News

The Forecast: Cloudy for the Foreseeable Future

The cloud has radically reshaped our day-to-day lives and is increasingly accepted as a highly convenient means for storing and accessing data, as well as offering valuable services and applications. However as Kim Loy, director of marketing at Vanderbilt, explains, the security industry has much more to do to maximize its full potential.

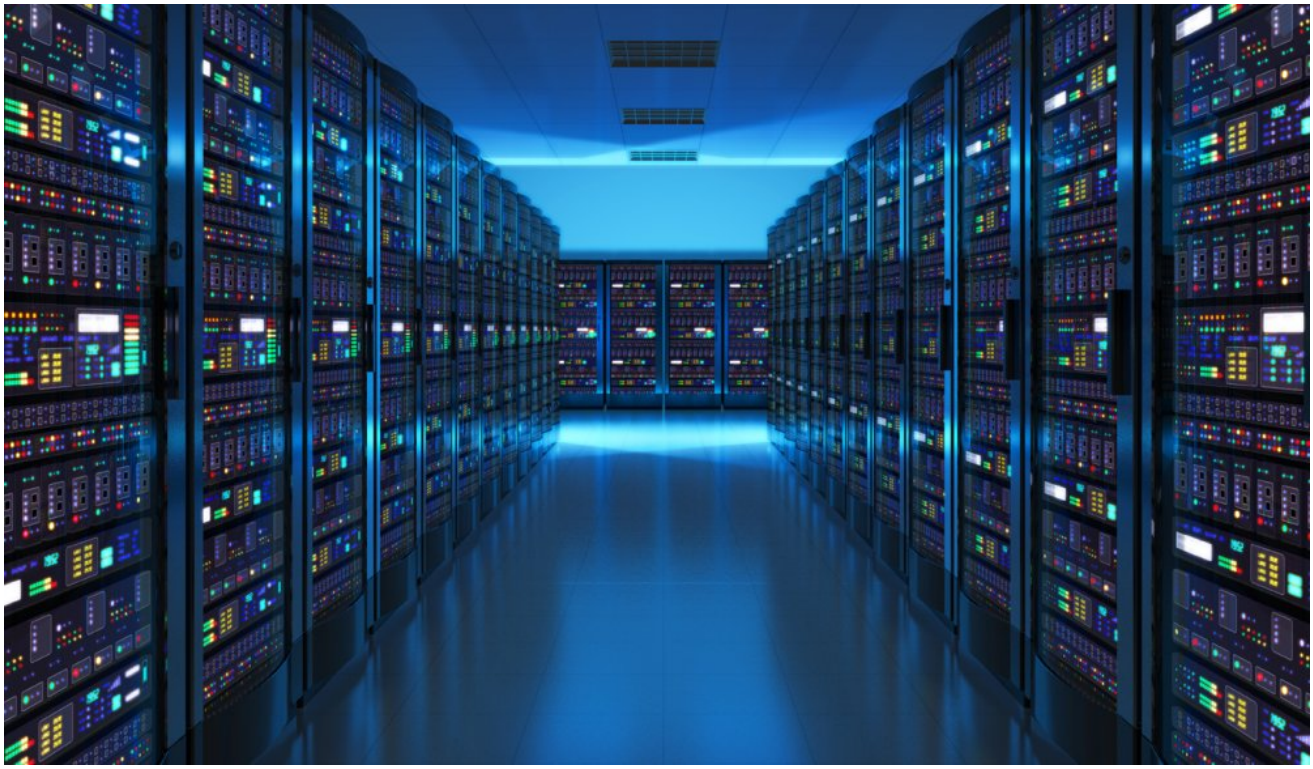
In the 1990s, the dawn of the internet saw cloud computing become a reality, with many enterprises quick to latch onto it. Since then, cloud services have become well established across almost all industry sectors and changing customer demands mean that many businesses are now reinventing their offerings to harness the power, flexibility and functionality it offers.

Growing concern

The adoption of cloud-based solutions by companies continues to grow at an astonishing rate. Cisco predicts that by 2020, global cloud use will account for more than 92 percent of total data center traffic. This surge in adoption also represents a huge uptake in spending, which Gartner predicts will exceed $1tn in purchases dedicated to the cloud by 2020.

Also, more and more businesses realize that leveraging the cloud is the most efficient way to solve emerging challenges. Given the clear indication about where the attention of enterprise customers is now being focused, cloud-based security applications for video surveillance and access control have been largely aimed at niche sectors and homeowners. In fact, very few solutions for enterprises have come onto the market.

The good news is, that's beginning to change, with the introduction of cutting-edge systems such as Vanderbilt's ACT365 technology, which allows a business owner or security manager to access the system 365 days a year from any internet connected device. Contrast this with a traditional security system that can only be accessed from a PC in a security office to retrieve important data. This is, at best, a reactive approach to security management and usually culminates in important events being missed and the same security breaches happening time and time again.



THE POPULARITY OF video analytics is also closely linked with the growth in cloud-based security. By allowing aggregation, analysis and presentation of data acquired from video

surveillance systems through an internet browser, data can be analyzed and presented in statistical reports and graphs. This makes information regarding people and vehicle movement, occupancy and activity readily available.

Protect and survive

The cloud offers major advantages to both installers and end users. For the former, no server specifications, no SQL and no complex network routing makes it easy to install. Remote diagnostics, technical issues and servicing can be carried out from a web portal or smartphone – by simply logging in via a username and password, it's possible to remotely view status, set and unset a system and access an event log. Last but certainly not least, it provides an opportunity to earn recurring revenue by charging the customer for hosting, additional customer service and providing fully managed security services.

Similarly, an end user can access a security system from anywhere at anytime and on any device, and manage multiple locations seamlessly from one unified interface. On the financial side of things, there are no upfront server costs, no back-ups to create and no need for complex network routing.

For both parties, dealing with technical or operational issues have traditionally been a time consuming, expensive and laborious task. With minimal data about a system usually remotely available, a site visit is often the only way to get to the bottom of a problem and make any system alterations that are required. In some cases it can also mean that a customer has to wait hours or even days for a problem to be rectified – something that few enterprises can accommodate. Remote access via the cloud changes all that.

Rules and regulations

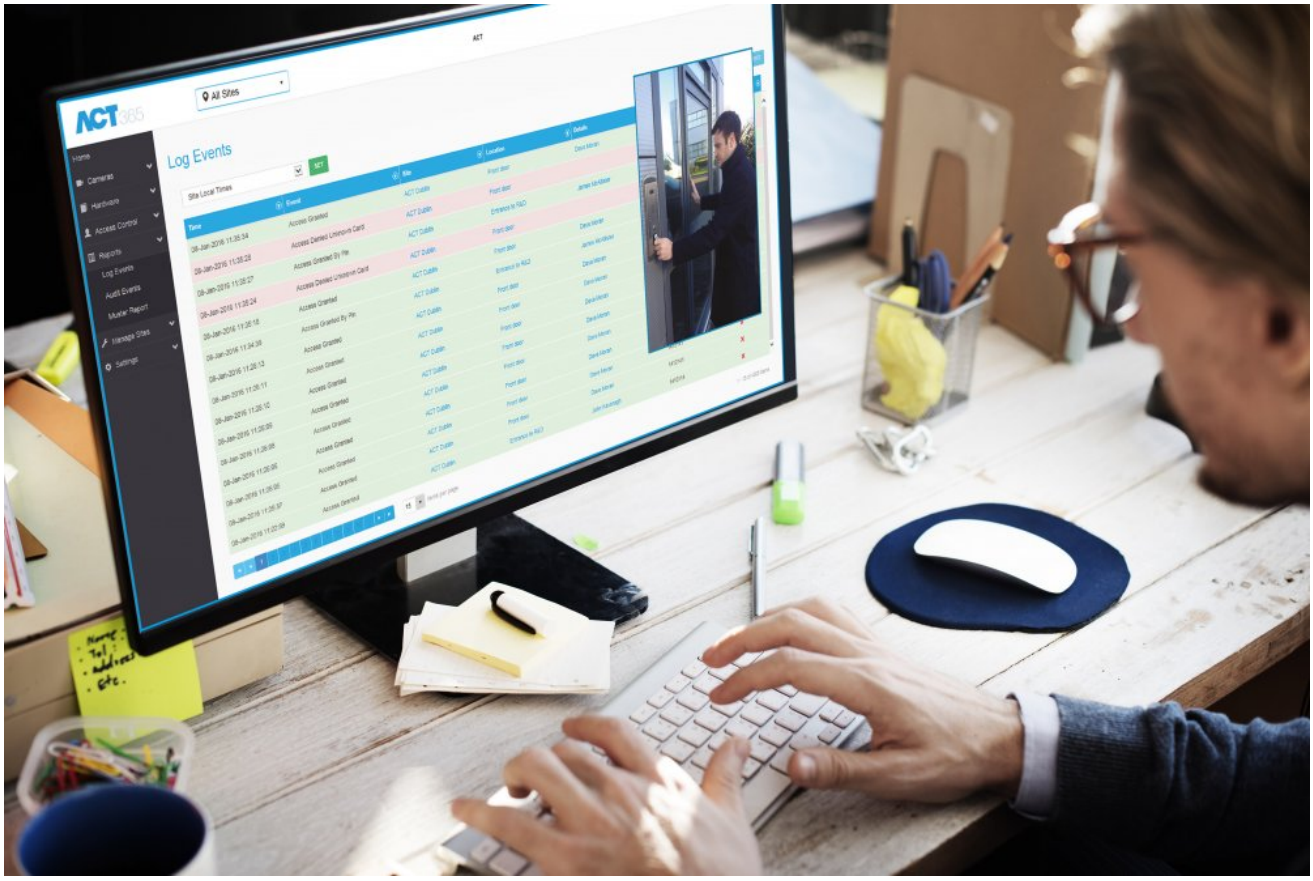
Despite all the positives, there is still significant reluctance from enterprises both large and small to embrace the cloud fully. Some users are concerned that they no longer have control of data that is kept on-site. Many security managers find the mere mention of 'the cloud' invites input from their IT department, making the specification and procurement of a cloud-based security system more complicated. Therefore, when choosing a vendor, users must ensure that they truly understand the technology to the degree that provides comfort to IT departments. Any system they design must also meet the requirements of any corporate IT policies that are in place.

CLEARLY, DATA PROTECTION is an area where failure is not an option. Security, legal and regulatory compliance, as well as data loss and leakage risks, are high on the list of barriers to cloud adoption. End users are right to be concerned about this issue, as on 25th May 2018, the General Data Protection Regulation (GDPR) becomes European law. Its primary objectives are to give citizens and residents control of their data and to simplify the regulatory environment for international business by unifying the regulation within the European Union (EU). It requires an organization that operates in the EU, or handles the personal data of people that reside in the EU, to implement a strong data protection policy, encompassing access, secure storage and destruction. Users and installers must seek out vendors that understand the implications of the GDPR and its potential impact on security systems that store and access data in the cloud.

There also appears to be a certain amount of confusion surrounding the cloud and incorrect advice from suppliers has resulted in failed or stalled programmes in 28 percent of organizations, according to research from The Bunker. It found that 70 percent had experienced some level of failure, preventing them from achieving their business goals, while 67 percent has sought advice from external consultants and 61 percent from their key suppliers.

Smart thinking

Just like enterprise networks, the cloud is not immune from hackers, with various attacks having been made against these types of platforms. As with any system – cloud or non-cloud – hackers will exploit security gaps left by the cloud vendor or end user. A study by BullGuard recently found that 66 percent of consumers are ‘very concerned’ or ‘highly concerned’ about potential hacking and data theft carried out against their internet connected devices, with 34 percent having already experienced a security incident or privacy problem in the past.



The exploitation of vulnerability could lead to a compromise of customer information and assets they are trying to protect. It therefore makes sense to work with a vendor that understands concerns about data integrity. For example, Vanderbilt’s SPC Connect 2.0 allows installers and end users to access an SPC intruder alarm control panel remotely via the internet, with all of its settings and other information stored in the cloud. The important thing is the use of the FlexC protocol, which uses AES 256-bit SSL encryption at server level – the same grade used by banks and hospitals. Likewise, installers can only be given access specific panels and this authorization can be withdrawn at any time to offer customers total peace of mind.

Delivering the goods

We all recognize that the cloud offers significant financial savings by enabling more cost-effective scaling, alongside the reduction in hardware maintenance and management costs. While an important consideration, security should not prohibit the adoption of cloud-based security and access control, as in many cases it can deliver a range of advantages including greater security, more resilience, ease of mobile user support, flexibility, reduced costs and a greater user experience. It is not without risk – but in the right hands this risk can be managed and minimized, and the benefits to organizations in moving to the cloud are compelling.

Download White Paper