

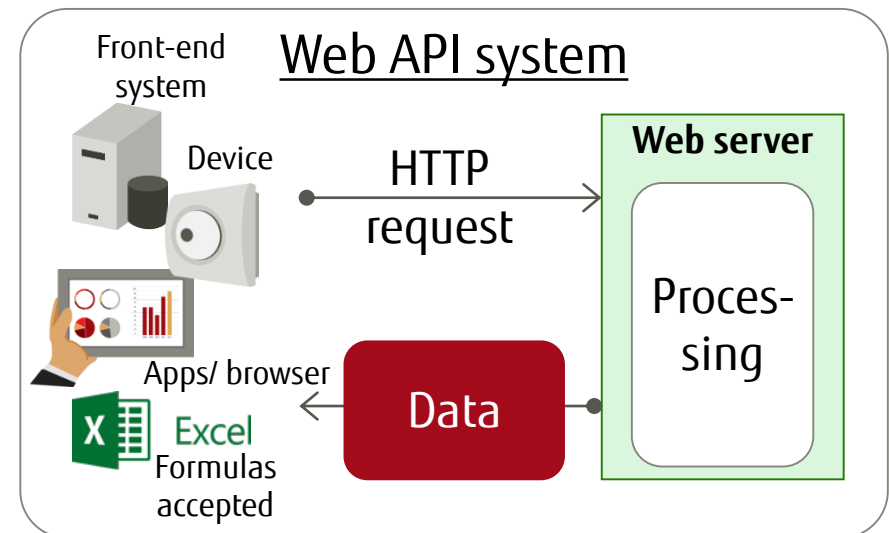
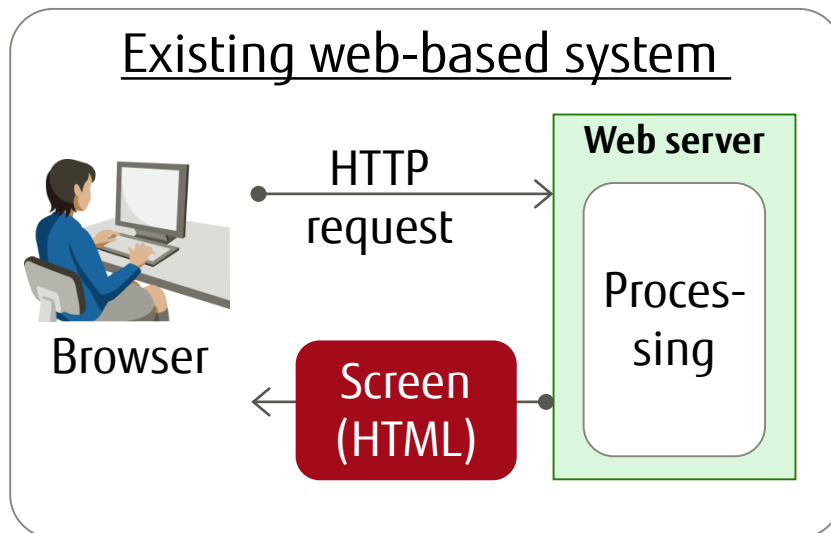
FUJITSU Cloud Service K5 API Management Service Functional Overview

July 2016
Fujitsu Limited

- Unauthorized copying and replication of the contents of this document is prohibited.
- The contents of this document may be changed without prior notice.

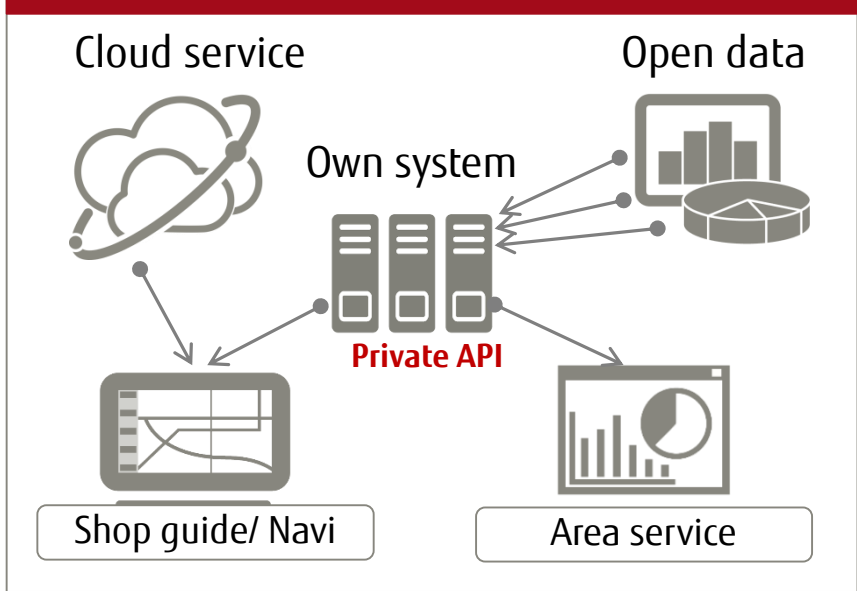
- About Web API
- Major Web API Usage Scenarios
- Service Overview
- API Management Features
- Functions for Publishing APIs
- API Development Flow
- API Proxy Functions
 - Policy
 - Flow
- Development Functions
 - Deploy Function
 - API Tracer Function
 - Publish Function
- Analytics & Monitoring Functions
 - Analytics
 - Custom Report
 - Dashboard
- Service Account and Environment
- Service Menu
- Billing Model
 - Pro Plan
 - Standard Plan
- Changing Plans
- Restrictions and Notes
- References

- Web API enables IT engineers to access various kinds of services through programming code
 - API users can access various functionality by aggregating many kinds of APIs. Engineers are starting to customize applications themselves or create new applications using APIs.
- Differences from existing web-based systems
 - Existing web-based systems provide data and functions via a screen (HTML-based).
 - The Web API only exchanges data. The client side is not necessarily a browser. (Any HTTP compatible format can be used)

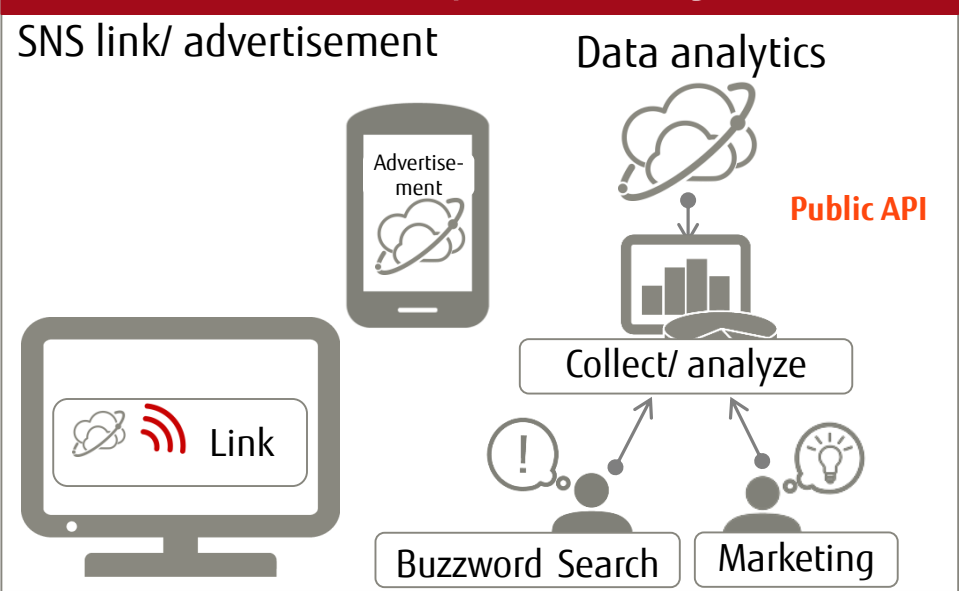


Major Web API Usage Scenarios

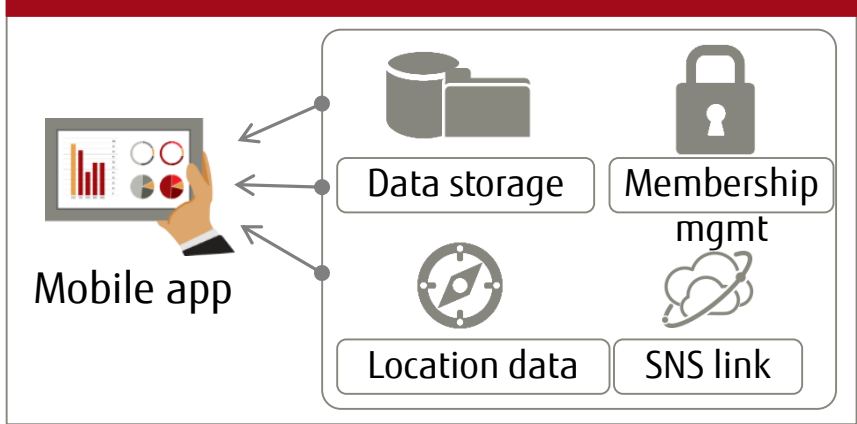
Service mash-up



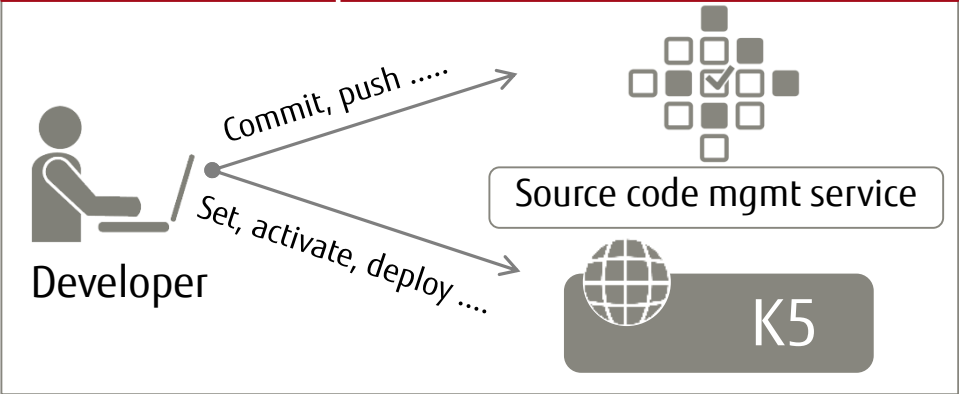
Community-wide usage



Mobile backend (MBaaS)

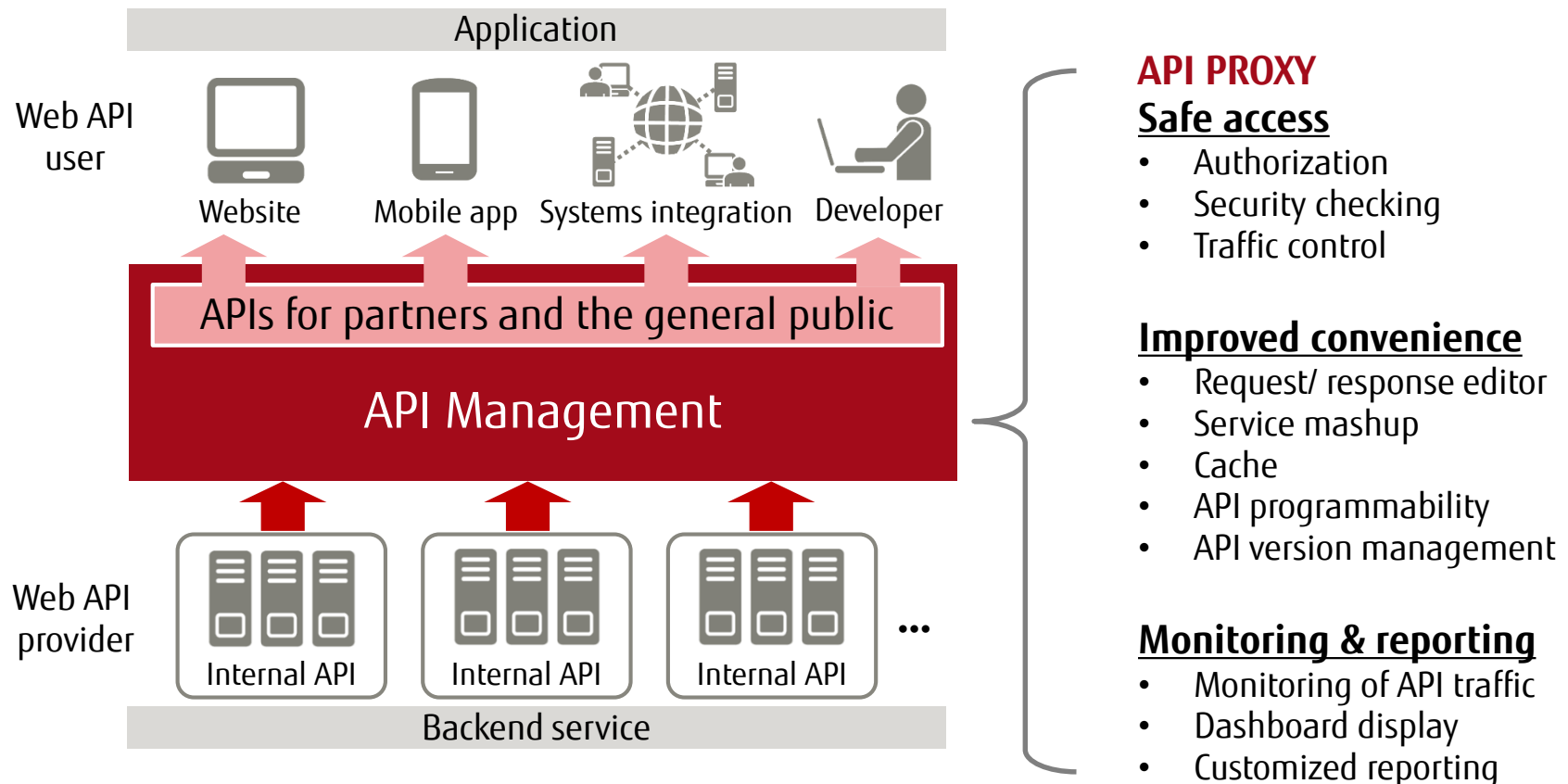


Cloud platform/ development environment



Service Overview

K5 API Management provides valuable functionality such as API development, publishing, enhancement and operation. K5 API Management will continuously contribute to your business.



Offered by FUJITSU Cloud Service K5

API Management Features

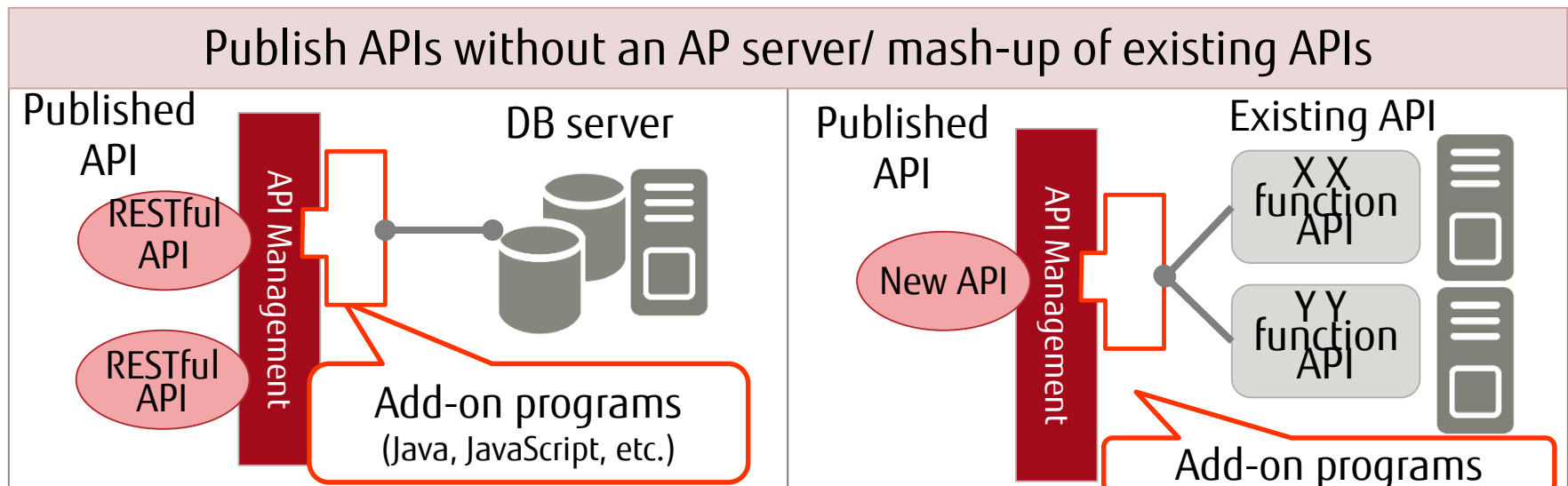
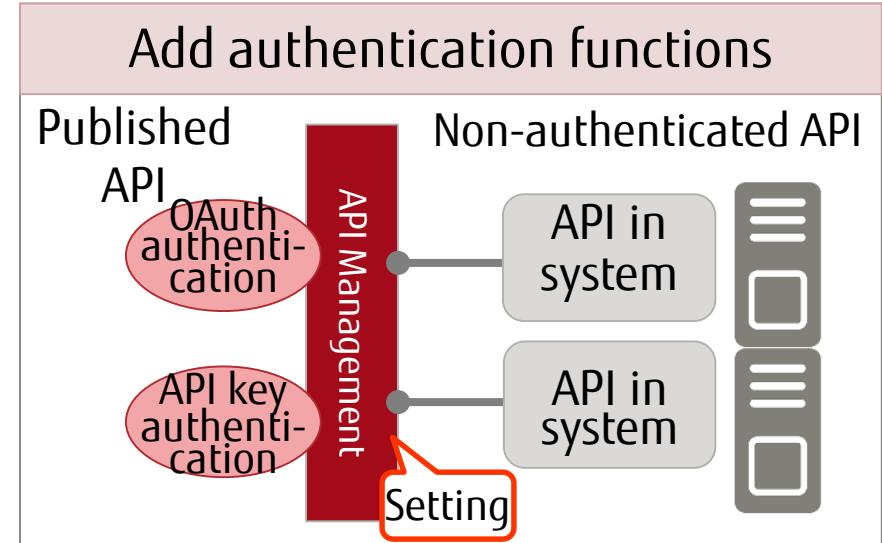
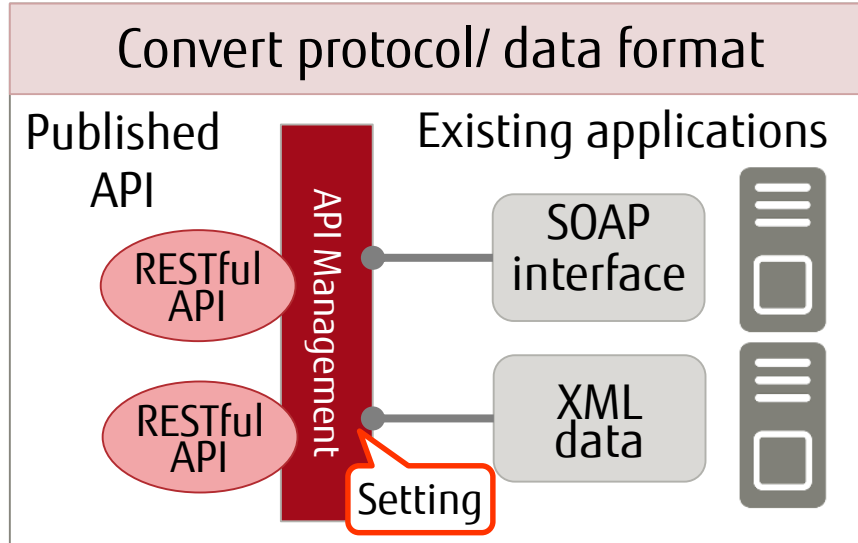
■ Functions provided by the API Management service

- Shared functions/ Private API functions
- Public API functions

Compatibility/ connection	Optimization	Security	API development	Shared functions Functions for Private API
<ul style="list-style-type: none"> Extract data from messages Convert XSL Convert SOAP to REST Edit requests Edit responses 	<ul style="list-style-type: none"> Response cache Key value store Limit the number of concurrent connections Prevent traffic spikes Limit traffic volume 	<ul style="list-style-type: none"> OAuth 2.0 Basic authentication SAML support LDAP link 	<ul style="list-style-type: none"> Add-on programs Development/ operation environment Non-stop deployment Multi-version management Policy/ flow editor Monitoring (API performance, errors) 	
Publishing	Analytics			Functions for Public API
<ul style="list-style-type: none"> Package APIs Set ACL (update/ reference) Limit traffic volume Assign key (API keys) 	<ul style="list-style-type: none"> Statistics for the operations administrator API developer usage statistics Application statistics Business statistics Report customization 			

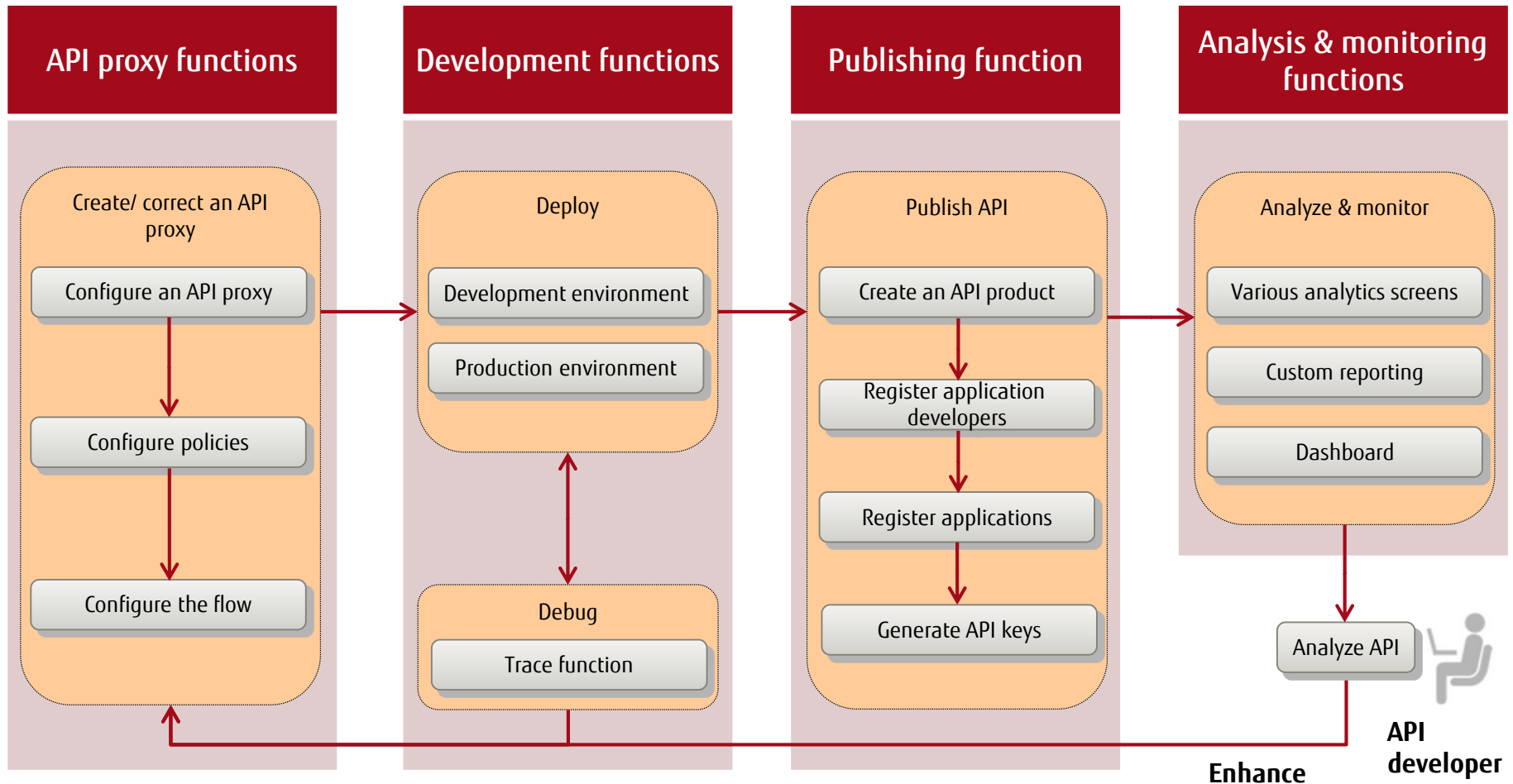
Functions for Publishing APIs

- Functions are offered to simplify the publishing of APIs



API Development Flow

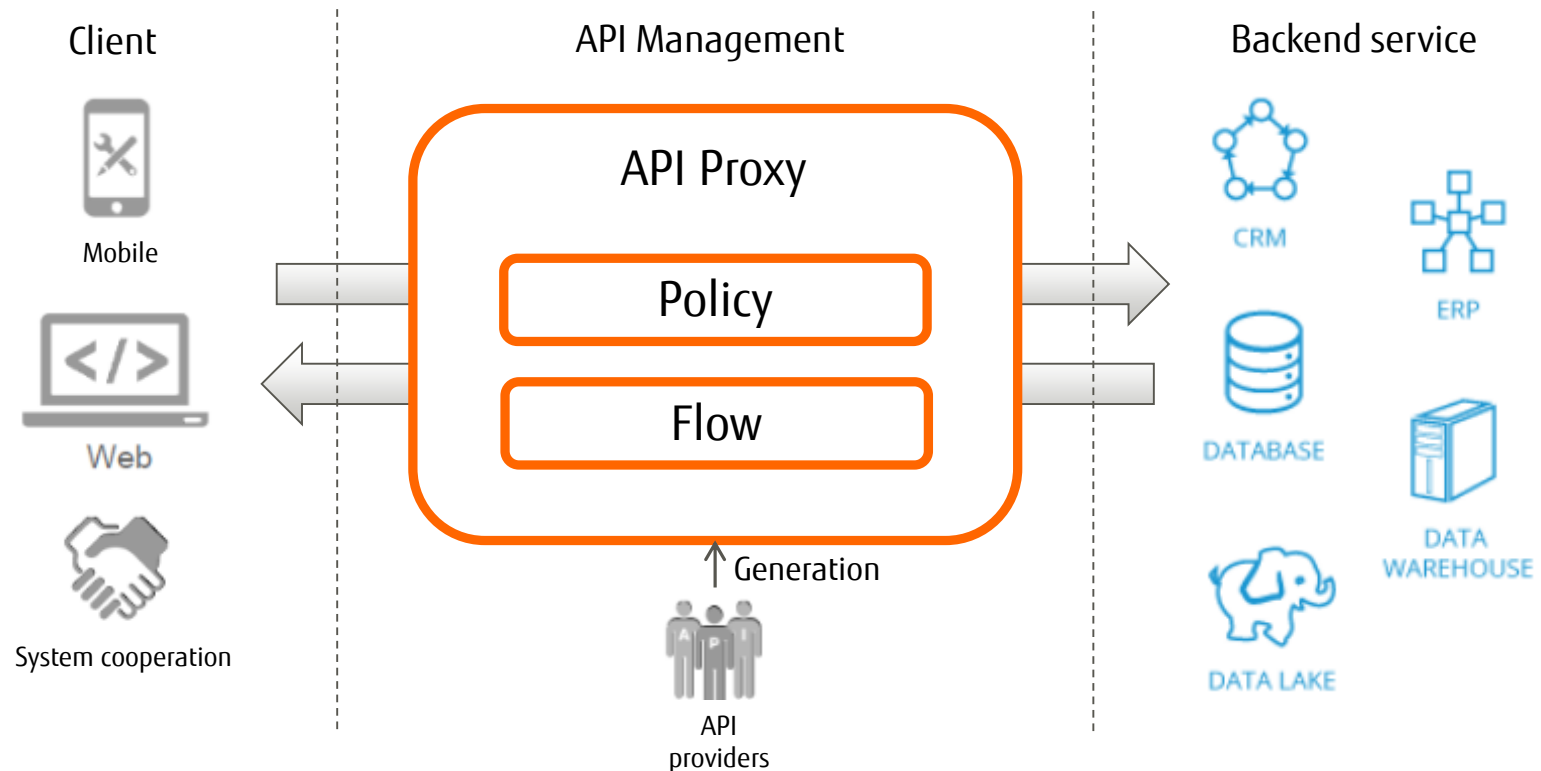
The following chart shows the process flow for developing an API using the API Management service



API Proxy Functions

The API Proxy is a core component of API Management and acts as a gateway. The API provider can flexibly edit the API request and response without writing any code.

- ✓ Policy (add various kinds of features to the backend service)
- ✓ Flow (control the processing sequence of the attached policy)



API Proxy Function – Policy

The Policy is easily attached to your API.
This significantly reduces the amount of coding required.

Reduce
Time to market

More than 30 functions can be added through configuration only, without any coding

- Authentication/ security
- Modification of request/ response information
- Caching
- Restriction of traffic volume
- Data format conversion
- Logging

*For all functions, please refer to: 'APIM: Reference: Policy'

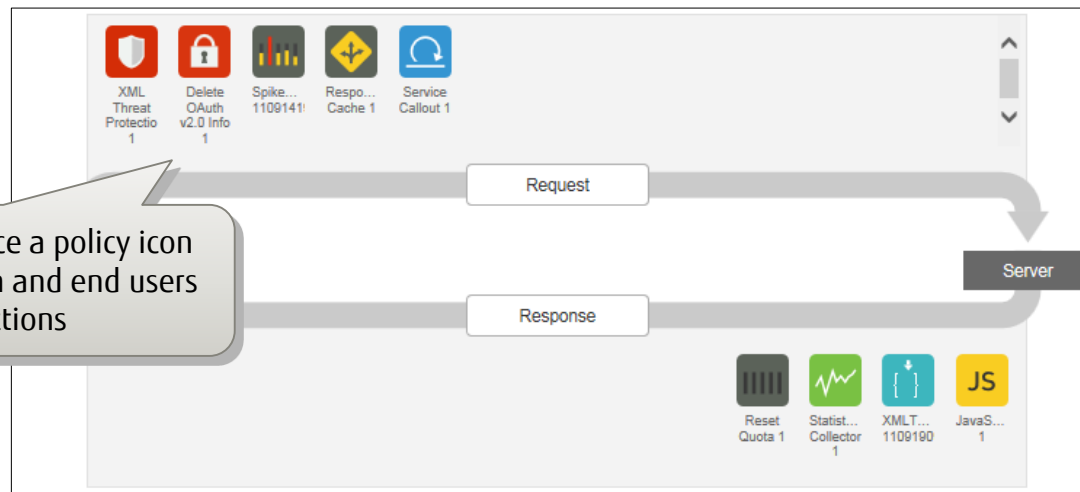
Custom functions can be added using scripts

- JavaScript
- Java
- Python

Backend services can be implemented on API Proxy

- Node.js

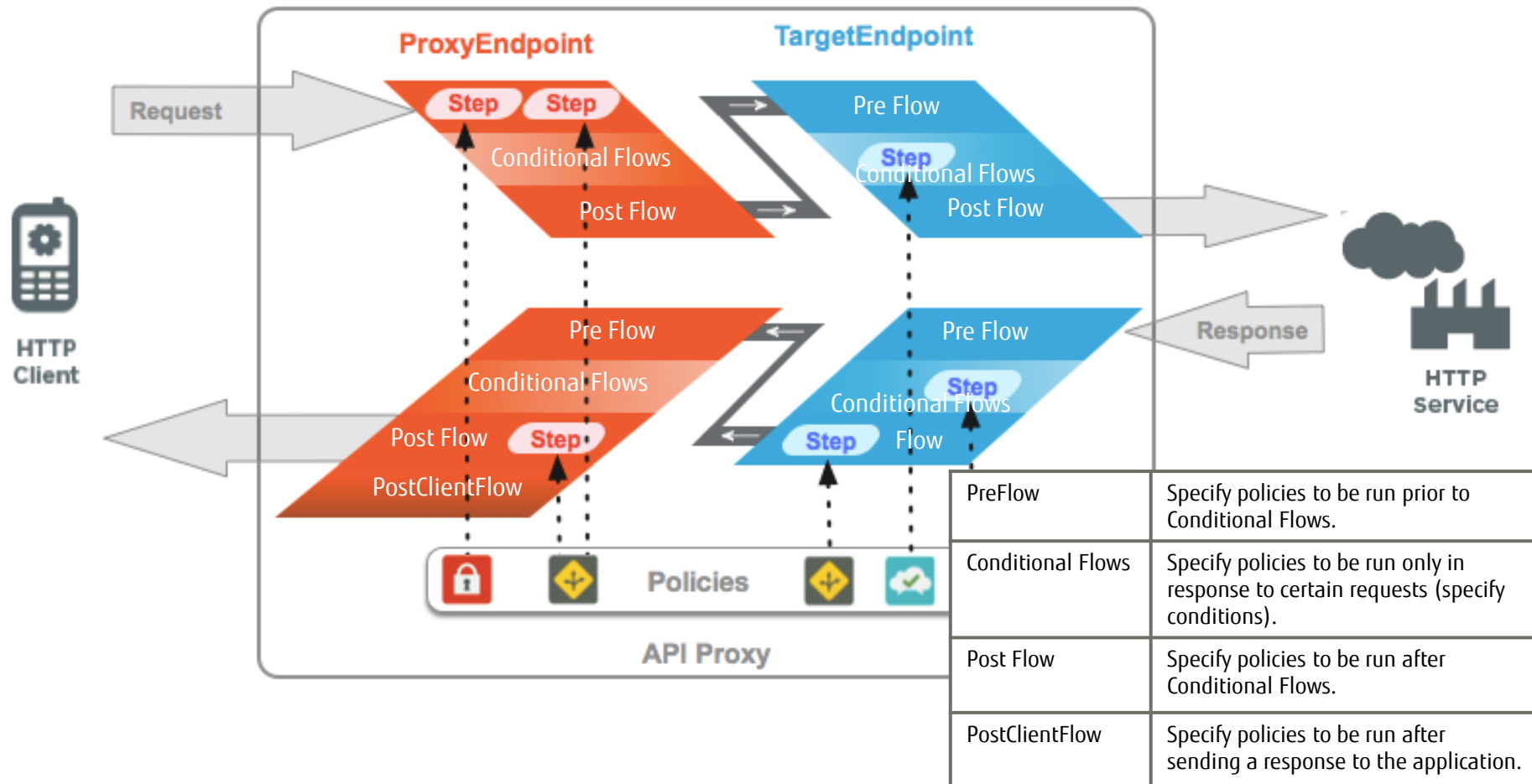
Administrators can place a policy icon on the API proxy screen and end users can use the added functions



API Proxy Function - Flow

Policies are run at the appropriate time.
The flow defines the policy order and scope for each API.

A Policy is easily attached
Using a GUI-based flow editor

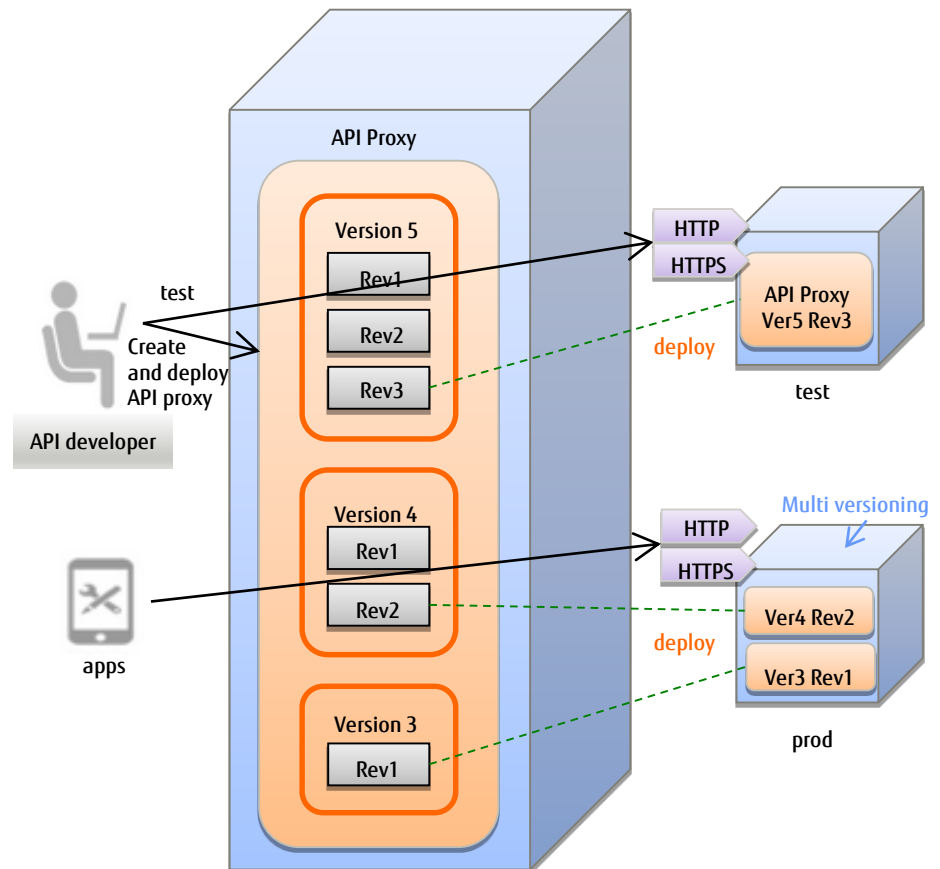


Development Function – Deploy

Realize effective API development using the Deploy, Version Management, and Environment functions

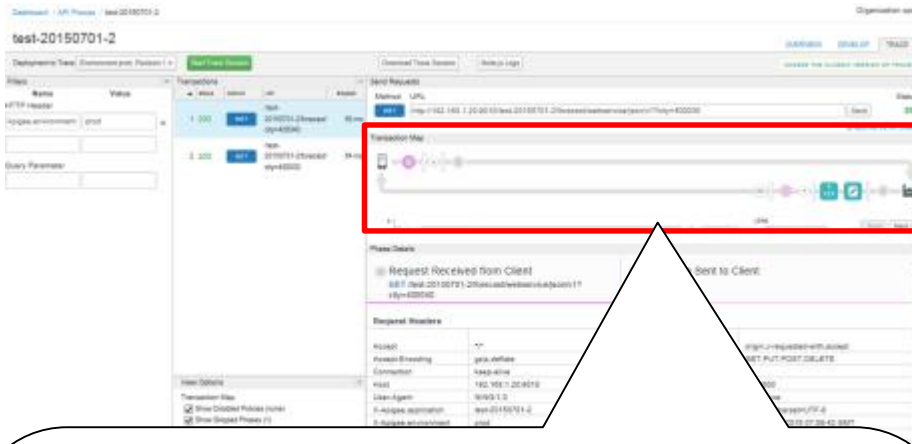
Supports agility

Feature	Item	Benefit
Deploy	Seamless	Deploy API Proxy with minimal change to backend applications
	Multi version Deployment	Support multiple version deployment in the same environment
Version Management	Version	API Proxy manages the lifecycle changes of API policy configurations
	Revision	Revision (smaller unit of a version) support
Environment	Test/ prod environment	Prepare both test and production environments
	HTTP/HTTPS	HTTP/HTTPS are available



API Tracer enables developers to debug APIs effectively by displaying API proxy transactions and clarifying each policy's result.

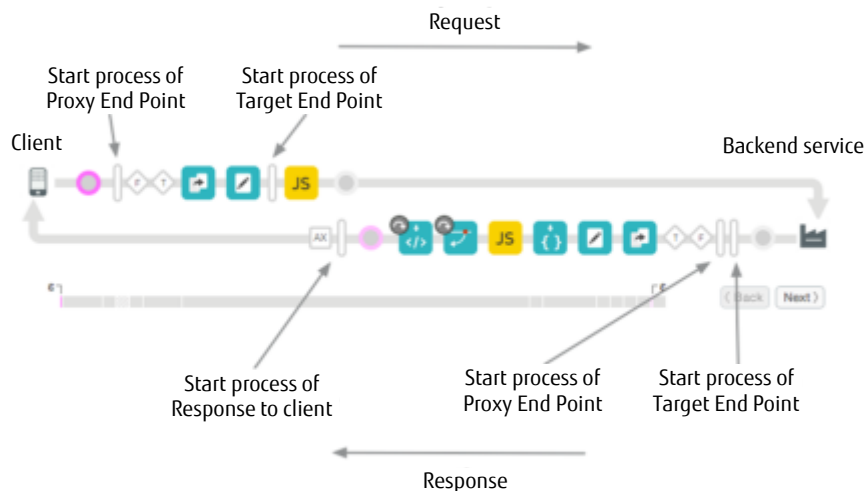
Effective troubleshooting



Transaction Map

- Displays each step of a transaction using icons.
- Details are displayed by clicking an icon.
- The masking function hides confidential information when icon details are displayed.
- End users can trace transactions using tools such as a browser, curl, etc.

Transaction Map



Filter

- Transactions can be filtered in the trace with the following conditions.
 - ✓ HTTP header
 - ✓ Query parameter

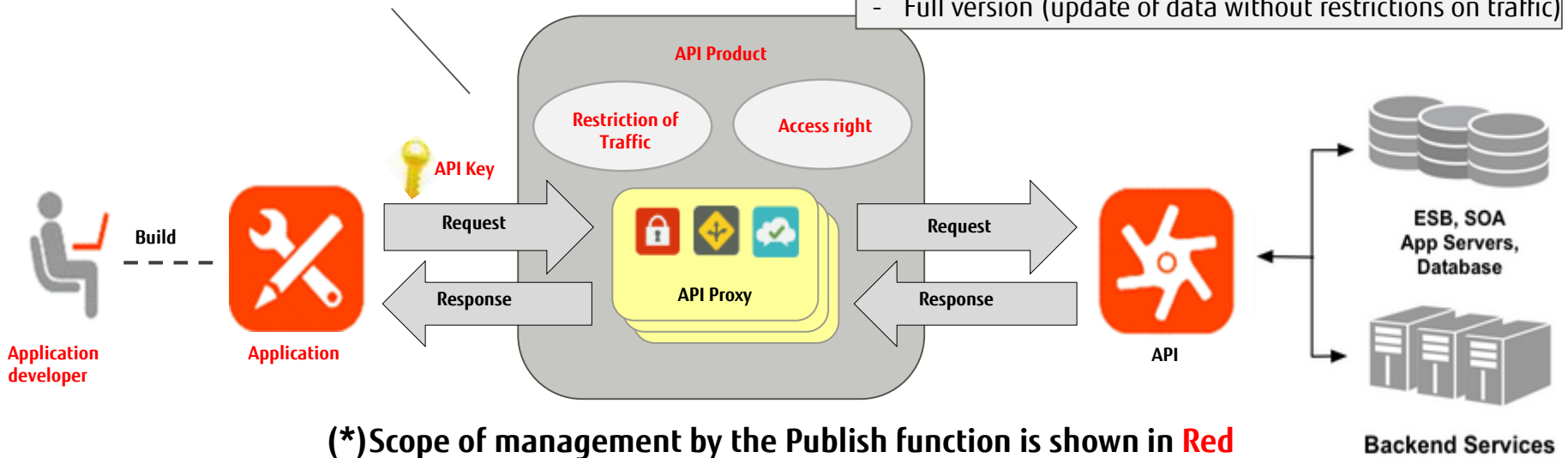
Offline Trace

- Results of a trace can be exported and imported via the online trace screen.

This function is used to publish the created APIs (API Proxy) to the application developers. It can publish packaged API Proxy as a product based on usage by configuring access rights and traffic restrictions.

Supports flexible product offerings which meet business demands

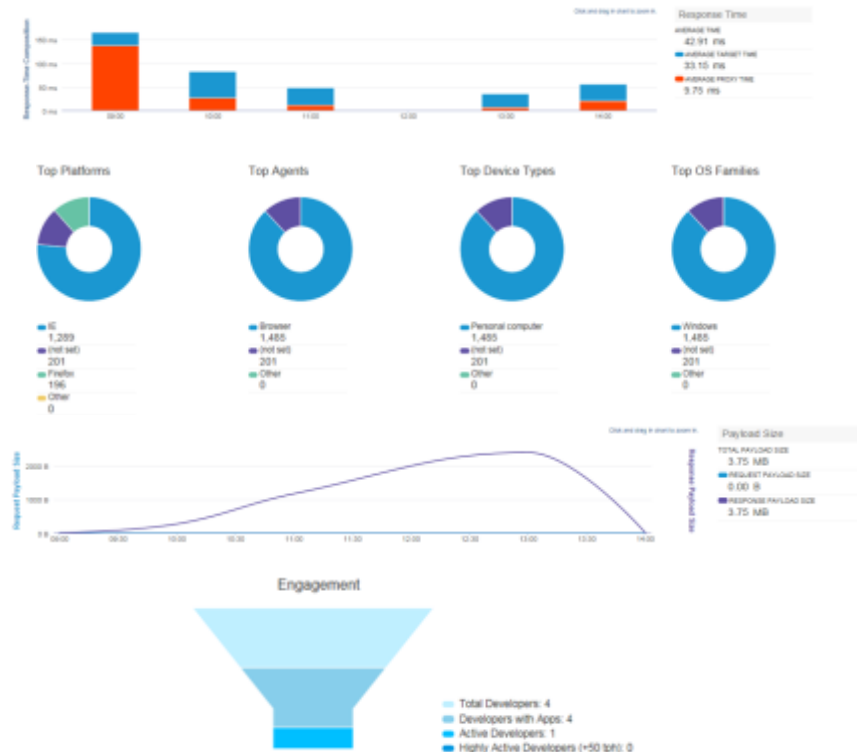
The API keys required to run an API are provided when application developers, applications and the products to be used are registered.



The Analytics service enables effective operation and boosts business using various kinds of real time reports.

- API traffic
- Real time monitoring
- Performance

Example of Collection of API Traffic



Analytics Screen

End users can monitor the information collected via the following 9 screens:

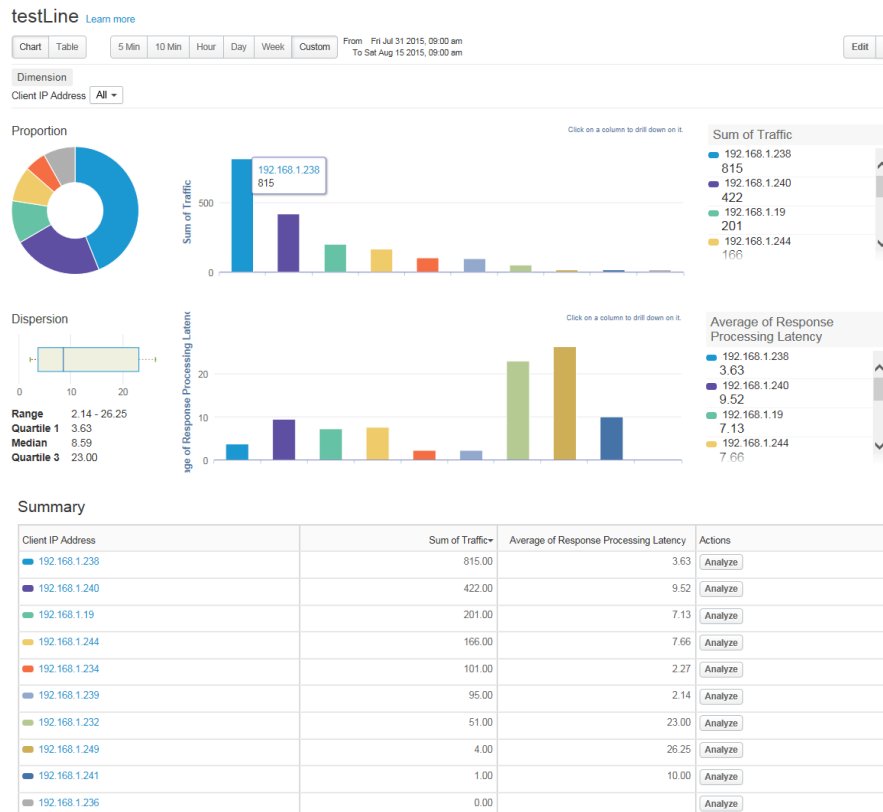
- Proxy Performance
- Target Performance
- Cache Performance
- Latency Analytics
- Error Analytics
- Developer Engagement
- Traffic Composition
- Business Transactions
- Devices

* For details of each screen, please refer to: 'APIM: Reference: Analytics List'

Custom Report enables users to create tailored reports by choosing the horizontal (Dimensions) and vertical (Metrics) axes.

Create your custom report

Custom Report Example



Dimensions

- Users can specify the type of information they want included in traffic reports, such as the IP addresses of clients, OS types, etc.
- End users can select multiple dimensions and then drill down to further analyze the statistical data.

Drill down example

The "OS" and "IP address" dimensions are selected to help analyze the usage of Windows by each IP address.

Metrics

- Users can select information related to API usage such as the number of requests, number of errors, response times, etc.
- The selected items are displayed using charts in the report.

Filter

- Statistical data can be filtered when Dimensions and Metrics are selected.

Dashboards provide end-to-end visibility using various metrics.

Dashboard

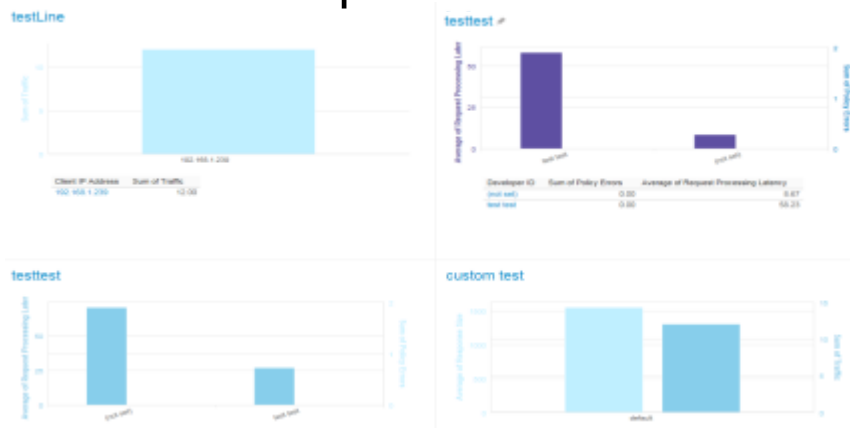


Description

The following two dashboard options are available:

- **Predefined dashboards**
Display all API Proxy traffic information on a single screen.
E.g. API Proxy traffic, developer usage, app error rates
- **Custom Report dashboard**
Four custom reports can be displayed on a single screen.
Further details are shown by clicking on the chart name.

Custom Report Dashboard



■ ID / Password API

- Notify the system administrator of the userID / password with administrative rights. This userID is permitted to add new user accounts.
- Four roles are available: Organization Administrator, Operations Administrator, Business User and User.

■ Organization, Environment

- One organization is activated per contract.
- Organization is a management unit of API Management.
- Test and production environments are available for each organization.

■ Service Menu

Plan	Billing unit	Comment
Pro		
Fixed Menu	Monthly	No. of API calls (* aggregated every 3 months) Fixed (Fixed Menu) + Pay-per-use (Extra Call Option) • Fixed: 25 million calls/ 3 months • Extra Call Option: Per 2.5 million calls
Extra Call Option	Per 2.5 million calls	
Standard		
Fixed Menu (3M)	Monthly	No.of API calls (* aggregated monthly) Fixed (Fixed Menu) + Pay-per-use (Extra Call Option) • Fixed (3M): 3 million calls per month • Fixed (10M): 10 million calls per month • Fixed (20M): 20 million calls per month • Extra Call Option: Per 1 million calls
Fixed Menu (10M)	Monthly	
Fixed Menu (20M)	Monthly	
Extra Call Option	Per 1 million calls	

■ Billing

- Fixed monthly fee + pay-per-use (Extra Call Option) are billed based on the number of API calls subscribed to for this service
- Fixed monthly fee: Fixed fee per month
Note: No. of API calls that can be made: 25 million/ 3 months
- Pay-per-use (Extra Call Option): Per 2.5 million calls
Note 1: Starts once the total number of API calls in a 3-month period exceeds 25 million
Note 2: Billed/ invoiced at 3-monthly intervals
However, if use of the service is canceled, billing/ invoicing takes place in the month that usage ends.

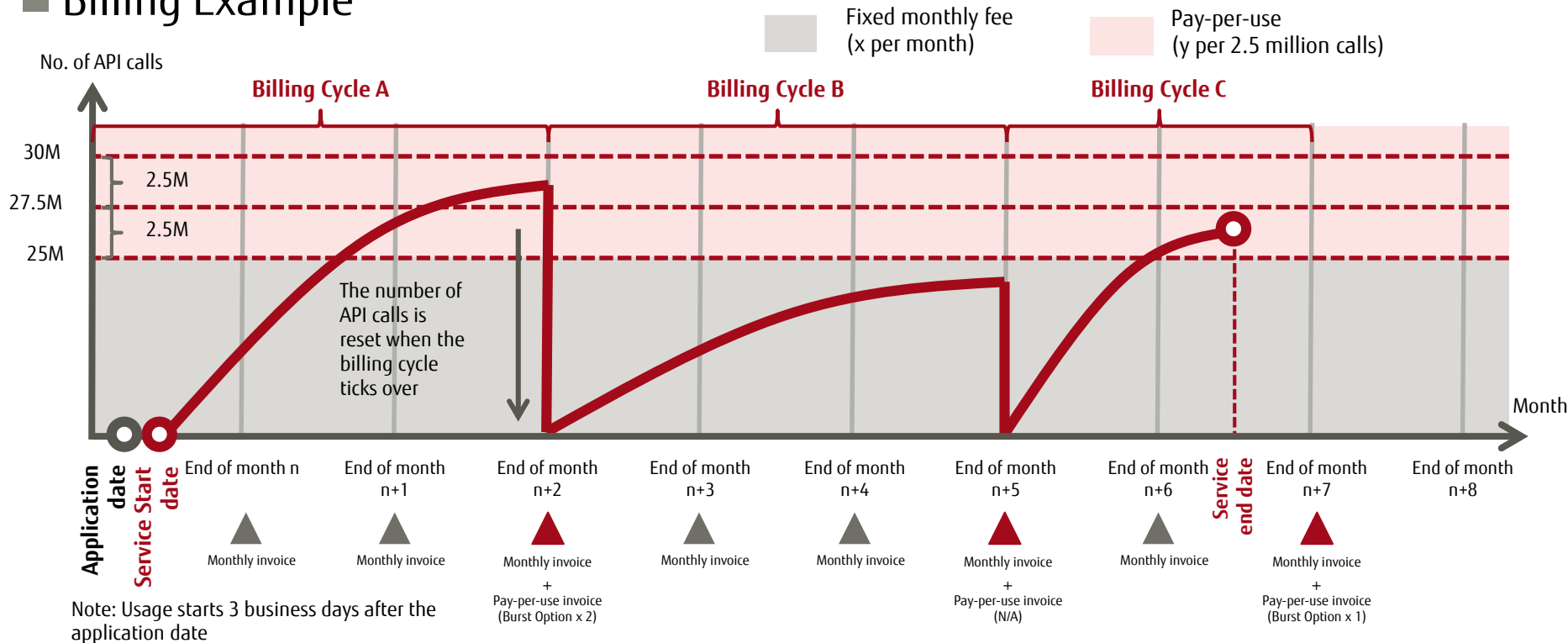
■ Service start and end dates

- The service start date is 3 business days after the date an application is lodged for using the service (i.e. the date an application is lodged via the PaaS portal).
- Fees are charged from the month in which the service start date occurs to the month in which the service end date occurs.
- The service end date is the date on which an application is lodged to turn off the service.

Refer to the next slide for billing example.

Billing Model (Pro Plan)

Billing Example



Billing Cycle A: Usage starts during month/ with pay-per-use

Aggregated quarterly, including usage start month. In the above example, the 25 million calls allowed under the fixed monthly fee plan is exceeded during the second month (month n+1), but is billed in the third month (month n+2) because of pay-per-use. Because 27.5 million < No. of calls ≤ 30 million, month n+2 is billed at $(x+2y)$.

Billing Cycle B: Continuous usage/ without pay-per-use

Pay-per-use billing does not apply because the total number of API calls for the quarter is less than 25 million. Month n+5 is billed at x.

Billing Cycle C: Contract canceled without the billing cycle reaching the full 3 months

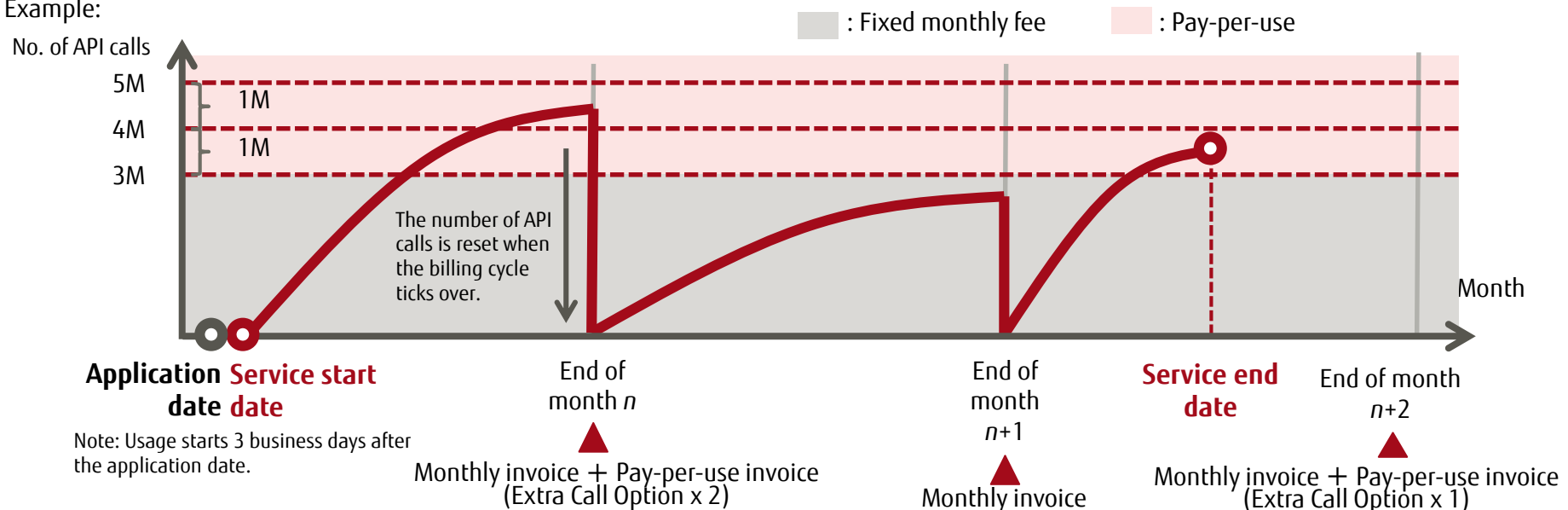
Usage ends during the second month (month n+7) of the billing cycle. Pay-per-use is billed at the end of the month in which usage ends. Month n+7 is billed at $(x+y)$.

Billing Model (Standard Plan)

■ Fixed monthly fee + Pay-per-use

- Fixed monthly fee + pay-per-use (Extra Call Option) are billed based on the number of API calls subscribed to for this service
- Fixed monthly fee: Fixed fee per month
Note: No. of API calls that can be made: subscribed Plan per month
- Pay-per-use (Extra Call Option): Per million calls
Note 1: Starts once the number of API calls in a month period exceeds the number of calls allocated by the Plan.
Note 2: Billed/ invoiced at monthly intervals
- Service start date and service end date
 - Same as the Pro Plan.

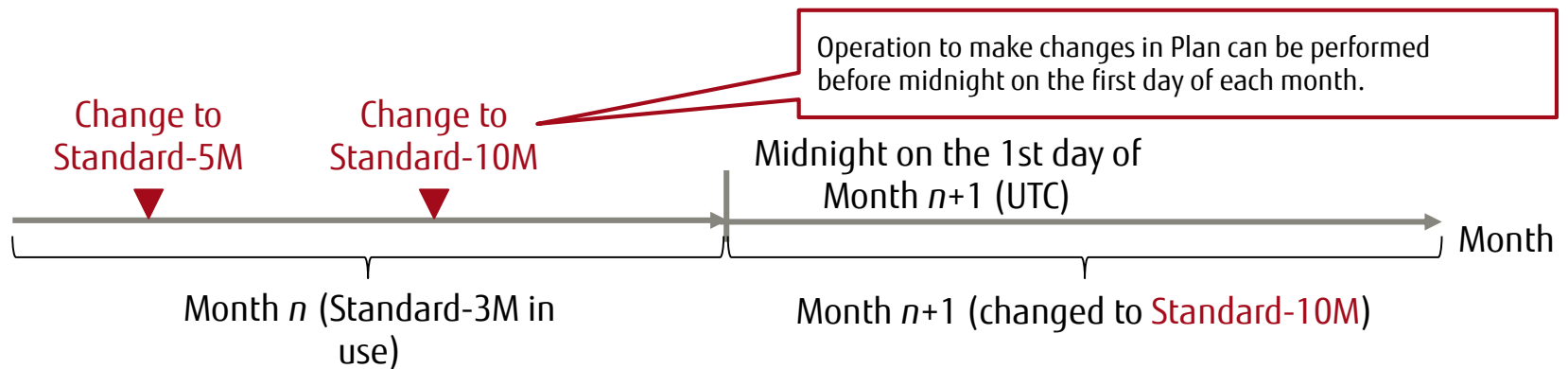
Example:



- The Customer may change their Plan to better suit their situation, such as the number of API calls and function usage.
 - The Customer can continue to use the same Organization, Environment, and registered API Proxies after changing the Plan.
 - There is no service down time (unable to log on to the service) while changing Plan.

■ How to Change Plans

- Plans can be changed via the "Service In Use" of the PaaS portal.
- The Customer will be billed for the Plan current at midnight (00:00) on the first day of each month (UTC).



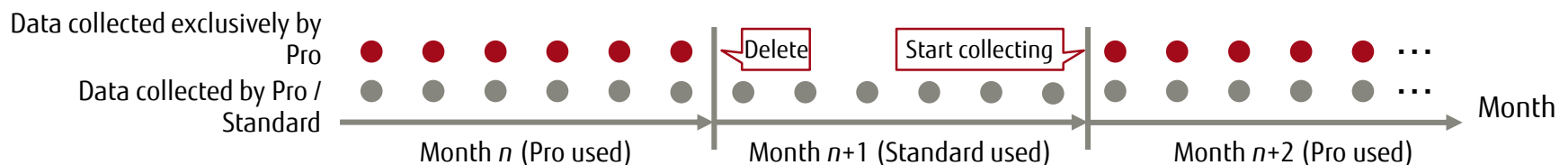
■ How to Change Plans

- Contact the Help Desk to change Plans from Pro to Standard or Standard to Pro. The Help Desk will advise the Customer on how to change plans.
For details, refer to the FAQ published on the K5 website.
- The timing of the notification of Plan change will impact when the change takes effect.
 - If notified on or before the 20th: Effective from the following month
 - If notified between the 21st and the end of the month: Effective from the month after the next month

■ Notes on Changing Plans

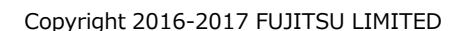
■ Analytics Service

- When changing from the Pro to Standard Plan, data collected exclusively via the Pro Plan will be deleted. Therefore, the Customer will no longer be able to use the Analytics patterns provided exclusively via the Pro Plan.
- When changing from the Standard to Pro Plan, data collected exclusively by the Pro Plan will start accumulating. Therefore, from the month in which the Pro Plan begins, the Customer can start using the Analytics patterns provided exclusively via the Pro Plan.



■ Billing









- Example: The following sample shows the Plan changed to Standard during the second month of the Pro billing cycle (B) (effective from the next month).



- Refer to the Service Description on FUJITSU Cloud Service K5 Website to confirm the regions in which this service is offered.
- The time required from application to start of service is as follows:
 - Within three business days from completing the application via the service settings application screen on the K5 PaaS Portal.










APIM: Reference: Policy - Traffic Management

API traffic processing (flow control, caching, etc.)








Policy	Description
 Quota	Uses the Quota policy to configure the number of request messages that an API proxy allows over a period of time; such as a minute, hour, day, week, or month
 Spike Arrest	Throttles the number of requests generated per second e.g. If set to allow 30 requests every minute(30pm) then 1 request will be allowed in 2 seconds. If it receives 2 requests within 2 seconds, then the 2nd request will be denied.
 Concurrent Rate Limit	Throttles inbound concurrent connections from your API proxies running on Apigee Edge to your backend services
 Response Cache	Caches the response from a backend resource
 Lookup Cache	Retrieves the data cached by Populate Cache
 Populate Cache	Caches data such as session IDs, authorization values, etc.
 Invalidate Cache	Deletes cached data specified in the conditions
 Reset Quota	Allows resetting of the no. of requests counted by the Quota policy based on specific variables

APIM: Reference: Policy - Data Processing








API data processing (format change, message modification, etc.)

Policy	Description
 JSON to XML	Converts messages from JSON format to XML format
 XML to JSON	Converts messages from XML format to JSON format
 Raise Fault	Generates a custom message in response to a status code (error condition)
 XSL Transform	Transforms XML to another format, such as HTML, plain text or other format
 SOAP Message Validation	Validates a message against an XSD schema or WSDL definition and rejects the message if it does not conform
 Assign Message	Creates or modifies an HTTP request or response messages (during an API proxy flow)
 Extract Variables	Extracts information from a request or response and sets a variable (with the specified message content)
 Access Entity	Retrieves the entity profiles of developers, apps, API products, etc. and places these in a variable
 Key Value Map Operations	Key / Value pairs can be stored, retrieved and deleted using PUT, GET, DELETE





API security restrictions (Authorization, Vulnerability Management, etc.)

Policy	Description
 Basic Authentication	Sets Basic Authentication (Base64 encoding and decoding)
 XML Threat Protection	Addresses XML vulnerabilities and minimizes attacks on your API
 JSON Threat Protection	Addresses JSON vulnerabilities and minimizes attacks on your API
 Regular Expression Protection	Rejects requests that include regular expressions
 OAuth v2.0	Allows you to configure (generate and verify access tokens, etc.) OAuth v2.0 endpoints
 Get OAuth v2.0 Info	Retrieves the attributes of OAuth v2.0's access tokens and authorization codes, etc.
 Set OAuth v2.0 Info	Adds or updates custom attributes associated with OAuth v2.0 access tokens

API security restrictions (Authorization, Vulnerability Management, etc.)

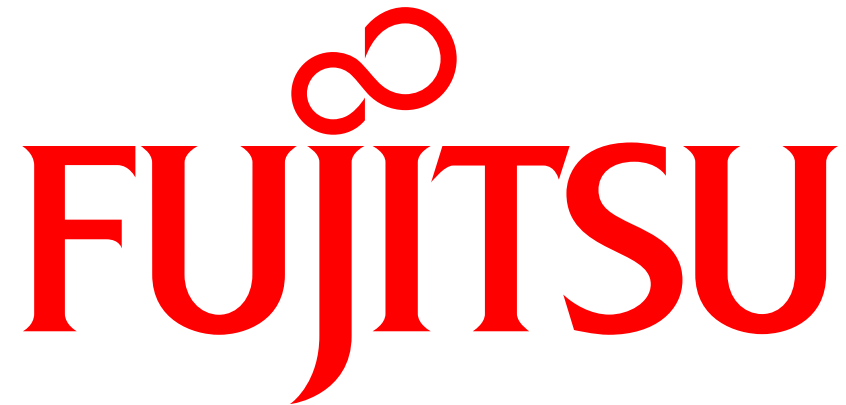
Policy	Description
 OAuth v1.0a	Allows you to configure (generate and verify access tokens, etc.) OAuth v1.0a endpoints
 Get OAuth v1.0a Info	Retrieves the attributes of OAuth v1.0a `s access tokens, authorization codes, etc.
 Verify API Key	Allows you to configure the API Key that allows access
 Access Control	Allows or denies access to your APIs based on IP address
 LDAP	Allows you to configure LDAP
 Generate SAML Assertion	Attaches SAML assertions to outbound XML requests
 Validate SAML Assertion	Validates SAML assertions that are attached to inbound SOAP requests and rejects them if they are invalid

Execute scripts and collect data in a message.

Policy	Description
 JavaScript	Implements custom behaviors using JavaScript
 Service Callout	Allows calls to an external service (from your API proxy flow)
 Statistics Collector	Collects statistics for data in a message, such as product ID, price, target URL, etc.
 Message Logging	Logs custom messages to a local disk or to syslog

Display traffic volumes, response times, no. of errors, etc.

Policy	Description
Proxy Performance	Shows API traffic volumes and average processing times
Target Performance	Shows traffic volume patterns, success and failure of requests, response times, success and failure of responses, and payload size of backend services
Cache Performance	Shows cache hits, cache hit rates and response times
Latency Analytics	Shows the response times for API and backend services
Error Analytics	Shows error data (no. of errors, status codes, etc.) for API proxies and targets
Developer Engagement	Shows the no. of your registered app developers and their access status, traffic generated by them and errors
Traffic Composition	Gives a quick glance at the top 10 traffic patterns of APIs, products, developers, and applications
Business Transactions	Shows traffic volumes, response times, error rates, and amount of data exchanged (aggregate of requests and responses) based on a request generated by a specific URI
Devices	Provides information on the devices (platforms, agents, device types, OS, etc.) being used to access your APIs
Reports	Allows free selection of the matrix and dimensions (time) and generates charts



shaping tomorrow with you