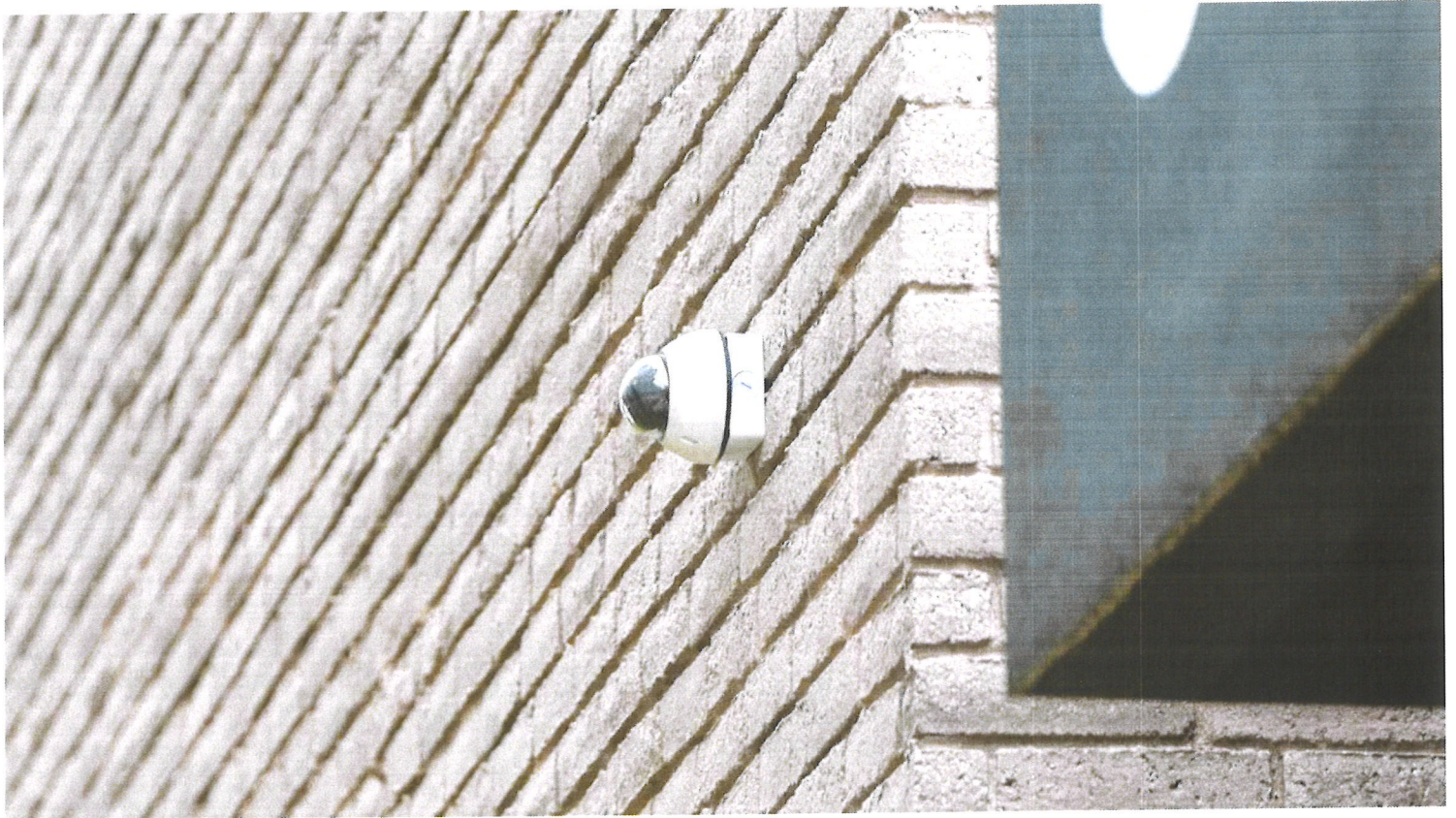




Security and encryption solutions

Verkada's solution was built with security in mind and features encryption in transit and at rest.

[See Verkada Security Updates](#)

[Device](#)

[Cloud](#)

[Product](#)

[Application](#)

Device security

At Verkada, security is the design foundation of our cameras.

Enterprise Controlled Encryption (ECE)

Verkada encrypts video data at rest (i.e., on the user's device or on Verkada's cloud servers) and in transit (i.e., as data moves among devices and the cloud). ECE builds on this encryption framework by giving customers more control over their data encryption. Leveraging a well-recognized technique called [client-side encryption](#), customers can choose to keep some keys to themselves, share them with Verkada if they need technical support, or with a third party for a variety of reasons. ECE improves on Verkada's already robust data protection measures—empowering customers with complete control over their data. ***Customers must opt-in and enable ECE for their devices. ECE will not be enabled for customers by default.***

Read our [blog](#), [FAQ](#), and [overview document](#) to learn more about ECE.

Durable design

Torx Screws and IK10 rated impact protection mean our cameras are some of the most durable and tamper-resistant on the market. Devices monitor their physical state, and notify organization admins if tampering occurs.

Firmware updates

Verkada cameras are designed to apply firmware updates automatically. That means you won't miss out when we roll out new features or critical security updates.

Automatic cloud backup available

Verkada cameras can automatically sync their local storage to the cloud, for high availability and data resilience. On-device data remains protected and encrypted.

Encryption at rest and in transit

Camera footage is stored locally on devices for up to 365 days and is encrypted using AES-128. We encrypt video data in transit to the cloud using TLS 1.2 or greater.

Cloud security

Verkada's Command Platform is hosted in Amazon's AWS cloud infrastructure which features some of the best data security and reliability in the world.

Cloud managed

Verkada cameras are only managed using outbound connections to the cloud, helping to protect against unexpected local network activity. Verkada devices do not require additional security hardware to be deployed on the network.

No port-forwarding

Verkada cameras do not require port forwarding; a major vulnerability and headache of enabling remote access on traditional NVR systems.

Local data residency

Certain regulations limit the processing and storage of an organization's data to its country of origin. Verkada is proud to offer processing and storage in the US, EU, and Australia.

Encryption at rest

Footage is encrypted at rest in the cloud using AES-256.

Product security

Verkada empowers you to control sign on, manage access to your systems, and gain visibility into when, where and how users access the system.

Single sign on

We support integrations with the most trusted Single Sign-On providers in the industry, including [Okta](#), OneLogin, Google Workspace, JumpCloud, and [Azure Active Directory](#).

Multi-factor authentication

Verkada supports multiple factors for authentication including Passkeys, TOTP and HOTP one-time passwords (e.g., using

Google Authenticator), magic email links and SMS codes.

Role based access control

Easily customizable access settings allow you to thoughtfully assign access to only the right people.

Support permissions

Verkada support personnel may only access customer information through Verkada's Support tools when explicit [support access is granted](#).

Enhanced audit logs

Audit logs help reveal who has accessed your system, and any changes they have made. Audit logs include actions by Verkada support personnel and are API accessible.

Application security

Security starts with us, but extends to each user who logs into our software. Verkada gives you the tools you need to control who has access to your system, and what they do with that access.

Regular penetration testing

We use external parties to conduct detailed penetration tests, covering device, application, and cloud security.

Bug bounty

Verkada recognizes the importance and impact of the broader security community, and awards leading bug bounty researchers awards of up to \$10,000 for confirmed security findings. Reported discoveries are investigated and promptly addressed.

SOC 2 type 2

Verkada validates compliance with industry standards in the design and performance of controls for handling customer data securely. A copy of Verkada's [SOC 2 Type 2 attestation report](#) is available.

Vulnerability disclosure program

Verkada believes in responsible security research and disclosure of security vulnerabilities. Responsible disclosure helps us promote the continued security and privacy of Verkada customers, products, and services. Please report potential security and privacy vulnerabilities to us via our [Vulnerability Disclosure Program](#).

Trust hub

Verkada's innovative, market leading approach to security in the Trust Hub

[Learn more](#)

Customers in regulated areas

[See all customers](#)