Calipsa Cloud

All in a fog over the cloud? We've got you covered.

Many companies are already using the cloud

Cloud computing enables businesses to implement smarter systems. Intelligent automation, customer-produced data, and smart devices are all made possible relatively cheaply, at a large scale.

Gathering and processing data (often in real time) offers all kinds of opportunities for improved operations and business intelligence - as well as an enhanced customer experience.

To monitor all this data and deliver new, improved products and services, companies will require a powerful, flexible and reliable IT infrastructure: cloud computing.

Benefits of the cloud

Flexible
The cloud allows you to connect and remotely manage multiple devices, even entire sites. Subscription models also give you the option to scale services up or down, in line with your business needs.

Secure
Many cloud based tools and cloud providers use encryption, authentication and tiered access controls to make sure that only authorized users have access.

Agile
Updates made over the cloud can be implemented instantly, and remotely. This means you can easily manage operations in several different sites, and that multiple users can carry out work instantaneously.

Easy integration
More often than not, cloud services have developed easy ways to integrate with your existing systems. This makes it easier to connect the different technologies your company uses - including IT and OT.

Is the cloud safe?

The short answer? Yes. The long answer? Yes - but for added security, compliance and peace of mind, don't rely on a cloud provider's security protocols as your only line of defense. Start by reading the government guidelines in your country, such as CISA in the US and NCSC in the UK. However, there isn't a one size fits all solution so do your research and consult with your firm's compliance and IT departments first.

Nearly all major cloud providers follow security protocols to protect BCSI (BES (Bulk Electric System) Cyber System Information), or more simply, the information transmitted and stored in the cloud. Most of these protocols involve encrypting information to make it much harder to hack. Look for the following:

Transport Layer Security (TLS)

Easy to spot, it's a "https://" web address. This layer of encryption prevents eavesdroppers and hackers from seeing information transmitted over the link you're visiting.

Information encrypted in all three states

At rest, in transit and in use. As the end user, you will need to determine the parameters of "in use" and review your own security protocols accordingly - however your cloud provider should have the essentials in place.

Encryption key management

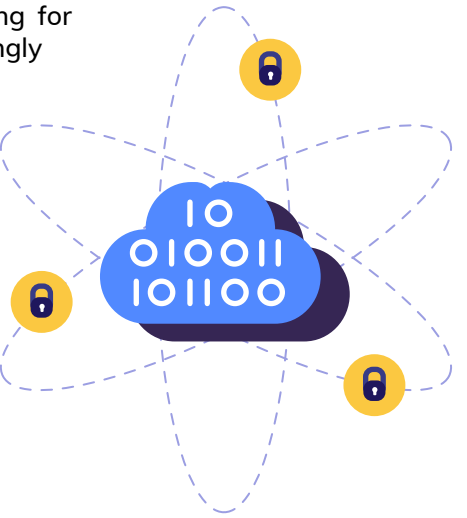
Consider whether you would prefer to manage your own encryption keys, or whether you want the cloud service provider to manage some or all of the encryption keys for you. There are pros and cons in both cases. From a compliance and information security perspective, managing your own keys is preferable, as even your cloud provider can't access your information. However, if you were to lose an encryption key, then in this case your cloud provider can't help you. When a cloud provider manages some or all of your keys, you can expect more operational support.

Find out how information is physically stored

For example, is storage spread out over a wide geographical area or all in one location? When information is stored over a wide area, it is harder to hack as servers are more spread out.

Using the cloud for security

As technology becomes more intelligent, it makes sense that physical security should follow suit. Physical security and cybersecurity have been merging for several years now; alongside OT, security technology is becoming increasingly smarter and moving online.

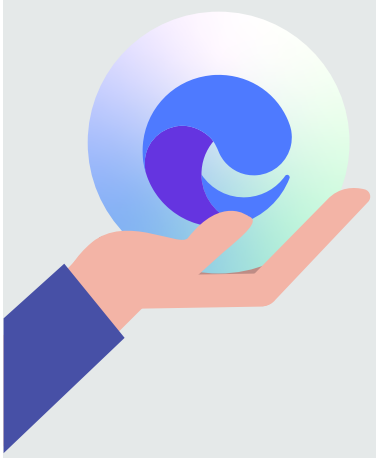


Many security providers use the cloud for the same agile and flexible benefits; it enables security teams to roll out even better real-time remote protection - ideal for sites which are difficult to protect adequately with security guards alone.

Cloud-based security solutions allow for much greater connectivity across multiple sites, which means you can monitor perimeter fences, motion detectors and security cameras faster and with much better oversight. It also stops your on-premise protection from becoming a sitting target; if a criminal were to destroy security equipment, remote security staff can easily spot that this has happened and either activate a backup (or redundancy) system, or notify law enforcement.

What happens if a breach occurs?

If the worst does happen and your cloud service provider is hacked, you should be prepared for this scenario. Your IT and compliance departments will already have some plans in place for your existing IT infrastructure, and many of the same protocols will apply in this case. As a third-party service, your cloud provider should have a defined plan in place, which should be laid out in the original service level agreement that you signed. However, to ensure that a breach is properly and swiftly resolved, at the point of signing you and your provider should establish your respective responsibilities and points of contact.



Is Calipsa safe to use?

Calipsa's Pro Analytics products are all cloud-based, which means we can provide you with the greatest possible flexibility, speed and ease of integration. However, security and customer confidence are our top priorities; below are the measures we take to ensure that Calipsa is safe to use.

- Our cloud provider is AWS, who have stringent cloud security policies. You can find out more about their security protocols and practices here: https://aws.amazon.com/security/
- We "hash" passwords, which means they are automatically encrypted, making them much harder to hack
- We require customers to authenticate their login credentials using Captcha, to reduce the risk of bots attempting to hack passwords; we also lock the login page after 3 failed attempts so that hackers can't run endless login attempts until they find the right email/password combination
- We set tiered user access, so that our customers can control which employees can access certain levels of information

Contact | Get started with Calipsa Pro Analytics

If you want to know more about how Calipsa's Pro Analytics can help your business or if you want to know more about how we use the cloud - then contact us at:

www.calipsa.io

info@calipsa.io