White Paper | February 2022

Security at the core of the Ava video security solution

Introduction

To deliver an effective security solution, the system itself must be secure.

From the outset, Ava has designed the Ava video security solution to have security at the core of all aspects of design and implementation. This includes:

- Using software development best practice and design for the Ava Aware Cloud® software, the Ava Cloud Connector™ software, and the software that powers the Ava Cameras.
- Careful consideration and selection of all components used within the Ava Cameras and the Ava Cloud Connectors.
- Designing, monitoring, and controlling the manufacturing processes used for all hardware, software, and cloud components of the system.
- Using an ISO 27001 compliant process for information security.
- Protecting all data using encryption, whether in transit or at rest.

About Ava Security

Ava Security designs and manufactures advanced video security solutions that benefit from cutting edge advances in machine learning. By using analytics on all cameras, all of the time, the systems can alert your key staff to issues as they happen, rather than you having to rely on painstaking searches of recorded footage after the event.

The development teams for the Ava Camera, Ava Aware, and Ava Cloud components use world-class secure development models on all products. This includes using security teams to maintain the security focus on all design and development activities for all Ava products.

Security incidents related to the products are handled by the Ava internal Product Security Incident Response Team (PSIRT) using the process documented in https://www.avasecurity.com/internal-security.

When an issue is found in an Ava product, patches are developed for the affected products. These patches are then released via the normal releases processes; first being deployed to the Beta Upgrade Channel before being released to the Stable Upgrade Channel. This enables additional testing to be carried out on the beta builds before upgrading your critical video infrastructure.

In addition, after both the Beta and Stable upgrade channels have been patched, Ava publishes security advisories for all security issues, including those found internally. You can find all the security advisory information for the Ava products at https://support.avasecurity.com.uk/support/solutions/folders/44001217217.

To receive notifications about new software releases and vulnerability advisories, subscribe at https://www.avasecurity.com/software-updates-security-advisories.

ISO/IEC 27001 accreditation

Ava Security is ISO 27001-accredited. (See https://verifeyedirectory.bsigroup.com/Certificate/IS%20734038 for information about our accreditation.)

ISO 27001 accreditation demonstrates that Ava Security is committed to ensuring the organization is very serious about information security. It also shows that as an organization we have been assessed by an accredited, certified, and competent third-party assessor (see https://www.bsigroup.com).

ISO/IEC 27001 is an international standard for managing information security, originally published by the International Organization for Standardization (ISO).

ISO 27001 is adopted by many organizations worldwide to demonstrate that they take the management of information and internal security processes seriously to protect their businesses and their customer's data. This gives you the confidence that Ava Security follows industry best practice.

Holding the ISO 27001 accreditation requires organizations to implement controls to manage and monitor security services in a number of common areas, such as Information Security policies, Organization of Information Security, Human Resource Security, Asset Management, Access Control, Cryptographic Control, Physical and Environmental Security.

In addition, this standard requires compliance for systems related to Operations Management, Communications Security, Security Acquisition, Development and Maintenance, Supplier Rrelationships, Information Security Incident Management, the Information Security aspects of Business Continuity Management, and Compliance.

This is a wide-ranging requirement that touches every element of Ava Security.

Development operations

Access to the Ava software development environments is controlled using multi-factor authentication — so only authorized specialists have access to the source code. Working for a security company, all employees have to undertake regular security training, and are trained on how to handle and manage any customer data.

All Ava employees must have suitable security software installed on their computers — including tools to prevent data loss, regularly updated anti-malware defense controls, and control software to restrict access to files and information.

To provide further protection, all source code must be manually reviewed and approved by other team members before it is merged into the product code-base.

Penetration testing

Ava Security contracts CREST certified providers to conduct penetration test security assessments of the Ava products. These tests help identify any security issues that, if they led to the compromise or abuse of systems, could negatively affect Ava customers. The reports received confirm that the Ava products are developed to a high security standard and are well protected against common vulnerabilities.

We also actively encourage customers and potential customers to carry out their own penetration testing on Ava systems, and work to resolve any issues raised by these external penetration tests.

These penetration tests and their subsequent reports form part of regular ongoing testing to ensure these high security standards are maintained.

Responsible Disclosure Program

Ava Security runs a Responsible Disclosure Program, encouraging external security researchers to test our products and to report any issues discovered.

Any vulnerabilities found in the Ava products are resolved in a timely manner, and, once they have been resolved, information about the vulnerabilities and their fixes is made public, whether the issue was found internally or by external security researchers.

Ava software

Ava develops the software that runs on the Aware Cloud, the Ava Cloud Connectors, and on the Ava Cameras.

The Ava Cloud Connector hardware and software work together and function as an server specifically designed for enabling Ava Cameras without on-board storage and third-party cameras to connect to the Ava Aware Cloud video management system. For the Ava Cloud Connectors and Ava Cameras, there is no direct access to the underlying file system, and both run a proprietary hardened Ava Linux distribution, creating a secure platform.

Ava uses an asymmetric key that it controls to sign all upgrade images. By checking these signatures before upgrading the Cloud Connectors or Ava Camera devices, any unauthorized modifications to the upgrade images are rejected, preventing third-party tampering with the upgrade images.

Some third-party, open source software is used in the Ava systems, and the internal software development procedures ensure that these open source components are maintained to ensure all relevant security patches are installed.

Ava Aware Cloud

Ava Aware Cloud handles the security of each function using appropriate mechanisms. The architecture of the Ava Cloud ensures that the data for each tenant is fully isolated and cannot be accessed by other customers.

All authentication is carried out using the accounts created within Aware Cloud. These accounts are under full customer control. This means that Ava Security or your Ava partner has no access to your data unless you either enable access via the Deployment Management Portal (DMP), or create accounts in your Aware Cloud specifically to allow them to see your data and configuration. The permissions granted to Ava Security or to your the Ava partner are set by you within your Aware Cloud deployment, and remain under your control at all times.

Only approved Ava devices can access the DMP, with access being strictly managed using the Google Identity Platform.

Cloud storage of video and metadata

By default, your video footage and metadata is only stored on your Ava Cloud Cameras, or your Ava Cloud Connectors. You can choose to configure your Aware Cloud system to also store your video data in the cloud, using Ava Cloud Storage, or to your own S3 cloud storage[1].

When backing up to the cloud, you can define the information to be stored (choosing from Alarms, Anomalies, Interesting video, Uninteresting video, and Saved clips). Each camera license includes 30 days of cloud storage by default. You can purchase additional licenses to provide longer storage for one or more cameras.

[1] With purchase of a suitable license

Certificates

Ava uses encrypted communication channels, such as HTTPS and TLS, for all communications between Ava Cameras, Aware Cloud and the Cloud Connectors. These channels are all secured using certificates and private keys which are stored in hardware where possible either backed by the camera TPM unit or within Hardware security modules within the Ava Cloud.

Each Ava Cloud Connector and Ava Camera is pre-loaded with unique certificates and keys during manufacture. These certificates and keys are used to prove the identity of the devices to each other, and to the Ava Cloud.

To provide secure access between your Cloud Connectors and the Ava Cloud, Aware Cloud creates the necessary certificates to ensure secure communications.

Cloud Connectors and Ava Cameras do not require any port forwarding, and all outgoing connections from your appliances and Ava Cameras use Port 443 on aware.avasecurity.com (or subdomains thereof).

Authentication and authorization

Ava Aware Cloud supports an advanced permissions system which allows for operators to only be granted access to the cameras, sites, allowing the principle of least privilege. Authentication is also supported through your own identity service (such as ADFS, Azure AD, Google, or Okta) using SAML integration.

Alternatively, they can use local user accounts with optional two-factor authentication (2FA) to access your Ava Aware Cloud video management system, where a hashed and salted password, created using PBKDF2 and SHA-512 to NIST guidelines (see https://pages.nist.gov/800-63-3/sp800-63b.html) is stored locally.

Role-based access control (RBAC)

In addition to requiring your users to authenticate to gain access to the Aware Cloud user interface, Aware uses role-based access controls (RBAC) so that each user has specific authorized access levels.

These access level are set by your system administrator. Each user is assigned a role, and that role controls the access the user has to the Aware Cloud software, for example the Aware tools (Rules, Alarms, Historic video, User management etc.) that they can access.

Your system administrators have complete control of who can access your Ava video management system and their levels of access. Remote access to your Aware Cloud deployments is controlled by your system administrators — so, for example, to allow an Ava Partner to monitor your system, or to enable the Ava Support team to assist in troubleshooting, you have to opt-in and create suitable roles for the Partner or Ava Support. Your system administrator can revoke this access at any time.

Credentials

The customer can change all credentials in Ava Aware Cloud — Ava does not hardcode default user names and passwords into any products.

For Ava Cameras and Cloud Connectors, all users are authenticated against local user accounts where the passwords are regularly rotated by Aware Cloud. This ensures that only authenticated users with suitable authorization can access the Ava hardware. These rotated, hashed, and salted passwords are created using

PBKDF2 and SHA-512 to NIST guidelines and are stored on the relevant Ava Camera or Cloud Connector.

This ensures that nobody can use default credentials to access your Ava video security solution, or any Ava hardware — there is no concept of "Super admin" users, so no access can be gained to any Ava deployment without the relevant permissions being granted by your own system administrator.

Securing data-in-transit

All data sent between your Aware Cloud, your Ava Cameras and your Cloud Connectors is encrypted in transit using industry best practices to prevent eavesdropping. Transport Layer Security (TLS) 1.2 is used, as well as FIPS-140-2 compliant Perfect Forward Secrecy ciphers, such as AES-GCM-256. All communications between the Ava components and the browser being used to monitor camera activities are encrypted using HTTPS, RTP over HTTPS, and DTLS.

For connections between your Cloud Connectors and your third-party cameras, HTTPS is used to encrypt the connection if at all possible. Video streams from third-party cameras use RTP over HTTPS, when available.

Secure communications channels

In all components for the Ava video security solution, data is always encrypted, whether at rest, or in transit.

Connections between your Ava Cloud Cameras or Ava Cloud Connectors and the Ava Cloud infrastructure are secured using TLS 1.2 with certificate-based mutual authentication backed by key material installed at manufacture time within the camera or Cloud Connector Trusted Platform Module (TPM).

Streamed video footage from Ava Cloud Cameras, either over a "local" (on the same subnet) or a "cloud" connection, is always end-to-end encrypted using DTLS and WebRTC.

Securing data-at-rest

All data from on-premise Ava Cameras and third-party cameras is stored securely on the drives within your Ava Cloud Connectors. This video data is stored on multiple dedicated hard disk drives, and uses erasure encoding to protect against disk failures.

Video data from Ava Cloud Cameras is stored on the camera, using surveillance-grade storage. The video data is encrypted before it is stored, and the encryption keys are stored separately from the video data.

Video Footage is stored encrypted at rest on the camera's SD card using AES-128 bit encryption, each video segment is encrypted with a randomly generated key which is backed and envelope encrypted with a 2048 bit RSA keypair stored within the customers own Ava Cloud video management system instance.

Because the data is encrypted before being stored, the data cannot be read without access to the encryption keys. This means that even if the data storage is stolen, the data itself is still protected, and therefore safe from confidentiality breaches.

Data residency

Ava Aware Cloud uses geographically isolated data centers and separate deployments for EU, US and Australian customers to protect data sovereignty and comply with data protection laws such as GDPR.

Instance separation in the cloud

Ava Cloud deployments are composed of multiple, scalable software components, all operating on a principal of least privilege.

The core components that have access to sensitive user data are isolated from those of other customers by a two-layer security boundary. This ensures that, even if one customer deployment was compromised, all other customer deployments and data remain secure.

Securing exported video recordings and links to video clips

The video that your Ava video security solution records could contain confidential or commercially-sensitive information.

When exporting this video, you can choose to encrypt the video files using password-protected AES-256 encryption. This prevents access to the recordings by anybody without the password.

When using link sharing, all data continues to be stored on the Cloud Connector or the Ava Cloud Camera. The shared links contain sufficient entropy as to be difficult to brute force in our lifetime, and our API is protected by various rate-limiting mechanisms to mitigate brute force attacks. The optional password that can be configured per clip further strengthens this.

Digitally-signed (watermarked) video

Exported video and the accompanying metadata files are also digitally signed, to verify that the video recordings and metadata have not been tampered with since being exported. Each video recording and metadata file in the exported archive has a hash, created using the SHA-256 cryptographic hashing tool.

These hashes are digitally signed using a key only known to the Aware Cloud system that recorded the video, and verified with the corresponding Aware Cloud certificate that is included in the archive.

Data deletion

When an Ava Aware Cloud customer instance is deleted, all data, including the encryption keys and any video footage and metadata is deleted and cannot be recovered.

Audit logs

The Aware Cloud software includes logging of important system events, such as somebody logging into the system, or somebody making changes to camera configurations etc. Using these logs, you can audit the access to your Ava Cloud Video Security solution, ensuring that only authorized current users are using the system. If you find that somebody that should no longer have access is still logging into your system, you can revoke their user account to lock them out of your system.

Hardware

The hardware components of your Ava video security solution are all designed with security in mind.

Ava Cameras

The Ava Cameras hardware is based around an Ambarella imaging processor.

This processor was chosen because it meets all of the Ava Security requirements and the market-leading technical capabilities for this component.

The Ambarella processor supports the Arm TrustZone technology to separate the secure cryptographic operations from the main application. Ava Cameras are equipped with a Trusted Platform Module (TPM) to provide the certificate storage for each camera.

For Ava Cloud Cameras, video storage is handled using surveillance-grade storage media, and is encrypted before storage to further protect your data. The private keys used to encrypt your data are not held on the camera, so that, even if the Ava Cloud Camera itself is stolen, the data held on-camera is still secure.

Ava Cloud Connectors

The Cloud Connector range of hardware appliances is based on Dell OEM servers featuring Intel Central Processing Units (CPUs) and NVIDIA Graphics Processing Units (GPUs). All data storage disks are surveillance-grade items. Cloud Connectors are also fitted with a TPM to provide the secure encryption key storage for each appliance.

Your Cloud Connectors are linked to and managed from your Aware Cloud video management system.

Manufacturing

The Ava Camera and Cloud Connector hardware are built by manufacturing partners. All manufacturing is carried out in factories in Europe, America or Taiwan.

As part of the manufacturing process, each device is pre-loaded with a digital certificate, to prove its identity to other devices and to the Ava Cloud.

The test software and related quality control processes for all Ava video products have been developed internally by Ava engineers. We continually monitor the results of this testing to ensure compliance with our standards and requirements.

A global company with offices in the UK, Norway, and the US, Ava delivers better, smarter security.

Organizations use the Ava Aware® open video security data platform to protect people and operations, allowing them to optimize for their evolving business needs, giving them more time to spend on the possibilities ahead.

To learn more about Ava's intelligent solutions and how you can enjoy proactive security, visit our website or schedule a demo with a member of our sales team at sales@avasecurity.com.

www.avasecurity.com

White paper first published May 2020, updated February 2022.