap, we recognize there are nuances between these teams in their hesitancy to migrate to the public cloud.

Compliance: Compliance teams are the stewards of one of the most strategic and sensitive assets their firms possess — communications between their firm and their clients.

Legal: For those involved in e-discovery processes, tried-and-true methods are powerful motivators. Many won't see the value in cloud-based archiving and e-discovery until a high-profile legal case arises.

IT: Technical teams may be more open to updating infrastructure. They should make the case that as their companies strive to achieve a mobile, remote ecosystem, it will be even more critical for disaster recovery and enterprise-level cybersecurity to keep pace.

> **"For most financial institutions, it's not a regulatory issue. If and when a firm chooses to move sensitive data to the cloud is typically a matter of risk tolerance."**
>
> **Dan McKay**
> AWS Financial Services
> Compliance Expert

Perception, reality and recommendations

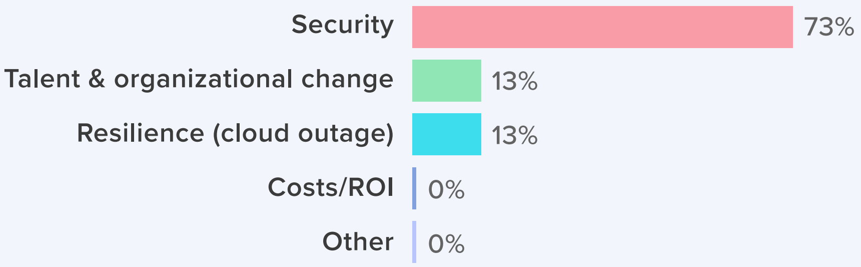
Getting cross-departmental consensus can be tough, especially when stakeholders are dealing with high stakes — for example, costly compliance penalties, legal ramifications and operational disruptions.

Here, we review the five most common reasons compliance, IT and legal teams are struggling with the decision to move to the public cloud, why these obstacles should be reconsidered, and recommendations for moving forward.

1. Concerns about data security in the cloud

Perception: There is a view that data in transit to the public cloud is less secure than data that's maintained behind a firm's firewall. Keeping data onsite may give the firm a level of comfort that could be lost if data is stored in the cloud. In fact, when asked about moving to the public cloud, firms consistently list data security as a leading concern.

"What concerns you most about migrating to the cloud?"



(FINRA Cloud Computing Conference 2022 attendees)

Reality: The reasons to maintain a traditional data center revolve around cultural norms and comfortable routines. The public cloud is more accessible, flexible and economical, with a level of security that is not available to most private or public companies. According to Gartner estimates, public cloud services will suffer at least **60% fewer security incidents** than those in traditional data centers.[1]

Recommendations:

- Consider cloud services that prioritize risk assessments and incident response plans
- Evaluate and compare legacy systems with cloud services against recent SEC cybersecurity guidance
- Examine how discovery applications use underlying security infrastructure
- Make sure cloud providers meet security recommendations of SSAE-16 SOC II, ISO 27001 and similar frameworks

Data security

Public cloud providers offer comprehensive, multi-layered, military-grade cyber defenses which far exceed what individual financial services firms can maintain with limited IT budgets. They also offer data redundancy and state-of-the-art disaster recovery.

[1] https://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf

2. Cultural resistance to change

Perception: There's pressure to maintain the status quo when existing technologies have worked for so long. On-premise compliance applications have decades of development baked in, including feature and access controls that were designed to operate in proximity to messaging and directory infrastructures.

Compliance	Legal	IT
Ultimately, the reputational risk for companies that continue to rely on out-of-date systems and applications will directly impact compliance. Failure to modernize can be seen as out of touch, which may negatively impact recruiting, and how prospective customers and employees feel about working with the firm.	Enabling flexibility to respond to the next discovery target is a more effective strategy than attempting to retrofit tools to address an email-centric era that has passed. According to a poll conducted by Everlaw, **95% of legal professionals** believe cloud-based discovery will become the norm within the next two years.[2]	A recent PwC survey noted that 77% of organizations planning to move to the cloud did not feel its workers had the requisite skills to support new infrastructure.[3] This type of inquiry assumes that technical staff, who work in a seemingly more complex environment *now*, could not adapt to the new technology with training.

Reality: This kind of resistance, while understandable in the financial services industry, fails to consider whether existing processes will continue to be sustainable. It's taking more energy and time for compliance staff to scan through mountains of messages or investigate false positives, rather than focus on the bigger picture — detecting patterns of risk before they become financial, legal, or brand liabilities. All of which might be avoided with more efficient, modern technologies.

Recommendations:

- Use the expertise of cloud and software providers to address potential compliance gaps
- Do a cost/benefit analysis on your discovery processes to understand what efficiencies can be gained with cloud-based, easily accessible content repositories
- Trust your technical staff and develop training where needed to extend their skillsets

> **"Public cloud allows you to get to business faster. It doesn't mean you don't get core cloud benefits of security, scalability, and resiliency from an infrastructure perspective, but it's not either/or. You get the benefits of picking up business agility while getting those core technology benefits as well."**
>
> John Kain
> Head of Business Development for Banking and Capital Markets, AWS

[2] https://complexdiscovery.com/a-cloudy-future-the-2021-ediscovery-cloud-adoption-report-from-everlaw/
[3] https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

3. Operational disruptions and compliance resilience

Perception: In this context, resilience is not just the unavailability of compliance applications due to a possible cloud service disruption. It's also the risk that compliance workflows can be impacted by cloud performance issues, which could slow data ingestion, search and retrieval, or the export of data required for time-sensitive compliance or legal tasks.

Reality: Public cloud services from providers like AWS are **designed to be scalable and reliable**. The cloud gives companies a richer set of choices for accessing and monitoring data to meet regulatory and legal requirements.

Recommendations:

- Firms can "dip a toe" into public cloud by starting with non-critical services and learning as they go
- An incremental approach can help firms acclimate to the growing dependence on digital communications tools
- An iterative migration enables firms to move data selectively and in smaller components that are easier to manage and with little risk for disruption

Operational disruptions and compliance resilience

Cloud scale easily translates into speed and reliability when ingesting, searching, reviewing, and exporting large datasets under severe time constraints. Scaling also enables the integration or embedding of advanced analytical capabilities to further refine and filter data before moving it to its next step in a workflow. Given today's content reality, moving processing closer to data storage locations is a much more effective strategy than the historical approach of moving the data to the processing.

> **"Fewer firms go 'all-in' on cloud at the start. Most start with some experimentation and use the lessons learned and results to progress from there."**
>
> Dan McKay
> AWS Financial Services Compliance Expert

4. Increased complexity of region-specific rules and regulations

Perception: As online services expand and the number of remote workers increase, firms are operating across geographic regions and jurisdictions. Managing cross-border data with regard to regulatory, privacy, and legal considerations with on-premise tools was already complicated. The idea of distributed data-storage locations may be considered far too complex or risky.

Reality: Data security and management is significantly better in a cloud ecosystem. The monitoring and surveillance offered by cloud providers, along with zero-trust network access, can help to allay regulatory and privacy concerns, regardless of location.

Recommendations:

- Evaluate and compare legacy systems with cloud services against Reg S-P customer data privacy requirements
- Look for public cloud providers that offer multiple geographic deployment zones around the world
- Evaluate cloud-native discovery applications with the capabilities to meet specific data protection requirements in markets that may require storing data locally for e-discovery

Regional regulations

Responding to ever-changing regulatory and data privacy landscapes requires the agility that only public cloud infrastructure can offer. It's simply impossible to build a data center in any reasonable period of time to address new rules or laws that require that data be maintained within a specific country.

5. Economic justification

Perception: Moving to the public cloud means abandoning an infrastructure that may still have years of useful life. It also means running two systems in parallel for a short time, which can elevate costs and require upfront investment. From an infrastructure viewpoint, an investment in the public cloud would be challenging to support — especially when it's considered to be non-revenue-producing.

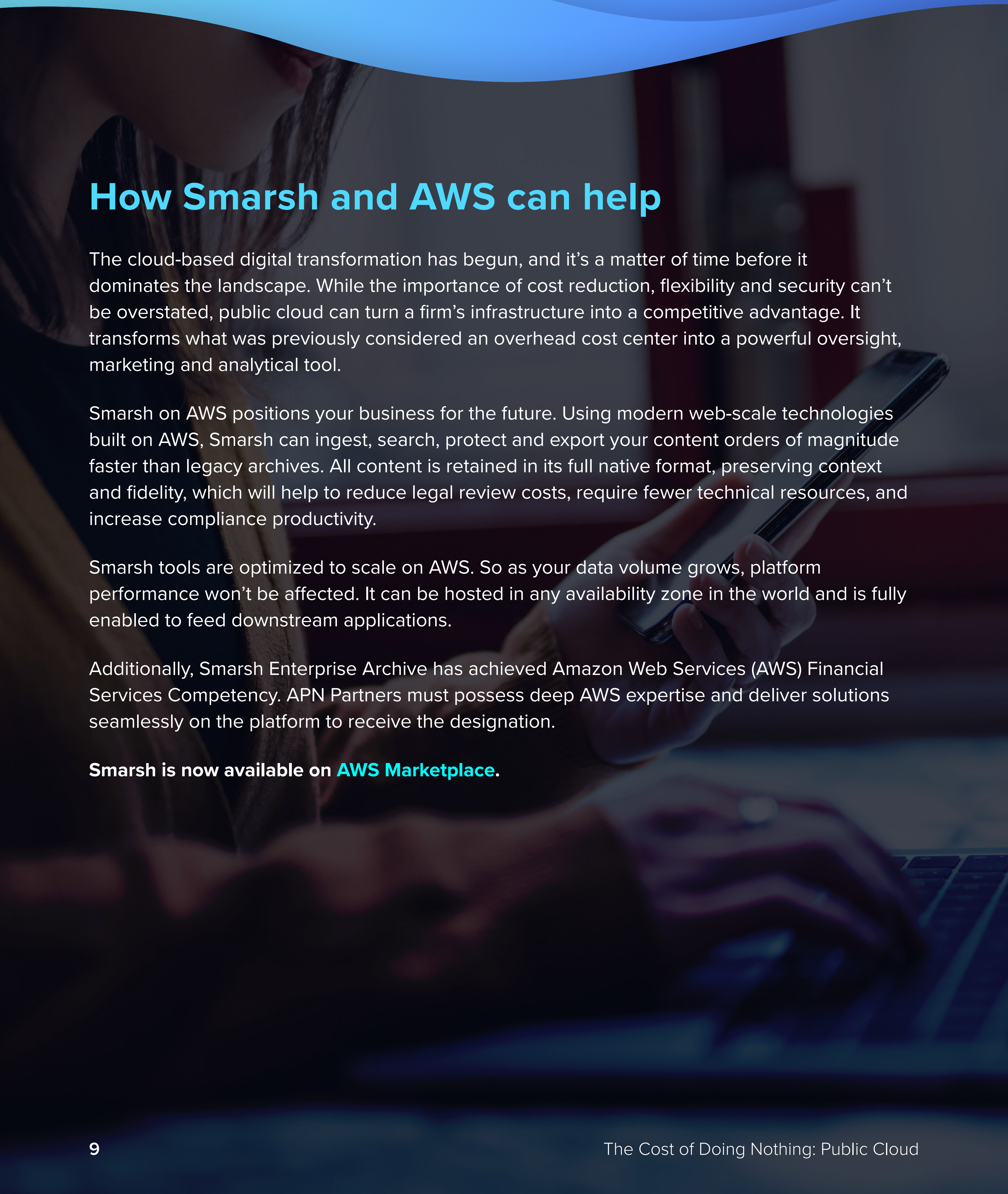
Compliance	Legal	IT
While cost savings may be realized in the longer term, initial investments and ongoing operating and storage costs have caused financial firms to revisit their cloud cost savings projections. With respect to compliance, the agility and scalability that cloud offers translates to improved response time and greater productivity for compliance staff.	Legal review is often inefficient and costly. Improved response time can make the difference between meeting a court deadline, or not. It also translates directly to productivity gains for corporate legal or internal IT staff.[4] For those leveraging outside service providers, the ability to filter content from a single-source cloud repository can be easily calculated on a per-GB or per-hour basis.	What is true for messaging can be true for a wide range of interconnected IT applications. Standardizing application interfaces in the cloud and truly creating one global platform allows vendors to know what components to upgrade. It also simplifies review and testing prior to release. Problems and incidents would be far less common and maintenance and support less resource intensive.

Reality: Value is not just a function of cost. Moving to the public cloud has a future cost-saving component and a huge reduction in capital investment — even if not in the short term. It also enables **reliable connection with customers** on the platforms they prefer to use.

Consider the following opportunities:

- Cloud services offer immense scalability and speed to market
- Cloud can make it faster and easier to support new technologies for communicating with potential investors
- Enabling hybrid/remote work is necessary for staying competitive

[4] https://complexdiscovery.com/a-2020-look-at-ediscovery-collection-task-spend-and-cost-data-points/



How Smarsh and AWS can help

The cloud-based digital transformation has begun, and it's a matter of time before it dominates the landscape. While the importance of cost reduction, flexibility and security can't be overstated, public cloud can turn a firm's infrastructure into a competitive advantage. It transforms what was previously considered an overhead cost center into a powerful oversight, marketing and analytical tool.

Smarsh on AWS positions your business for the future. Using modern web-scale technologies built on AWS, Smarsh can ingest, search, protect and export your content orders of magnitude faster than legacy archives. All content is retained in its full native format, preserving context and fidelity, which will help to reduce legal review costs, require fewer technical resources, and increase compliance productivity.

Smarsh tools are optimized to scale on AWS. So as your data volume grows, platform performance won't be affected. It can be hosted in any availability zone in the world and is fully enabled to feed downstream applications.

Additionally, Smarsh Enterprise Archive has achieved Amazon Web Services (AWS) Financial Services Competency. APN Partners must possess deep AWS expertise and deliver solutions seamlessly on the platform to receive the designation.

Smarsh is now available on AWS Marketplace.

smarsh®

Capture, archive and discover in the cloud.

Find us in AWS Marketplace.
Available Now!

aws Available in
AWS Marketplace

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals from more than 100 digital communications channels. Regulated organizations 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. 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 attorney regarding your compliance with applicable laws and regulations.

Guide - 06/22

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