SECURITY AT PLANET
AN OVERVIEW

Planet operates complex terrestrial and orbital computer networks and systems, comprising four interdependent security domains including: corporate security, space segment, data pipeline, and customer delivery. Below is an overview of these systems and their security approaches.

CORPORATE SECURITY

All Planet systems are accessed through centralized corporate security controls, encompassing the basic requirements and limitations that all Planet employees must adhere to for basic access. This includes facilities access and credentialing, centralized identity management, network security monitoring, vulnerability management, incident response, endpoint protection, and data protection.

The objective of corporate security is to ensure that each employee is appropriately credentialed and given access to only those systems and resources required by their duties, and to ensure that global controls are enforced. Employees undergo background examinations prior to employment, and once approved, receive electronic identities to Planet's systems and basic security training.

All endpoint equipment (e.g., computers, mobile devices, etc.) is encrypted with data at rest protection, where applicable. Network connectivity between all Planet points of presence (e.g, facilities, Earth stations, and data centers) is secured using industry-standard virtual network technology. In addition, Planet facilities use industry-standard physical access controls and surveillance, with sensitive areas partitioned and access restricted on an as-needed basis. Headquarters facilities have continuous security presence.

SPACE AND GROUND SEGMENTS

Planet operates its own spacecraft Mission Control center, as well as ground support networks, which all work together to form Planet's space and ground segments. Their primary security objective is maintaining the health and safety of all Planet spacecraft, which ensures Planet's ability to command the spacecraft, and protects the integrity of downlinked imagery.

Only Planet operators have the credentials to task and control the spacecraft for each of Planet's Mission Control systems, whose data is stored on secure cloud-based storage with a higher level of security on servers operated within the United States. In addition, firewalls filter network traffic of the servers running the Mission Control applications.

For the ground station network, there are a number of physical control measures in place at each location:

- All communications between space and ground terminals are encrypted.
- Each network port is either connected to known equipment or disabled.
- Physical storage devices are protected with full disk encryption, where applicable.
- The facilities themselves are protected with surveillance and remote monitoring.

Planet operates two constellations of spacecraft: the Dove spacecraft collect medium resolution imagery and the SkySat spacecraft collect high resolution imagery. Although different in design, all Planet spacecraft employ encryption and authentication on telemetry, tracking, and control channels. Imagery captured by the spacecraft are encrypted onboard and transmitted securely from the spacecraft to the imagery pipeline.

The image data is encrypted end-to-end in that the data once encrypted aboard the spacecraft, is not decrypted until it is delivered to secure ground processing systems. Further, Planet spacecraft are capable of rotating cryptographic keying material on demand. In the case of high resolution imagery, Planet utilizes ground based hardware security modules for encryption key generation and storage.

In addition to the communication and payload security measures described above, Planet monitors spacecraft telemetry for variations in the spacecraft's security configuration, complete with operator alerting and escalation to Planet's security team should anomalous behavior be observed.

SECURITY ASSURANCE PROCESS

Planet develops its platform using a secure development lifecycle implementing industry best known methods. This includes security training for all developers, formal security risk and objective assessment of all capabilities, security design reviews, active component dependency vulnerability management, active security testing, verification of critical systems via in-house and 3rd party penetration tests, and proactive survivability planning. Planet's secure development lifecycle leverages industry standard tools, guidelines and practices (OWASP, NIST, CWE) to identify and manage security vulnerabilities.

SECURE HOSTING

Planet's platform is hosted on Google Compute Platform (GCP), which is used for data storage, processing, and customer delivery. Data held in GCP, including corresponding metadata and backups, are encrypted during transit and at rest. Planet data in GCP benefits from layered encryption that Google provides to all of its customers, additional details about which can be found at https://cloud.google.com/security/encryption-at-rest/default-encryption/.

In addition to this, Planet's Security Team performs periodic security assessment and audits of our cloud configurations using a combination of Google's cloud security assessment tools and manual security assessment.

PLATFORM DESIGN

Planet's platform is operated within private network address space with restricted interface points to the broader Planet network and public internet. The platform is composed of many tens of thousands of short-lived worker instances processing and delivering imagery. Those instances are formed from declarative templates that ensure consistent operation and configuration, which limits the attack profile to controlled templates and short-lived workers.

Secure endpoints accept imagery only from Planet Earth stations according to an authentication mechanism that is controlled by Planet. When image processing is complete, final imagery products are forwarded to cloud storage for secure delivery to customers.

Planet's primary method of delivering imagery products to customers is over the public internet. Planet operates APIs and applications where authenticated customers may select imagery products for access or delivery, which also controls access and measures utilization. The customer delivery API and web interface aim to keep customer activity private on the platform. As a public interface, the API is resistant to tampering and ensures sanitized inputs.

The public APIs and applications are built using well-tested frameworks and ensure authentication of users using industry-standard, modern authentication practices. Authorization is controlled by Planet's account management team, and accounting is monitored per API request and metered data download. All accessible platform points are authenticated and encrypted. Additionally, Planet periodically actively validates the API interface for configuration, input sanitization errors, and penetration testing, with proactive remediation if errors or vulnerabilities are discovered.

Platform internal systems are subject to the same secure development processes and standards as the external systems. These systems are designed with a least privilege, minimum trust model, limiting access to people or systems to those required for the job or function. All internal access between systems and by employees to the platform is logged, and these logs are periodically audited to validate compliance.

SECURITY REPORTING

Planet's Security Team can be contacted at security@planet.com regarding any security concern.