

5 Reasons Cloud Security Outperforms Local Security



ARTICLE 03.29.18 DEAN DORTON

For years now, one of the reasons that organizations have not moved toward cloud computing systems has been due to concerns about security. However, as [more and more organizations](#) are adopting cloud-based or cloud-hybrid systems, cloud providers have progressively hardened and formalized security measures.

Today, the cloud is proving itself to be a safer environment for your critical data than on-premise, legacy systems. Here are 5 reasons why:

1) Physical security:

In many organizations, a locked door is all that separates your network from intrusion. Cloud security providers, on the other hand, typically use guards, security cameras, physical barriers, and other real-world measures to protect your data. This level of physical protection keeps unauthorized employees, vendors, and guests from accessing unauthorized systems, at least in the real world.

2) Disaster recovery:

Organizations need a concrete plan for disaster recovery that can be implemented at a moment's notice. An organization also needs to account for the security of backups in the form of protection from fire, earthquakes, or other natural hazards. Knowing that even if there were a fire in your offices, your data would remain safe and accessible provides extra security and peace of mind. Cloud storage providers use redundant systems so you always have a backup and have access to active disaster recovery plans in place and ready to go if you need them.

3) Security expertise:

For most businesses, the IT department has many areas of expertise and a broad array of responsibilities. This means that emerging security threats, new tools, and changing practices may not always be top-of-mind. Hiring an on-staff cybersecurity expert devoted to the task can be difficult and expensive. However, a cloud provider responsible for your data security has cybersecurity experts, who are tasked with nothing but protecting your data and staying on top of the latest threats. In addition, cloud-based cybersecurity providers are increasingly leveraging [artificial intelligence](#) and machine learning for constant vigilance and immediate response to threats and intrusions.

4) Always current and compliant:

Updating your local hardware and software to always be compliant with the latest security measures can be difficult, time-consuming, and expensive. Additionally, it isn't always easy to encourage staff to comply with the latest standards

and adopt best security practices. Cloud storage providers regularly update all their systems to protect against the latest threats and conform to the highest security standards, reducing the burden on your own IT department. It's easier to deploy updates or improve standards across your entire data system, providing greater protection and improving compliance.

5) Security auditing:

Cloud storage providers conduct thorough yearly security audits to ensure their systems are safe and current. Many organizations don't have the resources to devote to these kinds of systematic audits, so they don't get comprehensive reports of the state of their security and therefore struggle to identify and correct vulnerabilities.

Ultimately, data security is a shared responsibility, between an organization and their cloud solution provider, and between leadership and employees within an organization. Adopting a comprehensive, collaborative approach allows a business to leverage the security expertise and specialization of a cloud provider, and use a portion of the cost and time savings to apply stronger internal procedural security measures.

It's possible to get the reliability and accessibility of cloud storage, along with the security and control you need for your critical information.

[7 reasons to move to cloud financials now](#)