



Security at the core

With Avigilon Alta Video



Introduction

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

From the outset, Avigilon Alta Video has been designed to have security at the core of all aspects of design and implementation. This includes:

- Using software development best practice and design for the Alta Video software, the Avigilon Alta Cloud Connectors and the software that powers the Avigilon Alta-enabled cameras.
- Careful consideration and selection of all components used within the Avigilon Alta cloud-native cameras, Avigilon Alta-enabled cameras without on-board storage and the Avigilon Alta 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 management.
- Protecting all data using encryption, whether in transit or at rest.
- Actively investigating, and where needed, resolving vulnerability reports.



About Avigilon

Avigilon designs and manufactures advanced video security solutions and cloud-based access control systems. This white paper focuses on the Avigilon Alta cloud-based 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 Avigilon Alta-enabled cameras, Alta Video and the 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 Avigilon Alta video products.

Security incidents related to the products are handled by the internal Product Security Incident Response Team (PSIRT).

When an issue is found in Alta Video or the cameras made by Avigilon, patches are developed for the affected components. 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, Avigilon Alta publishes security advisories for any Alta Video security issues, including those found internally. You can find all the security advisory information for the video products at <https://docs.avigilon.com/bundle/alta-video/page/MoreInfo/head-advisories.htm>.

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



ISO/IEC 27001 accreditation

Avigilon's development and third tier technical support operations have achieved ISO/IEC 27001 certification as well as the Extensions 27017, 27018 and 27701 as part of the Motorola Solutions certification. (see https://www.motorolasolutions.com/en_xu/about/trust-center/compliance.html). In addition, SOC2 Type II reporting has been achieved including all of the trust criteria for security, privacy, processing integrity, confidentiality and availability.

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 Relationships, 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 Avigilon.

Development operations

Access to the Avigilon Alta 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 Motorola Solutions employees working on Avigilon Alta must have suitable security software installed on their computers, as well as 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

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

Customers, or potential customers, wanting to carry out their own independent penetration testing on Alta Video systems must ask for written permission and information about testing constraints before starting testing.

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

Responsible Disclosure Program

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

Any vulnerabilities found in the video 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.



Avigilon Alta Video software

Avigilon develops the software for Alta Video, the Avigilon Alta-enabled cameras and the Alta Cloud Connectors.

The Alta Cloud Connector hardware and software work together and function as a server specifically designed for enabling Avigilon Alta-enabled cameras without on-board storage, as well as third-party cameras to connect to Alta Video. For the Alta Cloud Connectors and Avigilon cloud-native cameras, there is no direct access to the underlying file systems, and all run a proprietary hardened Alta Linux distribution, creating a secure platform.

Avigilon Alta uses an asymmetric key that it controls to sign all upgrade images. By checking these signatures before upgrading the Alta Cloud Connector or Avigilon cloud-native cameras, 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 Avigilon Alta systems, and the internal software development procedures ensure that these open source components are regularly tested and maintained to ensure all relevant security patches are installed.

Alta Video

Alta Video handles the security of each function using appropriate mechanisms. The architecture of Alta 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 Alta Video. These accounts are under full customer control. This means that Avigilon Alta or your Avigilon partner has no access to your data unless you either enable access via the Deployment Management Portal (DMP), or create accounts in your Alta Video deployment specifically to allow them to see your data and configuration. Any permissions granted to Avigilon Alta or to your Avigilon partner are set by you within your Alta Video deployment, and remain under your control at all times.

Cloud storage of video and metadata

By default, your video footage and metadata is only stored on your Avigilon Alta cameras, or your Alta Cloud Connectors. You can choose to configure Alta Video to also store your video data in the cloud, using Alta Video Cloud Storage, to your own S3 cloud storage, or to your own on-premise Common Internet File System (CIFS) storage (with purchase of a suitable license).

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.

Certificates

Alta Video uses encrypted communication channels, such as HTTPS and TLS, for all communications between Avigilon cloud-native cameras, Alta Cloud Connectors and Alta Video. These channels are all secured using certificates and private keys which are stored in hardware where possible, either backed by the camera Trusted Platform Module (TPM) units or within Hardware security modules within Alta Video.

Each Avigilon cloud-native camera (or Avigilon Alta-enabled cameras without on-board storage) and Alta Cloud Connector 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 Alta Video.

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

Alta Cloud Connectors and Avigilon cloud-native cameras do not require any port forwarding, and all outgoing connections from your appliances and cameras use Port 443 on alta.avigilon.com or aware.alta.avigilon.com (or subdomains thereof).



Authentication and authorization

Alta Video supports an advanced permissions schema which allows for operators to only be granted access to the cameras and sites to which need access, 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, you can use local user accounts to access your Alta Video video management system. When using local accounts, 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.

For additional security these local accounts can be configured to use two-factor authentication (2FA).

Role-based access control (RBAC)

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

These access levels are set by your system administrator. Each user is assigned a role, and that role defines the access the user has to Alta Video, for example the tools (Rules, Alarms, Search, Historic video, User management etc.) that they can access.

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

Credentials

The customer can change all credentials in Alta Video — there are no hardcoded default usernames and passwords in any system components.

For Avigilon cloud-native cameras and Alta Cloud Connectors, all users are authenticated against local user accounts where the passwords are regularly rotated by Alta Video. This ensures that only authenticated users with

suitable authorization can access the hardware. These rotated, hashed, and salted passwords are created using PBKDF2 and SHA-512 to NIST guidelines and are stored on the relevant Avigilon cloud-native camera or Alta Cloud Connector.

This ensures that nobody can use default credentials to access your Alta Video deployment.

Secure communications channels

In all components for your Alta Video deployment, data is always encrypted, whether at rest, or in transit.

Connections between your Avigilon cloud-native cameras or Alta Cloud Connectors and the cloud infrastructure are secured using TLS 1.2 with certificate-based mutual authentication backed by key material installed at manufacture time within the TPM for the cameras.

Streamed video footage from Avigilon cloud-native 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-in-transit

All data sent between your Alta Video deployment, your Avigilon cloud-native cameras and your Alta Cloud Connectors is encrypted in transit using industry best practices to prevent eavesdropping. Transport Layer Security (TLS) 1.2 and 1.3 are used with IETF approved ciphersuites, such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. All communications between the Avigilon Alta components and the browser being used to monitor camera activities are encrypted using HTTPS, RTP over HTTPS, and DTLS.

For connections between your Alta 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.

Securing data-at-rest

All data from Avigilon Alta-enabled cameras without onboard storage and third-party cameras is stored securely on the drives within your Alta 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 Avigilon cloud-native 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 off-camera.

Video Footage is stored encrypted at rest on the camera's memory using AES-256 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 customer's own Alta Video cloud 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

Alta Video systems use 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.

Securing exported video recordings and links to video clips

The footage that your Alta Video deployment 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 Alta Cloud Connector or the Avigilon cloud-native 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 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 Alta Video deployment that recorded the video, and verified with the corresponding Alta Video certificate that is included in the archive.

Data deletion

Usually, when an Alta Video customer instance is deleted, all data, including the encryption keys and any video footage and metadata is "soft deleted" (marked for deletion) and held for 30 days, during which time, that data can be recovered.

After 30 days (or if the data has been explicitly hard deleted), the data is permanently deleted and can no longer be recovered.

Audit logs

The Alta Video software includes logging of important system events, such as when devices are added or deleted from the deployment, the configuration of Alta Video or the cameras is changed, and when users sign into or out of Alta Video.

The Audit logs also record information about how your users are viewing information within your Alta Video deployment — when users start viewing live or played-back video footage — in the Viewer logs section of the Audit logs.

Using these logs, you can audit the access to your Alta Video deployment, ensuring that only authorized current users are using the system. If you find that somebody that should not currently have access is still logging into your Alta Video deployment, you can revoke their user account either temporarily, or permanently, to lock them out of your system.



Hardware

The hardware components of your Alta Video deployment are all designed with security in mind.

Avigilon Alta-enabled cameras

The Avigilon Alta-enabled camera hardware is based around the Ambarella imaging processors.

These processors were chosen because they meet all of the Avigilon Alta requirements and offer 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. Avigilon Alta-enabled cameras are equipped with a TPM to provide the certificate storage for each camera.

For Avigilon cloud-native 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 camera itself is stolen, the data held on-camera is still secure.

Avigilon Alta Cloud Connectors

The Avigilon range of hardware Alta Cloud Connectors 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.

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

Manufacturing

The Avigilon Alta-enabled camera and Alta Cloud Connector hardware are built by manufacturing partners. All manufacturing is carried out in factories in Europe, North 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 Alta Video cloud.

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



Conclusion

With security being considered at every stage of the design, development and manufacture of all components within Alta Video security systems, you can be assured that your video is secure. In addition, Avigilon Alta investigates, and if found valid, resolves and publicly acknowledges all reported security vulnerabilities, highlighting the focus on creating secure systems.



To learn more, visit: www.avigilon.com



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2024 Motorola Solutions, Inc. All rights reserved. 09-2025 [SD03]