Cyber security checklist for cloud video surveillance solutions

In today's increasingly digital world, security is everyone's responsibility. When all your devices and systems are interconnected, they are immensely powerful. But this also makes them vulnerable to cyber crimes and liabilities. There's not much room for error. Review this checklist to make sure your cloud video security solution is always protected.

1 Choose hardware products that are secure from the ground up

You're not alone. You must choose vendors and work with distributors that value security standards, processes, and policies to deliver a high level of resilience against threats.

- Factory-installed certificates and keys to prove the identity of the devices to each other, and to a cloud instance
- Hashed and salted camera passwords created using PBKDF2 and SHA-512 to NIST guidelines
- Trusted vendors who carefully consider and control the manufacturing process
- Cameras and appliances equipped with a Trusted Platform Module (TPM) to provide secure encryption key storage
- Cameras and appliances preloaded with a digital certificate to prove their identity to other devices

2 Implement encryption everywhere

Protect your data against eavesdropping, man-in-the-middle attacks, and hijackers, and keep its integrity whenever you send, receive, or record footage

- At rest
- In transit
- Video recordings
- Metadata
- Firmware

3 Rely on solutions that provide automatic software upgrades and security best practices

Select vendors who design solutions compliant with international information security standards and who prioritize updating the software and firmware of all their devices.

- Automatic software and firmware updates, with latest security patches
- Product security incident response teams to ease cyber threats and strengthen your security
- Continuous vulnerability monitoring in both own and third-party code and public security advisories
- Full awareness of your system's health
- Solutions compliant to ISO 27001, including Information Classification and Handling, and Security Risk Assessment

4 Review system privileges

Deploy role-based access controls (RBAC) so that users of your security systems have authorized access levels set by your system administrators.

- Role-based access
- Rich permission system to allow you to control who has access to what
- Ability to prevent cloud operators from viewing video

Ava is a security-first company with a strong product and security culture. We believe that to deliver an effective security solution, the system itself must be secure. We have industry-leading portfolios both in video and cyber security and share secure development models and expertise across domains to ensure all our products are secure from the ground up. While it is impossible to guarantee 100% security, we follow internationally recognized security standards and processes to minimize the risk.

Learn more at:
https://www.avasecurity.com/library/ava-video-security-solution-cyber-secure-white-paper