Flock Safety

# Security Claims & Facts

**CLAIM**

Flock has inadequate security standards.

**FACT**

Flock is relentlessly focused on data integrity and security, and secures data in accordance with the highest industry requirements. This includes strict encryption standards that use a 256-bit key to convert plain text into cipher – virtually impenetrable to brute-force attacks. Flock adheres to the following security frameworks and certifications, amongst others:

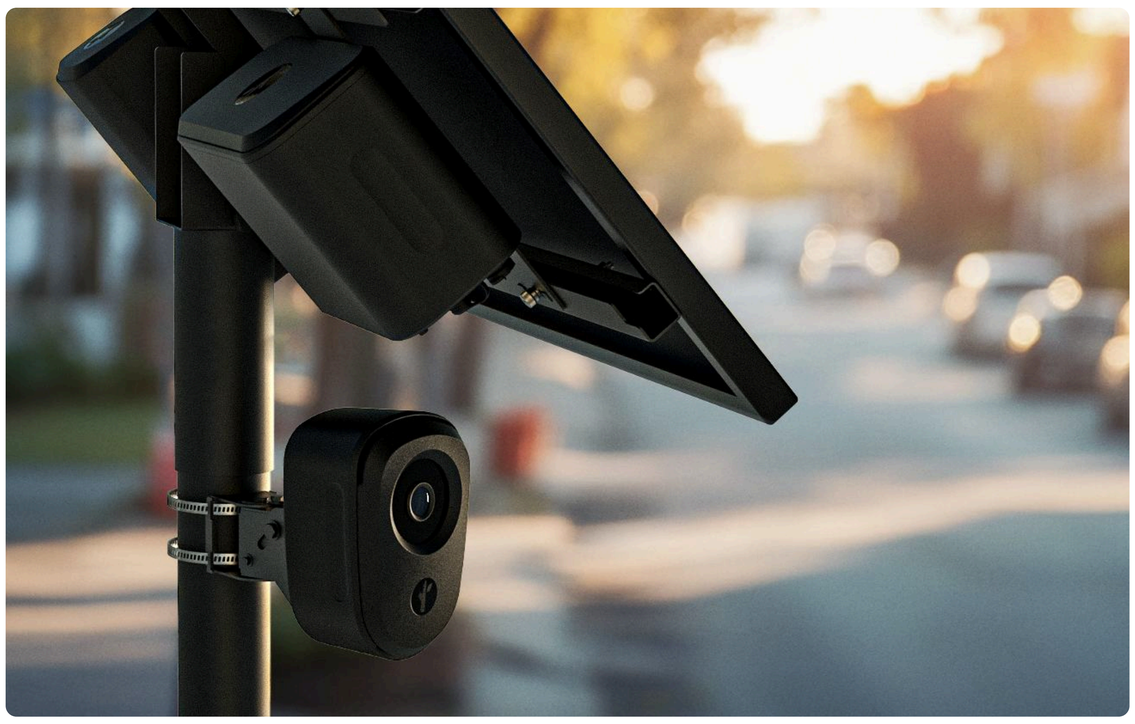
- ISO 27001 compliance certification (an international framework for IT security)
- SOC 2 Type II, assessed by an audit that assesses an organization's controls over its data and system
- NIST 800-53, an information security standard defined by the National Institute of Standards and Technology (NIST)
- Secure By Design principles program authored by the Cybersecurity and Infrastructure Security Agency (CISA)

**CLAIM**

Flock has been hacked.

**FACT**

Flock's platform has never been hacked. A recent YouTube video claims "80,000 cameras" have been hacked. This is false. The YouTuber in question gained limited access to one older generation camera that had never been connected to our system and had never received a security update, which we push out frequently. Flock cameras are not connected to each other; access to one does not provide access to any others. No access to Flock's cloud environment is possible via a camera. All customer data collected by Flock devices is encrypted at rest, in transit, and while stored in the cloud. Flock's cloud storage has never been compromised.



Flock Safety

CLAIM

It is possible to hack into Flock's cloud database from a Flock camera.

FACT

It is not possible to hack into Flock's cloud database from a Flock camera. Alleged vulnerabilities circulating on the internet have no effect on our cloud platform, where evidence and metadata is stored. Images sent to the cloud are fully encrypted in transit.

CLAIM

Flock does not update our hardware or mitigate identified vulnerabilities in our hardware system.

FACT

Flock publicly discloses identified vulnerabilities on a regular basis to the public vulnerability database maintained by MITRE, most recently in May 2025. Vulnerability identification and remediation is an ongoing process.

CLAIM

Flock does not require Multi-Factor Authentication for customers.

FACT

In November 2024, Flock made Multi-Factor Authentication (MFA) the default for all users, supported through common providers including Okta and Google Authenticator. For Single Sign-On (SSO), Flock supports multiple authentication methods including SAML, OIDC, and Azure-specific SSO. Following the decision to make MFA default, Flock proactively conducted outreach to thousands of law enforcement agencies to help them enable MFA, and the vast majority of Flock's law enforcement customers now use either MFA or SSO.

CLAIM

Foreign adversaries have access to the Flock system.

FACT

There is zero evidence that foreign actors have or have had any access whatsoever to Flock's system or cloud platform.