

The truth behind seven common cloud security myths

Why security concerns shouldn't stand between your
company and all the benefits that the cloud has to offer



Introduction

A Secure Home for Data & Processes

Giving up control over any process or system can always lead to concerns over potential risk, problems, or challenges. But transferring risk to a trusted third-party frees up organizations to focus on more important tasks. It lowers the total cost of ownership and can lead to process improvements.

As more companies shift computing resources, solutions, and processes such as labeling into the cloud, they're able to reallocate resources which were once spent

on servers, equipment, and IT support and to business-building projects and other priorities. The trend is gaining momentum: More than 60% of all corporate data is currently stored in the cloud — up from 30% in 2015 — and 94% of all enterprises are connected to online services that are hosted on the cloud.

As the cloud has matured, it has more than proven itself as a safe, secure option for organizations that want to optimize its benefits. This white paper explores some of



the main misconceptions that companies have about the cloud, dispels these myths, and provides a foundation for selecting the right software delivery option for your labeling and other business applications.

Connecting Data Services Virtually

Even risk-averse companies are moving into the cloud

A flexible, cost effective and highly scalable software delivery method, cloud computing supports mobility, collaboration, quality control and effective disaster recovery. It also provides software and platform updates that don't require an army of IT professionals to implement and use.

The cloud is popular. Gartner predicts more than 50% of enterprises will use industry cloud platforms to accelerate their business initiatives by 2027. Cloud-first strategies are now common, it adds, even among risk-averse organizations. It points to cloud security as the fastest growing segment in the market for information security technology and services.

Still, many companies are concerned about the security of their data and processes in the cloud. They understand how important it is to keep both safe and secure whether the data and processes are hosted on their servers or through a provider.

Therefore, when it comes to protecting their cloud environment, companies need a trusted partner with a dedicated team of certified security professionals. For best results, the team must understand best practices across policies, processes and controls involved in securing the data and the overall cloud infrastructure.

Even though a high percentage of companies are already using the cloud, some of them still cite security as the primary barrier to further adoption. What they may not realize is that their onsite data centers are most likely less secure than the cloud, where providers, whose businesses depend on secure delivery of cloud services, have invested heavily in physical and virtual security aspects. They have implemented sophisticated encryption technology, role-based authentication and other tools that ensure high levels of data protection.

The advanced security models implemented by cloud providers typically exceed what an in-house data centre has budget and expertise for. These attributes combined with the reduced costs and operational improvements that the cloud provides make it attractive for companies of all sizes and across all industries to manage solutions such as labeling in the cloud.



Getting to the Truth

Your top 7 cloud security questions answered

As more organizations abandon on-prem workloads and put more of their data and processes into the cloud, it can naturally raise some questions about just how secure those assets are once they're no longer hosted on-premises. Here are seven top cloud security questions that companies commonly ask and some answers to help put your mind at ease:

1) Where is my data hosted?

Rather than residing directly on your company's own servers, critical application data and assets, such as label designs and corporate artwork, are stored on servers located in a cloud provider's data centre and then accessed via the Internet. Access to the data itself will typically be controlled by your own application administrators, who will manage application users and their levels of access. The software provider should be able to provide support and retrieve useful analytics (e.g., the amount of storage being consumed) that both you and your provider can use to optimize performance and make operational improvements.

2) Would someone be able to hack our data?

Most security breaches don't happen when someone breaches a cloud data center. Instead, in rare situations, attackers typically exploit cloud application vulnerabilities. To prevent attacks, your provider would combine multiple mitigation strategies and security controls to protect your resources and data including: employee education, physical security, network security, web security, application programming interface (API) based cloud security, data encryption and regular security penetration testing at both the cloud infrastructure and application levels by an external party.

3) What specific measures are taken to ensure my data is secure?

Providers utilize industry best practices to protect your data and ensure the highest uptime possible. This includes practices such as encrypting data in motion and data at rest. Data encryption protects data from eavesdropping and provides an extra layer of protection in cases of unauthorized access. Your data is stored in database instances that are unique to you and not comingled, and security measures are in place to prevent anyone from accessing, modifying, or stealing this at-rest data. Also, security best practices are continuously evolving. To demonstrate completeness of their technical and organizational security measures, providers can choose to undergo 3rd party audits to certify their security



practice. These include certifications such as Service Organization Control 2 (SOC2), ISO27001 and National Institute of Standards and Technology (NIST). Cloud solution customers benefit greatly from these security measures. Ultimately, a certified cloud solution can result in an overall more secure corporate environment for cloud solution customers.

4) How has privacy improved over the past few years?

Over the past few years, regulators have taken swift action implementing laws and regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). These regulations deal directly with privacy to help ensure companies can avoid any large data privacy breaches. Providers today understand the critical nature of evolving legal and regulatory compliance mandates. These regulations outline specific requirements on behalf of data processors. At a minimum, all providers will ensure GDPR compliance and have a transparent Privacy Policy outlining your rights and your customers rights. Agreements such as Data Processing Agreement (DPA) can also define how data will be used. A cloud provider that is GDPR compliant and stays on top of applicable laws and regulations can help cloud customers ease the burden of regulatory compliance.

5) Should the vendor have a DPA in place?

A legal document between the cloud service provider and your company, DPA (Data Processing Agreement) establishes the scope and purpose of data processing; what data is processed and how it should be protected; the relationship between the controller and the processor; as well as the rights and of data subjects. While this document is oriented around the EU's General Data Protection Regulation (GDPR), it is also useful beyond the scope of doing business in the EU, as it clearly defines responsibilities and gives legal protection to cloud services customers. Together with Standard Contractual Clauses (SCC), a DPA with your cloud provider may be required for any company that does business in the EU and globally. Providers that have a DPA and SCC are typically going to have more mature processes as they would have developed the required processes to handle GDPR requests. Cloud service customers can benefit from these processes.

6) Are SaaS solutions safe and dependable?

Unlike on-premises software solutions, SaaS applications store data in the cloud and make that information easy to access from any location. When you work with a partner that values privacy and uses the best security protocols (e.g., multi-factor authentication, authorization, encryption, etc.) and is able to respond quickly and decisively in the event of a data breach, you can feel confident that your data is safe and secure online. The company



should also have disaster recovery protocols in place and offer high levels of availability. This is particularly important where manufacturing production systems, such as labelling, are involved. Also, to increase availability, cloud service providers will often choose to host their software solution on top of other large, mature hosting organisations such as AWS and Azure to benefit from their expertise and economies of scale.

7) Does the cloud provider have a CISO and DPO?

Since your cloud provider is taking on security responsibilities, most would have both a Chief Information Security Officer (CISO) and Data Protection Officers (DPO) in place. These are qualified employees charged with oversight of the entire environment from security and data privacy perspectives. The existence of a CISO is an indication of the willingness to invest in security. An independent DPO is a regulatory requirement, and this role represents willingness on behalf of the cloud provider to invest in privacy matters and maintain data subjects' rights even if this puts an additional burden on the cloud provider.

A Safe Place

Rest assured that with a trusted partner in your corner, your data and processes are [secure in the cloud](#)

Designed from the ground up for maximum data security, the cloud leverages encryption, physical and virtual security systems, authentication, and continuous monitoring to protect your data and processes against cyber security threats. A trusted provider will also store your data redundantly or operate in multiple regions for high availability in the event of any issues with access.

Despite some common myths, choosing the right cloud provider will offer better security than on premise systems can. That's because service providers devote resources to solving security issues that individual companies running systems on their own servers, computers and devices either can't afford to tackle, or they lack the internal technical expertise to do so.

At the end of the day, the partner behind the technology is just as important — if not more critical — than the technology itself. Companies should carefully evaluate their cloud providers. Find one whose deployment options put security and stability front and center, ensure that entrusted data is protected, and can verify security measures to protect data in the cloud.

Enable next level security and instil confidence

It's clear that cloud adoption is on the rise for many business systems and your labeling shouldn't be any different. Because at the end of the day, cloud-based labeling allows you to speed deployment and take fast, corrective actions to eliminate bottlenecks, improve time to market, and ensure compliance while future-proofing your labeling operations.

Loftware offers solutions built for the cloud. We offer everything you need to manage labeling, from label design and print to lifecycle management — enabling you to seamlessly implement, deploy, maintain, and scale your labeling with ease. We know that labeling is mission critical to your business, which is why we offer a safe, secure, highly available platforms to meet your needs. We also guarantee the best print performance on the market, and we provide round-the-clock performance monitoring and support.

To find out more about the top benefits of labelling in the cloud, [download](#) the report [7 Business-Boosting Benefits of Labeling in the Cloud](#).





No matter what the challenge – digital transformation, time to market, or brand authenticity – Loftware can help you make your mark. We understand how global supply chains work and know that each item you produce, and ship is an expression of your company's brand. We can help you improve accuracy, traceability, and compliance while improving the quality, speed, and efficiency of your labeling. Our end-to-end cloud-based labeling platform helps businesses of all sizes manage labeling across their operations and supply chain and our solutions are used to print over 51 billion labels every year. Loftware also fosters supply chain agility and supports evolving customer and regulatory requirements, helping companies save over \$200 million in fines annually. And with over 500 industry experts and 1,000 global partners, Loftware maintains a global presence with offices in the US, UK, Germany, Slovenia, China, and Singapore making us a trusted partner for companies in automotive, chemicals, clinical trials, consumer products, electronics, food & beverage, manufacturing, medical device, pharmaceuticals, retail/apparel and more.

For more information, please visit www.loftware.com.