Cloud-Based Evidence Management Platforms

Sharing evidential quality footage with external stakeholders securely

What is a cloud-based evidence management platform?

A 'cloud-based evidence management platform' – sometimes called a 'digital evidence management platform' – is a securely hosted solution that enables users to easily store, share and manage evidence with external stakeholders.

Is a cloud-based evidence management platform the same as 'remote access cloud surveillance'?

No, remote access cloud surveillance refers to a platform that allows authorised users to log in remotely via the web to access many (if not all) core features.

These features include access to live and recorded footage, camera control, alarm notifications and reports. Remote access is more commonly used for internal purposes, for example, giving field-based operatives within an organisation (security guards, maintenance teams, process management personnel) access to surveillance solution capabilities.

Remote access surveillance can also quickly 'scale up' resource within a control centre. For instance, a city hosting a major event may wish to temporarily have more surveillance operators active to monitor larger volumes of people and crowds. A web-based surveillance solution allows this without investing in additional hardware and infrastructure.

By contrast, a cloud-based evidence management platform only gives authorised users access to recorded footage and supporting information deemed relevant to a specific incident. For this reason, it is often seen as a 'soft entry' to cloud-based surveillance and a preferred option for sharing information with external stakeholders, such as the police, emergency responders, authorities, citizens, and insurers.

Is it only video surveillance footage I can share?

Most solutions support uploading multiple file types (video, audio, image, text). Solutions enabling multiple formats are essential as they allow 'evidence packs' to be built relating to a specific incident. So, for example, information could be provided that might be useful for ongoing investigation and corroborating evidence.

SYNECTICS

Solutions should also allow for augmentation (not alteration) of video content with bookmarks/tags, comments, annotations, and observations made by the operator.

Suppose you select a cloud-based evidence management solution from a provider other than your primary surveillance solution. In that case, it is crucial to confirm the solution is 'agnostic' and will support the upload of video from any source. For example, Synectics' Cloud Evidence Locker is compatible with Synergy, third-party surveillance solutions, and the upload of multiple file types, including any MP4 file.

Being able to upload video files from any source is also helpful for crowd-sourced evidence, such as mobile phone footage from a witness to an incident.

How do I control who can upload and/or view evidence?

Very easily. Authorised administrators of the solution can set permissions for individual users and specific user groups to control who can upload, view, and download evidence. The precise control of user permissions can be automatic (x always has access to evidence in the cloud) or case-by-case (for this specific incident, x has access to evidence stored in the cloud).

With Synectics' Cloud Evidence Locker, relevant external parties can also upload evidence once an incident has been opened. For instance, a city centre control room operator could spot a riot unfolding, open an incident, and share the footage with specific police officers. Footage from their body-worn cameras could then be uploaded to the same incident to keep all associated evidence together in one place.

Do I have full traceability of the evidence I've shared?

Yes. Much more so than systems that rely on footage being physically downloaded to disk for collection by an external party.

Leading cloud-based solutions ensure that all actions are logged. This means that whenever video and supporting evidence are added, viewed, supplemented, or downloaded, there is an immutable record of this activity for full traceability. Your solution should support the generation of "any time" evidence certificates detailing this information.

How can I be sure evidence held in the cloud is secure?

Cloud-based evidence management solutions are highly secure. To achieve globally recognised accreditations, data centres and networks must pass stringent cyber security requirements. Moreover, providers of hosted cloud environments, e.g. Microsoft Azure, continuously monitor for anomalies and even employ in-house 'hackers' to seek out potential vulnerabilities to keep pace with evolving cyber threats.

It is, however, important to check the data encryption measures in place for transferring data from devices to storage/to the cloud.

Our Cloud Evidence Locker features security measures, including end-to-end encryption and user authentication, plus the built-in cyber advantages provided by Microsoft Azure.

Is the information shared in this way evidentially compliant/admissible in court?

Yes. If your solution adheres to the security measures outlined in this Tech Note, it is fully compliant and admissible.

Be aware of the data security standards and codes of practice specific to your country. In the UK, for example, your cloud evidence management platform provider should be able to ensure that you can adhere to NCSC Cloud Security Principals, and the Digital Imaging and Multimedia Procedure V3.

Is using a cloud-based evidence management solution compliant with data protection laws?

Yes. Such solutions often help users meet data protection requirements more easily. For instance, with Synectics' Cloud Evidence Locker, AI-enabled facial redaction tools enable users to mask sensitive data before it is shared to maintain data privacy.

For more information on our Cloud Evidence Locker, watch this short video

Literature Reference: CBE-TN/0123/A4 Iss 1