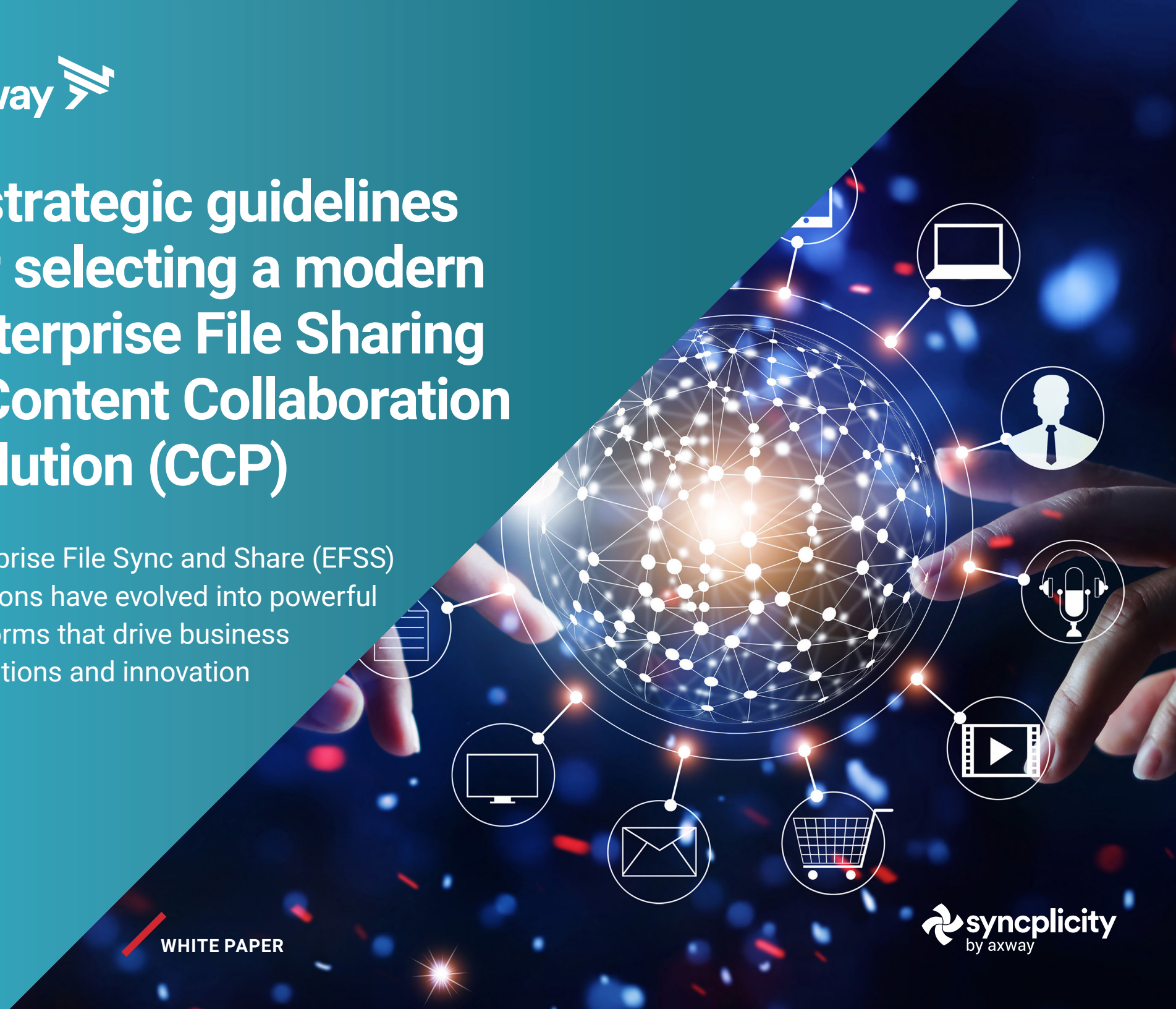
axway

7 strategic guidelines for selecting a modern Enterprise File Sharing + Content Collaboration Solution (CCP)

Enterprise File Sync and Share (EFSS) solutions have evolved into powerful platforms that drive business operations and innovation



WHITE PAPER

syncplicity by axway

We've become accustomed to the cloud. We keep our family photos, kids' soccer schedules, and favorite recipes on Dropbox and OneDrive without a second thought. It's not a surprise that some corporations think those same consumer products will suffice for their businesses as well. After all, those companies offer enterprise licenses, so they must be suitable for enterprise use, right?

In some cases, the answer will be yes. Businesses that aren't concerned with security issues or regulatory requirements may be well served by the same electronic file sync and share (EFSS) solutions that their employees use at home.

But the rest of us need a robust EFSS solution that's built for business from the ground up. Modern experiences and ways to work that boost productivity along with ensuring compliance and security, require an enterprise-grade architecture.

How many of these challenges are you facing today?

- ☐ Rise of cloud-computing
- ☐ Legacy storage cost
- ☐ Legacy infrastructure – file servers
- ☐ Content security and protection
- ☐ Data sovereignty and control
- ☐ Global digital workforce
- ☐ Shadow IT
- ☐ BYOD programs
- ☐ Secure internal + external sharing

If you checked any of these boxes, you need a modern, enterprise-grade CCP solution.

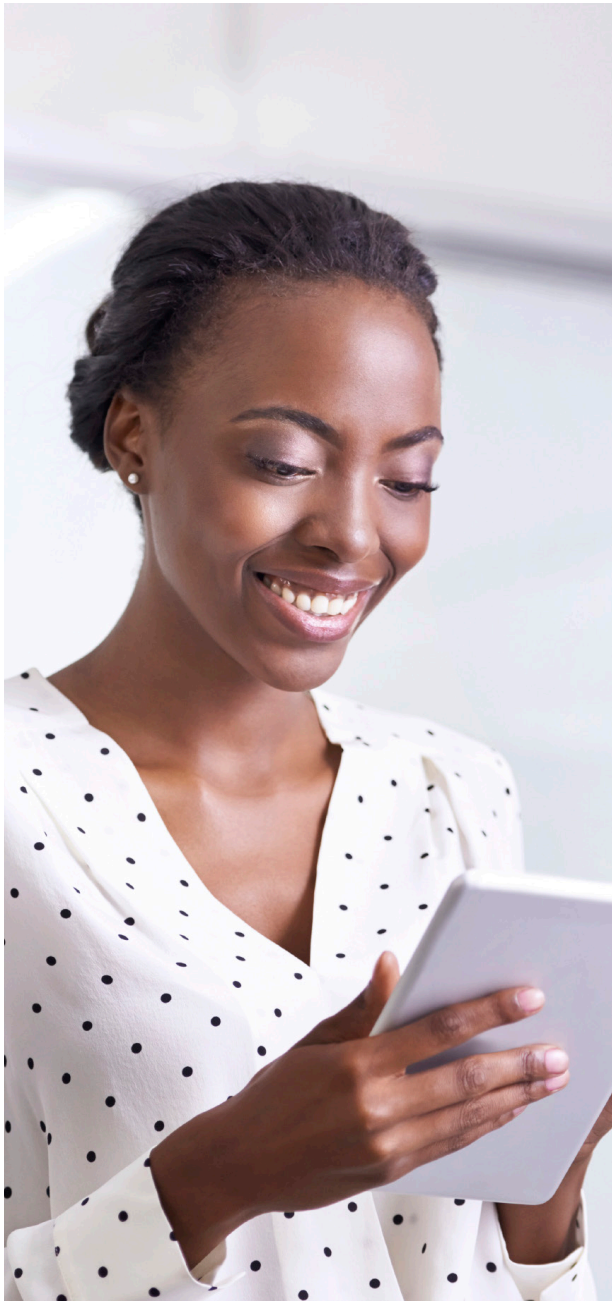
Simple file sharing is out

Many organizations underestimate the complexity of their file sync and sharing needs. After all, they just want to move files around. That seems like it should be easy.

In actuality, an EFSS solution needs to be as complex as the business it serves. And businesses are evolving at a rapid pace. In just the past few years, the typical enterprise has already had to negotiate a lot of changes in business and technological practices; now, digital transformation is table stakes to remain competitive, and enterprises are focusing on converting all their processes from paper to the digital realm. They need more from their EFSS systems than just file sharing and syncing; they need powerful and sophisticated ways to manage collaboration, policies, and storage options. This trend is so distinct that Gartner has redefined the EFSS sector as the content collaboration platform, or CCP sector. We will use the acronym CCP throughout the rest of this document.

To determine whether a CCP solution will support their company's strategic goals, CIOs should consider seven key criteria.

7 Criteria for Selecting a Modern CCP Solution



01

User experience

The user experience starts with design. In the case of CCP, the design should be invisible. Users should be able to go about their work without deliberately syncing or sharing a file. It should just happen.

A poorly designed solution annoys users, but more importantly, it lowers their productivity. In fact, 57% of office workers say they spend an hour a day looking for missing documents.[1] Those documents may be on somebody else's hard drive or, worse, they may be on somebody else's personal Dropbox or OneDrive.

When workers are not provided with a convenient enterprise solution, they tend to use the tools they favor outside the workplace. Their intentions are good, but their actions create risk. Documents stored outside the network are effectively lost to the enterprise—and if they're on a worker's personal file-sharing service, they may be protected only by a re-used or inadequate password that's already for sale on the dark web.

Many organizations still require remote workers to access corporate assets through a virtual private network (VPN). A VPN will give them access to files, but VPNs don't provide the collaborative workflows and automation that are essential to productivity.

Workers need access to files through an app that lets them stream and share content without having to log on, download, or email any files. These capabilities promote the modern new ways to work that help drive higher levels of productivity that digital transformation is intended to deliver.

Productivity essentials

- ☐ Access to all enterprise content
- ☐ Securely receive and share files
- ☐ Sync once, available everywhere
- ☐ Secure external sharing + collaboration
- ☐ No magic folder required
- ☐ Real-time backup
- ☐ Predictive analytics
- ☐ Consumer-grade mobile applications
- ☐ Offline access
- ☐ Automatic version control and restore capabilities

Source: 1 Figueiredo, Debora. "Are you wasting your employees' time at work?" Developing People Globally. March 24, 2016.

02

GDPR

The General Data Privacy Regulation (GDPR) is causing a lot of confusion among businesses around the globe. Some think the new laws are only relevant to EU-based businesses, but that's a dangerous misconception. Companies based outside the EU must comply if they do business with even one business or individual inside the EU. The penalties for non-compliance are severe: at the lower level, fines are 2 percent of total global revenues or €10 million, whichever is greater, and at the higher level, they are 4 percent or €20 million.

GDPR, PCI, & HIPAA

Although the Big 3 bodies of regulatory requirements do not map directly to each other, they are close cousins. If your CCP solution is capable of supporting one, it is probably capable of supporting the others. Ask your vendor how its solution can help you remain compliant.

To avoid these penalties, businesses need data sovereignty. Data sovereignty is the idea that content is subject to governance according to the laws of the nation where it is stored. That can be challenging in a connected enterprise that runs much of its business in the cloud and on virtual machines.

A GDPR-compliant CCP solution must allow customers to choose the SaaS location where metadata is stored, and the location where actual content is stored, whether in Azure, AWS, on-premises, or in a hybrid storage environment.

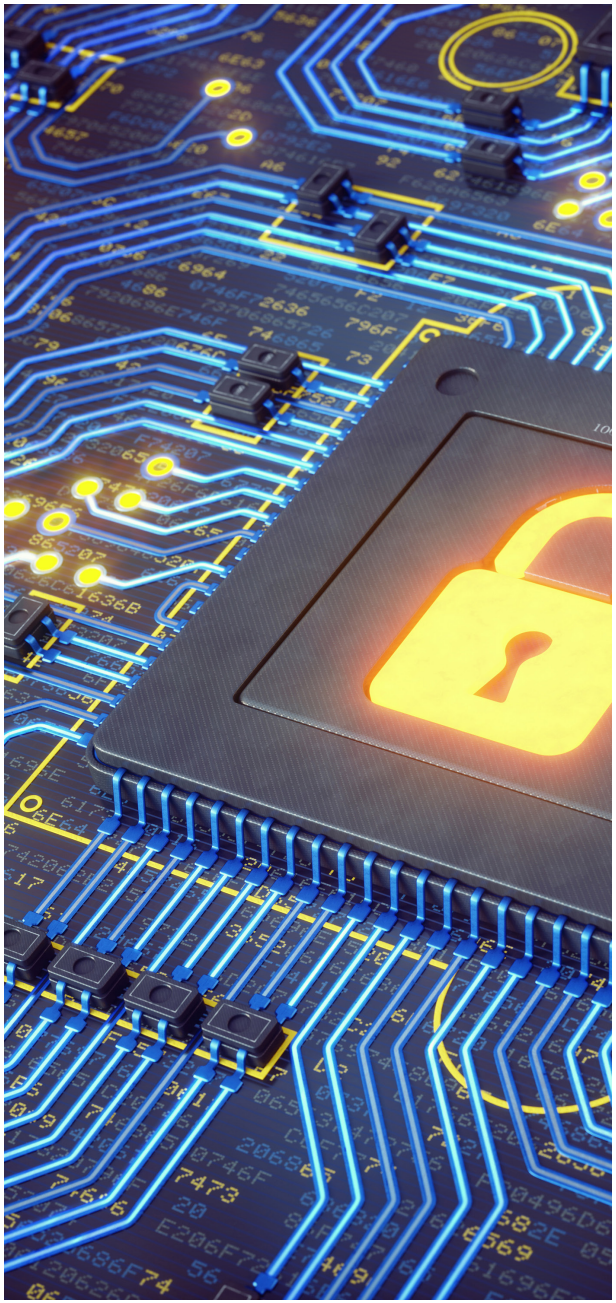
Zero content knowledge is a mandatory requirement for a GDPR-compliant CCP solution. Zero content knowledge means that a vendor encrypts customers' files so they can only be read by the customer — never the vendor or anyone else. This security architecture supports GDPR compliance by protecting an enterprise's data from unauthorized access, whether by a malicious actor or a government subpoena.

To meet GDPR requirements, enterprises need a solution that supports role-based security policies that govern which data can be accessed and shared. The solution should also integrate with major data loss prevention products to mitigate the risk of losing *personally identifiable information* (PII) and *protected health information* (PHI).

On-premises and private storage should be an option. Many EU-based businesses prefer to have their data on site, so they can be certain private customer data is contained within the EU region.

Syncplicity supports data sovereignty

Syncplicity provides built-in location control that gives customers the choice of where their data is stored. Users never have to think twice about which region they're accessing; a single sign-on provides access to both, and the location of the data is always invisible.



03

Ransomware

Not long ago, ransomware was a way for petty thieves with some programing know-how to collect a few bitcoins. In just a short time, ransomware has evolved into a far more malignant threat: ransomware attacks have been co-opted by nation-states with strategic agendas. These nation-states don't want cryptocurrency; they want to disrupt commerce. Some analysts even think that WannaCry and Petya were more than malicious attacks — they were tests of cyberweaponry.

Enterprises are right to be nervous about ransomware; according to Cisco, ransomware is growing at a pace of 350 percent a year. The ransom itself is just part of the cost; remediation, penalties, litigation, and making customers whole are other costs, and they add up quickly. In addition, once a company pays a ransom, it becomes known as a good target and other hackers are likely to pile on with more ransomware attacks.

Ransomware doesn't take data; it just encrypts it so its rightful owner can't use it. The good news is that there is one simple way to render ransomware relatively harmless: back up your files.

Surprisingly, a lot of companies don't do this very well. They think they need to focus solely on protecting their network perimeters to be safe. But most companies have volumes of unstructured data tucked here and there among their networks and endpoints.

Maybe a financial analyst has a PDF on a mobile device, or a scientist has placed sensitive R&D documents in the recycle bin on a desktop.

An enterprise CCP solution eradicates ransomware worries. It won't stop ransomware attacks from happening, which is true for any security solution because, as the saying goes, "a hacker only needs to get lucky once." But it will make the attack irrelevant because the enterprise will be able to replicate and restore its files. Businesses with this capability can tell hackers to take a walk; the files that were encrypted in the attack just become useless ones and zeros that can't be leveraged against their rightful owners.

A CCP solution that replicates and restores files as part of its core product offering reduces the spend on backup software and speeds recovery times. Faster recovery times, in turn, reduce the costs and lost revenue associated with a ransomware outage.

Syncplicity aids in ransomware mitigation across industries

- A global pharmaceutical firm hit by Petya used Syncplicity to recover quickly
- A global commercial airline saved $3 million on backup software by deploying Syncplicity
- A major chip manufacturer has over 100,000 employee laptops protected using Syncplicity

04

Cloud vendor lock-in

Cloud vendor lock-in happens when a company that has moved part of its business to the cloud can't move out because migration will be too painful. The legacy solution is not easily integrated with replacements, or the data located in the legacy solution is structured in a way that will make a complete migration uncertain. Maybe all the files will be moved, or maybe they won't.

Enterprises should only consider CCP solutions that are decoupled from storage choice. Storage choice relates to more than just the vendor; it is also relevant to moving files between the cloud, on-premises, or hybrid storage. This flexibility is essential to business agility, which is further enhanced by a solution that enables automated migration.

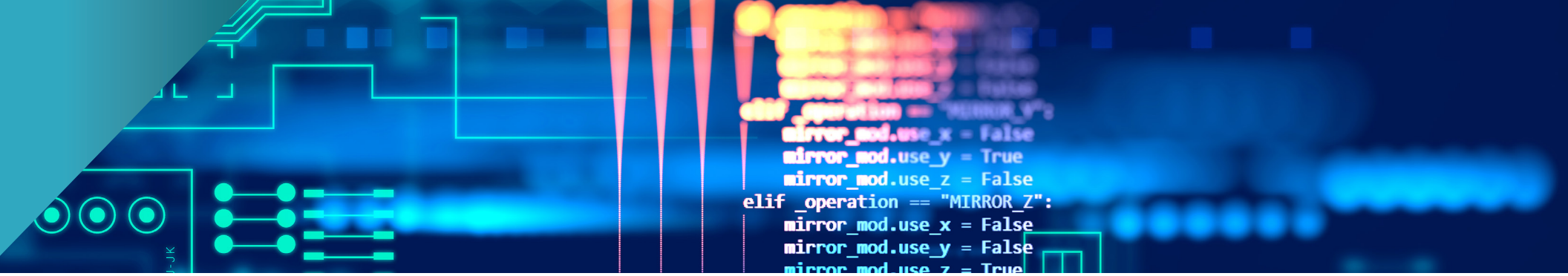
A case in point is GDPR. EU-based companies that were using US data centers now have to move all their files to servers in their own regions. For those with a robust CCP solution, moving files is the work of an ordinary day rather than a cross-organizational initiative.

A more mundane use case would be an enterprise's decision to move from, for example, AWS to Azure. A CCP solution needs to work with both systems, and the transition must be seamless or the company will take a productivity hit as workers become used to their new logins and workflows. It will also take a cost hit while the IT team fields calls from frustrated workers.

The ability to make such a move provides a strategic advantage when the time to negotiate a new contract comes around. If the new terms aren't satisfactory, an enterprise that has control of its data can go elsewhere without disrupting the user experience.

Q. Who has the largest, fastest CCP deployment in the world?

A. The answer is Siemens, and they're saving $24 million per year through storage consolidation with the help of Syncplicity.



05

External sharing

Sharing content beyond the four walls of the enterprise requires security controls beyond those necessary for sharing files internally. This is especially true when sensitive content is shared and regulatory requirements come into effect.

Security and compliance are relevant for most businesses, but some have a heavier burden than others. Financial firms move vast volumes of customer PII, manufacturers and life science organizations must protect their intellectual property, and healthcare providers are responsible for data that's considered the most valuable merchandise on the dark web: PHI.

Security is top of mind for organizations that share files, but it's not the only concern. Usability must be preserved for users both inside and outside the enterprise. A bad user experience is in itself considered a security vulnerability; when users don't like enterprise tools, they find ways around them. Files end up on personal file sharing accounts, on thumb drives, or on hard drives, and are effectively lost to the enterprise.

An enterprise that shares files with trading partners should look for four features:

1. Secure and user-friendly external sharing capabilities with frictionless external user onboarding
2. No additional cost for external sharing
3. Affiliate sharing controls that allow enterprises to control levels of trust proffered to specific trading partners
4. Rights management and DLP controls to prevent sensitive content from being shared accidentally or maliciously

These four features make the CCP solution easier for everyone to use, resulting in improved operational efficiencies that can have a meaningful impact across complex supply chain ecosystems.

"External sharing is critical to Texas A&M University. Axway Synpclicity's new controls give me confidence that my teams can share files and folders securely among our trusted group of organizations. In today's digital world, the firewall is no longer the boundary for data and information sharing. These enhancements enable us to lock down sharing within a trusted group of affiliated organizations, helping us stay compliant and secure – maintaining central control while enabling easy end-user collaboration."

Danny Miller, CISO System Chief Information Security Officer at Texas A&M University

---

06

Machine collaboration

Automation is no longer a competitive advantage; it's a fact of life. Businesses require their workers and partners to interact with automated applications, systems, and devices. They should require their CCP solutions to do so as well.

But many CCP solutions are incapable of supporting machine collaboration. Humans have to intercede to manually move unstructured files in and out of the CCP solution. This decreases operational efficiency, erodes asset utilization, and degrades the user experience.

For instance, think of a bank sending a mortgage application to a home buyer. A CCP solution that doesn't collaborate with machines may force the lender to download documents from one system, upload them to a secure signing solution, and then forward the signed document to a loan officer and an underwriter. An automated CCP solution will handle most of that workflow, automatically routing documents between the home buyer and financial organizations with the click of a button.

In other use cases, an MRI machine might automatically share a patient's results with a radiologist, doctor, and insurance company. A pilot might send instructions from a plane's IoT sensors straight to a ground crew so spare parts can be ready upon touchdown.

Efficiency gains like these require a sophisticated CCP that's capable of advanced file routing, automation that integrates with legacy and custom applications, and API-based integrations to popular cloud applications.

Automation is more powerful with content collaboration

Industry-leading companies have connected Syncplicity to their automated processes. The result?

- Improved operational efficiency and customer experience
- Improved asset utilization in IoT use cases
- Mobility added to existing systems
- External sharing added to existing systems
- Cloud-based distribution capabilities added to existing systems

07

Customer success

Customer success hinges on two cohorts: the users and the IT team. A CCP provider should offer a communications program to promote user adoption based on use case and business objectives. The program should not be a one-time affair, but should include paths to move users from performing standard tasks to engaging with more advanced capabilities. The solution should have reporting features that allow usage patterns to be monitored and tracked so the enterprise can understand how its CCP solution is performing.

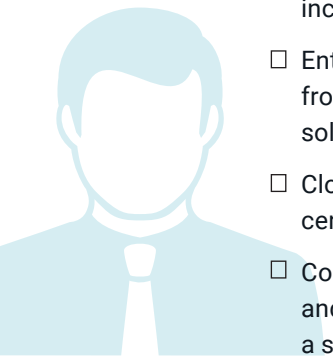
The IT team will need help understanding the CCP solution's features. Implementation should begin with a review of the enterprise's use cases, security, and infrastructure. The results should be used to establish criteria for success and develop a project plan that aligns with the requirements. Only then is the system ready to be configured, deployed, and provisioned.

Experience frictionless onboarding with Syncplicity

IT-readiness. Syncplicity provides an IT-readiness package that trains IT departments, helps set up security and administrative controls, and ensures compliance requirements are met.

User engagement. Syncplicity helps drive adoption by providing guidance and support based on best practices and marketing activities, such as email nurture campaigns, kick-off events, and tips and tricks.

The CIO's keys to success



- ☐ User adoption is critical to success and ROI, but it's not the only thing: CIOs must balance increasing compliance demands and a darkening threat landscape when selecting a CCP.
- ☐ Enterprises with regulatory, security, and supply chain concerns require CCP solutions built from the ground up for enterprises. Consumer systems that are now marketed as business solutions lack the auditing and encryption capabilities necessary today.
- ☐ Cloud vendor lock-in is increasingly common in the CCP market. Enterprises should be certain they can migrate their files anywhere they want, whenever they want.
- ☐ Collaborating beyond the four walls of the enterprise with customers, patients, suppliers, and constituents is significantly more demanding than internal-only file sharing. Choose a solution that is robust enough to meet those needs.
- ☐ Advanced automation and integration with enterprise applications and IoT use cases is rapidly pushing CCP beyond the boundaries of human-centric collaboration. Choose a solution that is designed to leverage technology as it evolves over the next few years.

axway_WP_7_guidelines_enterprise_file_share_en_042018