

**PUBLIC SECURITY OVERVIEW**  
**PLANET CLOUD**

# Contents

- Contents ..... 2
- 1. Our Commitment to Security ..... 3
- 2. Infrastructure & Network security ..... 4
  - 2.1. Google Cloud Run ..... 4
  - 2.2. Google Kubernetes Environment ..... 4
- 3. Data Protection ..... 6
- 4. Identity & Access Management ..... 7
- 5. Application & Development Security ..... 8
- 6. Monitoring & Threat Detection ..... 9
- 7. Incident Response ..... 10
- 8. Compliance & Certifications ..... 11
- 9. Responsibilities ..... 12
  - 9.1. Customer responsibilities ..... 12
  - 9.2. InfoVista responsibilities ..... 12
- 10. Security Contact & Reporting ..... 14

## 1. Our Commitment to Security

At Infovista, we understand that security is more than just a feature — it is the foundation upon which trust is built. Every day, our products and services — whether delivered as SaaS platforms, on-premises solutions, or hybrid deployments — process and safeguard sensitive information for organizations worldwide, and we take that responsibility very seriously.

This Security Overview outlines the measures, practices, and principles we follow to protect your data, ensure service availability, and maintain the integrity of our platform. We are committed to transparency, so you know exactly how we approach security and what steps we take to stay ahead of evolving threats.

Our security program is guided by internationally recognized standards and frameworks, including:

- **ISO/IEC 27001** – Information Security Management Systems (ISMS).
- **SOC 2 Type II** – Controls related to security, availability, processing integrity, confidentiality, and privacy.
- **GDPR & CCPA** – Data protection regulations for the EU and California.
- **NIST Cybersecurity Framework (CSF)** – Best practices for identifying, protecting, detecting, responding to, and recovering from security incidents.
- **NIS2 Directive, EU Cyber Resilience Act (CRA) & EU Cloud Security Framework** – European regulations and initiatives designed to enhance cybersecurity resilience, product security, and cloud service trustworthiness.
- **ETSI & ITU-T Recommendations** – Security guidelines and best practices tailored to the telecommunications industry.

By aligning with these standards, we ensure our security approach is comprehensive, globally relevant, and adapted to the specific challenges of telecom and cloud-based environments. We continuously monitor, test, and improve our systems to provide a secure, reliable, and resilient environment for your business.

Security is a shared responsibility — and together, we can ensure the confidentiality, integrity, and availability of your information.

## 2. Infrastructure & Network security

Planet SaaS is hosted within Google Cloud Platform (GCP) data centres in the United States, leveraging Google-managed infrastructure and containerized services for scalability and isolation..

### 2.1. Google Cloud Run

It includes:

- Component: Quota allocation per account user and access control
- Data stored in Google Cloud SQL Server instance
- Secrets stored in Google Secret Manager
- Public URL accessible via service account credentials
- Load balancing and networking handled by GCP (serverless deployment model)

### 2.2. Google Kubernetes Environment

It includes:

- Component: System including compute and data storage resources
- Stores and accesses all tenant data except for quota allocations
- Each tenant is isolated in a Kubernetes cluster including:
  - 1 load balancer
  - 1 cloud NAT gateway (High availability)
  - 1 VPC network
    - 2 subnets (1 control plane + 1 workload)
  - 5 DNS records in a shared Cloud DNS zone
    - Admin
    - Health
    - Rancher
    - Planet (Application)

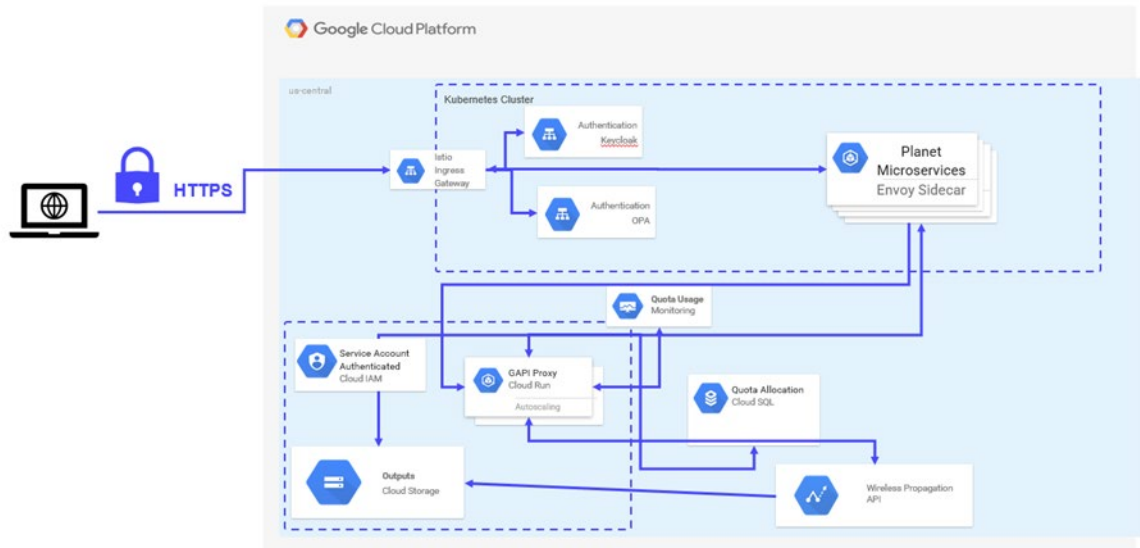
Physical security of Google data centers is extensive and includes:

- Perimeter and Access Control, implemented via physical fencing and barriers, access cards, alarms, and security corridors
- Surveillance and Monitoring, including 24/7 camera coverage of interior and exterior areas, access logs, and activity records, as well as intrusion detection systems
- Environmental and Emergency Controls including redundant power systems and cooling infrastructure, fire detection, and fire suppression systems
- Patrols by security staff and strict pre-approval procedures for access to data center floors

Software security is central to the Google Cloud infrastructure design and includes:

- Ingress and egress filtering at network segment boundaries to prevent IP spoofing.

- Service authentication via strong cryptographic credentials that can be used to establish trust with other endpoints and enforce security policies
- GCP provides multi-layer isolation, including virtualization and container sandboxing technologies
- Assigning dedicated machines for sensitive services, such as the cluster orchestration service and some key management services



**Figure 1: Planet Cloud architecture overview**



### 3. Data Protection

Data collected includes application telemetry (user session data, token usage, etc.), network configuration data, and user contact details as part of user profile creation.

Application telemetry is stored in Google Cloud Monitoring and encrypted via TLS for connections outside of Google's network. Inside Google's network, data in transit is protected in a variety of ways, such as Application Layer Transport Security (ALTS) for service-to-service communication.

Data at rest is protected with AES256 Encryption based on Google-owned and Google-managed encryption keys. For data such as telemetry which is stored on Google's network, platform-wide backup and automatic replication strategies are used to ensure availability.

Data retention and backup schedules follow Infovista corporate policy and comply with legal and contractual obligations. At minimum, monitoring information is retained for two years and daily backup of instances is performed.

Access to Planet SaaS services is secured through industry-standard transport encryption (TLS 1.3 or higher) and strict authentication controls. All external API requests require validated user sessions protected by modern token-based authentication mechanisms.

All data is stored on servers located in the USA.

## 4. Identity & Access Management

Planet SaaS supports Single Sign-On (SSO) with SAML 2.0.

It supports Role-Based Access Control (RBAC) which ensures that users have the least privileges necessary for their role, according to the plan selected for the Planet SaaS tenant.

Planet SaaS enforces secure session management, including automatic timeouts after periods of inactivity, and secure token handling. Session parameters can be customized to meet customer security policies when required.

## 5. Application & Development Security

The Planet SaaS development team adheres to an Agile software development methodology, enabling rapid iteration and continuous improvement while maintaining a strong focus on security and compliance.

All code changes are regularly reviewed by technical leads who are responsible for final approval. This ensures that every modification aligns with our secure coding standards and architectural guidelines, and that potential security issues are identified early in the development lifecycle.

As part of our Agile process, we designate specific sprints for security auditing and remediation. During these sprints:

1. The codebase is scanned using automated security tools to detect vulnerable packages, outdated dependencies, and insecure components.
2. Identified vulnerabilities are triaged and addressed promptly.
3. Where a fixed version exists, affected libraries and modules are updated to minimize exposure to known threats.

These practices are embedded into our development lifecycle to ensure ongoing compliance with internal policies. Our approach supports traceability, accountability, and proactive risk mitigation.

## 6. Monitoring & Threat Detection

Planet SaaS is hosted on Google Cloud Platform, which leverages a range of tools to monitor production services, detect suspicious activity, and mitigate the impact of potential threats. In addition, the Infovista SaaS team continuously monitors the platform to identify and respond to any emerging risks.

A rigorous security process is also embedded in the Planet Cloud delivery pipeline, ensuring a minimal number of vulnerabilities through continuous security scans performed throughout the entire development lifecycle.



## 7. Incident Response

Our 24/7 Security Operations Center (SOC) monitors for anomalies using SIEM and IDS tools. In the event of a breach, customers are notified **within 72 hours** (GDPR-consistent), following our incident response plan.

A root cause analysis is provided promptly for significant incidents.

## 8. Compliance & Certifications

Planet SaaS holds ISO/IEC 27001 certification, the internationally recognized standard for Information Security Management Systems, demonstrating our commitment to protecting data through robust, risk-based controls. While ISO 27001 is our formally certified framework, we also operate in alignment with other globally recognized security and privacy requirements, including GDPR for EU customers and CCPA for US customers. Our controls and processes undergo independent third-party audits on an annual basis to validate their effectiveness and ensure ongoing compliance.

Certifications are renewed annually, with summaries available on request

Where required and agreed in advance, Planet SaaS can accommodate ad-hoc security and compliance audits in collaboration with specific customers, following mutually approved scope, methodology, and confidentiality agreements.

## 9. Responsibilities

Security in the cloud is a shared responsibility between InfoVista and our customers. While InfoVista manages the underlying infrastructure, application security, and core platform services, customers retain certain responsibilities related to how they configure, use, and manage their environments within Planet SaaS.

### 9.1. Customer responsibilities

#### **Password Management**

Users are responsible for maintaining the confidentiality and integrity of their login credentials. This includes:

- Creating strong, unique passwords that are difficult to guess and not reused across multiple platforms
- Storing passwords securely, using password managers when necessary, and never writing them down or sharing them with others
- Changing passwords regularly, especially if there is any suspicion of compromise.

#### **Session Security**

To prevent unauthorized access, users must ensure that active sessions are properly managed:

- Logging out from active sessions when stepping away from a workstation, especially in shared or public environments
- Following strong password and session management practices
- Locking screens when leaving devices unattended

#### **Data Classification & Input Controls**

Ensuring that the data you upload into Planet SaaS complies with your own regulatory obligations. Planet SaaS does not process Personal Identifiable Information (PII) unless explicitly agreed via a Data Processing Agreement (DPA).

#### **Endpoint Security**

Securing the devices and networks from which your users access Planet SaaS:

- Maintaining operating systems and software up to date with the latest security patches
- Using antivirus and anti-malware tools to detect and prevent threats
- Avoiding unsecured public Wi-Fi networks when accessing sensitive applications or data

#### **Incident Reporting**

Promptly notifying InfoVista of any suspected compromise, misuse, or unauthorized access to your Planet SaaS environment.

### 9.2. InfoVista responsibilities

#### **Infrastructure Security**



Planet SaaS is hosted in a secure cloud environment that provides multiple layers of protection, including firewalls, intrusion detection and prevention systems, and logically segmented networks to ensure tenant isolation and data confidentiality.

### **Application Security**

The Planet SaaS application is developed following secure coding best practices and is continuously tested through automated vulnerability scanning, regular patch management, and independent penetration testing to maintain a strong security posture.

### **Availability & Resilience**

High availability and service continuity are ensured through redundant infrastructure, automated system backups, and documented disaster recovery and failover procedures designed to minimize service disruption.

### **Compliance & Certification**

Planet SaaS operates under InfoVista's ISO 27001-certified Information Security Management System (ISMS) and aligns with key global privacy and data protection frameworks, including GDPR, CCPA, and other applicable standards.

## 10. Security Contact & Reporting

As a customer of Planet SaaS, we want to ensure you get the best possible support experience. That is the reason why all support requests should be submitted through our [Planet Cloud Support Portal](#).

To submit a request, simply log in to the [Planet Cloud Support Portal](#) and open a ticket (Registration required). Our team will assist you as quickly as possible.

To register for the Planet Cloud Support portal, as a new Planet SaaS customer, you will need to register on our support portal to access assistance and resources. Please follow the steps below to create your account:

1. Go to [Planet Cloud Support Portal](#)
2. Click on Customer Login.
3. Select Not a member? to begin the registration process.
4. Complete the registration form and ensure you select "RAN" as your product line.
5. Submit the form to finalize your registration.
6. Once submitted, you will receive an email with your user account details, allowing you to access the Infovista portal

