Headless
& API date

SESSIONE TECH

API Gateway per garantire la governance di un progetto di trasformazione digitale headless

DENIS SIGNORETTO, INTESYS IT ARCHITECT E SENIOR PROJECT MANAGER

Intesys Liferay

Headless
& API date

SESSIONE TECH

Headless & API date
Edizione 2019

un anno fa ...

API as a Product

Developers

What are their needs?

API Architect

- Comprende i **bisogni operativi**
- Introduce, fa comprendere e utilizzare gli **strumenti di specifica**
- Assicura **tecnicamente qualità**, **documentazione**, **esempi**
- Garantisce **uniformità** e **adesione** agli **standard**
- Garantisce protocolli di **sicurezza**
- **Monitoring** ai fini delle **performance** e **disponibilità** delle API

API Product Manager

- Comprende i **bisogni degli stakeholder e promuove l'adozione delle API**
- Assicura strumenti per garantire **documentazione**, **facilità** di **utilizzo** e **integrazione**
- Promuove l'adozione delle API nel sistema azienda
- **Tiene sotto controllo e massimizza il ROI (Return of Investment)**
- API Analytics, **valuta KPI delle API**

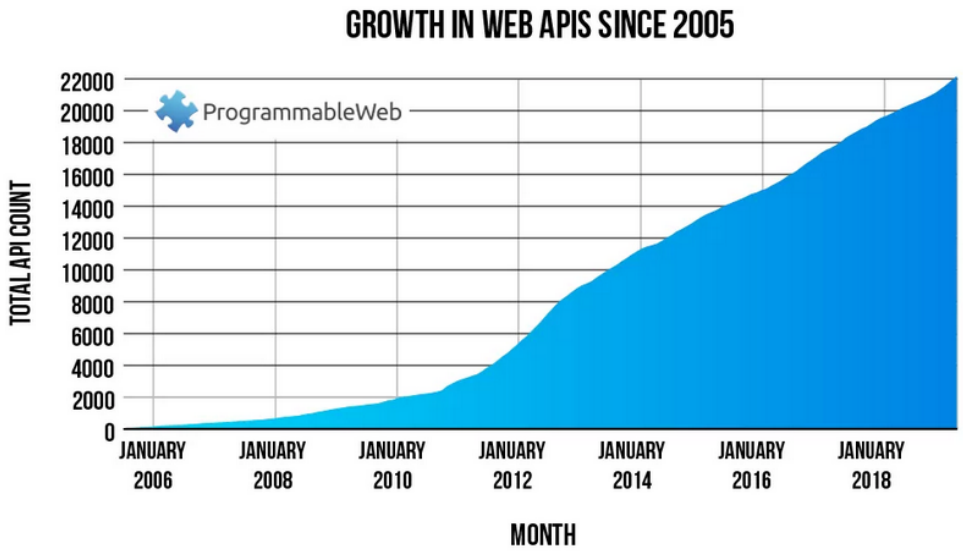
Headless
& API date

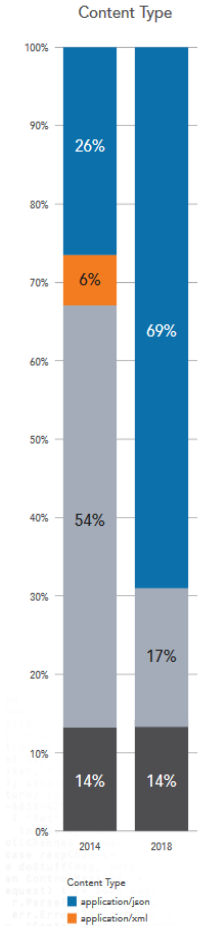
SESSIONE TECH

Perché è sempre più importante dotarsi della API Governance?

Intesys.it

Crescita delle API





RISE OF API TRAFFIC

In 2014, Akamai researchers asked a relatively simple question: How much of the HTTPS traffic on our network is API compared to HTML? In other words, we wanted to know what portion of the traffic we see, and by extension the Internet as a whole, is content formatted for machines—some of which is triggered by human activity, and some of which is automated data exchanged behind the scenes without direct human interaction. The assumption had been that API traffic was a small portion of our traffic, but an informal analysis of our statistics revealed that API traffic accounted for 47% of all layout and data traffic we saw.

This was a major revelation—one that fueled a multitude of conversations in the past four years. We recently decided it was time to look at API traffic again, and the results were once again surprising: The traffic classified as APIs currently accounts for 83% of all hits, while HTML traffic has fallen to just 17%.

This shift in traffic patterns has significant ramifications in the security industry. Many, if not most, controls that have been historically used to protect the servers and systems that are the origin of traffic are focused


APIs will become the
#1 Attack vector by 2022
Gartner®

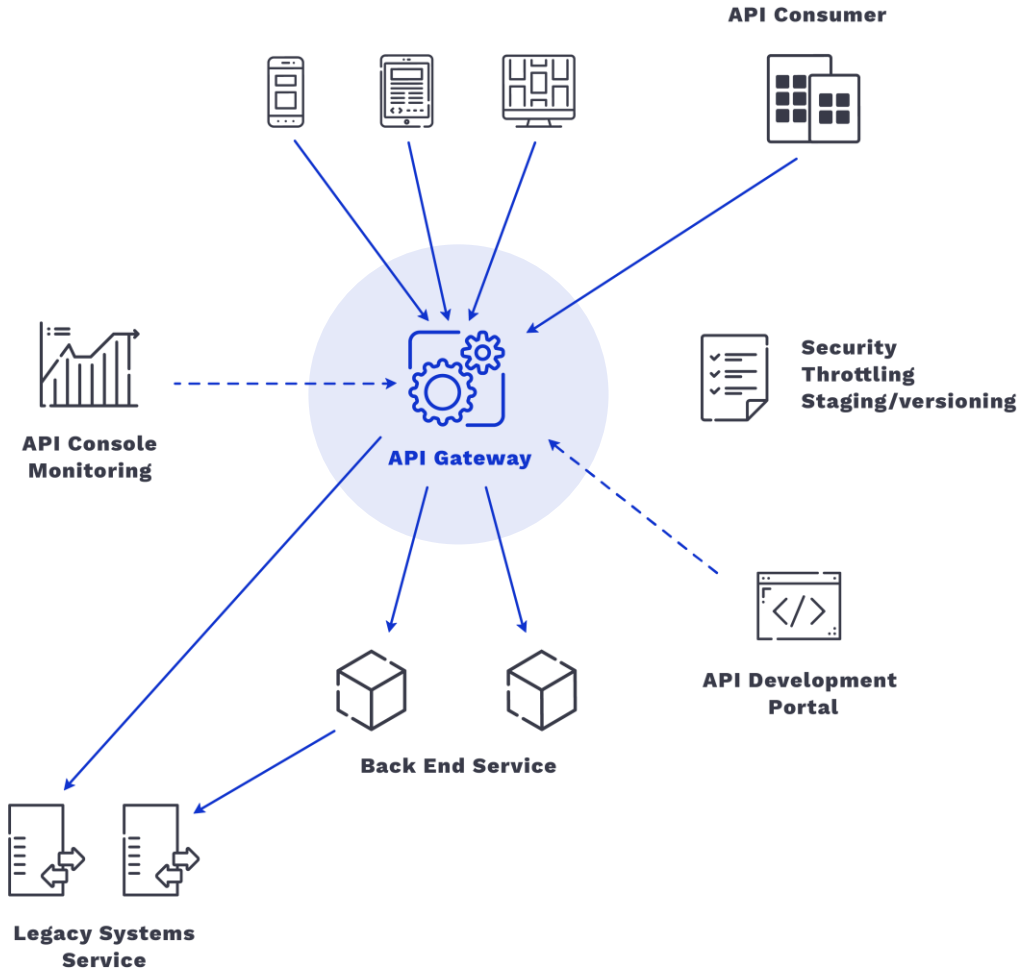
Headless
& API date

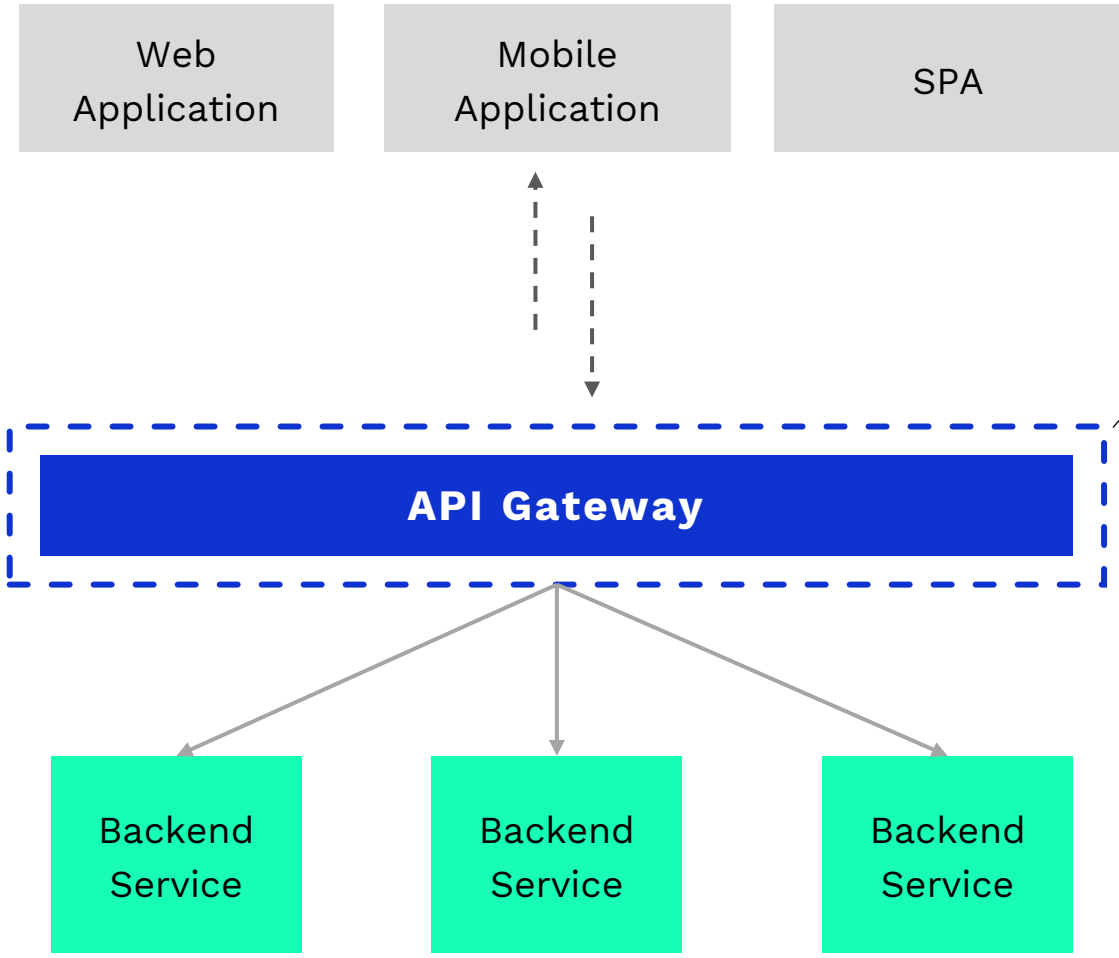
SESSIONE TECH

Quali strumenti a supporto della API Governance?

Strumenti di API Management

- **API Gateway**
  - Security & Performance & Audit
- **API Analytics**
- **API Portal**
- **API Lifecycle Management**
- **API Monetization (Billing)**





Principali funzioni dell'API Gateway

Security
- Transport Security
- Authentication and Authorization
- Security attacks prevention

Performance
- Caching
- Routing & Balancing
- Throttling
- Quota

Altro ancora...
- Event Logging & Tracing
- Orchestration
- Mediation & Transformation
- ...

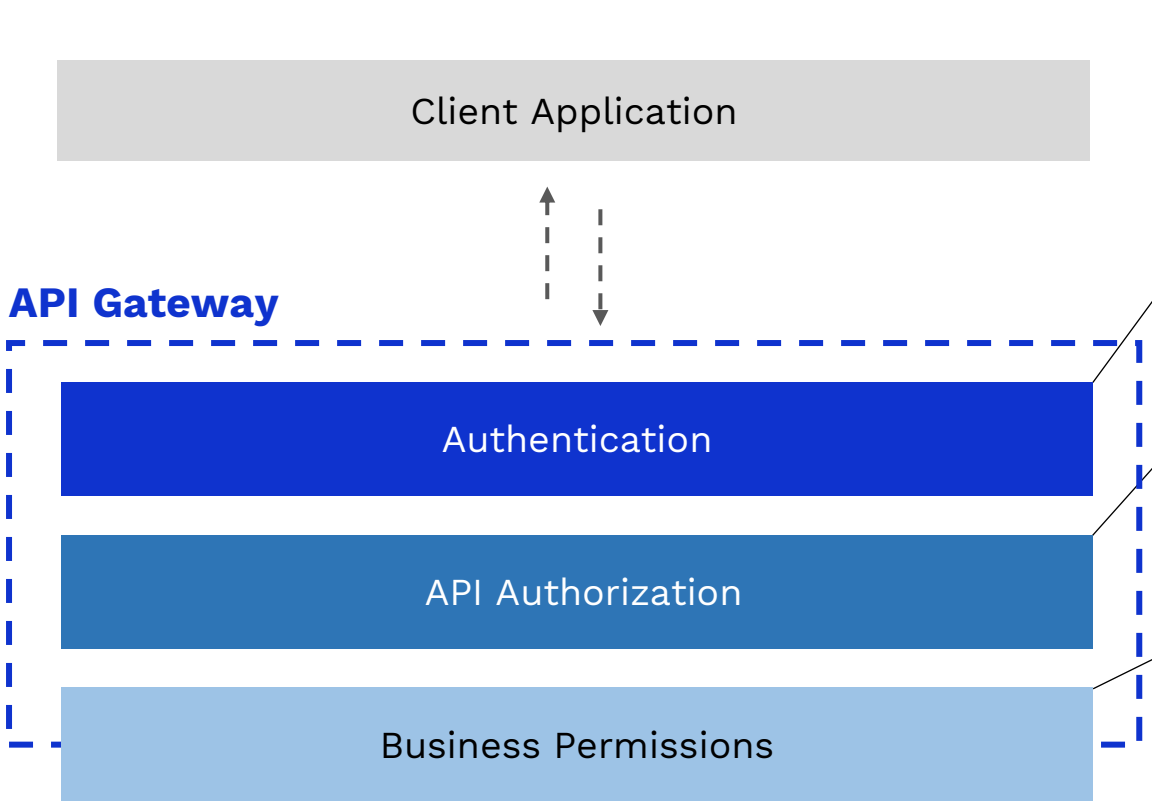
Headless
& API date

SESSIONE TECH

Security
API Gateway

Intesys.it

API Authentication & Authorization



Come autentico una richiesta?
Quali protocolli di sicurezza adottare?

Il client è autorizzato a usare l'API?

L'utente loggato sul client è autorizzato
ad accedere alla API/risorsa?

L'utente accede solo alle risorse
e ai dati a cui è stato autorizzato?

La risorsa può subire
l'azione richiesta dalla API?

API Authentication & Authorization

Autenticazione delle API: Bearer Tokens & API Key

- Access Token: JWT Token vs (Opaque)
- API Key

I protocolli standard più largamente diffusi
per l'autenticazione e autorizzazione delle API

- **OAuth 2.0 / OAuth 2.1**
- **OpenId Connect**
- **SAML 2**

- Oppure SSO Custom

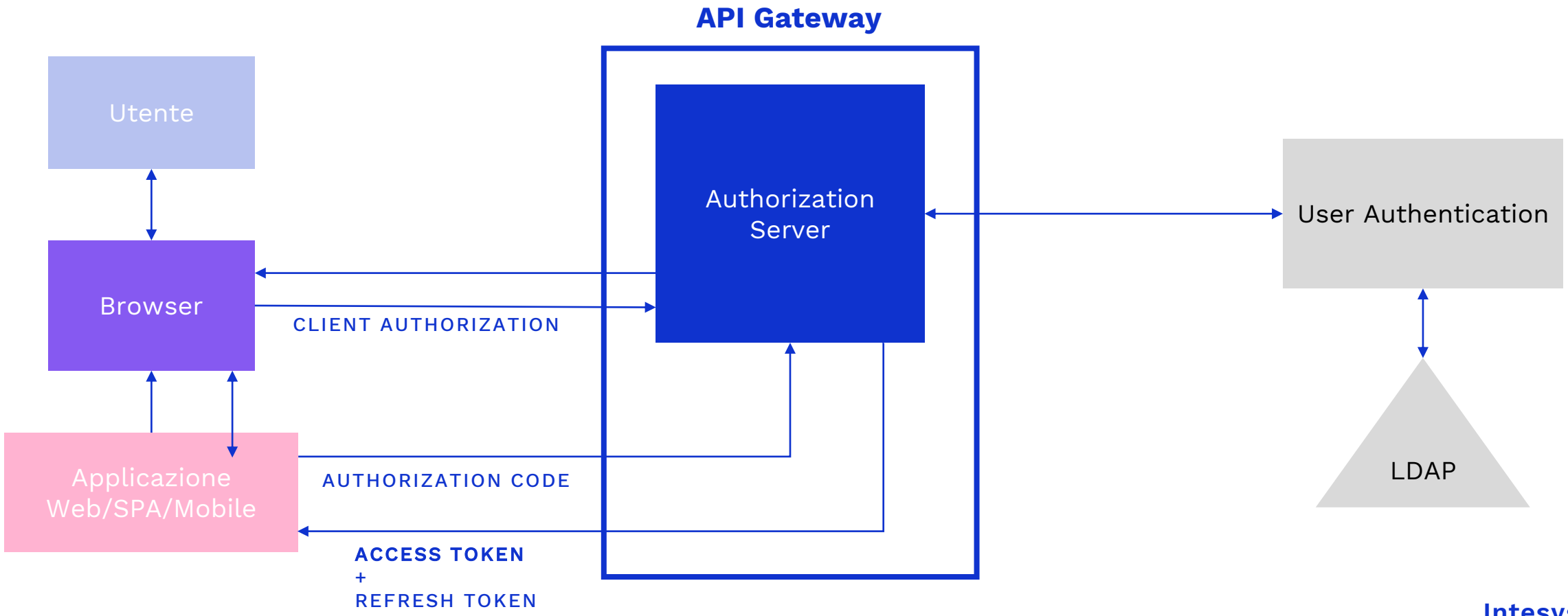
RFC6750 - Bearer Tokens
Request Header Field
Form-Encoded Body Parameter
URI Query Parameter

RFC6749 - OAuth2 Core
Authorization Code
Implicit
Password
Client Credentials

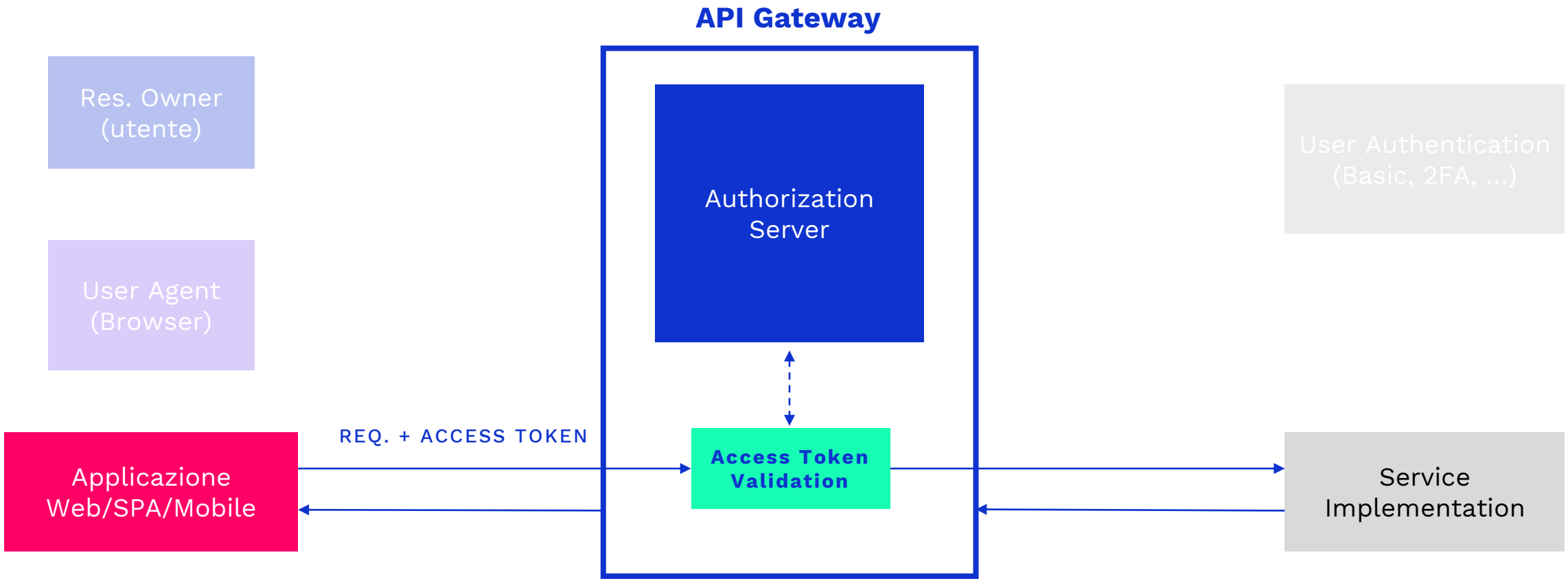
FLUSSI DI AUTENTICAZIONE

Come scambiare, in modo sicuro, un token di autenticazione?

OAuth2: Authorization Code Grant



Authenticated API call



Flussi dei protocolli standard

- Le **credenziali** utente vengono scambiate solo tra **browser e authorization server**
  - Non dobbiamo delegare a chi realizza l'applicazione aspetti di sicurezza
- I protocolli standard:
  - **coprono già una serie di possibili attacchi** e sono già implementati dagli API Gateway
  - coprono già **funzionalità quali refresh, rotazione** e **invalidazione** dei token

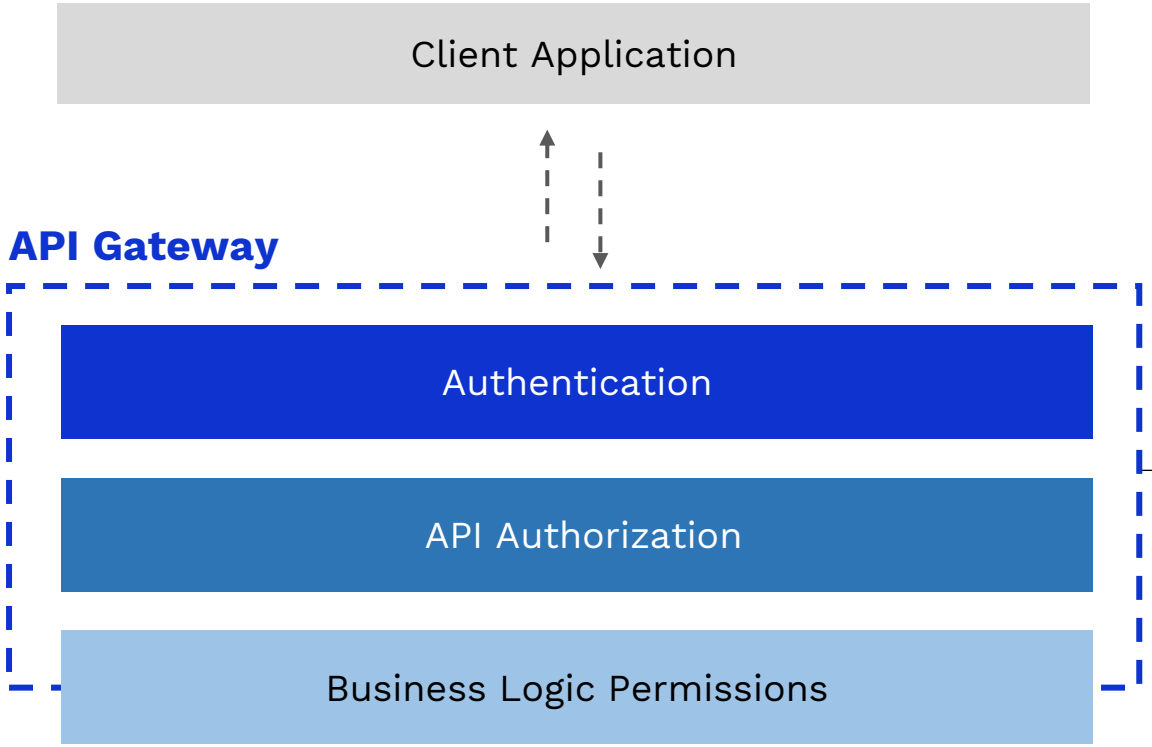
Headless
& API date

SESSIONE TECH

API Gateway Security: API Authorization

Intesys.it

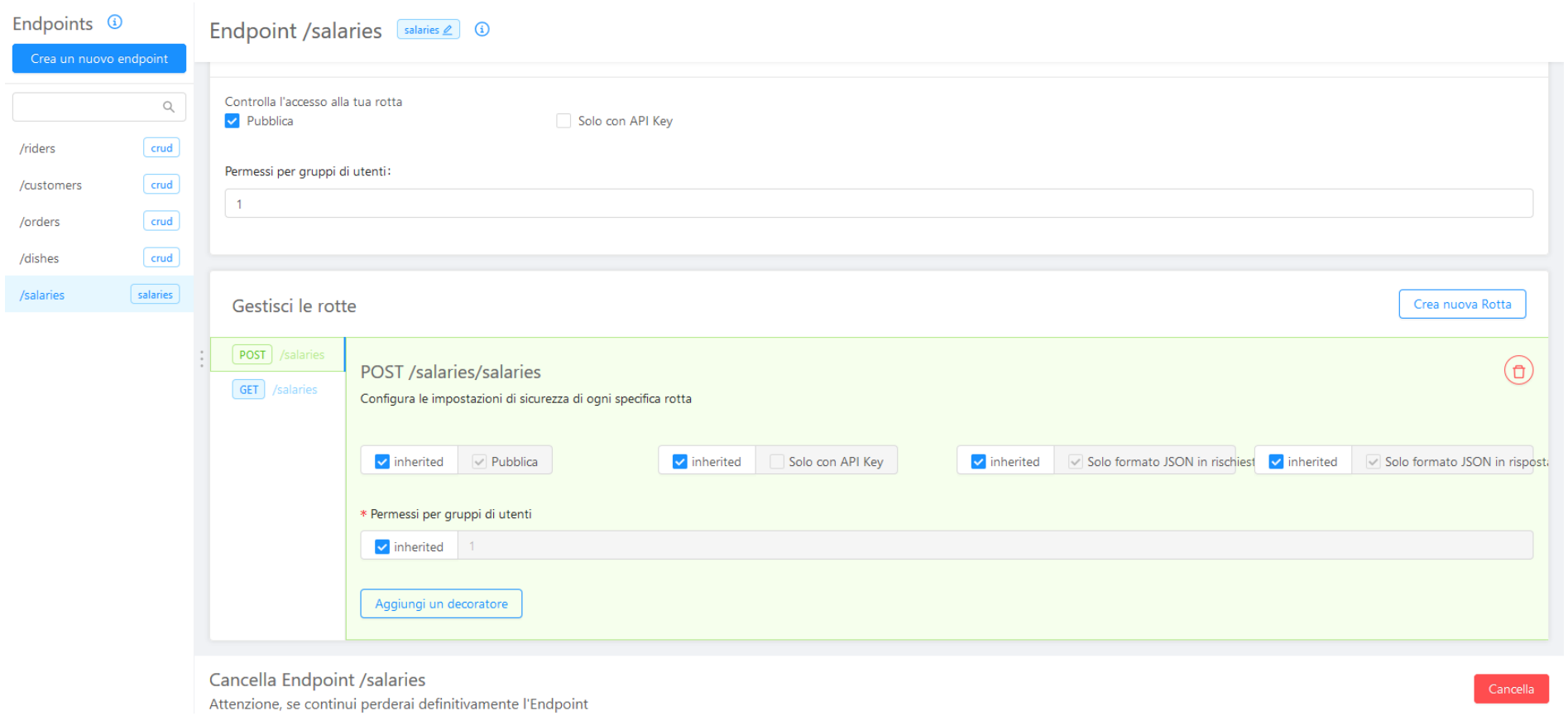
API Authentication & Authorization

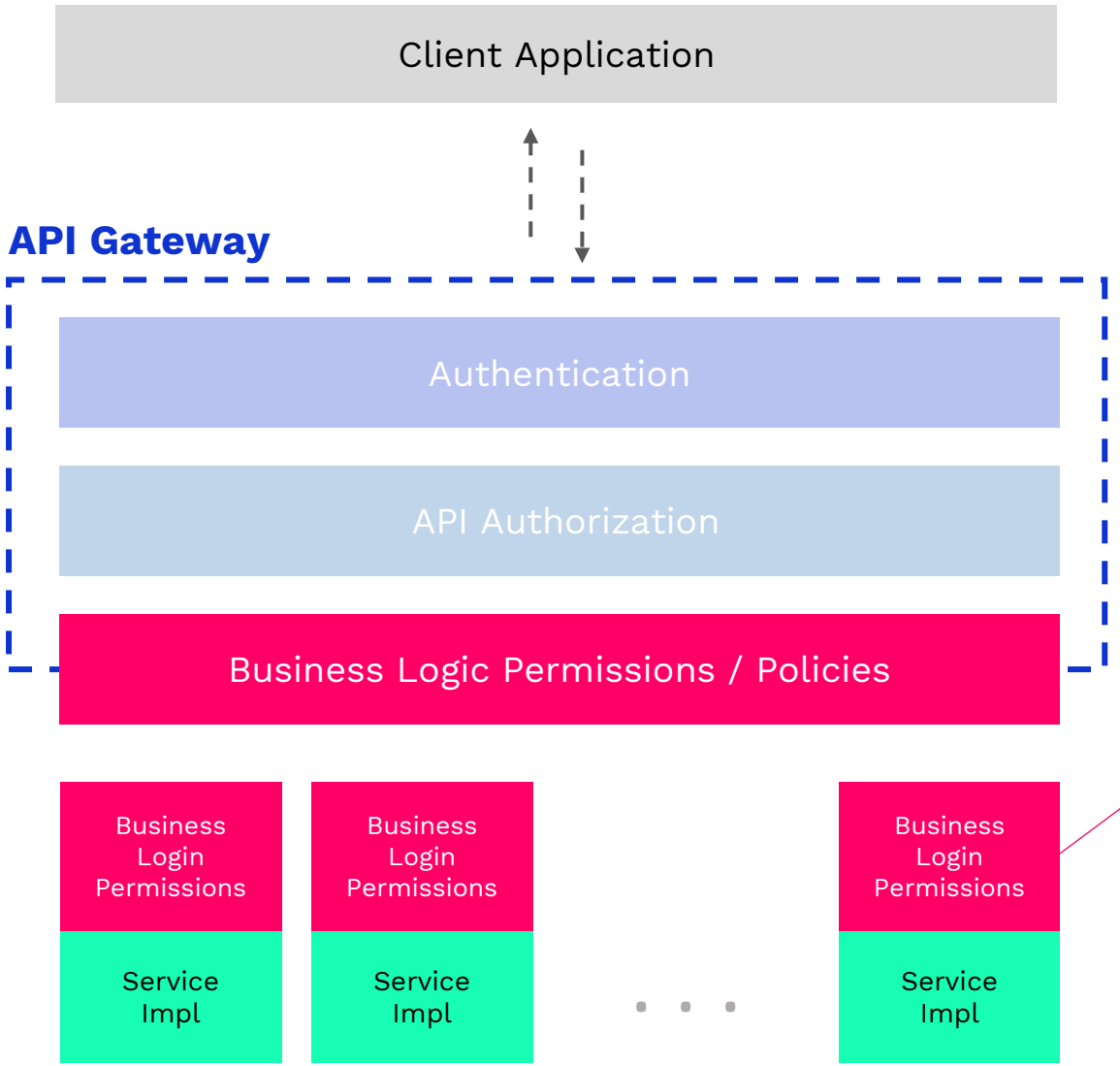


Il client è autorizzato a usare l'API?

L'utente loggato sul client è autorizzato ad accedere alla API/risorsa?

API Gateway & Resource Permissions





L'API rispetto all'utente torna tutti e soli i dati che questi può vedere?

La risorsa può subire l'azione richiesta dalla API?

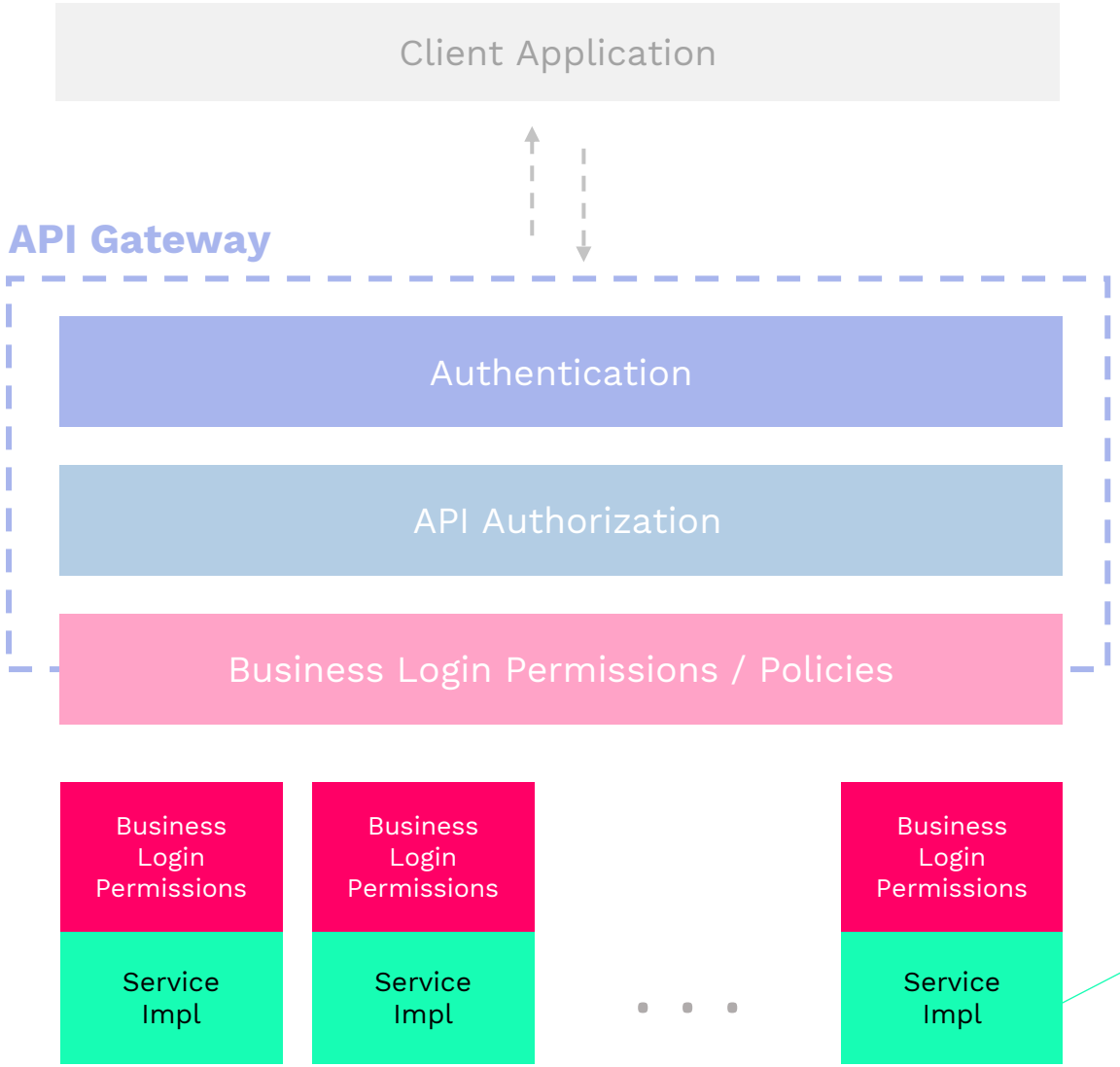
Headless
& API date

SESSIONE TECH

Security

… non basta un API Gateway

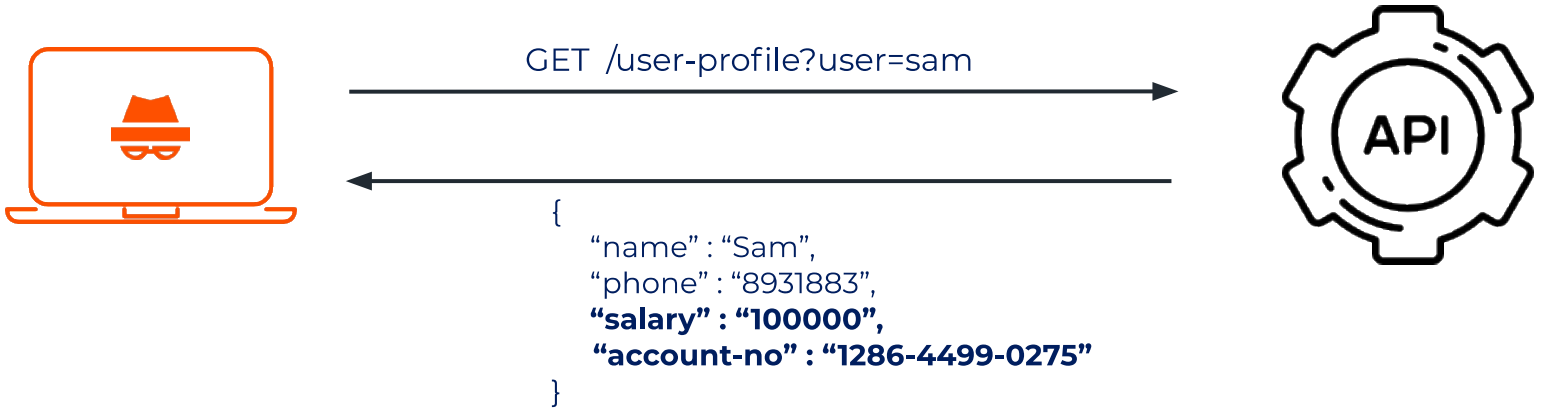
Intesys.it



L’API è implementata secondo linee guida per un codice sicuro?

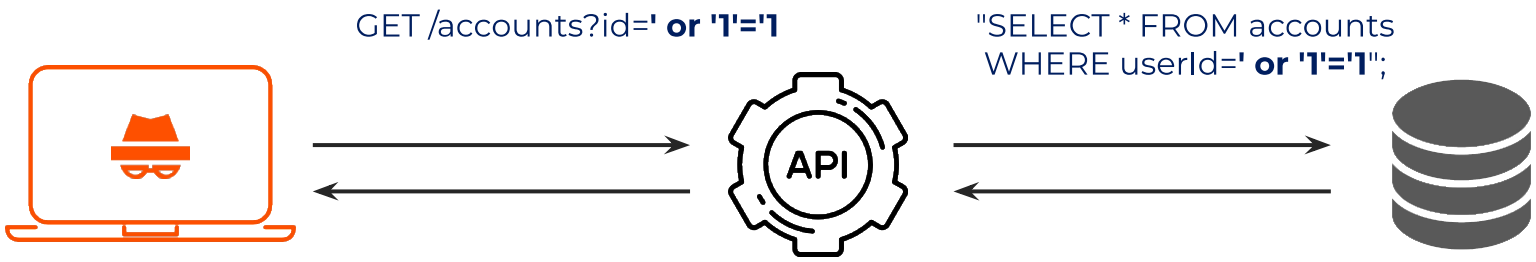
OSWAP ha censito vari tipi di attacco alle API

Ad esempio: «Excessive Data Exposure»



OSWAP ha censito vari tipi di attacco alle API

Ad esempio: «API Injection»



[{“name” : “Sam”, “phone” : “78144753”, “credit” : 500000},
{“name” : “Mary”, “phone” : “43211234”, “credit” : 1000}]

OWASP API Security Project

Watch 97 Star 570

Main | Acknowledgments | Join | News | RoadMap | Translations

What is API Security?

A foundational element of innovation in today's app-driven world is the API. From banks, retail and transportation to IoT, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, SaaS and web applications and can be found in customer-facing, partner-facing and internal applications. By nature, APIs expose application logic and sensitive data such as Personally Identifiable Information (PII) and because of this have increasingly become a target for attackers. Without secure APIs, rapid innovation would be impossible.

API Security focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of Application Programming Interfaces (APIs).

API Security Top 10 2019

Here is a sneak peek of the 2019 version:

- **API1:2019 Broken Object Level Authorization**

  APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user.

- **API2:2019 Broken User Authentication**

  Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising system's ability to identify the client/user, compromises API security overall.

- **API3:2019 Excessive Data Exposure**

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

API Security Information

Builders | Breakers | Defenders

Downloads or Social Links

API Security Top 10 2019 (PDF)
GraphQL Cheat Sheet
Mailing List

Code Repository

OWASP Cheat Sheet Series
Introduction
Index Alphabetical
Index ASVS
Index Proactive Controls
Cheatsheets
AJAX Security
Abuse Case
Access Control
Attack Surface Analysis
Authentication
Authorization Testing Automation
Bean Validation
C-Based Toolchain Hardening
Choosing and Using Security Questions
Clickjacking Defense
Content Security Policy
Credential Stuffing Prevention
Cross-Site Request Forgery Prevention
Cross Site Scripting Prevention
Cryptographic Storage
DOM based XSS Prevention
Database Security
Denial of Service

GraphQL Cheat Sheet

Introduction

GraphQL is an open source query language originally developed by Facebook that can be used to build APIs as an alternative to REST and SOAP. It has gained popularity since its inception in 2012 because of the native flexibility it offers to those building and calling the API. There are GraphQL servers and clients implemented in various languages. Many companies use GraphQL including GitHub, Credit Karma, Intuit, and PayPal.

This Cheat Sheet provides guidance on the various areas that need to be considered when working with GraphQL:

- Apply proper input validation checks on all incoming data.
- Expensive queries will lead to Denial of Service (DoS), so add checks to limit or prevent queries that are too expensive.
- Ensure that the API has proper access control checks.
- Disable insecure default configurations (*e.g.* introspection, GraphiQL, excessive errors, etc.).

Common Attacks

- Injection - this usually includes but is not limited to:
  - SQL and NoSQL injection
  - OS Command injection
  - SSRF and CRLF injection/Request Smuggling
- DoS (Denial of Service)

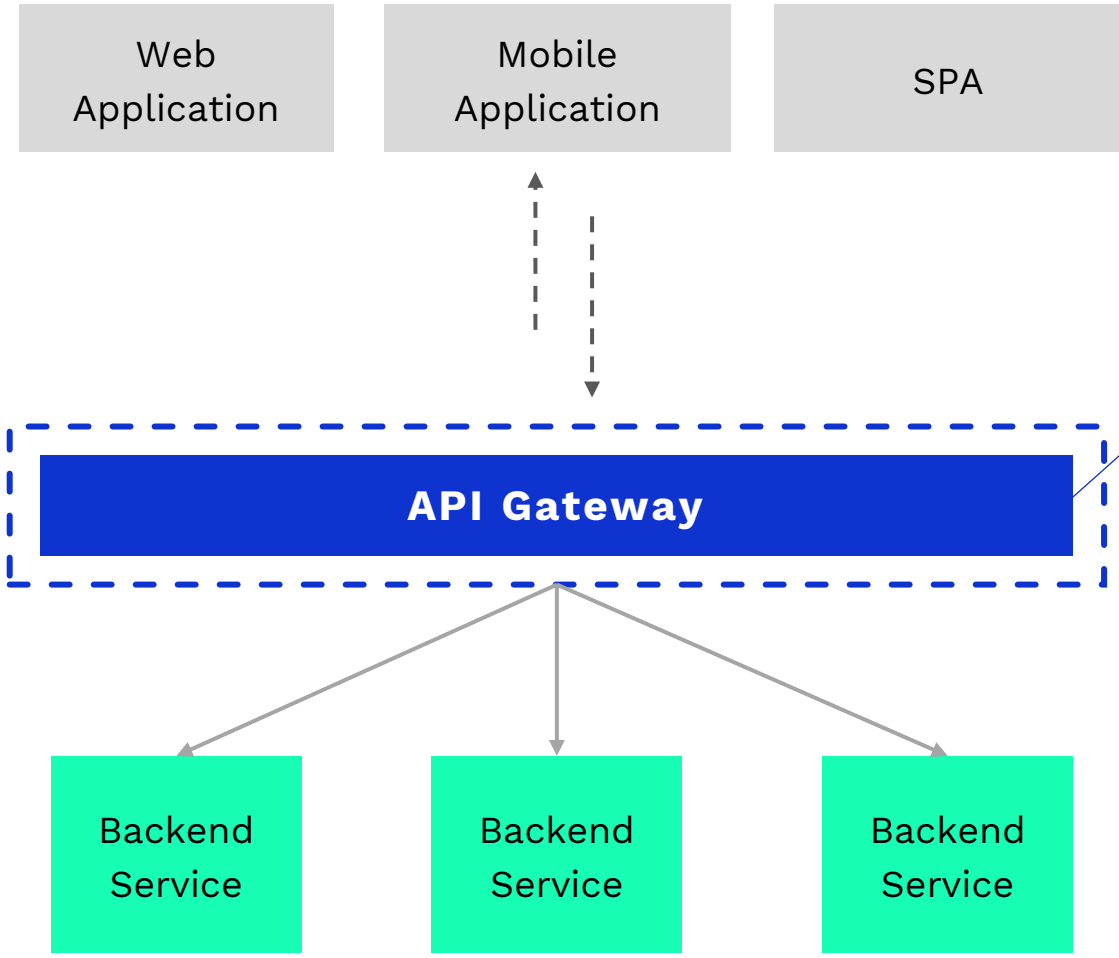
Table of contents
Introduction
Common Attacks
Best Practices and Recommendations
Input Validation
General Practices
Injection Prevention
Process Validation
DoS Prevention
Query Limiting (Depth & Amount)
Timeouts
Query Cost Analysis
Rate Limiting
Server-side Batching and Caching
System Resource Management
Access Control
General Data Access
Query Access (Data Fetching)
Mutation Access (Data Manipulation)
Batching Attacks
Mitigating Batching Attacks
Secure Configurations
Introspection + GraphiQL

Headless
& API date

SESSIONE TECH

API Gateway Performance & Audit

Intesys.it



Principali funzioni dell'API Gateway

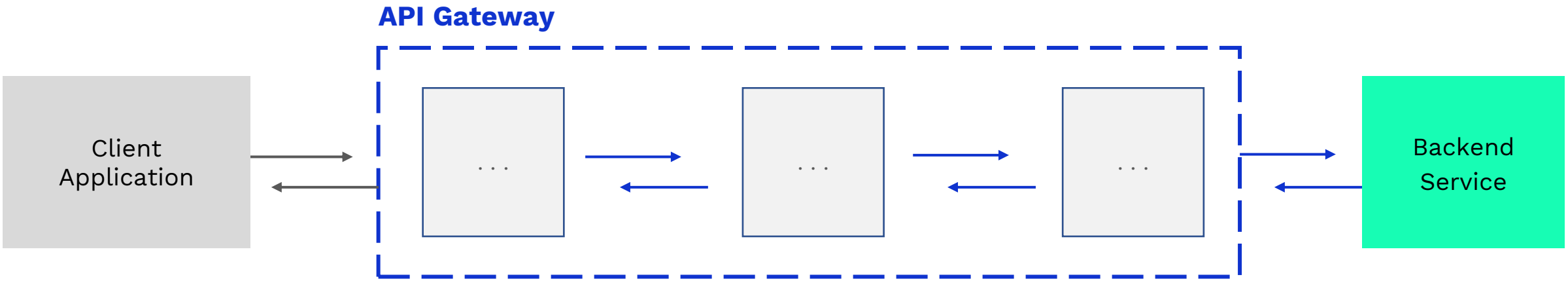
Performance

- Caching
- Routing & Balancing
- Throttling
- Quota

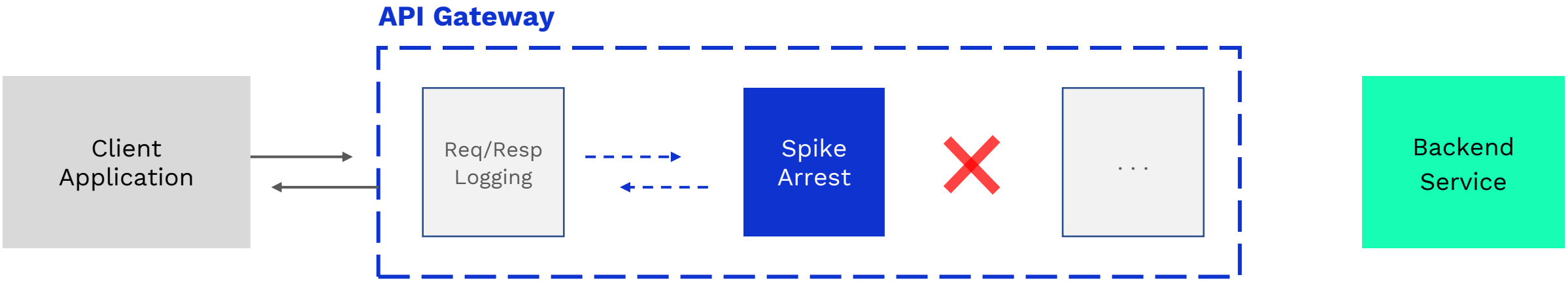
Altro ancora...

- Event Logging & Tracing
- Mediation & Transformation
- ...

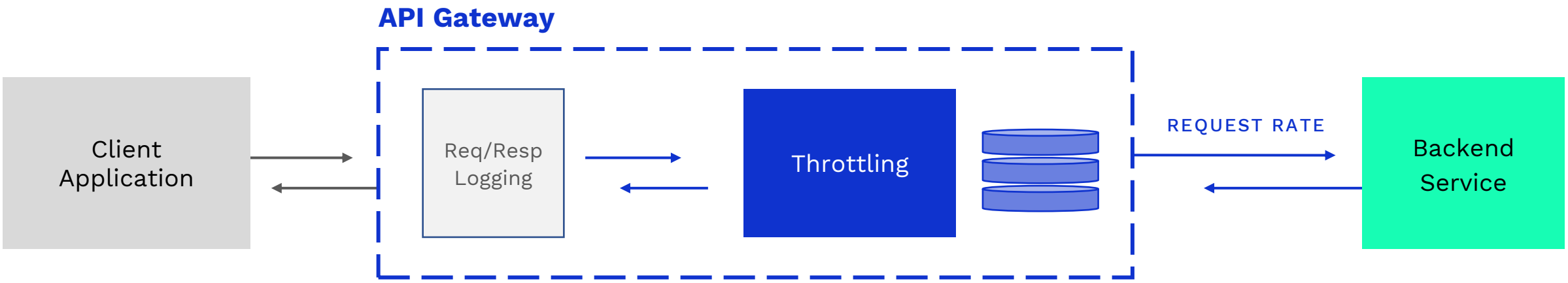
API Gateway performance



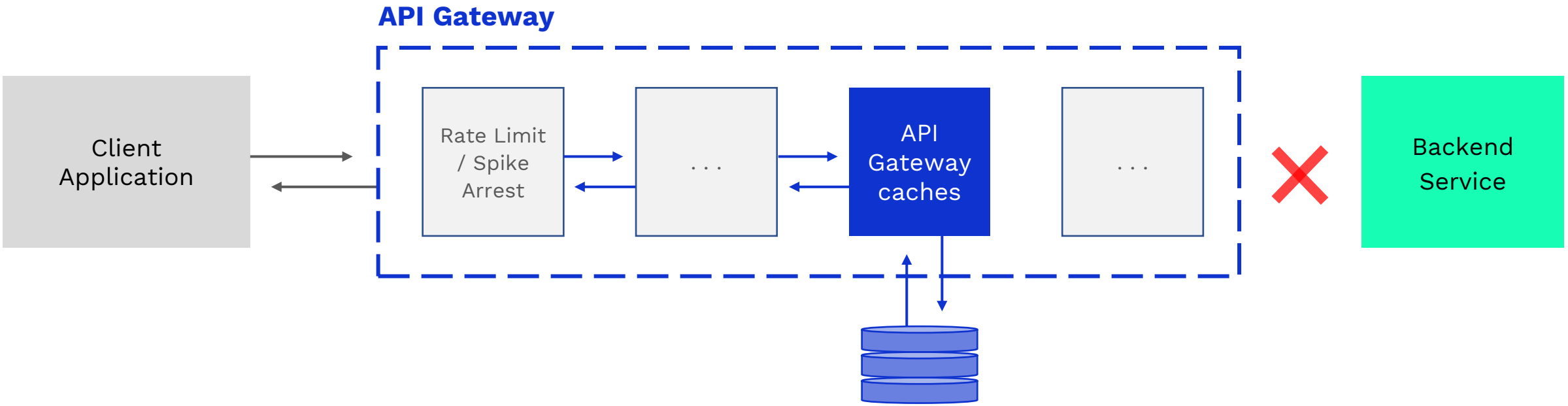
API Gateway performance: burst/spike arrest



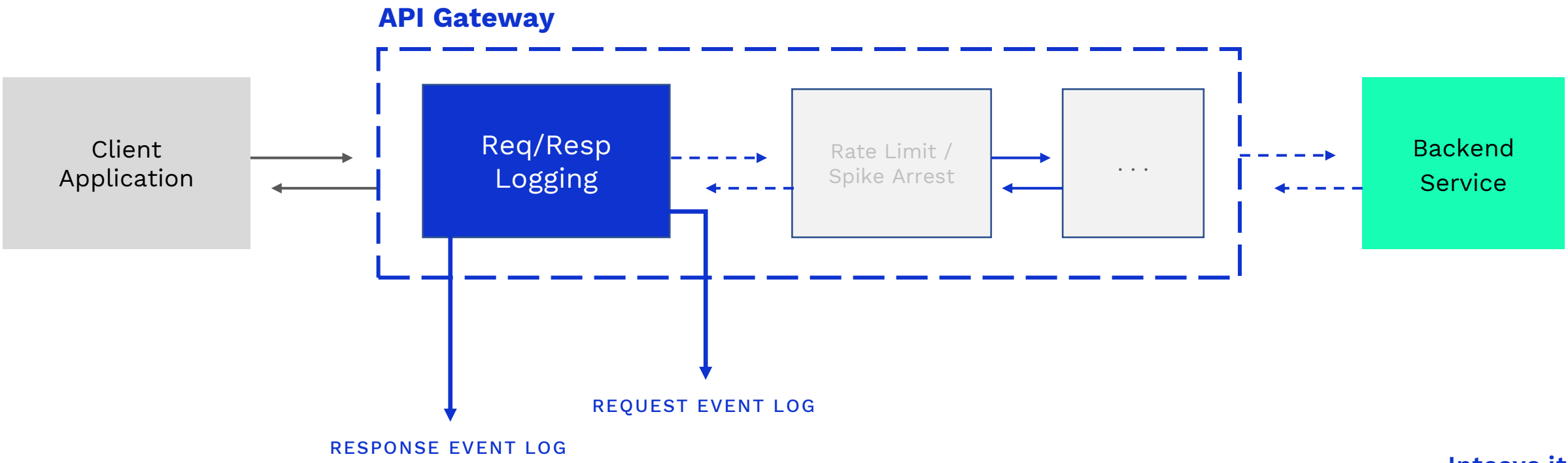
API Gateway performance: throttling & fixed rate



API Gateway performance: caching



API Gateway performance: event logging



Conclusioni

API Gateway e governance

- API Gateway è uno strumento che copre diversi **bisogni di governance operativi**
- **Centralizza la gestione della sicurezza** e adotta **protocolli standard**
    - (!) Da solo non è sufficiente a garantire la sicurezza
- Gioca un ruolo importante a garanzia di **performance** e della **resilienza**
    - Throttling, timeout, quota, aiutano nel design di applicazioni concepite già con logiche di fallback
- Per una **governance a tutto tondo**, serve affiancarlo con altri strumenti di API Management tra cui:
    - **API Portal**, **API Analytics**, **API Lifecycle Management**

Headless
& API date

Grazie

Denis Signoretto

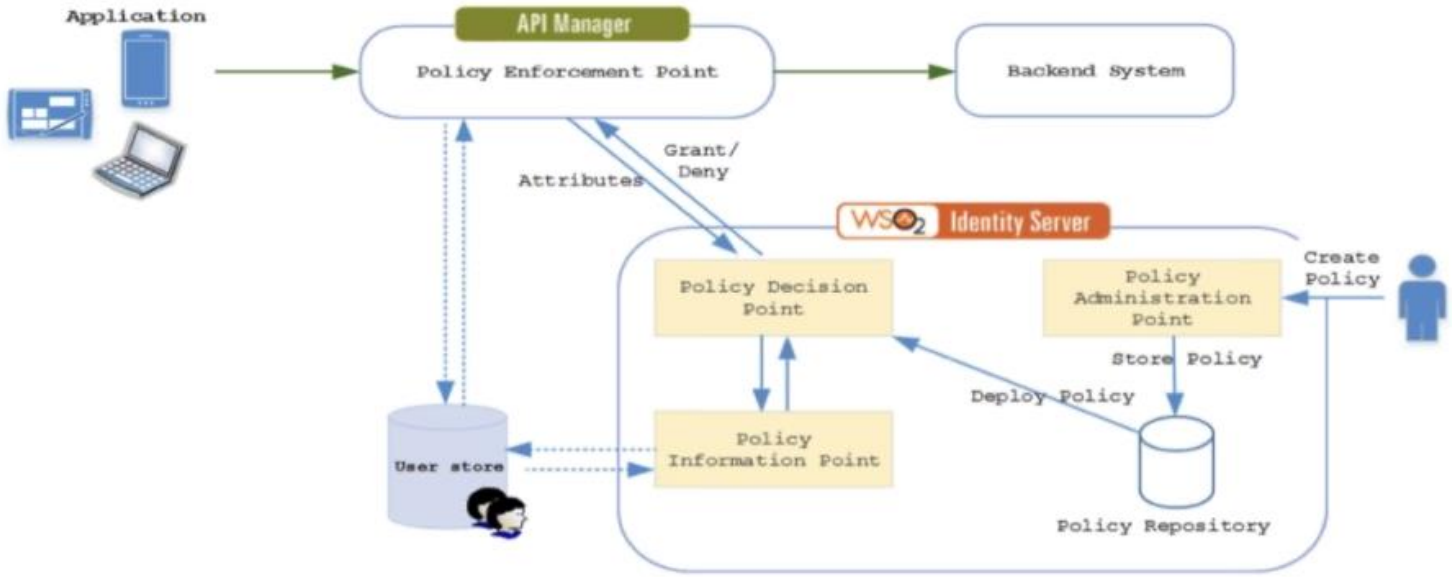
INTESYS IT ARCHITECT E SENIOR PROJECT MANAGER

Intesys Liferay

API Gateway & Policy

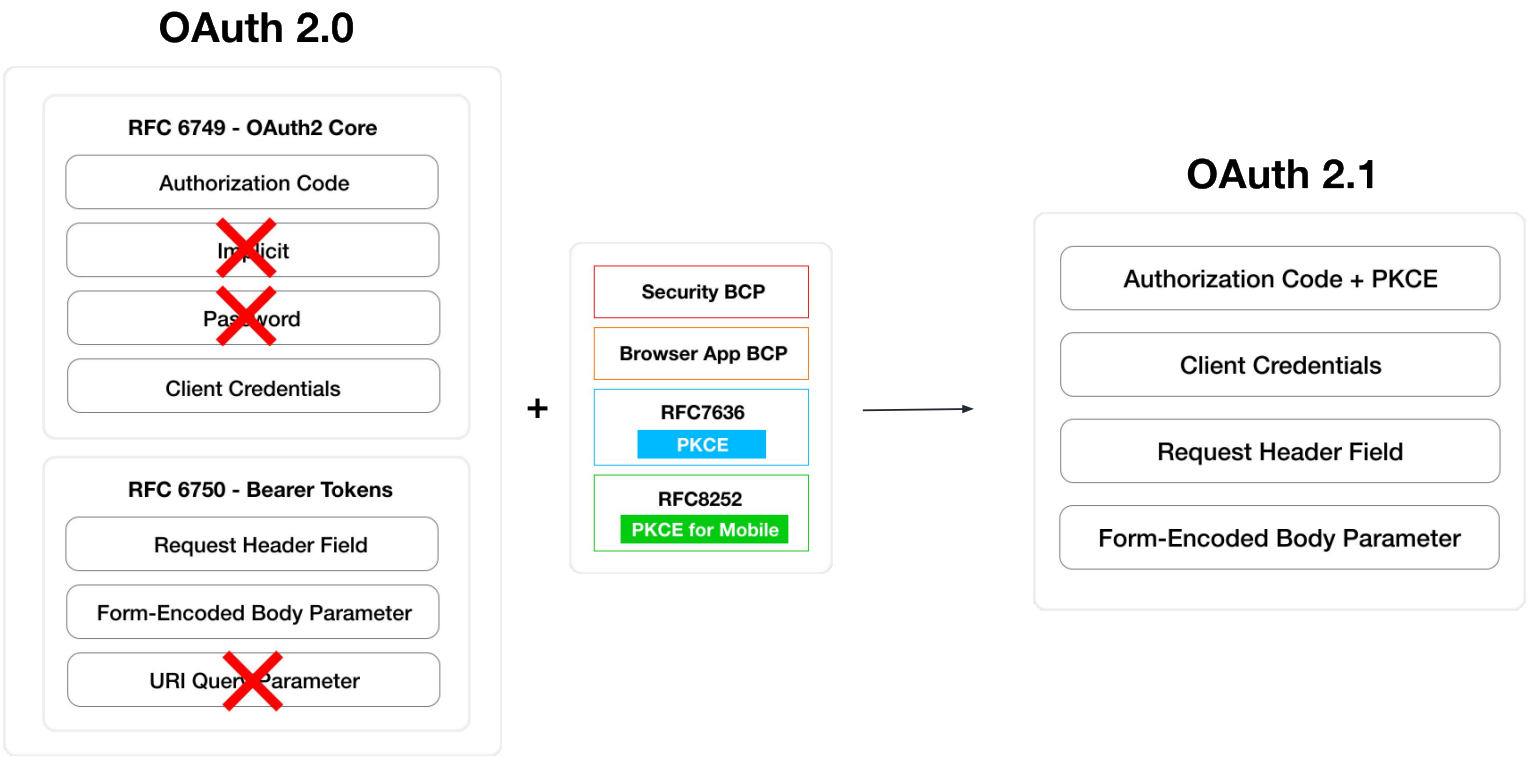
API XACML policy rules

Immagine



Flussi di autenticazione OAuth2 e OAuth2.1

OAuth2 sta evolvendo al passo con le nuove tipologie di applicazioni e req. di sicurezza



Headless
& API date

Grazie

Denis Signoretto

INTESYS IT ARCHITECT E SENIOR PROJECT MANAGER

Intesys Liferay

THE END!