Build your own On-prem Enterprise File Sharing & Content Collaboration Platform

In-depth review of FileCloud's hyper-secure EFSS capabilities by Broadband-Testing

BROADBAND TESTING

First published May 2022 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet: HTTP://www.broadband-testing.co.uk

TABLE OF CONTENTS

.....i

TABLE OF CONTENTS..... 1

BROADBAND-TESTING 2

EXECUTIVE SUMMARY 3

WHAT TO LOOK FOR IN A CONTEMPORARY DATA STORAGE AND CONTENT COLLABORATION SYSTEM. 4

PRODUCT ANALYSIS 6

Initial Deployment And Management.....7
The User Experience.....8
A Look At FileCloud In More Detail.....9
Gartner Peer Insights: Customer Survey Results 12

USE CASES 13

1: Control Around Data Residency 13
2: Access To Existing Enterprise Content.....14

IN CONCLUSION 16

Figure 1 – FileCloud Content Model.....6

Figure 2 – FileCloud Management GUI 7

Figure 3 – The User View Of The FileCloud World.....8

Figure 4 – The Content Lifecycle: FileCloud Perspective.....9

Figure 5 – Compliance Issues Flagged Up.....12

Figure 6 – Securing Data Residency.....14

Figure 7 – Setting Up NTFS Network Shares 15

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECUTIVE SUMMARY

- Data is increasingly the most valuable asset of almost any company or business yet, often, it is stored in a rudimentary way with little to no security, ease and breadth of access – for controlled collaboration - or migration necessities.

- As cloud-based storage has grown exponentially over the past few years, it has become perceived as "the norm" for many companies and users yet, in many cases – where data is sensitive and/or of particular value - 3rd party cloud-based storage is far from ideal. Think of user types such as government, defence, financial institutions, legal, manufacturing, education… Not actually being able to directly manage the location of that data is also a potential – and expensive – liability.

- While ease of use and scalability are generally seen as primary benefits of a cloud-based approach, that doesn't mean an On Premise (OnPrem) solution – with potentially far greater security and manageability – can't be just as easy to deploy, configure and manage, and equally scalable. Another factor often thrown into the ring by cloud-based solution providers – that of low operating costs – is often a fallacy, as businesses find out to their (literal) cost. Low starting prices can hide the true operating costs of a cloud-based solution once data rates start ramping up – which they will and do!

- Often data storage solutions provide very fundamental user access and management options – little or nothing more than a desktop/laptop OS does. Moreover, Enterprise-level requirements such as compliance, data governance and wide-ranging security requirements, including Data Leak Prevention (DLP) and Digital Rights Management (DRM) are completely overlooked. It means that valuable data can be completely unguarded beyond basic security access.

- With its flexible OnPrem driven content management solution, FileCloud is looking to offer an Enterprise-focused alternative, designed from the ground up to include all the aforementioned features and beyond, including workflow automation. Moreover, unlike a typical cloud-based solution, it doesn't force you into migrating existing data into a new home, but supports existing network shares, meaning rapid deployment times.

- Depth of features and flexibility doesn't come at the cost of complexity. In use, FileCloud is as simple as a Windows or Mac desktop – or indeed any of the cloud-based storage solutions. So, from an end user perspective, there is no extensive, additional training requirement – just a familiar way of accessing their data. From a collaborative perspective, the amount of fine tuning on everything from access rights to retention policies and all stops in between, means that it provides a global solution that is secure in all aspects and compliant across different continents.

- When evaluating the FileCloud offering, even Gartner could see no direct competitor, other than by taking a DIY approach which, for the vast majority of businesses, is a completely unrealistic – expensive and unattainable – option.

WHAT TO LOOK FOR IN A CONTEMPORARY DATA STORAGE AND CONTENT COLLABORATION SYSTEM.

Until the rise of the Internet, businesses were primarily defined by what product or service they offered and their value was based around the profitability of those offerings – what they made and/or delivered *was* their business.

But with the Internet and the movement of sales and marketing online (even if only for directing human traffic to physical locations) came the gathering of data. Amazon is the obvious "in your face" case here, but it applies equally to any business where customers register online and start to provide personal data that shapes their buying profile. It is much the same story within a company itself; staff are managed via internal or 3rd party software – all their personal and company-related data is stored and used throughout (and effectively beyond) their time with that company.

Now, add in the impact of the pandemic and the enforced adoption of more WFH/WFA (Work From Home/Anywhere) employee strategies and that online data becomes more crucial – and more vulnerable to exposure or capture – than ever. Content and workforce collaboration systems have been around in one form or another for decades now, but it was the pandemic impact that saw them explode into use. So, add in the geographical dispersion of users, combined with a huge increase in remote location-based online meetings and project collaborations and it becomes clear that – other than ease of access (a given) – factors such as data security, residency, compliance, governance and user access management (beyond a basic allow/deny policy) become mandatory controls. In many cases the data/content *is* the business now; should that data be breached or leaked, the consequences are potentially – and genuinely – disastrous for the company concerned. It is also important to understand that data and content are about far more than the file type and the contents therein.

The widespread adoption of cloud-based storage, cloud simply being the latest version of "outsourcing" in reality, has seen vendors – in many cases – switch from an OnPrem to a cloud focus. But is this really what every company wants – data and content that is effectively out of their control, physically and geographically – when that data is their crown jewels? Cloud-based storage is essentially promoted on the basis of ease of access and cost. The former is an absolute, but the latter often shocks customers once data levels start to ramp up. Moreover, support for existing data repositories is often largely – or totally – lacking, meaning mass data migration is often an unwanted, timely and expensive part of the move to the cloud. Yes, there are scenarios where a cloud-based solution can indeed make a lot of sense, as it does with many other IT infrastructure services, but it is most certainly not a "one size fits all" solution – anything but.

At Broadband-Testing, at the beginning of 2020 we attended and reported on a data, application and platform migration event for the financial sector in London's City and Docklands areas (think major global banks, merchant banks etc) and the primary concern among all was the security, governance and compliance of the related data content. Note – this was pre-pandemic, so the stakes are now significantly higher, in terms of the data and user dispersion since. Concerns were equally over the cost and difficulty of the migration and the training costs involved in learning how to administer new platforms, then losing that expensively-trained staff and starting all over again.

It is not solely the financial sector that is concerned over the security and governance of its data and content. The same case can be made for many verticals, from government and defence, through healthcare/pharmaceuticals, manufacturing, legal, energy and utilities, education and others. That does not make it a minority requirement. Even relatively small businesses with a very high content value/turnover – think legal or accounting, for example – have a natural inbuilt and "healthy" paranoia for the health of their data. The question is: how aware are these businesses of there being an alternative to the "in your face" cloud-based services whose marketing cloud invades every Internet session you embark upon?

Storage providers focused solely on cloud-based services typically cite high CapEx (Capital Expenditure) costs, the equally costly difficulties of maintaining systems internally, extended implementation times and a lack of flexibility – and even security – with OnPrem solutions. Historically, they have a point – but the IT world has changed beyond recognition from 20 years ago. Even those cloud-focused solution providers admit that TCO (Total Cost of Ownership) is a benefit of going OnPrem, that complete control over every aspect of the solution is now another huge OnPrem benefit and that users are not 100% reliant on having Internet connectivity in order to access their data content. Moreover, they admit that cloud-based solutions are fundamentally restricted in terms of customisation and – in many cases – advanced feature options (see the section on the power of metadata later in the report).

In other words, you sign up to that providers' way of maintaining your data and content – not one that is designed specifically for your own business case. In many ways this is like traditional Enterprise applications of the past, where you (expensively) bought into their very fixed software methodology, with little or no capability to adapt their solution to your own company requirements. Modern DevOps approaches have made Enterprise software far more flexible than in the past, so why effectively step back in time, in terms of how your data and content is managed?

Imagine, then, an OnPrem solution that – therefore – has all the benefits cloud-based providers agree it has, but that also has none of the cited negatives and restrictions they use to validate the cloud-only option. Best of both worlds? That is certainly the aim of FileCloud – the subject of this report – in bringing OnPrem into the contemporary world as a valid cloud-based alternative. First, it is important to stress that FileCloud can provide cloud-based services, or indeed a hybrid solution, but its focus is on revolutionising the OnPrem approach.

We will now take a look at the FileCloud OnPrem solution, including deployment options, such as supporting existing networked data shares, administration and the range of Enterprise-level features that are designed to differentiate the FileCloud solution from generic cloud-based alternatives.

PRODUCT ANALYSIS

FileCloud is a complete file sharing, data management and content collaboration system.

In this sense, it goes far beyond populist file sharing applications, looking to provide every element of an Enterprise-strength file system, from breadth of management features, including key global features such as compliance management and extensive security options (from layered access control to DLP and DRM), workflow automation and extensive data classification options. This depth of functionality sets FileCloud aside but, above all else, it is the ability to run this as a cloud-style system but on your own infrastructure, OnPrem – a massive security and management benefit for many customer types, as well as making longer term TCO more predictable and affordable. That said, FileCloud is available as a pure-cloud service, or indeed as a hybrid, but it is the OnPrem deployment option that is the true differentiator.

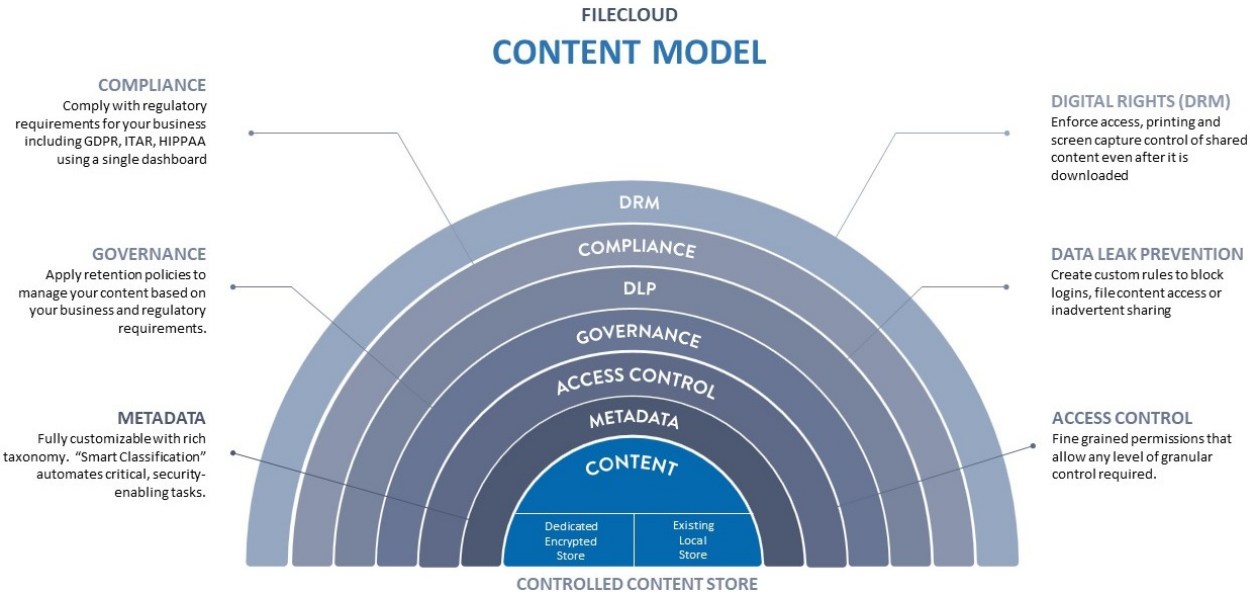


Figure 1 – FileCloud Content Model

The FileCloud world is best viewed as a layered content model – almost a content/storage equivalent of the old OSI network reference model, for those familiar with that classic conceptual depiction of networking layers that became the industry norm.

Taking the model approach from bottom up, we've already noted in this report that – to many companies now – their data content is everything. There are two key aspects to that content; accessibility and security. In a sense, these are contradictory elements – the easiest form of data access is open access, but – given its value in a contemporary world – that data needs to be as secure as possible. Foremost, then, is to take an approach where that content is as close to the users as possible, as easy to find as possible, but only to those who have the rights to access that content.

The starting point here is in deploying and configuring FileCloud to maximise both those elements, so we'll now look at some hands-on interaction with the product itself.

Initial Deployment And Management

For all the talk of FileCloud differentiators, all would be for nothing if the product then proved slow and difficult to deploy, configure and manage, but that "cloud-like" ease of deployment and accessibility is at the heart of the product. The basics are achieved potentially within minutes or an hour at the most. Windows, and Linux platforms are all supported for server deployments, as are mobile endpoints (IOS/Android). Everything is managed from a single GUI. Configurable alerts on FileCloud activities start being sent to a chosen administrator as soon as the platform is deployed, so it's operating from the get go.

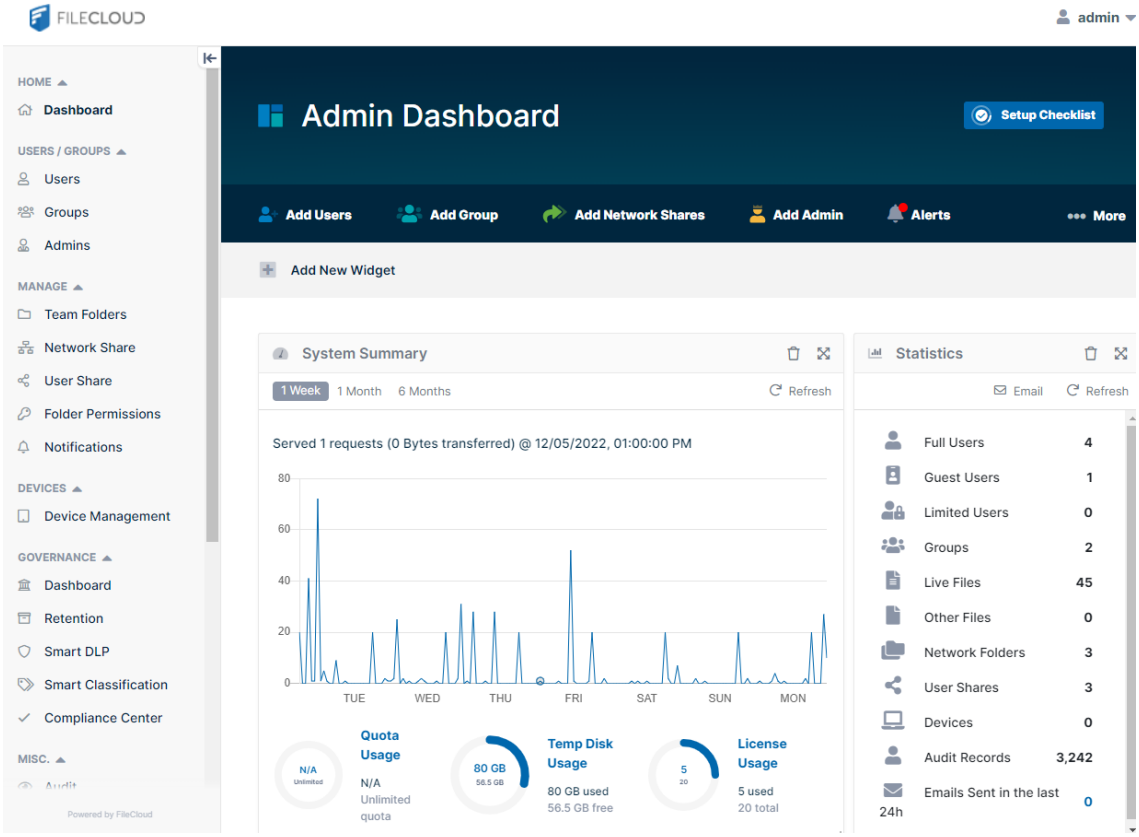


Figure 2 – FileCloud Management GUI

While the basic walkthrough of file and content setup and user management is straightforward enough, FileCloud does provide backup assistance in the form of a Setup Checklist you can refer to from the Dashboard. This enables you to cover off the basics, through the user accounts management (Authentication), Network Shares (see next), Sync and Backup, Customisation and additional configuration tasks, such as setting up team folders (see User Experience).

Importantly, unlike most cloud-based file storage and sharing platforms, FileCloud does not require you to migrate all your content to the new location as part of the deployment process, but supports existing network file shares, including Active Directory (AD) based NTFS-specific shares, as well as standard network share paths. For many companies, this could save days of deployment time, as well as minimising the ongoing management requirement – see Use Case 2 later in the report. There's a classic saying in IT "If it ain't broke, don't fix it" – the less change you need to make, the better!

The User Experience

Looking from a user – rather than administrator – perspective, again the FileCloud approach would hit the buffers if the user experience were compromised, or simply very different to what they know and expect.

Users are creatures of habit; changing the working methodology can result in significant production losses, or even increased staff churn and turnover. However, the FileCloud user experience is comfortingly familiar.

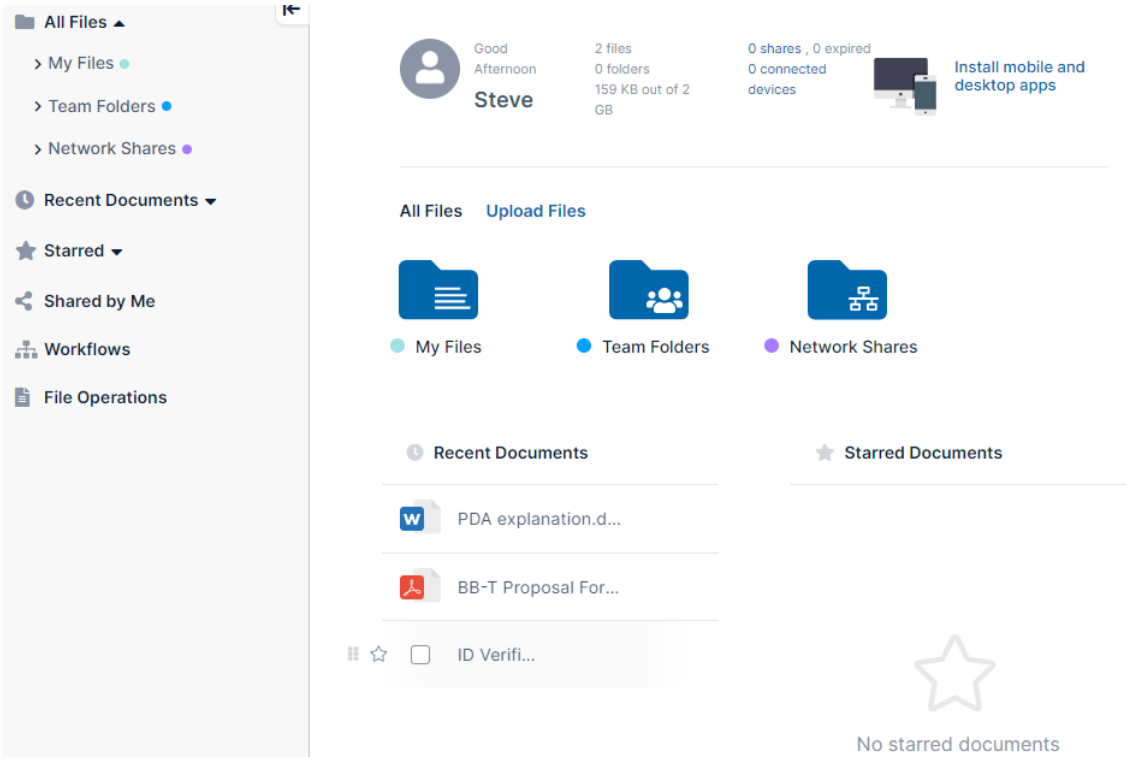


Figure 3 – The User View Of The FileCloud World

The user interface is reassuringly simple and focuses purely on ease of access to their content. Four basic file folder types are created – My Files (personal), Team Folders (for team collaboration work) and the aforementioned Network Shares as well as a 'Shared with Me' folder (when files are shared with you by another user). Standard, Windowsesque menus and drag and drop techniques are the "drive" requirements – nothing more.

On the right of the user interface screen is a summary of their activity (can be hidden) with one-click access to related documents. Also from the user interface, the mobile app version of FileCloud can be downloaded directly (AppStore or GooglePlay) as can related sync applications. So, users do have the ability to alleviate the support burden by performing some routine setup tasks themselves.

A Look At FileCloud In More Detail

Content – data files – have far more relevant information contained within them, that is potentially useful for searches and access control, than most people consider.

Key with the FileCloud approach is to make use of every single element of those files and content to maximise that mantra of ease of access, but as secure as possible. In practice, it's not as simple as that – security expands beyond access controls to issues such as DLP and DRM, as well as guaranteeing compliance across the globe. Tied in with the latter are the retention policies that satisfy both business and regulatory requirements – data governance, in other words. Here, again, is where FileCloud distances itself from the pack; consumer-oriented, cloud-based storage solutions, and even those with added "Enterprise" bells and whistles are far from comprehensive in covering off all of these requirements. Yet, from an Enterprise viewpoint, take a look at that Content Model and say which of those layers couldn't be seen as mandatory within a business environment, in what is a world with global reach, regardless of physical location?

It is also important to understand that the content storage world is not static; data is added relentlessly, archive strategies need to be managed, retention policies need to be updated as legal requirements and government rules change… In other words that data goes through a lifecycle, so FileCloud mirrors that lifecycle approach to its content management. Here is where the flexibility and breadth of content definition becomes fundamental to the FileCloud approach. It helps define how that content is managed through every step of its lifecycle:

Data retention: the content's life will vary from location to location, data type, and many other variables, but the defined retention policy stays in place throughout.

DLP: using rule-based management factoring in any data element to track – such as metadata – data leaks, whether accidental or malicious, can be monitored and controlled.

Archiving/Change monitoring: the data retention policies can auto-define when archiving or data expiration takes place. At the same time, FileCloud monitors for content changes, in which case the revised data file effectively commences a new lifecycle.

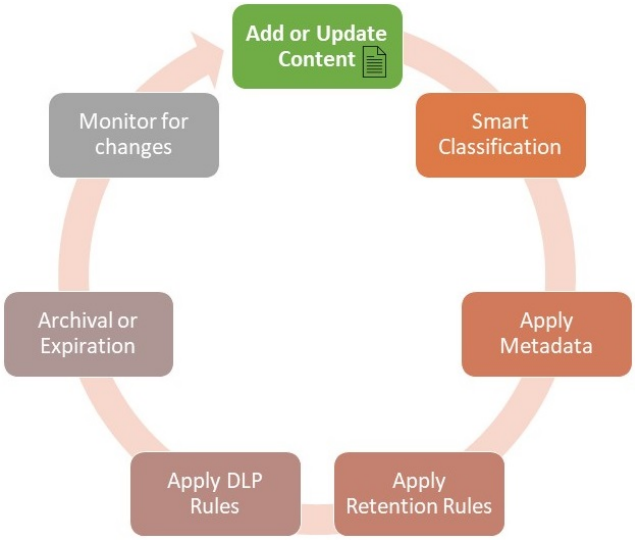


Figure 4 – The Content Lifecycle: FileCloud Perspective

FileCloud OnPrem Versus The DIY Approach

No less a body than Gartner made the point that FileCloud's only real competition is a do-it-yourself approach, manually gathering together and integrating the many and various components that the FileCloud platform consists of.

Without even analysing this approach in any depth, it would seem obvious that it is fraught with complexity and limitations, despite the seemingly "open platform" offering unlimited options. In practice, relying on a number of different 3rd party components means that all those elements must continue to be supported by their creators on an ongoing basis. Should any element become end-of-lifed or simply no longer supported, the DIY approach means then finding replacement components and recommencing the integration from scratch. Even when all the elements continue to be available and supported, every time one is updated, more potential configuration and integration woes await. In general, updating and improving a DIY solution, in the same way a platform vendor such as FileCloud will, is going to be, at best achievable in a very expensive fashion (time and components costs) and – at worst – impossible, so you end up with a static solution that will become out of date.

At Broadband-Testing, over the years, we have had the opportunity to compare – across various spheres of IT – specialist products versus their DIY equivalent, and in every case the DIY approach failed miserably – and usually expensively.

Looking at the potential ways to exploit every element of a data file – and the content within – using FileCloud reveals a wealth of information on which to base a search, a methodology for data procedures – retention, tracking and tracing, regulating compliance (sovereignty and residency) – or providing very specific, or very broad, access, to satisfy every user and group requirement.

This ability to use any element of content means, in turn, that access control is incredibly flexible, both from a user and administrative perspective. In each case it provides considerably more options than is typically the case with a cloud-based solution and can be combined with other elements of FileCloud – such as workflows or retention policies – meaning the access controls apply over a content's lifecycle. It also means that file access can be every bit as flexible OnPrem as within a public space, yet it is secured from ever being on a public share.

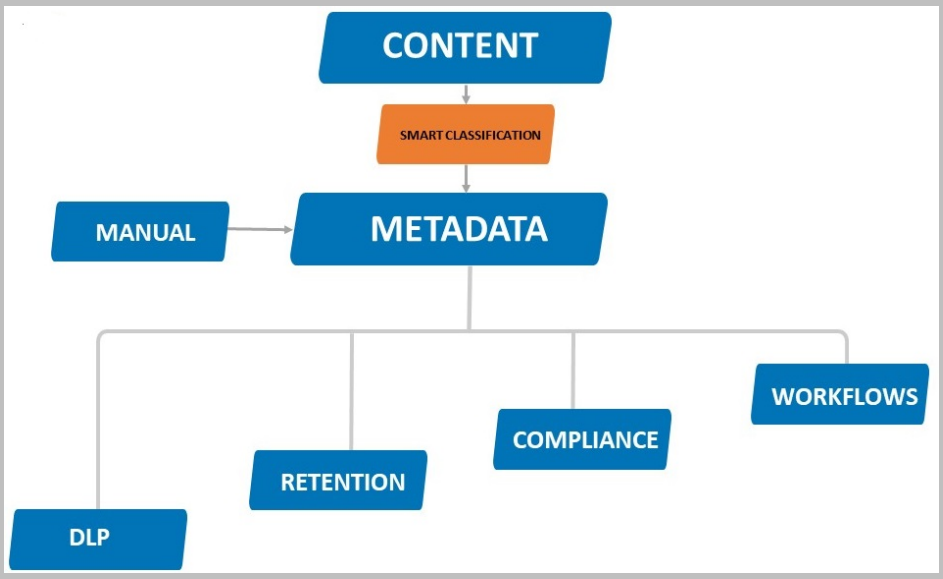
At all levels, data governance is fully controllable in an entirely flexible fashion. A perfect example here is with regards to DLP. As noted earlier, whether intended or otherwise, data is often leaked; in worst-case circumstances it could ruin a business. The FileCloud system acknowledges and manages not simply the threat of DLP, but also how it interconnects with every other aspect of data governance. Using a rule-based approach to DLP management it can interact with the other elements of FileCloud to automate the security of data to prevent the leaks from occurring.

The Power Of Metadata

File metadata (broadly described as descriptive, administrative and structural) has enormous value in its own right, yet is often ignored by leading storage providers.

It is structured data that provides additional information about files and folders and is fully utilised within FileCloud, including the automatic import of all metadata from a number of applications and data types. Administrators can manage metadata attributes and sets, and define permissions based upon specific metadata. Within the context of FileCloud, metadata has many different applications, in terms of using it to organise content to enforce policies and behaviours, such as DLP, data retention and data governance. Used with FileCloud's Smart Classification system, custom metadata can be used to automate file tagging and apply retention policies across all uploaded data.

One such example would be where an invoice – say in PDF format – has been tagged to search on the word "hardware", which has been added to the metadata. The system could then automatically identify that invoice as a hardware invoice for classification purposes. Equally this could apply to content with, for example, a social security reference or a debit card number. From a human search perspective, it could literally save hours or even days of manual effort, often in a scenario where time is precious and the inability to track that content down is expensive. From a FileCloud perspective it means metadata is potentially at the heart of every element of the platform, especially when combined with smart classification.



Add in the compliance management - controlling regulatory requirements including GDPR, ITAR and HIPAA – and the data governance/residency story is fully covered. For example, once compliance has been enabled for each and/or any standard, any issues preventing compliance are immediately flagged up to the administrator.

DRM is another aspect of data governance that is fully managed by FileCloud in a proactive, not reactive, way. In the latter case, DRM disputes are notoriously complex, expensive and time consuming to resolve, so better to simply prevent it in the first place.

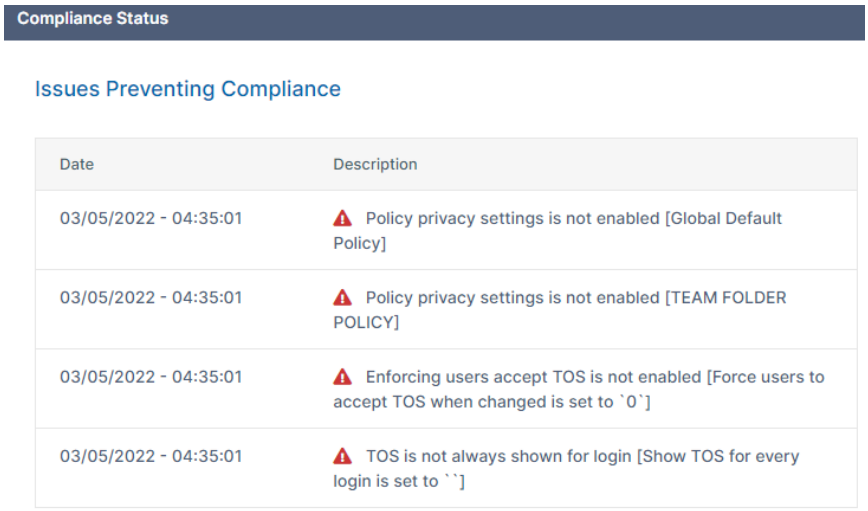


Figure 5 – Compliance Issues Flagged Up

Again, flexibility is key here. Within FileCloud you can protect exactly what aspects of content you need to, including down to the ability to let a given user see only part of a file at any one time. An integrated DRM viewer allows total control over document views, from zero, through partial, to complete visibility. Even the number of access times can be limited.

Gartner Peer Insights: Customer Survey Results

In addition to providing our own Broadband-Testing view of FileCloud's offering, we also felt it worth sharing the thoughts of Gartner's Peer Insights survey customers directly about their experiences with the product. The complete survey is available from this link:

https://www.gartner.com/reviews/market/content-collaboration-tools

Here are some example customer summaries from the survey:

The best cloud-based substitute solution for data sharing and collaboration

"The FileCloud software from CodeLathe has been a huge success in our company. Everything from the implementation of a demo through the sales process and the long-term support is top notch. The product works exactly the way you would expect, and has well thought out features that competitor products simply don't provide. There's nothing in the market that stands out like FileCloud in terms of price, usability, support and features. If you're looking for a file sharing solution for small companies up to enterprise organisations, don't miss this gem."

The Best Cloud-Based Substitute Solution For Data Sharing And Collaboration

"Our entire team uses FileCloud to secure their information, and it includes encryption features. We'll use antivirus and ransomware protection to automatically scan our data. It gives us complete control over our company's data.

We do not wish to construct a new document flow/workflow; instead, it will work with our existing network. We will be able to share files with our clients in a secure and easy-to-access manner by using FileCloud. It was a great fit for us when we wanted to give all of our user's OneDrive-like access to our internal file servers. The user experience is amazing, and it's very straightforward to set up and connect to our internal storage."

Efficient Content Collaboration Tool

"Provides organisational transformation services by combining different tasks into a unified automated framework. It is indeed a cloud-based application. Accessibility, governance, invoicing, monitoring, and analytics are all wonderful benefits. Online business help is available 24 hours a day, seven days a week. SaaS (Software as a Service) is an option. It simplifies the process of creating and operating a private cloud. Our full squad uses the FileCloud to preserve our information, and it includes encryption abilities. We'll use antivirus and ransomware protection to automatically scan our data."

Best Solution For Education For Securing And Sharing Our Files With File Cloud Safely

Overall Comment: "We are using the FileCloud to secure our files and our entire teams use it and it offers encryption features. We will be doing automatic scanning for our files using antivirus, ransomware protection. It offers complete control of our enterprise data. We don't want to create a new documents flow/workflow - it will be functioning with our established network. By using FileCloud we will be sharing the files securely to our clients and made easy to access."

USE CASES

1: Control Around Data Residency

Any business needs to know where its data resides and what local rules and regulations – compliance, for example – applies in each case.

With a cloud-based solution, data residency is often questionable at best. With FileCloud's OnPrem approach, the local ownership of the content impacts positively on every aspect of data governance, with complete control over data residency and – at the same time – data resource from the content and data store itself, through every aspect of the application and OS stacks, and the entire storage network infrastructure from a security and authentication perspective.

In a public space, all of these in theory are at risk or, at best, uncontrollable. Moreover, in many use cases, the required features are simply unavailable.

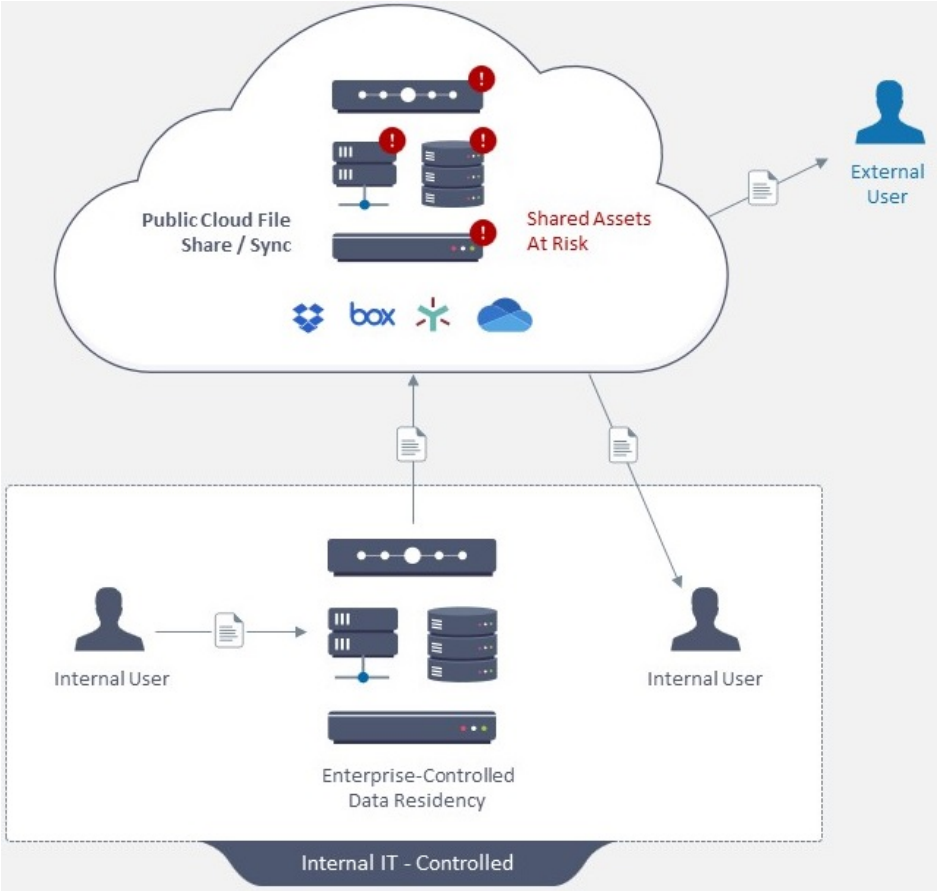


Figure 6 – Securing Data Residency

The result of FileCloud's approach is a multi-layered and fully interconnected approach to managing data residency. It provides secure file and document sharing and completely controlled – and secure – team collaboration, with full data governance and compliance – all in a single system, fully secured and managed OnPrem, but with the flexibility of a cloud-based solution.

2: Access To Existing Enterprise Content

We noted earlier in the report that a major issue for companies potentially moving to a cloud-based data and content storage solution is that all of that content has to migrate to the new platform. For businesses with potentially petabytes of content accessible via existing local network shares, this is a major – and expensive – obstacle. With FileCloud however, pre-existing files and shares – and storage – can be fully integrated. In contrast, with a cloud-only scenario, how can an organisation make network file server data accessible via the cloud without moving that data? Moreover, how can they then share it with 3rd parties as required, without asking them to move their own data? As we've noted earlier in the report, FileCloud does not require you to migrate all your content, but supports existing network file shares, including AD based NTFS-specific shares, as well as standard network share paths and Smart Mount shares for specific access needs.

In terms of flexibility in providing access to those shares, FileCloud supports aggregating users into groups, allowing an administrator to assign file and folder share permissions to specific groups, rather than applying global or user-specific policies only. This feature is available across the full range of permissions, including share links, metadata, team and network folder, and NTFS permissions.

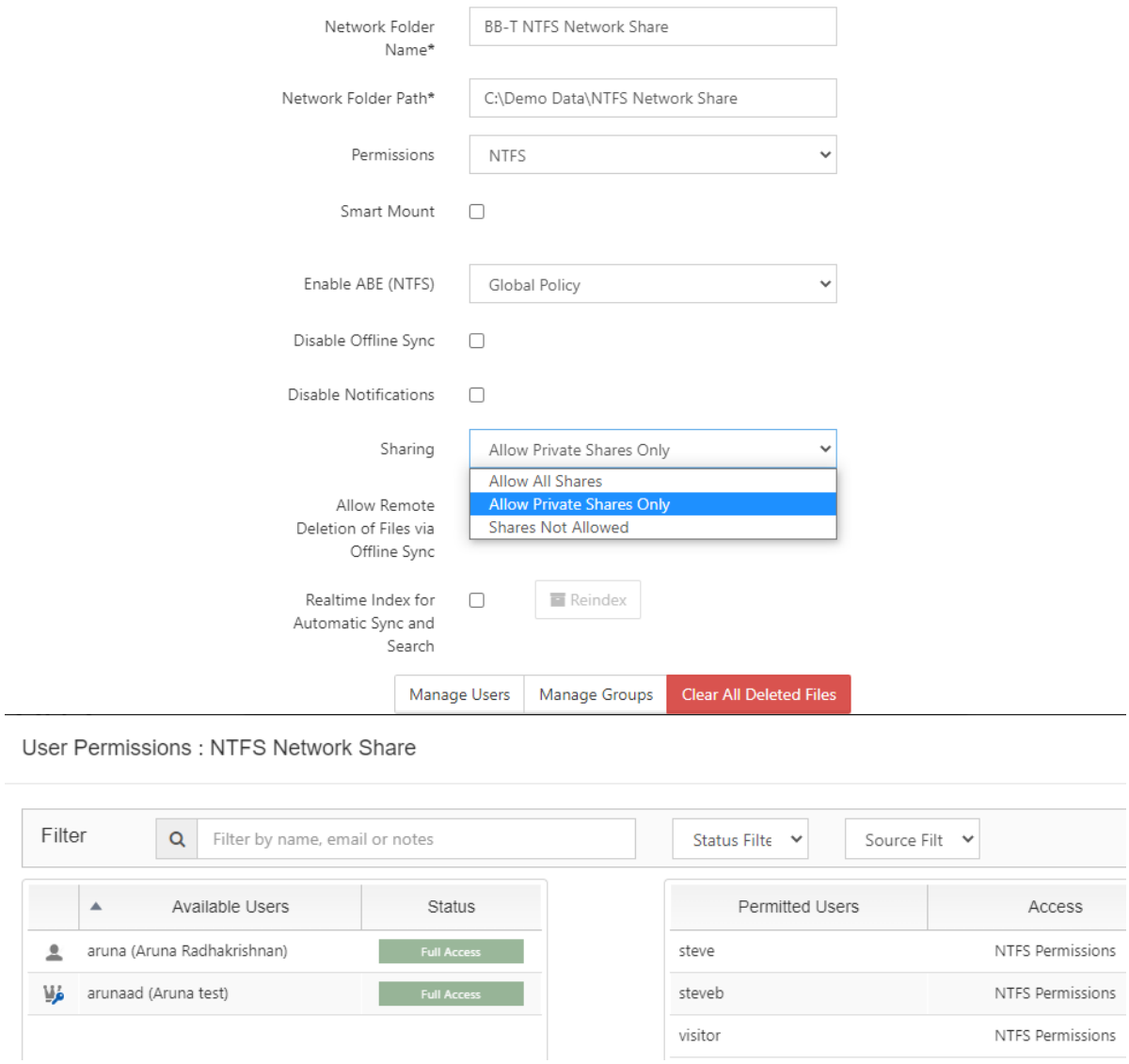


Figure 7 – Setting Up NTFS Network Shares

Moreover, shares extend to Amazon S3 bucket network folders and Azure blob storage network folders, so the concept is a fully hybrid one. Add in that aforementioned AD support and the vast majority of use cases are covered from an integration perspective. For Smart Mounted file shares the use case is simple – it is simply too much work for an administrator to create individual folders for each and every user, but FileCloud's methodology allows the creation of one general folder, combined with individual access mechanisms, massively reducing the admin workload. A classic example would be for the HR department, when dealing with confidential employee information.

Finally, but importantly, there is also a thin client option to view remote network files offline rather than having to be online in order to access them.

IN CONCLUSION

On the face of it, FileCloud has achieved what many might have thought impossible – to provide a secure, ultra-flexible and ultra-comprehensive Enterprise-level OnPrem solution for file and content storage and management, with the ease of use and deployment of a consumer-oriented, cloud-based service.

Yet it has achieved exactly that. Not only does it offer the security and manageability of having all content OnPrem, but it adds an entire content lifecycle feature set – all fully integrated – to the basics offered by most cloud-based alternatives. Every aspect of data governance, residency and security is covered – including compliance, DLP and DRM. True Enterprise features such as workflow automation, multi-layered access (user and content) control, smart data classification and full integration with existing network data shares make FileCloud stand out from any potential alternatives. It is currently sitting atop a league of one!

In summary then, what FileCloud offers is a flexible, OnPrem-driven content management solution, designed from the ground up to include all the aforementioned features and beyond, none of which comes at the cost of added complexity. In use, FileCloud is as simple as a Windows or Mac desktop – or indeed any of the cloud-based storage solutions out there.