Alfresco®

Secure Data Management: Addressing the Weakest Link in Government Security

Once upon a time, this was the best possible way to protect government assets.

Those days are over.

Welcome to Now.

In the wake of the 2016 presidential election, America grappled with news that Russian hackers had interfered with U.S. democracy. The weakest link proved to be the human factor. The Clinton campaign manager had unwittingly granted access to his entire email inbox.

In a 2016 survey of federal cyber executives, 42 percent of respondents indicated that people are their agency's greatest vulnerability to cyberattacks. The Pfc. Manning, Edward Snowden and Harold Martin cases certainly show that classified information can be stolen by inside actors. Additionally, a recent article revealed that in 2015, two-thirds of government data breaches were due to accidental leaks—data spillage—that exposed 21 million identities, compared with six million by hackers.

The Obama administration earmarked $19 billion for the 2017 cybersecurity budget, $5 billion more than the year before. In recent years, government cybersecurity has focused on creating a secure perimeter. Such crucial efforts often conflict with users' need for real-time collaboration with constituents, agencies and stakeholders that reside outside the perimeter.

As a result, users resort to workarounds that undermine the best security efforts. The Clinton email server investigation revealed that antiquated State Department systems made it difficult to get work done and that diplomatic information routinely transited outside the classified system.

Across most agencies, exponentially growing information is kept in siloed repositories. Authorized users have no easy way of identifying where the content they need is stored, how many copies exist, what the classification level is and what should be archived or destroyed.

Today, it is not enough for government cybersecurity measures to reinforce the perimeter. Most cybersecurity experts agree that there is always a way in and that "data breaches are [only] an issue of when", not if. In the cloud era, keeping all information fenced in is becoming less feasible anyway. China was invaded three times despite erecting a Great Wall that was too high to climb, too thick to topple and too long to go around. The gatekeepers proved to be the weakest link.

This is why modern content services solutions work with users, not against them, by securing data at the source and in motion. They give authorized users secure access to the information they need, the ability to safely collaborate with outside stakeholders and the capacity to be fully productive.

Challenges

What are the main challenges facing agencies in securing users' IT environments?

- ✓ ***Reducing the surface attack area by eliminating unnecessary data***—It is estimated that only 0.5 percent of all digital content is ever analyzed and used, yet most agencies have no clear idea of the information they are storing, let alone what is redundant or expired and should be destroyed.

- ✓ ***Securing data at the source***—Agencies must identify what needs to be safeguarded and assign security levels to that content. Yet the proliferation of discreet solutions—content services, records management, task management, etc.—creates silos of information that prevent holistic data management. Single sign-on technology does not provide for a granular access control of data in a manner that is scalable.

- ✓ ***Securing data in motion***—The need for collaboration with outside agencies and constituents, and for cloud systems, creates holes in the defense perimeter. Government must enable users to safely share content inside the context of approved business processes. The alternative to providing an approved enterprise solution is far riskier because it forces users to resort to unvetted solutions to collaborate.

- ✓ ***Securing ALL types of information***—Users are deluged under an increasing torrent of unstructured data (Word documents, Excel spreadsheets, multimedia, videos, images, spatial data, etc.). In fact, 80% of the data stored by government agencies is unstructured in nature. All content, regardless of its nature, must be tagged, organized and safeguarded.

- ✓ ***Eliminating human error***—Expecting individuals to consistently follow tedious data inventory processes is not scalable. A study of a sample of U.S. State Department files found that even highly trained workers had inadvertently declassified the majority of the content. Rules-based auto-classification and archiving reduces mistakes and increases compliance.

- ✓ ***Phasing out antiquated systems***—Outdated applications do not support best practice security measures. Testifying on the Office of Personnel Management's security breach, former Director Katherine Archuleta explained that employees' biometrics data and Social Security numbers stored by OPM were not encrypted because encryption couldn't be done feasibly with the agency's antiquated systems.

- ✓ ***Providing an audit trail***—Chief information security officers must be able to show that good information governance measures had been put in place should an incident ever occur.

How Agencies Can Address These Challenges

First, agencies must unify data across all repositories. Open standards-compliant enterprise content services can natively communicate with the vertical solutions (task management, case management, grant management, correspondence management, etc.) that make up the enterprise portfolio. Open standards also allow select information to be shared with other agencies or outside partners.

With inefficiencies removed, all of the agency's information can be governed in a holistic way across all internal departments. All structured and unstructured content can be tagged and organized. This establishes a repeatable, scalable data inventory process. It allows agencies to minimize the surface attack by eliminating unnecessary repositories of sensitive data and focusing on what truly needs to be secured.

This approach also greatly boosts efficiency within the organization: it permits advanced cross searches on all types of content (documents, email, videos, social media); cuts costs on storage, hardware, licenses and maintenance; reduces errors through unicity of data and versioning; and allows fast responses to Freedom of Information Act requests.

The next step is to implement intelligent access controls and monitoring. It means delivering the right content to the right person at the right time and in the right place, integrated with the systems that each person uses to do his or her work. Enabling secure outside access and collaboration means that security follows content to whatever person or place it is sent while confirming that access controls are properly maintained.

Users can't interrupt their business process to assign security protocols. It has to be built into the solutions they use. The use of rules-based auto-classification, records compliance and security protocols to create, receive, maintain, manage and dispose of records across their lifecycles greatly reduces human errors.

The project must follow an open, collaborative approach. Enterprise content services and records management initiatives typically have a 50 percent failure rate because the business owner is not consulted. Data decisions must be made in agreement between business owners, data custodians, chief information security officers, and chief information officers.

By applying a security solution that organizes and prioritizes content in a transparent way, and then applies that security throughout the entire associated business process, agencies can empower their content, rather than simply securing it.

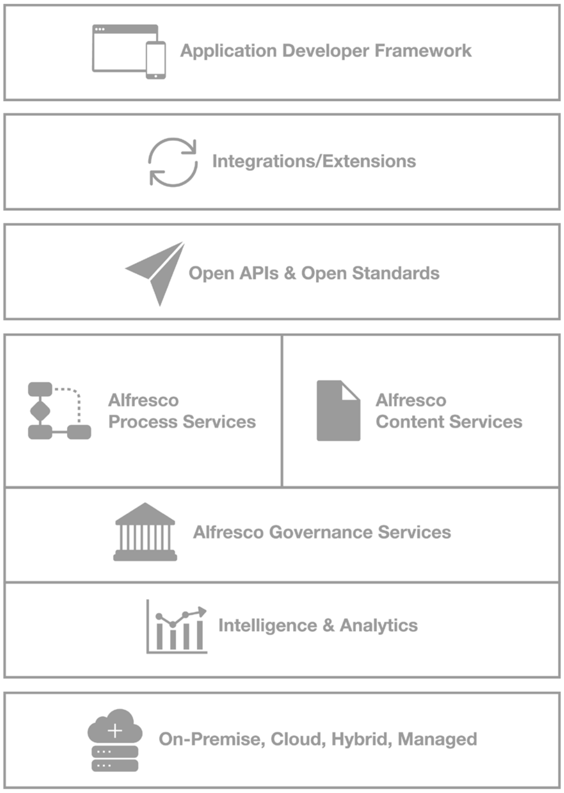
Most important, users have access to the information they need, no more and no less. By working with them and not against them, the system greatly boosts employees' satisfaction, compliance to security protocols and productivity.

About Alfresco

Alfresco helps agencies advance the digital flow of government business by modernizing content, process and governance services on a single, integrated platform that meets DoD 5015.02 compliance standards for records management.

The Alfresco Platform eliminates the burdens of legacy technology systems and delivers the highest levels of security and compliance standards. It secures content at rest and in transit and includes enhanced automated security features such as designated records management roles for workers and intelligent classification of records. With the Alfresco Platform, government can harness the power of digitization, automation, cloud and open source technologies to meet program needs in key solution areas:

- Compliant Records Management
- Task Management
- Case Management
- Digital Asset Management
- Grants Management
- FOIA Management
- Correspondence Management
- Data Management
- Workflow Management
- Email Management


Application Developer Framework
Integrations/Extensions
Open APIs & Open Standards
Alfresco Process Services
Alfresco Content Services
Alfresco Governance Services
Intelligence & Analytics
On-Premise, Cloud, Hybrid, Managed

The Alfresco Digital Business Platform lets IT teams quickly develop and implement modern solutions that accelerate digital transformation and enable leaders to make intelligent, fact-based decisions. The open, modular platform is easy to build on, integrate and extend for faster time to value for your agency.

Alfresco eliminates the need to purchase and support multiple applications on disparate systems, saving organizations millions of dollars. Agencies at all tiers of government use the Alfresco Platform to modernize operations, work smarter and more collaboratively, and achieve breakthrough efficiency.

The Alfresco Digital Business Platform delivers a comprehensive enterprise-wide solution. With Alfresco government agencies can enable real-time, informed decisions, create intelligence and deliver real value for the organization, employees and citizens.

The Alfresco Platform Enables Agencies to:

- Securely Govern Information and Records in Transit and at Rest
- Modernize IT Systems to Increase Efficiency and Reduce Costs
- Deliver Outstanding Experiences for Employees and Citizens
- Build Intelligent Business and Mission-Essential Solutions at Breakthrough Speed
- Accelerate the Pace of Innovation Across the Enterprise
- Securely Comply with NARA 2019, FOIA, ISO and Cloud and Open Source Mandates

To find out how Alfresco can help you advance the digital flow of government business to deliver on your mission and slash costs, visit www.alfresco.com

Alfresco®

Learn more at **alfresco.com**
Alfresco Americas: +1-888-317-3395
Alfresco EMEA: +44 (0)1628 876 500
Alfresco Asia Pacific: +61 2 8607 8539
Contact Sales: **info@alfresco.com**