Reliance HIGH·TECH

Every cloud has a silver lining

Why moving your security systems to the cloud brings financial and operational advantages

The cloud beckons

Despite widespread use in our work and personal lives, there is still reluctance from some organisations to utilise the cloud within their security infrastructures. This is unfounded, as the numerous financial and operational advantages from using the cloud to host security systems are becoming ever clearer.

The cloud has radically reshaped our day-to-day lives and is accepted as a highly convenient means of storing and accessing data, as well as offering valuable services and applications. According to multi-cloud services provider Faction, a staggering 92% of organisations had a presence in the cloud in 2022, undoubtedly driven by the rapid increase in digitisation post-Covid.

Moving on up

Given its unstoppable rise, it is surprising that some enterprises are still unwilling to fully utilise the cloud as part of their security infrastructures. Perhaps understandably, not having potentially sensitive footage and information on-site disquiets some security professionals, and it's certainly true that data protection is now an area where failure is not an option.

Meanwhile, legal and regulatory compliance, as well as data loss and leakage risks, are often cited as barriers to adoption. However, the truth is that many of the fears and objections surrounding the cloud are often misguided and, by carrying out due diligence and working with the right security partner, data can be safer in the cloud than on a user's premises.

Checks and balances

Of course the cloud is not literally located in the sky – preferring instead to reside in data centres - and it is vital to ascertain where those facilities are geographically located and what physical and network security protocols they have in place. Choosing a data centre that has achieved international information security and continuity compliance standards, such as ISO 27001 & 22301 respectively, is a necessity.

Data centres also need to be physically secure to protect the building and IT equipment housed inside. You can have what appears to be a very secure looking facility only to find it's built on a floodplain, in a suburban area under a direct flight path, or located in the centre of a metro area – not exactly out of harm's way from natural or man-made threats such as flooding, riot and terrorism.

Some cloud naysayers cite potential network downtime as a barrier to adoption. However, resilience has been addressed within the data centre sector and they should have access to abundant and redundant power and connectivity links, plus their servers should be sufficiently cooled and energy optimised to ensure as close to 99.999 per cent availability as possible. N+1 redundancy – in other words the duplication of critical components or functions of a system – alongside predictive diagnostics, watertight support contracts, and on-site spare equipment - are also prerequisites.

Money matters

The cloud may allow an end user much more flexibility in terms of secure remote connectivity, allowing them to access their security system from anywhere, at any time and on any device; or to manage multiple locations seamlessly from one unified interface. From a financial perspective, there are no upfront server costs, no back-ups to create, and no complex network routing or interruption to service while software updates and hardware upgrades are carried out. Users only pay for the computing power, storage and resources used.

A cloud-based security solution will, of course, require some on-site hardware such as cameras, most of which can be repurposed at minimal expense. Yet instead of data being fed back to an on-premise server or PC, all information goes back to an off-premise cloud platform utilising private cloud services or familiar names such as Microsoft Azure or Amazon Web Services.

There are of course genuine reasons that a cloud-based system may not suit a particular application or end-user, so it is definitely not a 'one size fits all' solution. Cost, risk, compliance, complexity are all things that need to be considered in a balanced way to make a decision.

A hybrid approach

What many people don't realise is that it doesn't need to be 'all or nothing'. One example could be to take the storage offsite, but leave the rest of the system as traditional technology on site. This type of system might consist of an on-site video surveillance storage solution recording a minimal amount of local footage, whilst medium and long-term storage is located in the cloud. For large amounts of data storage - particularly over long periods of time - this could be significantly more cost effective than having mass physical storage on site - not to mention the running cost, energy costs, maintenance cost, increased disaster recovery and reliability.

In the very rare and unlikely event that the 'internet' connection (WAN) goes down, surveillance footage would be stored locally for a defined period of time. However, as soon as the 'internet' connection is restored, all of the information is synchronised back to the cloud and stored – ready to be retrieved as required. Let's be honest have you ever lost any photos on Apple iCloud, or Google cloud due to a crash at their end?

Going deeper

The popularity of video analytics is closely linked with the growth of cloud based security. By facilitating the aggregation, analysis and presentation of data acquired from video surveillance systems, information can be presented more easily in statistical reports and graphs. This makes data regarding occupant behaviour, vehicle movement and space utilisation readily available to be acted upon.

The cloud also provides expanded data storage which offers users the opportunity to use video management systems to intelligently filter information they have stored in order to remove what isn't needed and only keep what is required. This data can then also be used for analysis, as well as implementing machine learning and even artificial intelligence based applications.

Multiple storage options will always be available, with varying cost implications, so filtering stored information will improve cost control. End users also benefit from greater scalability, as new resources can be provisioned within minutes.

Benefit check

The arguments in favour of using the cloud for security purposes are compelling. Far from being a weak link in an organisation's security chain, the cloud is more reliable, secure and well provisioned, delivering a range of advantages including greater resilience, ease of mobile user support, flexibility, minimal capital expenditure, reduced operational costs and an improved user experience. If it fits the application - what's not to like?!

That said, moving to the cloud is a big step, and it's vital that organisations work with the right supplier to make it happen. Do they have Cyber Essentials Plus? Are they certified to ISO 27001, or ISO 22301? These establish competence in cyber security and business processes and ensure your data will be safe at all times as you make the transition.

For details on how the cloud can help you, email info@reliancehightech.co.uk

Reliance HIGH·TECH

The Columbia Centre
Station Road
Bracknell, Berkshire
RG12 1LP

www.reliancehightech.co.uk

Tel: 0845 121 0802
Email: info@reliancehightech.co.uk

Service Desk: 0845 121 0808
Monitoring Centre: 01977 696600
Lone Worker Help Desk: 0800 840 7121

CYBER ESSENTIALS CERTIFIED PLUS

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi ISO 22301 Business Continuity Management CERTIFIED