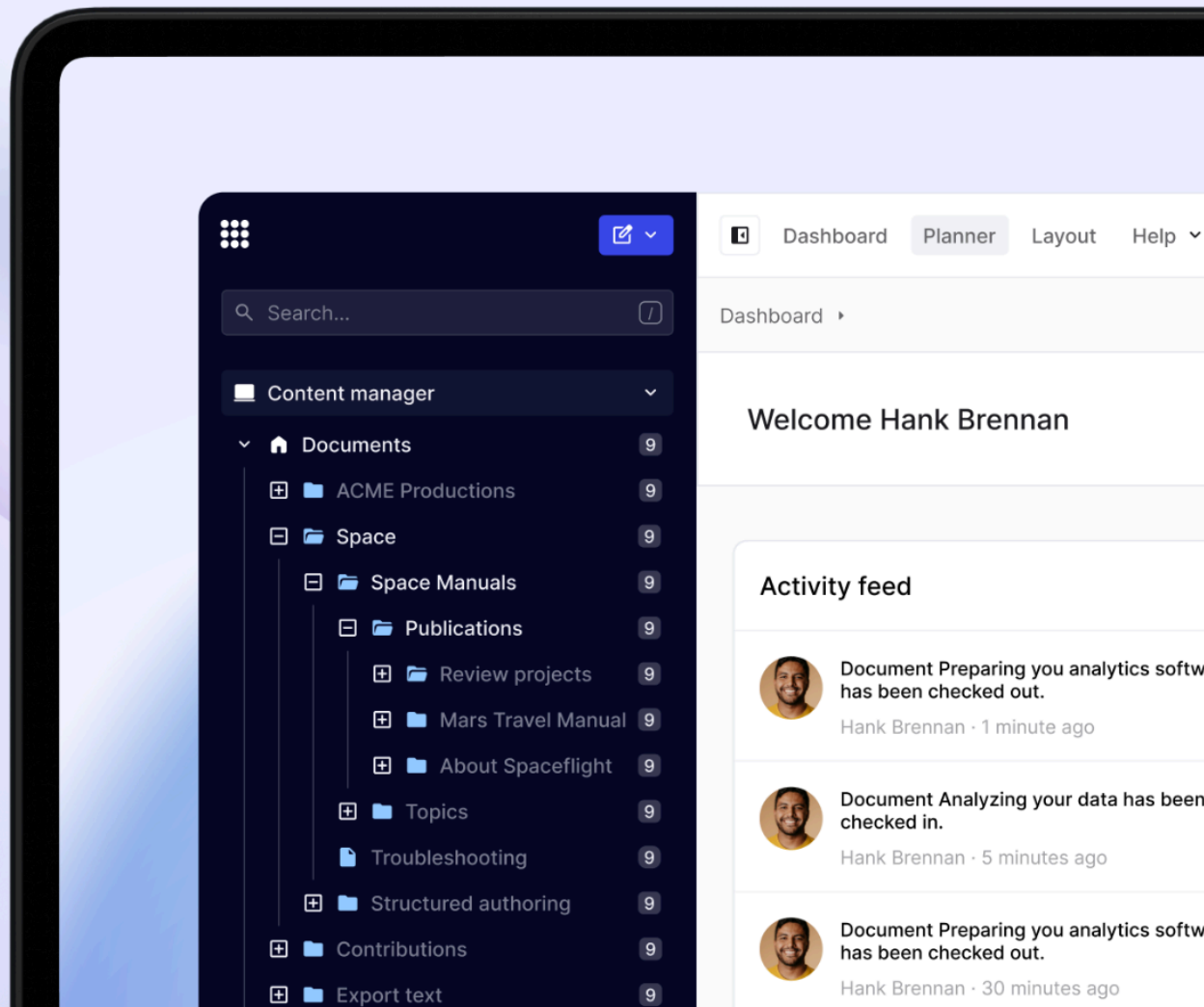







From On-Premises to Cloud: Making the Case for Cloud-Based Component Content Management



I. Executive Summary

Many organizations, particularly those in pharma, financial services, and manufacturing, still believe that on-premises component content management solutions (CCMS) hold a significant advantage over "off-premises," i.e., cloud or SaaS (software as a service) solutions.

The typical advantages listed for remaining - or even newly opting for - an on-premises solution are:

-  Security
-  Customization
-  Speed/latency
-  Price control
-  Reliable connectivity

However, the up-front investment and ongoing resources required to implement, maintain, and upgrade/migrate an on-premises solution for content management quickly show that it is rarely worth it when weighing the risks versus rewards in the medium to long-term. No solution is risk-free, after all. So, how do you justify it as a reasonable business cost?

Despite some high-profile hacking stories in the news, with the proper security and privacy processes coupled with a reliable and trustworthy vendor, any business in any industry can use a SaaS component content management solution without worrying about a data breach or loss.

This whitepaper explores the nuances of both on-premises and cloud-based CCMS solutions. We examine the advantages and challenges associated with key features of a hosting environment, shedding light on why cloud-based platforms are increasingly becoming the preferred choice for forward-thinking organizations.

We're also diving into the particular concerns of one country, Germany, addressing important considerations for working with a cloud-based CCMS.

II. Introduction

One critical aspect of business is effectively managing technical and business documentation. Whether it's product manuals, technical guides, regulatory documents, or standard operating procedures, it is paramount to organize, update, and distribute accurate and up-to-date documentation and information quickly and efficiently. This necessity becomes even more pronounced in industries where compliance, accuracy, and timeliness are non-negotiable.

A component content management system is a method of content authoring and management where information is broken down into discrete, reusable components (structured authoring). These components, such as topics, paragraphs, text snippets, and images, are stored in a centralized repository and can be assembled dynamically to create various documentation tailored to different audiences, channels, or contexts.

Component Content Management Systems come in various forms, each with advantages and considerations. Traditionally, organizations have favored on-prem solutions, where the software and data are housed within the company's infrastructure. These solutions offer a sense of control over security, customization, and connectivity, which has long been perceived as essential for sensitive or mission-critical content.

However, the landscape has evolved, and the emergence of cloud-based, or Software-as-a-Service (SaaS), Component Content Management Systems (CCMS) has sparked a paradigm shift in how organizations approach content management. Cloud-based CCMS platforms leverage remote servers and internet connectivity to provide scalable, flexible, and cost-effective solutions. Despite initial apprehensions surrounding security and control, cloud-based platforms offer numerous benefits that outweigh the concerns.

SaaS is the largest cloud-computing segment and a standard enterprise organization delivery model. The SaaS market is expected to reach US\$ 282.20 billion in 2024, of which US\$ 69.82 billion is from Europe.

[Source: Statista](#)

In the next section, we'll perform a comparative analysis of cloud-based CCMS and on-premises CCMS, focusing on each solution's hosting environment (hardware, software, infrastructure).

Before we continue, it is important to note that we are using the term cloud-based CCMS to refer to both cloud-hosted and SaaS.

III. Comparative Analysis: On-Premises vs. Cloud-Based CCMS

To get started, check out the following chart highlighting the differences between on-prem and cloud-based CCMS.

Note: You can read the full whitepaper from start to finish or select a capability to skip to that section linked in the table below.

Capability/Feature	On-Premises	Cloud/SaaS
<u>Security</u>	Responsible for all security, including network, hardware and software, user access and authentication, security training, monitoring, and remediation.	The CCMS provider provides security in the cloud environment, including advanced encryption, identity and access management, and threat detection systems. Typically adheres to security certifications such as ISO 2001, SOC 2
<u>Costs</u>	Responsible for paying for the entire environment, including servers, software, and CCMS licenses, as well as resource training and ongoing maintenance	Pay a single subscription, typically yearly, that covers all costs, including the environment, CCMS, and support.
<u>Scalability</u>	Build for future expansion, paying upfront for future expansion, or build for now and add on as needed, risking running out of storage space or slow performance.	Automatically scale storage and performance as needed with no impact on your end users. Scale up for busy times and scale down when no longer needed. Move to a higher subscription level when required.

Performance & Reliability

Responsible for monitoring and improving the performance and reliability of the entire environment.

The CCMS runs on high-performance services in global data centers

Data Backup & Recovery

Responsible for creating and managing backups and, if needed, a complete disaster recovery environment.

Cloud-based CCMS have regular, automated backups and geographically distributed data centers for enhanced disaster recovery.

Upgrades & Maintenance

Manage upgrades to the entire environment, including the network, servers, and software. Requires resources to work off hours and all changes to be fully tested in staging environments to ensure minimal downtime.

Regular upgrades and maintenance in off hours. All changes are thoroughly tested before implementation, and downtime is minimal.

Integration with Other Systems

Custom integrations to enable systems to work together inside the network (s).

Integration typically happens through secure APIs and pre-built connectors for e-learning systems, translation management systems, knowledge bases, and other content delivery platforms.

Internal and External Collaboration

Network access is required to access the CCMS. External access would happen through a VPN.

Anytime, anywhere access to the system with security protocols in place. Invite external parties to collaborate on content without needing to give them access to anything but the CCMS (explicit permissions).

Service & Support

The internal team is responsible for infrastructure and hardware/software support. The CCMS provider does support the CCMS and may be required to be onsite for support.

CCMS provider provides all support through SLAs and is fully remote.

Security

A CCMS must safeguard sensitive information, ensure regulatory compliance, mitigate the risk of data loss, and defend against cyber threats. By implementing robust security measures, organizations can effectively protect their valuable information and mitigate the potential consequences of security breaches.

Security measures include:

- **Network Security:** Deploying firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to prevent unauthorized access and mitigate potential threats. In addition, all network traffic between clients and servers must be encrypted to protect data in transit.
- **Authorization and Access Controls:** Authentication mechanisms, such as multi-factor authentication (MFA), verify users' identities before granting access to the CCMS. Authorization policies based on roles and permissions control users' access to functionality and resources.
- **Data Encryption:** Encrypting sensitive data stored within the CCMS protects it from unauthorized access or tampering. Robust encryption algorithms ensure the confidentiality and integrity of data at rest.
- **Patch Management:** A patch management process helps prioritize and deploy security patches promptly, addressing known vulnerabilities and reducing the risk of exploitation by attackers.
- **Audits and Monitoring:** Regular security audits and assessments must be conducted to identify vulnerabilities, assess risks, and ensure compliance with security policies and regulations. In addition, monitoring and logging mechanisms must be implemented to track user activities, detect suspicious behavior, and respond promptly to security incidents.

All of the above activities are required regardless of whether the CCMS is on premise or cloud-hosted. What's different is who is responsible for ensuring these security measures are in place and managed continuously.

Organizations that manage an on-prem component content management system are responsible for ensuring that this comprehensive set of measures to protect the system, data, and infrastructure are in place. You will need a security team trained on the latest technologies, processes, and certifications related to the CCMS and the hosting infrastructure. In most cases, you already have some of this infrastructure in place for other systems; the focus here is on what's required to support the CCMS.

A cloud-based CCMS takes on all these security measures for you, investing in cutting-edge technologies, such as advanced encryption, identity and access management, and threat detection systems. They implement continuous monitoring and

threat detection to detect non-compliance issues or malicious threats and automatically implement security updates and patches.

"The cloud certainly has its risks, but SaaS environments also enable quicker time-to-respond to a breach or to push an update or patch. With today's dispersed workforces, the agility, speed and reach inherent to SaaS environments are tangible advantages most organizations should not pass up."

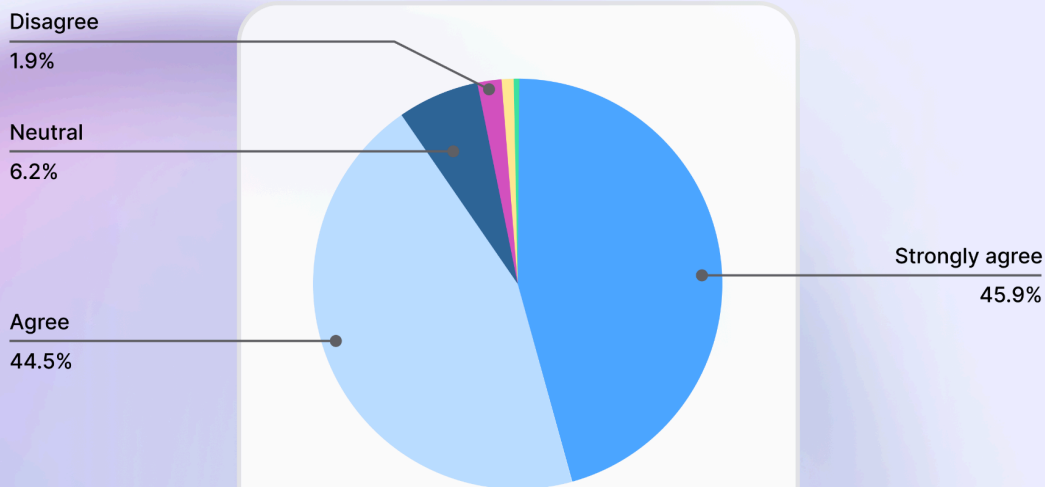
Source: Security Magazine

A couple of other key security differences between on-premises and cloud-hosted CCMS:

Security Certification: To prove their security practices are in place, a cloud-based CCMS applies for compliance certifications, such as ISO 27001, an international standard to manage information security.

An organization can apply for these security certifications as well, but they are fully responsible for the work involved in achieving - and maintaining - these certifications, which takes a great deal of time and expense.

Paligo has proven to be a reliable SaaS platform (i.e minimal downtime, reliable updates, trustworthy data privacy and security).



Source: internal Paligo user survey, March 2024

Data Sovereignty: Many countries have laws related to how organizations must store and manage data collected in their country (GDPR is an EU regulation that applies to any company doing business in the EU). These data sovereignty rules and regulations vary from country to country, and organizations that operate in multiple countries must ensure that their data is managed according to the laws of each country.







Data sovereignty can be challenging for a company that uses an on-premises CCMS if it only has one data center. Depending on a country's particular laws, they may be required to have data centers in more than one country, which can be costly. As well as needing to manage multiple data centers, the organization may be required to acquire additional CCMS licenses or deal with transmitting data securely between data centers for processing (if allowed). Not only does this take time, resources, and budget, but it opens the door to security risks.

A cloud-based CCMS that serves customers in multiple countries is responsible for ensuring it adheres to each country's laws and governance structures. Where necessary, they host their software in data centers in each country and ensure all security and privacy regulations are met.






Cost Considerations

Let's examine the costs related to hosting a CCMS.

An on-prem installation can have a substantial initial capital investment:

-  Servers (multiple if you want to have a load-balanced environment) and backup servers in the event a primary server fails
-  Load balancing software
-  CCMS software licenses
-  Backup and anti-virus software
-  Network Services
-  Encryption software

In addition to the capital investment, there are other costs associated with an on-premises installation, including:

-  Resources to install and manage the hardware and software
-  Ongoing maintenance of servers
-  Ongoing maintenance of all software involved, including upgrades or patches.
-  Monthly costs to run the environment (power, cooling systems, security, etc.)
-  Resources to manage security



Keep in mind that these are the costs for a single environment. If you need multiple environments to support global customers, expect costs to increase by the number of data centers you need. Also, servers degrade or break over time, so be prepared for additional hardware and infrastructure costs.

Now, let's look at the costs of a cloud-based CCMS. First, there are no upfront capital costs in this case. Instead, these costs are built into a monthly or yearly subscription cost for the CCMS. You pay the same subscription rate yearly, assuming your requirements stay the same.

Subscriptions are typically renewed yearly, so you have predictable costs. If you decide not to renew your subscription, you aren't on the hook for licenses, hardware, or infrastructure costs. Instead, you can migrate your content from the CCMS into a new environment.

Scalability

When you first implement your CCMS, you have a reasonable estimate of how much content you will need to store and how much that content will grow over time. With this information, you can formulate what size server environment you need. With an on-prem environment, you have two choices:

- Set up the environment for the content you have today, with some room for growth. This would be your minimal server environment.
- Set up the environment for the content you know you will have in the next five or more years. This environment requires extensive upfront investment to support future expansion. So, you are carrying extra expenses for a setup you don't need now but have estimated you will need in the future.

Neither of these options is optimal. In the first choice, if you suddenly find yourself with more content than your environment can support, you will need to quickly ramp up the infrastructure and hardware (and possibly CCMS licenses) to support your needs. Updating infrastructure and hardware is not easily done. If you are under tight compliance and regulations, ensuring the updates are implemented and tested properly will take even more time.

If you choose option two, then you are spending money on an environment you don't need in preparation for a future state. Spending money on something you don't need is never a good choice when budgets are tight.

The story is very different with a cloud-based CCMS. A CCMS hosted in a cloud environment provides instant scalability - scale on demand - to accommodate your growing needs. In this model, you only have to pay for the services you need. As your needs grow and you require more storage space or additional processing power, your CCMS provider's environment can automatically scale to meet those needs. You don't have to wait for more servers to get added or data storage; your environment will automatically grow with you.

Performance and Reliability

When you host your CCMS internally, you depend on that local infrastructure's reliability. If you haven't built it strong enough or secure enough, you face potential performance issues during high-traffic periods or risk a cyber hack.

On the other hand, a cloud-based CCMS runs on high-performance services in global data centers. These data centers are built with enhanced reliability and have Service Level Agreements (SLAs) in place to ensure 24/7 uptime.

The Public Cloud worldwide market is expected to reach US\$ 679 billion in 2024 - led by AWS, Azure, and Google. It's important to know which Public Cloud a cloud-based CCMS uses.

[Source: Statista](#)

Data Backup and Disaster Recovery

Along with the live server environment, you also need customized backup and disaster recovery solutions if something happens to your live environment. Data backups should happen daily, and the backups should be stored on different servers and, in some cases, in different data centers.

A disaster recovery solution provides a duplicate environment or set of servers that can be brought online in the event something happens to your live environment. Depending on the importance and sensitivity of your content, that backup environment may need to come online immediately or within a short time window.

If you don't have a disaster recovery plan or are storing your backups on the same servers as your production environment, you risk losing your content with no recourse, as well as not having access to your CCMS to manage content.

With a cloud-based CCMS, you don't have to worry about data backups and disaster recovery environments. Cloud-based CCMS have regular, automated backups and geographically distributed data centers for enhanced disaster recovery.

Upgrades and Maintenance

Maintaining your server environment is time-consuming and requires skilled resources. If you need to take the CCMS environment offline to patch a server or apply an update to the CCMS or other support software, your CCMS will be offline as long as the updates take.

With a cloud-based CCMS, you get automatic updates with minimal downtime. New features and enhancements can be added with little to no impact on your business. In addition, upgrades are tested before they are implemented so as not to impact production. Downtime is typically minimal and happens during off hours.

Addressing Data Protection and Compliance Concerns in Germany

According to a recent study of German companies, 46.5% use cloud computing technology for their business processes, while 11.1% plan to. A further 18.2% of those companies surveyed are still discussing whether or not to introduce the technology.

[Source: IFO Institute](#)

In another study, 56% of companies want more than half their IT applications in the cloud in the next five years (only 15% do today).

"The most important goal for companies in their cloud activities is to reduce costs (64 percent) and reduce CO2 emissions (63 percent). A majority of 57 percent also want to convert IT applications to platforms and software-as-a-service and increase IT security."

[Source: Bitkom](#)

While cloud-based solutions are being used in Germany, some concerns remain. According to Marc Achtelig, [Technical Documentation Consultant at Indoition](#), there are a few things that drive their concerns:



"In Germany, we tend to think that a system is good if we can fully control it. We can't fully control a hosted solution. So, we see this as a strong disadvantage, but we don't see the benefit of not managing the system ourselves."

Marc Achtelig, Technical Documentation Consultant at Indoition

Achtelig also said that German companies are concerned about data sovereignty. Data sovereignty refers to the idea that data and content created, processed, and stored are subject to the laws of the country where it is created. In Germany's case, two regulations affect how data is stored and managed in German companies: the ([German Federal Data Protection Act \(BDSG\)](#)) and the EU's General Data Protection Regulation ([GDPR](#)). Any cloud-based system must ensure it can comply with these regulations.

There may also be company compliance standards to consider:

"In many cases, there are specific compliance requirements. These can require compliance with standards that a company has set up independently. Or it can be requirements to comply with a company's client standards. Suppliers will also need to adhere to these standards."

The answers to German companies' concerns will ultimately depend on the cloud-based CCMS they are evaluating. Here, we will address five key concerns by explaining how the Paligo CCMS and the Paligo-hosted environment answer them.

Concern	Paligo CCMS
How secure is a cloud-based CCMS? (Is it safe? Is encryption safe?)	<p>Paligo utilizes the most established measures and platforms for security, with hosting on Amazon EC2, complying with the strictest security standards (SOC1, 2, 3/SSAE 16, ISO 9001, ISO 27001, and many more).</p> <p>256-bit SSL TSL encryption is used by default, and additional levels of security are available on select plans.</p> <p>Backups are made hourly, and each backup is stored for 90 days. Should an event occur, recovery can be accomplished quickly due to the level of control provided by this environment.</p> <p>Paligo also uses two-factor authentication to confirm a user's identity when they try to log in.</p>
Does the CCMS support GDPR? BDSG?	<p>Paligo does support GDPR.</p> <p>In addition, Paligo works with customers to ensure other compliance and legal requirements are met regarding content storage and security.</p>
Where is my content stored?	<p>Paligo has an EU-specific data center for the European Union hosted in AWS (located in Dublin, Ireland).</p>

Are we locked into the CCMS forever?

Paligo offers two types of XML exports to ensure no vendor lock-in. You can export your content as DocBook 5.1 XML format or as the Paligo Export Format, intended primarily for moving individual pieces of content between Paligo instances.

Can we customize the CCMS to support our specific requirements?

Paligo offers services for custom imports and layouts as needed, and to a limited extent custom filtering attributes.

Security is a big concern for many companies regardless of country, but it's important to understand that cloud-based solutions are no more at risk than on premise solutions. What raises the risk for any environment is the level of security and data protection implemented.

“Two-thirds (64 percent) of companies using cloud computing say they have had no cyberattack at all on the cloud environment in the past twelve months. A quarter (26 percent) reported attacks, although their own security measures were effective. Only 1 percent fell victim to a cyber attack on the cloud environment that caused major disruption to operations.”

[Source: Federal Data Protection Act \(BDSG\)](#)

The truth is that cloud-based CCMS platforms are compatible with German standards and guidelines. The key is to ensure the system is fully secure and complies with country-specific regulations and company compliance rules. You ensure that by asking questions.

Integration with Other Systems

You will likely need to integrate other systems with your CCMS (e.g., translation management, collaboration, customer support). With an on-premises solution, these integrations often require custom development to connect systems, and this integration will need to be managed and updated as the systems change. Also, the systems must exist within the same organization and infrastructure or require custom network access through VPNs or point-to-point networks.

Without the integration, the potential for data silos is high, resulting in duplicate content across systems and outdated or inaccurate content in one or more systems with no way to know which has the most up-to-date content.

These challenges don't exist with a cloud-based CCMS. Integration typically happens through secure APIs and pre-built connectors. For example, you can connect your CCMS to your helpdesk knowledge base through an API integration. As you publish new content in your CCMS, it is automatically published to the knowledge base.

A cloud-based CCMS is compatible with many third-party applications, including e-learning systems, translation management systems, knowledge bases, and other content delivery platforms.



“The integrations are easy to set up and use, and we use them to publish to both Zendesk and Amazon S3. We have recently started translating our help center into Japanese using the built-in Paligo functionality. Very easy and efficient. Highly recommended for anyone looking to switch to a cloud-based platform.”

Paligo user review on G2

Collaboration

So far, we've discussed the differences between on-prem and cloud-based CCMS from a hardware, software, and infrastructure perspective. However, there are other benefits to using a cloud-based CCMS, particularly collaboration and remote working.

With a cloud-based CCMS, you can access the system anytime, anywhere. So, whether you are in the office or a remote worker, working from home, at a partner site, or elsewhere, you can access the CCMS to do your work.

If you are working with outside collaborators, you can easily give them access to perform specific functions, such as reviewing and commenting on documents, and be sure that functionality like tracking changes and version control are applied.



“With our last documentation tool, it was necessary to download a desktop application, connect it to the repo containing the support site, and then download the entire site if we needed to edit something; publishing the site meant pushing it back to the repo and then deploying it. Paligo simplified this process by handling everything within a web browser. Critically, this allows us to update and deploy documentation from any machine with an internet connection, without having to download and authenticate an entire application.”

Paligo user review on TrustRadius

Compare this ease of access and collaboration with an on-premises solution. Everyone who needs access to the CCMS must be on-prem or have remote access through a VPN (which comes with many security and privacy concerns). Also, because your CCMS is hosted on an internal network, you can't give external partners access to review and comment on documentation.

Service and Support

We put this last, but it's not the least important. When you host your CCMS on-premises, you are responsible for all service and support of the environment. You will have a support contract for the CCMS itself, but major issues require the CCMS provider to send someone onsite to help you. Onsite support will cost more and could cause delays if you have to wait for the right resource to be available for an onsite visit.

On the other hand, the service and support of a cloud-based CCMS is much easier. The CCMS provider is fully responsible for the environment; you don't have to worry about anything. Support persons don't have to come onsite; they can access your CCMS remotely, help you troubleshoot issues, set up new features and functions, and respond to questions easily and quickly.

IV. Conclusion

The debate between on-premises and cloud-based component content management solutions is not a matter of preference but a strategic decision that can significantly impact an organization's efficiency, security, and scalability.

While traditional on-prem solutions have historically been favored for their perceived control over security, customization, and connectivity, cloud-based solutions have evolved to meet the needs of organizations that demand the highest standards for security and compliance. Cloud-based CCMS solutions offer a compelling alternative that provides many benefits that outweigh the concerns once associated with cloud-based software.

In this paper, we have shown why cloud-based CCMS solutions represent the future of component content management, offering a combination of security, scalability, performance, and collaboration that empowers organizations to thrive in an increasingly digital world.

We welcome the opportunity to show you how the Paligo CCMS provides the capabilities discussed in this paper. You can find [Paligo's Security and Compliance information here](#) and if you have any questions about trust, security and compliance at Paligo [our contact information is available here](#).

V. Recommendations

So what's next? Do you invest in an on-premises CCMS or a cloud-based one? Your decision must be an informed one because there is no one right answer, just the right answer for your organization.

Take the time to map out your requirements on several levels:

- What features and functionality do you need in a CCMS?
- What systems do you need to integrate with, and where are they located?
- Do you require remote access for employees or partners?
- How much storage and processing power will you need now and in the near future? Is that growth substantial, or is it still unknown?
- Do you have an existing data center and infrastructure in which you can place a CCMS?
- Do you have resources with the right skills and availability to manage an on-prem solution?

- Do you have the budget to set up and maintain an on-prem environment? And if you do, is it the best use of your budget and resources?

You must consider the long-term benefits and strategic advantages of adopting a cloud-based CCMS versus an on-premises solution.

VI. About Paligo

Paligo is a cloud-based Component Content Management System (CCMS) with powerful single-sourcing content reuse for technical documentation, training content, policies and procedures, and efficient knowledge management.



[Find out more about Paligo today](#)