The Police's Duty to Protect Data in the Cloud

Veganism, the plastic backlash, social media, ride-hailing services – these are some of the biggest trends that defined the 2010s, and in the enterprise tech world, one of the most notable trends has been the rise of the cloud. According to a recent study, 91% of businesses in 2019 used public cloud. Jumping on the cloud bandwagon is the UK's police force, recently migrating the Police Open Systems from its on-premise servers to Amazon Web Services.

The public cloud giant has made over £123 million from the UK's public sector, which includes HMRC, the NHS and the DVLA. It is of little wonder the public cloud has gained such popularity, providing benefits in scale, functionality, cost savings and agility. However, this interest in public cloud adoption is only recent – the public sector has been the most reluctant to move off-premise.

According to Gartner, this hesitation is due to major concerns in security and privacy. Many feel storing data off-premise robs them of the control needed to ensure its security. This is a far graver issue for the police force, who have the responsibility to ensure, not only the physical safety of civilians, but also that of their sensitive data.

Data protection – at the heart of gaining public trust

In recent years, data privacy has become of increasing public concern. This is partly due to the implementation of the GDPR, as well as the media coverage of major data breach scandals, such as Equifax, Facebook and Cambridge Analytica. Government departments and entities depend on the public's trust. In fact, the Met Police states its ultimate vision is "to be the most trusted police service in the world." That trust must be earned.

Public confidence is gained when its members clearly know the purpose for disclosing their data and feel it's a valid exchange. An example is the controversial use of Live Facial Recognition technology. Following its investigation, the ICO made the poignant question, "How far should we, as a society, consent to police forces reducing our privacy in order to keep us safe?" It went on to remark that using LFR in an ungoverned manner "[damages] trust . . . in the fundamental model of policing by consent." Nonetheless, police officers often need sensitive information to carry out their jobs, and delays in obtaining crucial information, due to unforthcoming members of the public, can effectively hinder a case.

"

Public confidence is gained when its members clearly know the purpose for disclosing their data and feel it's a valid exchange.

"

Now that the police has moved its databases and systems to the cloud, it must ensure the data stored is, to begin with, stored for a justifiable reason, shared with authorised personnel only, protected from human error, closely monitored and encrypted should it fall into the wrong hands. How can the police achieve this when the public cloud, though not inherently insecure, cannot conclusively guarantee data protection?

Keeping the cloud's streets safe

This lack of confidence in cloud security impelled iStorage, the award winning and trusted global leader of hardware encrypted data storage solutions, to develop a cloud data storage security solution – cloudAshur. The cloudAshur hardware encryption module (your encryption key), which works with numerous cloud providers, allows users to encrypt data to ensure the ultimate lockdown of data stored in the cloud, share encrypted data with authorised users in real-time, and manage and monitor cloudAshur devices centrally. The cloudAshur can be used to encrypt data locally on a PC or MAC, as well as encrypt files shared via email or file sharing software that can only be decrypted with an authorised cloudAshur module.

To be a truly secure solution, it is imperative that the encryption key is stored away from the data. The cloudAshur hardware encryption module encrypts all data in transit and at rest with a FIPS certified randomly generated AES 256-bit encrypted encryption key, which is stored and protected within a dedicated iStorage secure microprocessor (Common Criteria EAL4+ ready). The cloudAshur grants the user full and secure control of the encryption key, thus protecting the data even if the cloud account is hacked.

Additional features of the cloudAshur solution include:

- A unique Five Factor Authentication
- Tamper proof & tamper evident design
- IP68 Certified (Dust & water resistant up to 1m)
- Secure and instant collaboration in the cloud
- Remotely disable or reset user cloudAshur modules if suspicious activity is noticed, impeding access to files stored in the cloud
- Monitor file activity
- Time fencing and geofencing

The police can benefit from the flexibility and cost reductions offered by the public cloud, but with this, they must also shoulder the responsibility of shielding sensitive data. The cloudAshur will finally provide the police force the control so very needed to ensure data privacy in the cloud, which is fundamental to gaining the public's confidence and indeed becoming the most trusted police service in the world.

cloudAshur - hardware encryption module

iStorage®

iStorage is the trusted global leader of award-winning, PIN authenticated, hardware encrypted portable data storage & cloud encryption devices. iStorage offers the most innovative range of products to securely encrypt, store and protect data to military standards; safeguarding valuable and sensitive data to ensure compliance with stringent regulations and directives such as GDPR, HIPAA, SOX, NRC, GLB and DHS Initiatives. Today, iStorage products are used by government, military, multinational corporations as well as consumers in over 50 countries, with the mantra that encryption is an essential commodity required by all.