A company’s most valuable asset is its data. But as a particularly vulnerable resource, it is always at risk of possible loss or corruption via natural disasters, theft, power outages, and malware. As such, the question of data security often comes up when companies consider alternative data-storage options such as colocation and the public cloud.

Colocation versus the Public Cloud

The public cloud is a network of servers that businesses can hire on a pay-per-use model. Cloud computing transfers the routine management of a company’s servers and network infrastructure onto the cloud provider, leading to a big boon to companies with minimal IT staff. However, relinquishing control over data and IT resources can be one of the major downsides to the public cloud. The infrastructure is out of your hands.

On the other hand, colocation refers to the practice of leasing space within a secure offsite data center where customer-owned servers and network equipment are hosted. The customer remains in control over the operation and maintenance of their servers and hardware while the data center provides the infrastructure including space, power, bandwidth, cooling, security, and redundant systems.

Many data centers also offer managed services that can be leveraged to monitor and manage IT infrastructure. Managed colocation can be offered as a complete turn-key solution where the customer owns the hardware but the data center manages all aspects of its operation, from updates to troubleshooting.

Some colocation data centers also offer managed backup and managed firewall services. Managed backup services ensure the restoration of both physical and virtual data in case of disaster or loss. Managed firewall services relieve businesses of the need to manage multiple firewalls across many sites, which can be a huge drain in terms of time and resources.

Data centers should have the appropriate certifications to prove compliance, maintain a high level of physical and cyber security, and follow best practice procedures that are audited annually by independent third party evaluators.

There is also a need for facilities to be certified to the highest industry standards and compliance requirements such as HIPAA and SSAE16. Physical security is also important, such as 24×365 site monitoring through security operations, ID cams, motion sensors, alarms, and recording, as well as biometrics scanning and access control.