ANNEX V

SUBSCRIPTION SERVICE DESCRIPTION

The Cleafy Cloud Platform focuses on proactive attack prevention to combat fraud at its source. Cleafy seamlessly integrates cyber security with fraud management, ensuring end-to-end visibility of Monitored Online Services across web and mobile channels and the fastest, most efficient threat response from a unified defense platform.

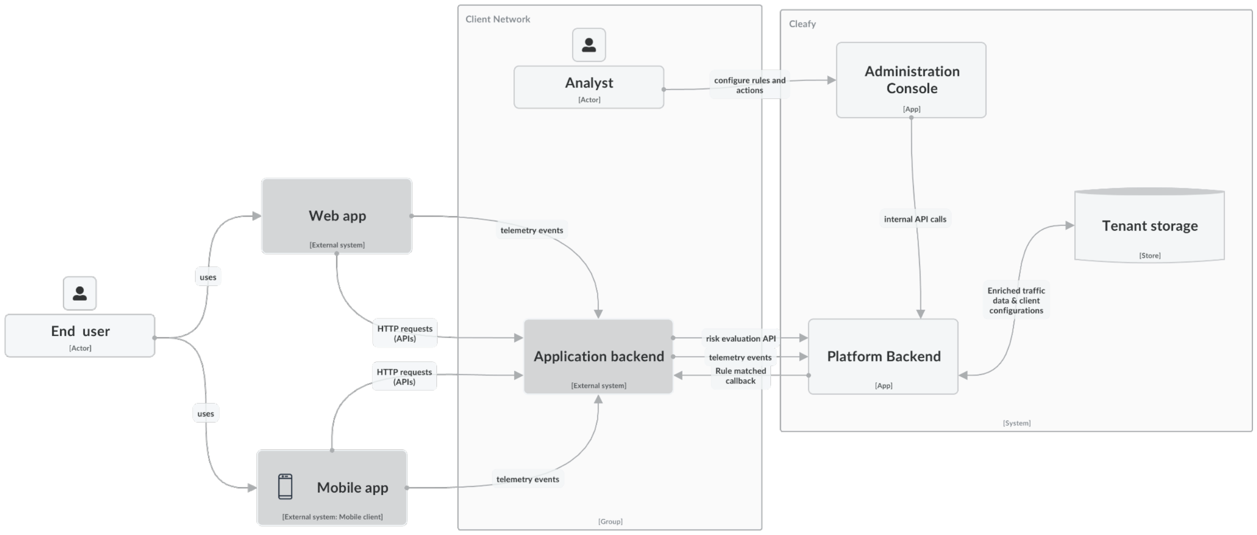
Cleafy Core Technology provides real-time threat detection and protection based on several patented technologies for malware detection, behavioural and transactional analysis to detect today's most sophisticated attacks to online services, such as those committed by identity theft (phishing, vishing, smishing), Malware attacks (Man-in-the -Browser, Man-in-the-Middle, RAT-in-the-Browser, app repackaging, SMS theft, Mobile Overlay applications) and other attack vectors used by fraudsters to commit ATO, ATS fraud, APP scams and more.

Cleafy's approach to online fraud detection is based on the continuous monitoring of the application traffic (even before the authentication phase) and real-time risk assessment that enables the Cleafy Cloud Platform to automatically activate adaptive threat responses, including dynamic application protection, according to the defined security posture. In addition, through Cleafy Threat Intelligence, also known as the ASK platform, our Threat Intelligence team collects and analyses all potential signals of zero-day compromises and carries out advanced analyses to define and deploy IOCs capable of recognizing and detecting the newest fraud attacks.

Cleafy Core Technology spans 9 Areas, 20+ Modules, and 300+ Tags, incorporating behavioral biometrics, behavioral analysis, device telemetry, user prediction, bot detection, transaction risk analysis, and advanced threat intelligence—all within a unified framework.

TECHNICAL DESCRIPTION:

Cleafy Cloud Platform infrastructure assets are built on Google Cloud Platform (GCP), deployed in strongly segregated single-tenant stacks across various regions. Each client has its own stack instance, leveraging several GCP cloud services, such as Cloud Load Balancers, Compute Engine and Cloud Armor.



The diagram above illustrates the main data flows between Cleafy and external systems (dark grey boxes), including

- the Web Application, i.e. the web portal used by end users to browse their account, send and receive money.
- the Mobile app, i.e. the iOS and Android application installed on end users’ mobile devices.

- the Application Backend, i.e. software services (APIs) and infrastructure, e.g. Application Delivery Controllers (ADC) or CDN distributions, deployed by the client to serve requests from both browsers and mobile devices.

Clients must integrate Cleafy with Monitored Online Services via their ADC (Application Delivery Controller) to instrument and intercept web traffic. On the other hand, to capture events occurring in the Mobile app, clients must integrate either an Android or iOS Mobile SDK in their own mobile app. Backend to backend API integrations are also available to evaluate the risk level of transactions and other user activities, and also receive notifications (webhooks) to internal endpoints when traffic matches specific detection rules.

An administration console is also available for analysts to tune the detection system and monitor end-user sessions in real-time.

Engineering teams at Cleafy develop, test, deploy and maintain both software and infrastructure changes following a Secure SDLC (Software Development LifeCycle), leveraging a set of third-party tools, such as

- Jira Software, as a ticketing system for both maintenance (defects and operations) and roadmap (user stories, epics, features).
- Jira Confluence, for both internal/technical documentation and user manuals.
- Zendesk, as a ticketing system for customer support (helpdesk).
- Bitbucket, as a git repository and CI/CD pipelines.
- Sonar and Snyk, for SAST vulnerability scanning and code quality.
- StatusPal, to provide service monitoring capabilities to our Customers
- Auth0, to protect and integrate the administration console with a MFA or Customer IAM
- ELK Stack to centralize and collect security logs and events
- Google GCP and Workspace to provide IaaS/PaaS and domain services