



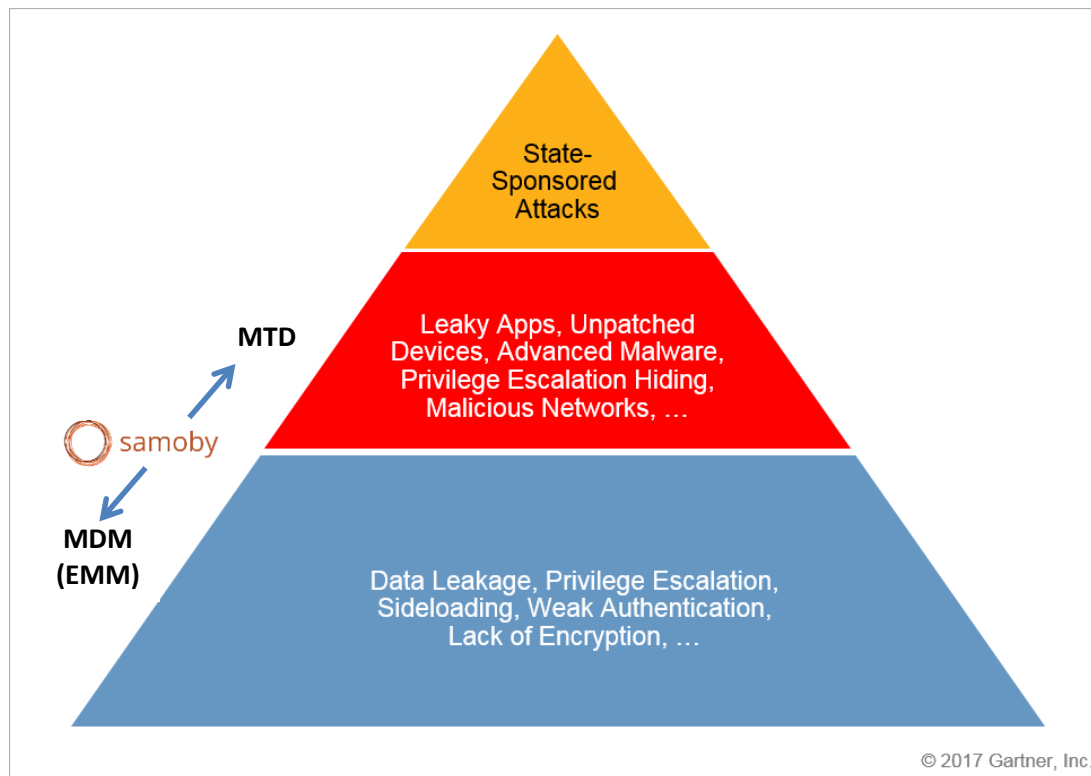
Mobile Threat Defense, supervision, and usage monitoring

Mobile security is not just MDM

Forecasts for 2019, is that 33% of all malware will come from mobile apps (7,5% today, twice more than 1Y ago).

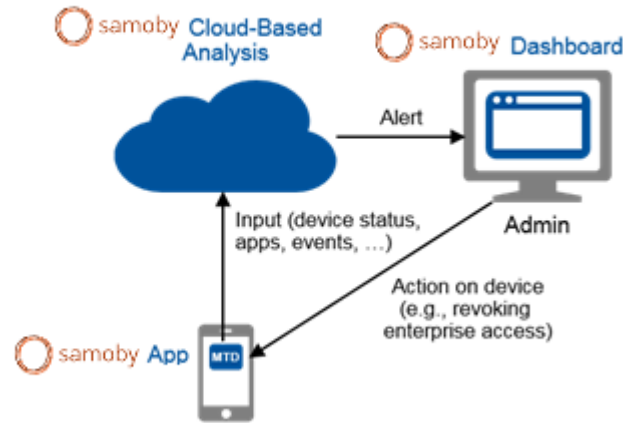
“Mobile Threat Defense”, as defined by Gartner, complements MDMs-EMMs security features by offering real time features MDMs do not.

Samoby offers a real time protection covering both MTD and EMM/MDM (Enterprise Mobility Management) security features



Samoby, a real time platform for mobility

Samoby is an enterprise cloud solution that provides real-time mobile services including threat protection, and usage management.



Security

Samoby helps you have a clear view of new security threats brought by extensive use of mobile, in particular “BYOD”, by creating a central source of information in the cloud, and constantly auditing your employees devices, performing automatic mitigation actions such as disabling access to corporate applications.

Real time detection

- Network threats: Unsecure connection, ARP Spoofing fake SSL, Man in The middle Attacks, Security downgrading, Phishing, unsecure websites, and Ips
- User threat: transferring large amounts of data, connecting to hacking webs or proxies, travelling to sensitive countries or places...
- App threats: Unknown source, Malware, vulnerabilities, suspicious permissions, shared location.
- Device Threats: Security parameters (allow apps from unknow source, ...), root/jailbreak detection, OS versions, Security patches,...

Mitigation

- Data connection Blocking by app
- App usage blocking
- VPN Enforcement
- Remote wipe
- Alerts, notifications, automatic incident creation
- Remote configuration

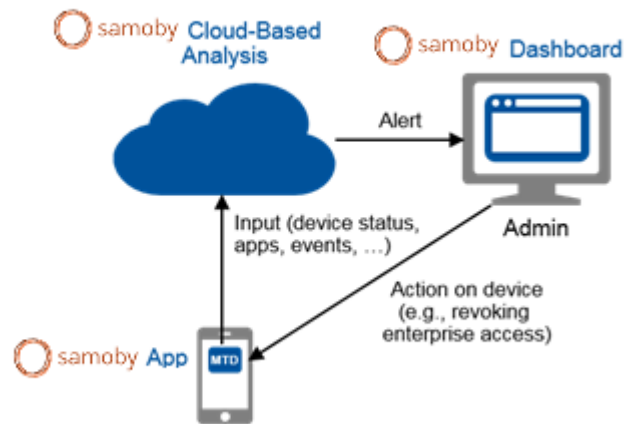
Security – Historical

All mobile events are stored on a cloud platform for immediate or forensic analysis

- Events such as IP connection, app install/uninstall, network AP used, arp tables, can be analysed later to list devices that might have been attacked by a known threat
- Individual devices historical can be audited to identify risky or malicious behaviour

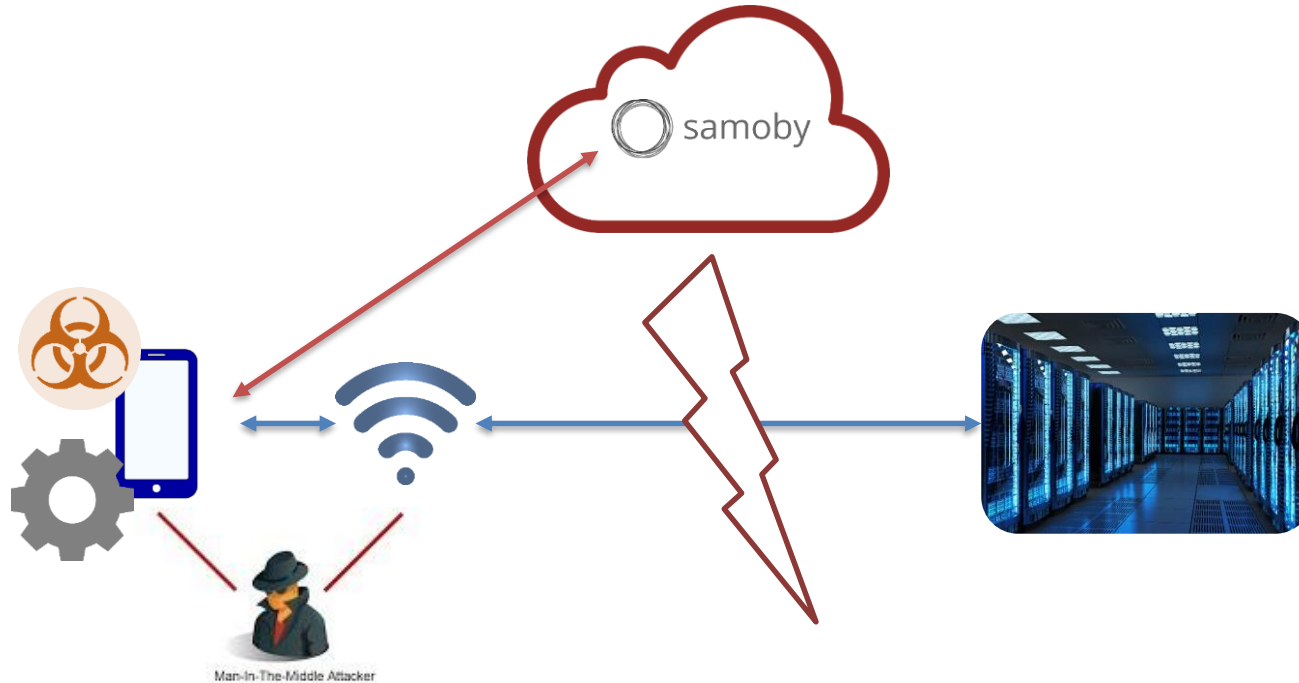
A central Cloud platform helps you take control of scattered devices, in real time and afterwards...

- Not only can you know instantly what is happening now everywhere in your “global extended network”, you will not lose trace of what happened even though you lose or reinit a device.



Samoby Use case #1: BYOD security

Prevent unsecured devices from accessing corporate apps and data:



Employee device is constantly monitored by Samoby

In case of network attack like MiTM or Phishing,...

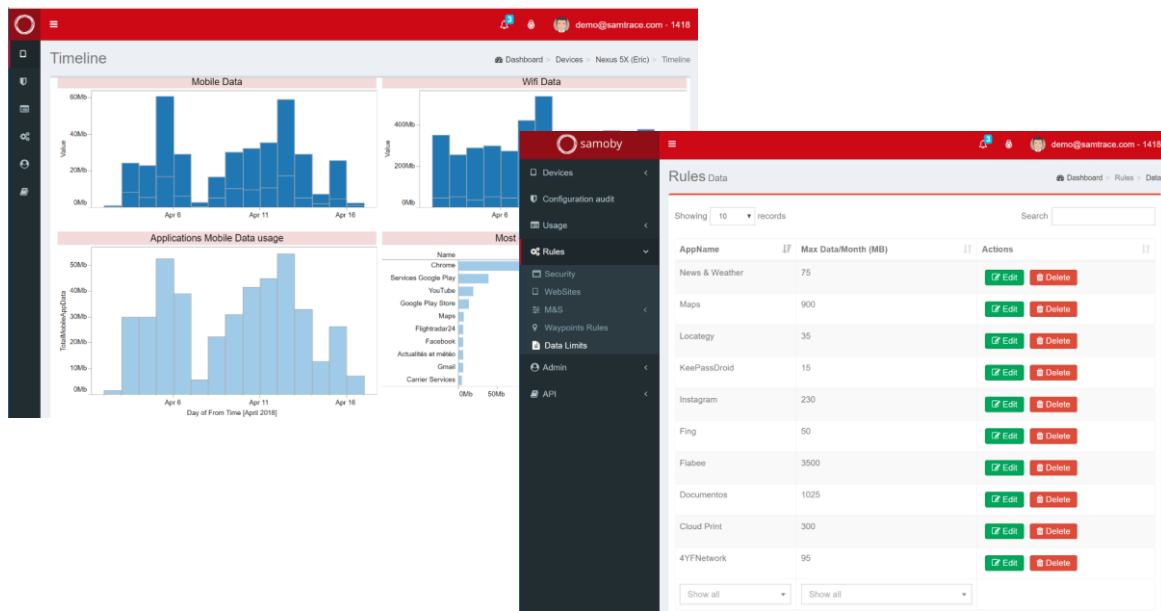
Malware installation,...

Or unusual behaviours,...

access to corporate systems and data is automatically disabled by Samoby

Samoby Use case #2: Roaming control

Have details on how data plan are used when roaming and set up limits for each app:



Samoby supervises each device individual roaming data usage per app

Individual data usage limits can be set for each app

Notifications can be sent to user or admin whenever a user registers in a new roaming network

Admin can see if device is configured properly to use data roaming, can check or set proper data plan and set up limits.

Use cases: mobile expenses

As workplace goes mobile, you need to gain control over mobile costs such as bandwidth usage and licenses.

Samoby gives you detailed analytics of data traffic and use of each app. Define company rules on which, where and when apps can be used, websites visited, calls made. Do not pay for unused apps.

Real time information

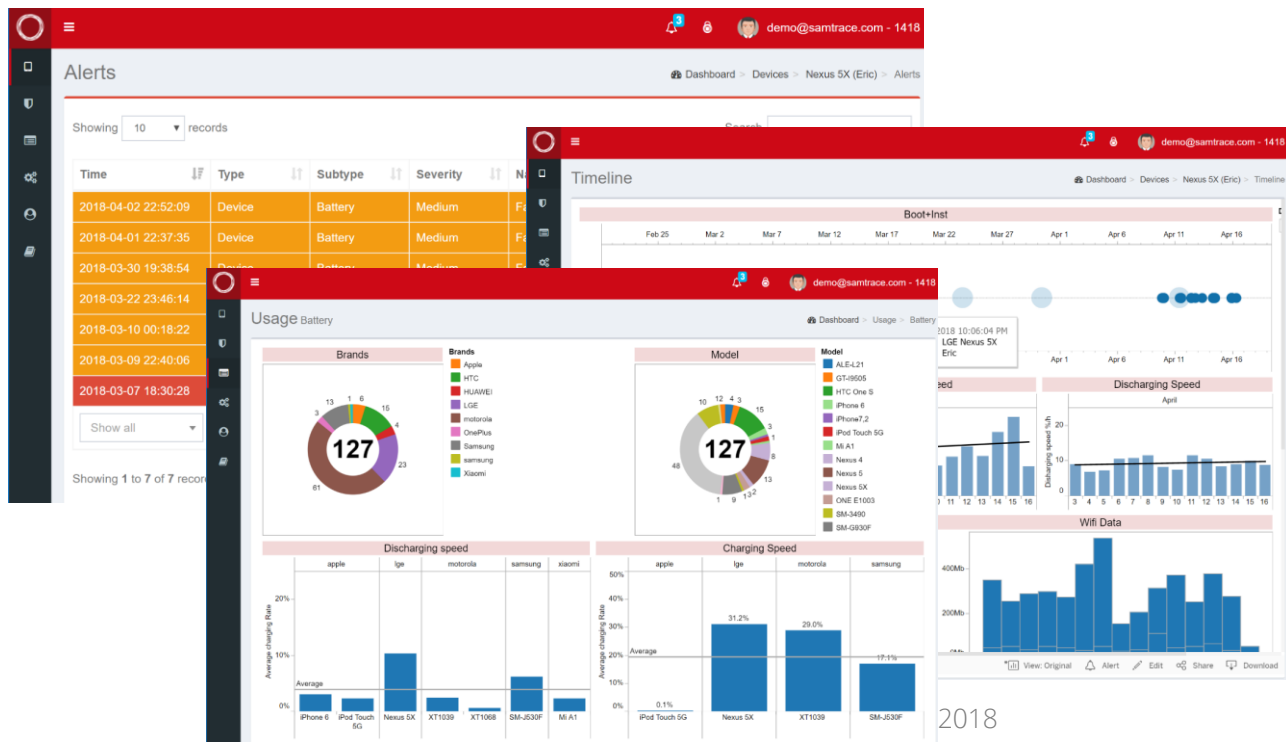
- App usage Logs and analytics
- Analytics of data connection global use, drill down by apps and/or user, roaming.
- Call Logs and analytics
- Web browsing Logs and analytics
- Geolocation

Benefits

- Know which are the most used corporate apps, do not pay for unused licence, invest in enhancing the one people need
- Selectively block or limit the use of apps by time, location, Data plan consumption.
- Know where your data plans are spent. Detect top data consuming apps, limit use following company policies, roaming, hour, location,...
- Limit outgoing/incoming calls: hour, location, black/white list, etc. For example, block roaming outside a list of countries.
- Limit web access by sites category.

Samoby Use case #3: Proactive maintenance

Reduce calls and emails to helpdesk by detecting incidents before user reports them



Receive **alerts** or generate tickets when abnormal hardware behavior is detected

Access **detailed device history** and parameters for a better diagnosis

Have some **benchmark** information of all devices in your fleet for selecting best models

Use cases: enhancing M&S

Proactively detect and automatically remediate device problems, give a better service and reduce smartphone and tablets Maintenance & Support costs.

Reduce MTTR (Mean time to resolve) by having accurate device information and history.

Key features

- Early detection of hardware failures: memory, battery, stability, etc.
- Access to a complete and updated information on Hardware, versions, installed apps, and device configurations.
- Access to device history: memory CPU and Battery state over time, app install/uninstall history,...
- Easy integration with other corporate tools: ITSM (incidents, problems, CMDB,...), infrastructure monitoring, ITOM, SIEM, SAM.

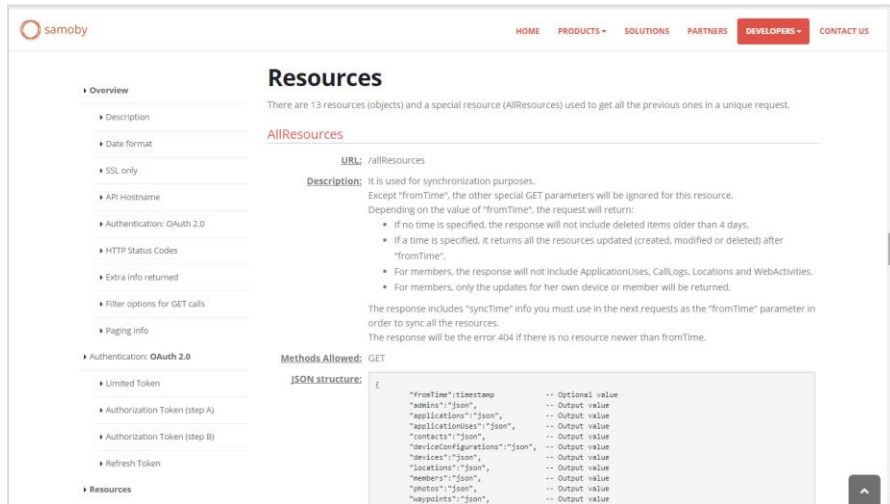
Benefits

- Proactive maintenance, decrease number of incidents opened by users.
- Reduce response time from helpdesk team
- Benchmarking and analytics: know which devices fails most, and why.
- Mobile world is integrated with corporate world, and processes can easily be automated in order to apply company standards, have a better productivity, trackability and analytics.

Samoby RESTful APIs

Samoby provides two RESTful API with OAuth authentication:

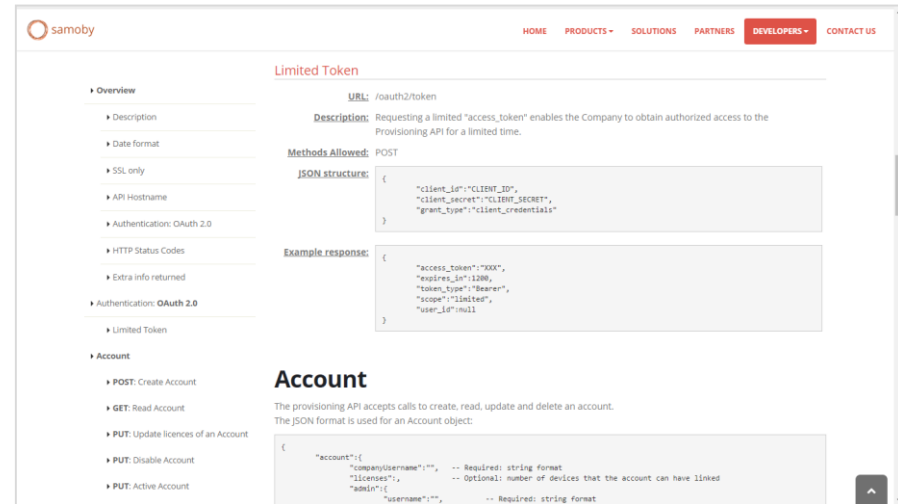
- Provisioning API: to create, read, update and delete users.
- Open API: enables easy integration to provide real-time intelligence for Enterprise Services (ITSM, ISAM, ITOM, SAM, ad-hoc alerts, etc..).



The screenshot shows the 'Resources' page in the Samoby developer portal. The page title is 'Resources' and it contains the following information:

- Overview:** There are 13 resources (objects) and a special resource (AllResources) used to get all the previous ones in a unique request.
- AllResources:**
 - URL:** /allResources
 - Description:** It is used for synchronization purposes. Except "fromTime", the other special GET parameters will be ignored for this resource. Depending on the value of "fromTime", the request will return:
 - If no time is specified, the response will not include deleted items older than 4 days.
 - If a time is specified, it returns all the resources updated (created, modified or deleted) after "fromTime".
 - For members, the response will not include ApplicationUses, CallLogs, Locations and WebActivities.
 - For members, only the updates for her own device or member will be returned.
 - The response includes "syncTime" info you must use in the next requests as the "fromTime" parameter in order to sync all the resources.
 - The response will be the error 404 if there is no resource newer than fromTime.
 - Methods Allowed:** GET
 - JSON structure:**

```
{
  "fromTime":timestamp           -- Optional value
  "admins":"json",              -- Output value
  "applications":"json",        -- Output value
  "applicationUses":"json",     -- Output value
  "contacts":"json",           -- Output value
  "deviceConfigurations":"json", -- Output value
  "devices":"json",             -- Output value
  "locations":"json",           -- Output value
  "members":"json",            -- Output value
  "photos":"json",             -- Output value
  "waypoints":"json",          -- Output value
}
```



The screenshot shows the 'Limited Token' and 'Account' pages in the Samoby developer portal.

Limited Token

- URL:** /oauth2/token
- Description:** Requesting a limited "access_token" enables the Company to obtain authorized access to the Provisioning API for a limited time.
- Methods Allowed:** POST
- JSON structure:**

```
{
  "client_id":"CLIENT_ID",
  "client_secret":"CLIENT_SECRET",
  "grant_type":"client_credentials"
}
```
- Example response:**

```
{
  "access_token":"XXX",
  "expires_in":1200,
  "token_type":"Bearer",
  "scope":"limited",
  "user_id":null
}
```

Account

- The provisioning API accepts calls to create, read, update and delete an account.
- The JSON format is used for an Account object:
- JSON structure:**

```
{
  "account":{
    "company/username":"", -- Required: string format
    "licenses":,           -- Optional: number of devices that the account can have linked
    "admin":{
      "username":"",      -- Required: string format
    }
  }
}
```

Samoby architecture



iOS



Samoby agent and
real-time collector

- 0.04% CPU consumption
- Less than 1% battery
- Less than 1MB/day of Data
- Smart and proprietary algorithms to optimize mobile resources usage

Samoby real-time service

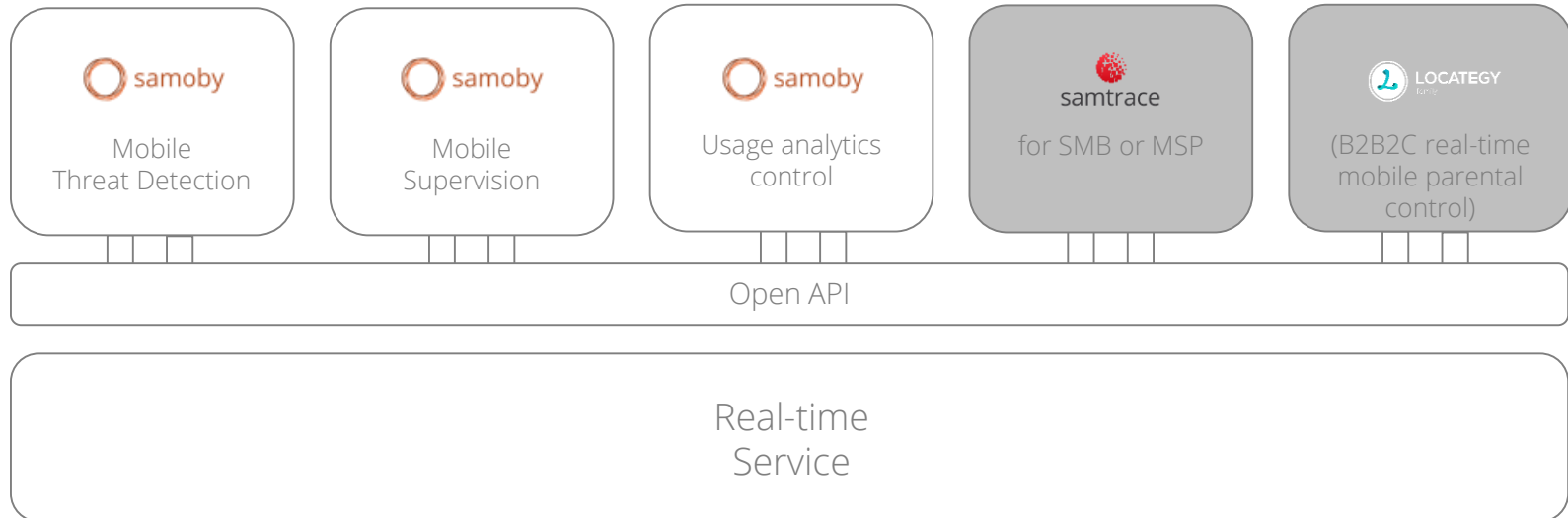
- More than 2 million events managed per day
- More than 2.5 million monitored apps
- Latency 50ms (0.05s)
- Guaranteed uptime with a 99.99% SLA available
- Worldwide coverage
- Get started in minutes from our SaaS platform delivered from AWS
- On premises deployment
- Multi-tenant configuration
- OEM and white labelling approach
- Encryption end to end
- All requests are logged

Samoby native admin
apps and dashboard

- HTML5 dashboard
- Native Android app for admin
- Native iOS app for admin
- HTML5 app for mobile admin

Samoby: Real-time platform modularity

The **Samoby** service is build on top of the real-time platform that delivers a range of real-time, mobile added-value services for Enterprise and individual. It includes Mobile Device and App Discovery, Threat defense, App remote control, configurable alerts, tracking, configuration management, among others



About Us

Founded in 2008, we're developers of cloud-mobile **Value-Added-Services** (VAS).

We do cover mobile corporate and SME needs, providing cloud administration, rich-Open API and native mobile apps.

Our products have been selected by leading **Managed Service Providers** and **Telcos**, **Independent Software Vendors** and **Systems Integrators**.





Samoby Technologies S.L.
Marie Curie 8-14, Barcelona 08042, Spain
www.samoby.com

Some data

5 countries & 3 continents

15 Medium or large size companies -  70,000 employees 1,000 devices managed

9,000 small companies

near 100,000 managed devices

Close to 2,000,000 supervised apps