

Lucida Architecture Overview.

ZAHID HOSSAIN | DIR ENTERPRISE ARCHITECTURE

FEBRUARY 2021

AGENDA

Context

Why are we doing this project? What are the expectations of our stakeholders?

Approach and Architecture Choices

How are we solving this problem?
What qualities will the solution will have to have to satisfy our stakeholders expectations?
Solution Patterns and technology choices
Business benefits

Appendix 1: Application Architecture

Component model & Interaction models
Key architecture decisions
Deployment diagrams

Appendix 2: Solution Capabilities and Technologies Behind Them

Micro Frontends
API Gateway
Standard-based and component level security mesh

Appendix 3: Lucida Phase 2 Project Roadmap

Key Question:

How do we please our stakeholders?

#2

"Customer satisfaction is low. Some clients are leaving MedImpact because our systems (used by clients) are not modern and user friendly.

Market and client expectations are changing faster and faster and we need stay ahead to meet their expectations.

I need to showcase a friction-free, holistic, modern, customer-friendly, industry leading client experience before the 2021 sales cycle."

▲ Modern unified and differentiating client experience

▲ Fast development (speed to market)

#3

"We have built and matured many IT assets and process automation over the years. They play important roles in servicing our clients and members.

I need to bring all these applications together and create a unified, modern UX for our clients without having to rewrite our backend systems.

The solution must be robust, delivered fast, and expected to be evolved fast (as market expectations change)

The solution must be available securely in the open internet.

We want to enhance our reputation as modern technology solution provider."

- ▲ Utilize existing assets and processes (where possible)
- ▲ Quality, adaptability, and maintainability
- ▲ System complexity must not be visible to the end user
- ▲ Speed, Speed!

#1

"It is difficult and time consuming to do business with MedImpact.

I jump through different applications to manage and monitor my Rx Plans.

The systems are outdated and do not speak my language.

It is not easy to help my members with their issues and questions."

- ▲ Client frustrations and disappointments
- ▲ Not living up to the expectations

Key Takeaways...

These are **not competing** use cases; they are rather **complementary** (three sides).

We must be able to support all these needs simultaneously to be successful

We must reimagine our processes, organization, and systems in the context of these new realities...

Solution Characteristics:

What qualities the solution must have to satisfy the stakeholder needs?

SOLUTION CHARACTERISTICS

Modern, Intuitive, Seamless, User-centric Experience

brings all relevant functions together seamlessly from the user perspective

#1

Composable and Autonomous

Composable at run-time. UX components and backend services are designed, built, deployed, and managed independently





#3

Standard-based Security and Accessibility

each component is secured independently and collectively as a security mesh





Interoperability – Standard-based Integration

Backend business services are accessible using standard protocols, secured, and managed uniformly across the enterprise.







Solution Building Blocks:

What solution patterns and technologies will enable these capabilities?

SOLUTION CHARACTERISTICS

PROTOCOL | TECHNOLOGY

Modern, Intuitive, Seamless, User-centric Experience

brings all relevant functions together seamlessly from the user perspective

NEW UX STANDARDS

Single Page Responsive Web App

Composable and Autonomous

Composable at run-time. UX components and backend services are designed, built, deployed, and managed independently

MICRO FRONTENDS | SINGLE-SPA

Standard-based Security and Accessibility

each component is secured independently and collectively as a security mesh

OIDC | IBM SECURITY VERIFY

Interoperability – Standard-based Integration

Backend business services are accessible using standard protocols, secured, and managed uniformly across the enterprise.

API FIRST APPROACH
API GATEWAY | GRAVITEE

Benefit to MedImpact and our clients

What will be the benefits of this solution?

Business Benefits

SOLUTION CHARACTERISTICS

PROTOCOL | TECHNOLOGY

BENEFIT HIGHLIGHTS

Modern, Intuitive, Seamless, User-centric Experience

brings all relevant functions together seamlessly from the user perspective

NEW UX STANDARDS

Single Page Responsive Web App

- ✓ **Customer satisfaction**. Modern, intuitive, guided user experience.
- ✓ **Differentiate** in the marketplace.
- ✓ **Better MI branding.** Incorporate MedImpact's new branding.

Composable and Autonomous

composable at run-time. UX components and backend services are designed, built, deployed, and managed independently

MICRO FRONTENDS | SINGLE-SPA

- ✓ One-stop shop for clients and MI Employees for all things PBM.
- **Speed-to-market**. Significant increase in our ability to deliver solution fast and keep pace with continuous change in stakeholder expectations.
- ✓ **Operational efficiency.** Significant reduction in complexity of managing IT assets that come together to deliver holistic user experience. Participating software products evolve independently.

Standard-based Security and Accessibility

each component is secured independently and collectively as a security mesh

OIDC | IBM SECURITY VERIFY

- ✓ **Client confidence** in our security posture.
- Customer satisfaction. Seamless sign-on with their organization's security credentials.
- ✓ Enable business capabilities safely and securely.

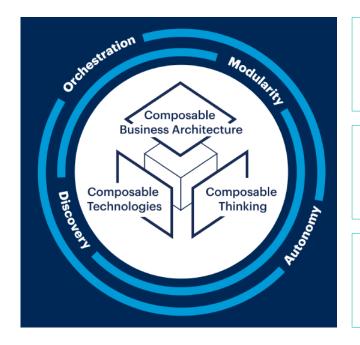
Interoperability – Standard-based Integration

Backend business services are accessible using standard protocols, secured, and managed uniformly across the enterprise.

API FIRST APPROACH
API GATEWAY | GRAVITEE

- Enables superior digital experience.
- ✓ **Speed-to-market and accessibility**. Ability to build, deploy, secure, monitor, and **consume** APIs in days.
- ✓ **Operational efficiency.** Better management and visibility of services (time +\$).
- **Resiliency and scalability**. Self-healing and automatically scalable infrastructure.

Takeaways



LUCIDA IS THE FACE OF MEDIMPACT TO OUR CLIENTS

Lucida will help us stand-out in the marketplace

COMPOSABLE - PLUGGABLE - AUTONOMOUS

Lucida is architected for speed-to-market, flexibility, autonomy of management/evolution of business functions

We must think and organize as an ecosystem of autonomous teams

API - API - API

API is the foundation for meeting the expectations of the digital age. Think of API as the new front End for our Applications

Thank you!

Appendix 1: Lucida Application Architecture

Lucida Component Model

User Experience

Responsibility

Presentation View Generation Validation (Meta-data driven) Application State Management and Routing Functional Entitlement SECURITY

IAM

Responsibility Authentication (SSO & FSSO) Coarsegrained Autorization User Administration

IBM Security Verify

Public Cloud (SaaS)

Stateful

N/A

OIDC | SAML

API Gateway

Responsibility

Access Control

Policy Orchestration (flow control)* Mediation

Throttling Data Maskina Cachina SECURITY

APIS

Multigrained (Micro & Macro) Services

Responsibility

Backend end validation Business Rules Banckend workflow Data Entitlement SECURITY

COTS/Legacy Apps/SOAP

No/Minimal Change

Technology Client Browser

Angular

Stateful State

Micro Front Ends Pattern Container UX

COMPOSITION UX (at run time)

Security Cross-site Request Forgery (CSRF)

-- Same Origin Policy (SOP)

-- Explicit vs Implicit Authentication Cross-origin Resource Sharing (COORS)

(DOM-based) Cross Site Scripting (XSS) - Inner HTML

Content Security Policy (CSP) Sub Resource Intigrity (SRI) Web Socket Security (future)

Deployment DMZ Web Server or through

API Gateway (as an API)

Run Time User Browser Gravitee

Stateless

Mediator

OIDC based Authentication Attribute (group/org) based Access Control IBM Security Verify for Token Validation APP Key/Secret

DMZ/Web Server Intranet

Kubernetes

Various

Stateless

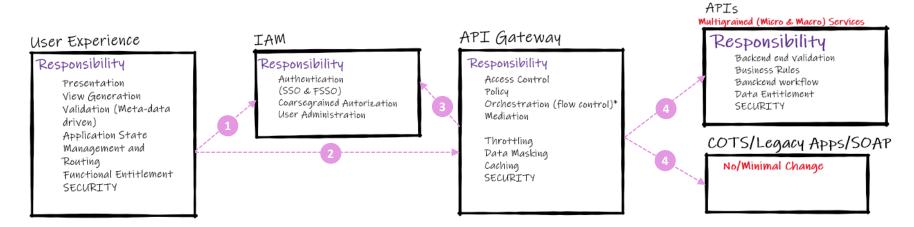
Various

Private Endpoints. (only open to API Gateway)*

Intranet/Cloud

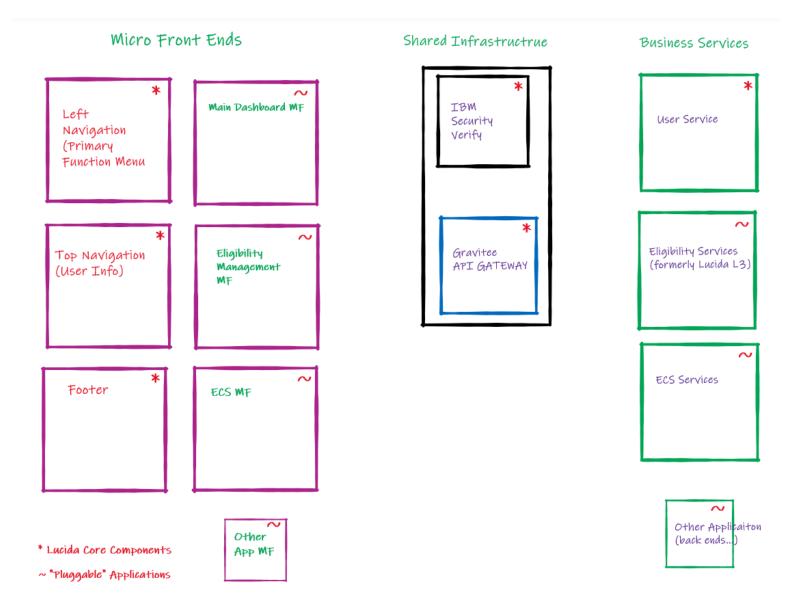
Various

Lucida Component Model

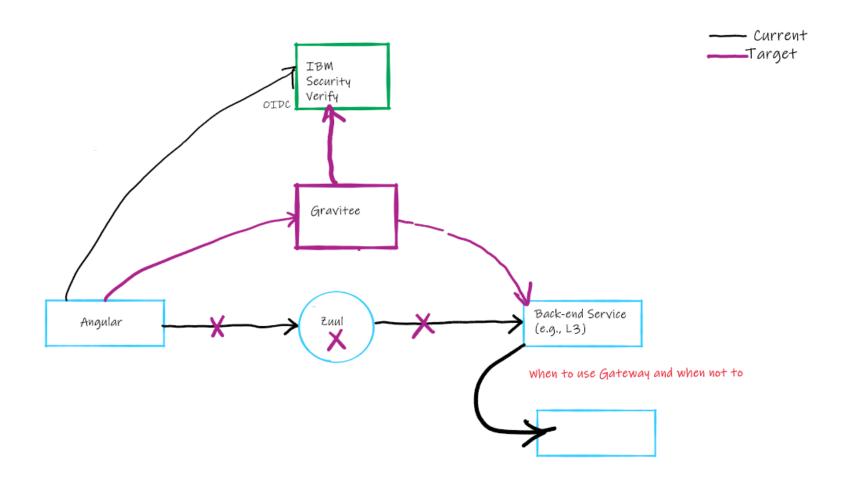


Technology	Client Browser Angular	IBM Security Verify	Gravitee	Various
State	Stateful	Stateful	Stateless	Stateless
Pattern	Micro Front Ends Container UX COMPOSITION UX (at run time)	OTDC SAML	Mediator	Various
Security	Cross-site Request Forgery (CSRF) Same Origin Policy (SOP) Explicit vs Implicit Authentication Cross-origin Resource Sharing (COORS) (DOM-based) Cross Site Scripting (XSS) - Inner HTML Content Security Policy (CSP) Sub Resource Intigrity (SRI) Web Socket Security (future)	N/A	OIDC based Authentication Attribute (group/org) based Access Control IBM Security Verify for Token Validation APP Key/Secret	Private Endpoints. (only open to API Gateway)*
Deployment	DMZ Web Server or through API Gateway (as an API)	Public Cloud (SaaS)	DMZ/Web Server Intranet	Intranet/Cloud
Run Time	User Browser		Kubernetes	Various

Lucida Core and Pluggable Components



Lucida Interaction Model



Key Architecture and Scope Decisions

IDENTITY & ACCESS CONTROL

- 1. All Authentication and Authorization (micro-front-ends, API Gateway) will be implemented using OIDC framework! Implications: Existing Reverse Proxy (WebSeal) apps will be updated to support OIDC and retire WebSeal
- 2. Lucida project will NOT redesign/rearchitect LDAP group/role structure. May alter or introduce new roles/groups.
- 3. Functional Entitlement (UX user menu) will utilize existing USER/RESOURCE solution (may be revisited in the future releases of Lucida)
- 4. Following our standard, IBM SV will be the IDP for IAM functions. IBM SV will be the SOR for "User-info" (group/role, org, etc.)

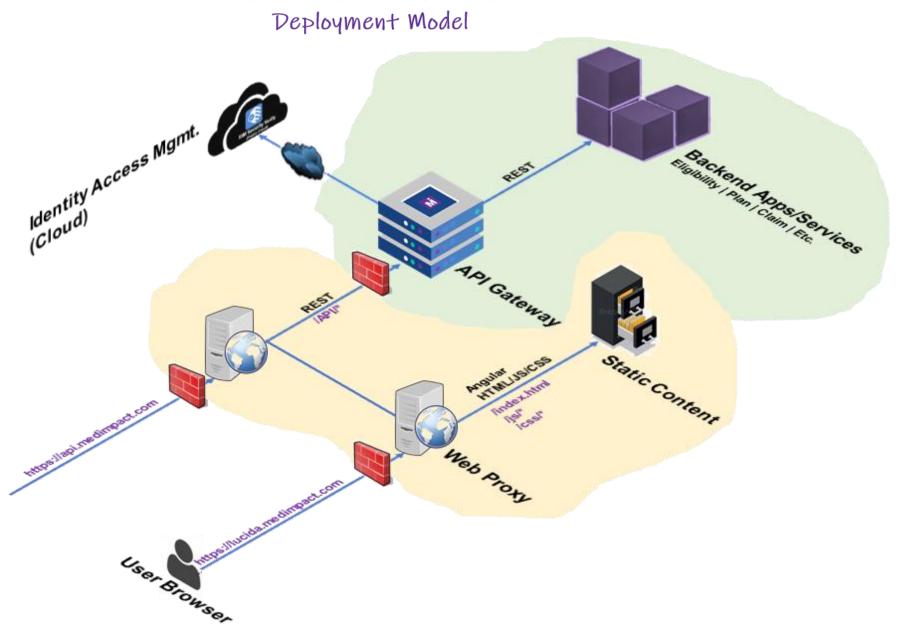
API and API GATEWAY

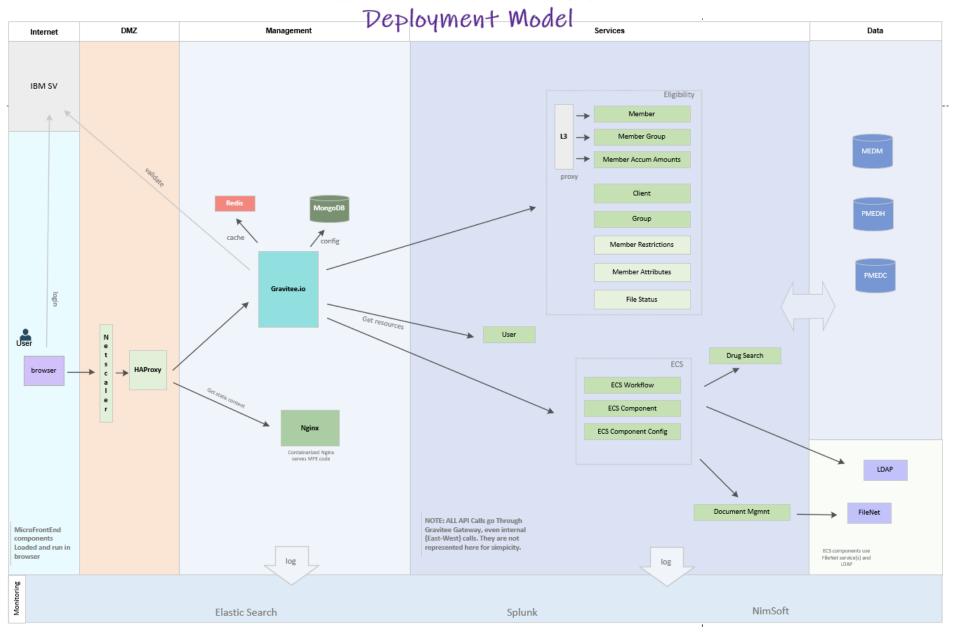
- 1. Gravitee will be responsible for all API Gateway functions (see Lucida Application Architecture for list of responsibilities by component type)

 Implications: Zuul or other components playing the API Gateway functions will be replaced with Gravitee
- 2. API Gateway is responsible for management/configuration and access control enforcement of APIs (user attribute based)
 Implications: API access management will NOT utilize User Service (currently used for UX Functional Entitlement)
- 3. API Gateway will require "Access Token" for API calls, the Gateway will validate the token and get "user info" from IBM SV. Gateway will cache the "user-info".
- 4. API Gateway will be agnostic of the calling application, i.e., Gateway will not be specific to an app.
- 5. APIS will be STATELESS.
- 6. API end-points exposed via the Gateway will be known as "Outer APIs". The backend private service end-points will be known as "Inner APIs"
- 7. The Inner APIs will be secured and only be allowed be to called by the API Gateway.

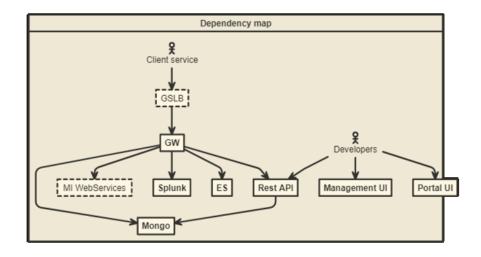
USER EXPERIENCE

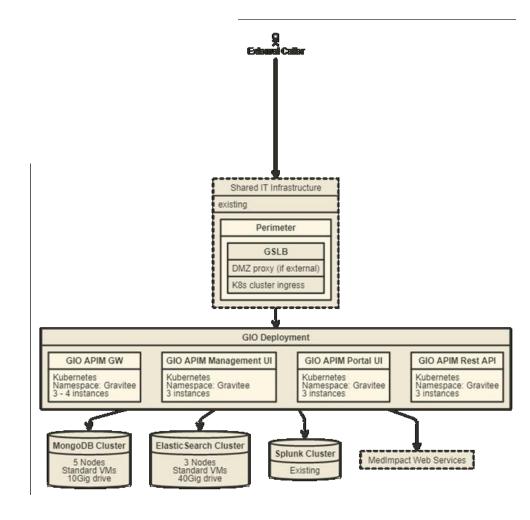
- 1. Micro Front End design pattern/framework
- $2.\ \mbox{OIDC}$ based authentication and authorization using IBM \mbox{SV}
- 3. Single-SPA
- 4. ECS: Do NOT build a separate front-end for Lucida. Enhance current code-base.
- 5. ECS: Prioratize look and feel changes over work-flow enhancement for phase 1.*******





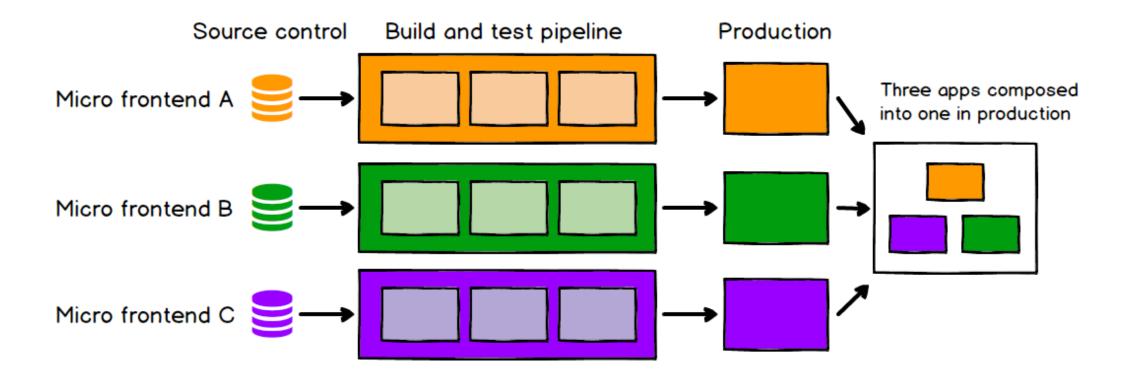
API Gateway (Gravitee) Deployment Model



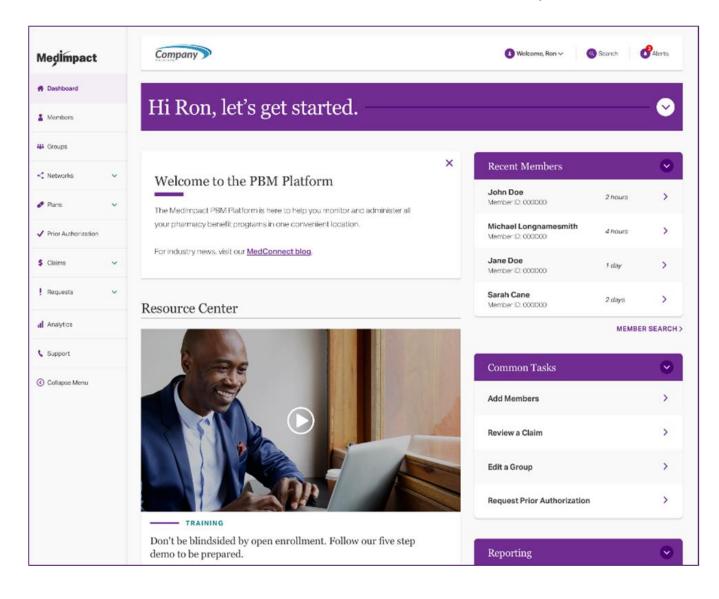


Appendix 2: Micro Front Ends (Single-SPA), API Gateway (Gravitee), and IBM Security Verify

Micro Front Ends



Micro Front Ends



Micro Frontends

Angular

Client-side Security

Persona Driven UX

Multiexperience

Different apps for different personas and modalities

Omnichannel









API Gateway

EMR

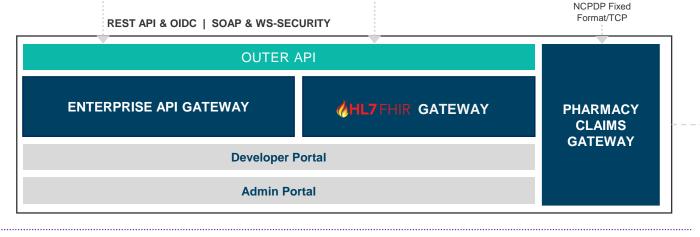
ePrescribing, ePA (Surescripts, CoverMyMeds)

MULTIEXPERIENCE

Different apps for different personas and modalities

API MANAGEMENT LAYER

- OIDC-based end-user Access Control
- Security & Monitoring
- Traffic Management
- Transformation
- Data Masking
- Caching



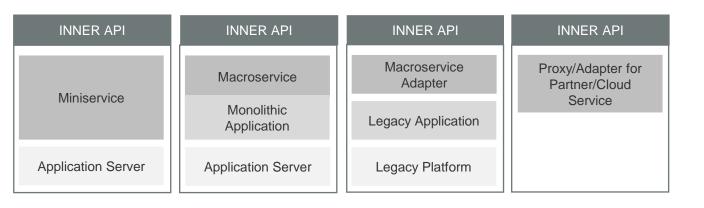
Plan Sponsor/

Third-party App

API Consumers

MULTIGRAINED SERVICES

- Macro/Mini/Micro
- New/Old
- On-premises/Cloud
- Internal/External



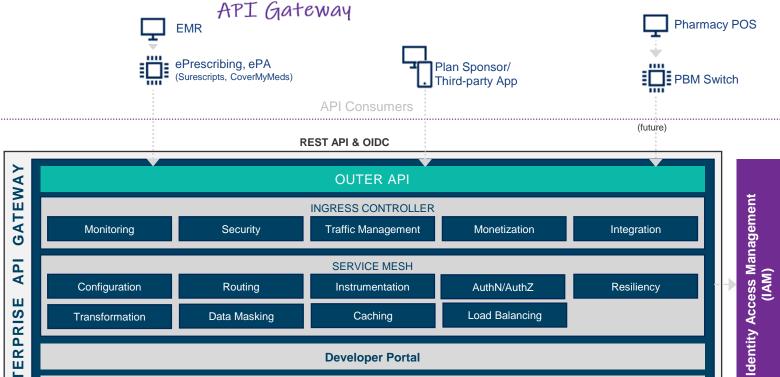
Identity Access Management (IAM)

Pharmacy POS

PBM Switch

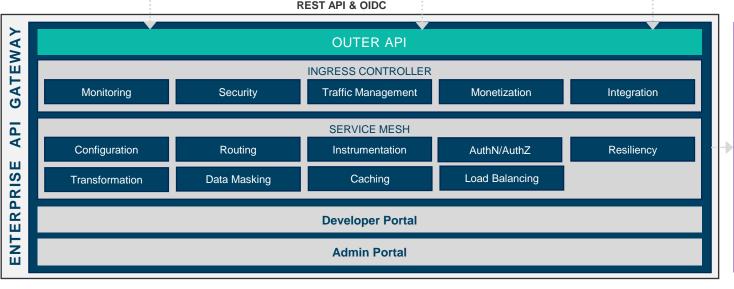
MULTIEXPERIENCE

 Different apps for different personas and modalities



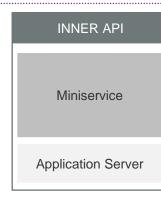
API MANAGEMENT LAYER

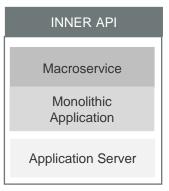
- OIDC-based end-user Access Control
- Security & Monitoring
- Traffic Management
- Transformation
- Data Masking
- Caching

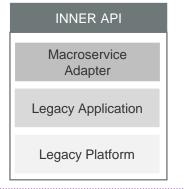


MULTIGRAINED SERVICES

- Macro/Mini/Micro
- New/Old
- On-premises/Cloud
- Internal/External







Proxy/Adapter for Partner/Cloud Service

INNER API

Identity and Access Management

User Groups

3+ **Identity Providers**

SSO/FSSO Brokers

Application Categories







MI public cloud applications exclusively used by MI employees



MI EMPLOYEE APPS MI private cloud applications exclusively used by MI









IBM SECURITY VERIFY Client Employee IDP (MI Managed Identity)



IBM SECURITY VERIFY

SSO/FSSO Broker for non-SaaS Apps



MI AND PARTNER APPS

MI private cloud applications used by both MI employees and client employees









CONSUMER APPS

MI private and public cloud applications used exclusively by consumers

- ✓ Standard-based (OIDC/SAML) SSO and FSSO capability
- ✓ Multi-factor and scenario-driven authentication model
- √ Layered access control*

Appendix 3: Lucida Phase 2 Roadmap

		Lucida	Roadmap Phase 2		
Events & Milestones	Lucida Prod Release 1 - End of February			Lucida Prod Release 4 - End of May	Lucida Prod Release 5 - End of June
Business Feature roduction ealization	Gravite API Gateway in Production IBM OIDC in Production Existing ECS UX Styling adherence to corporate standard Existing CTP UX Styling adherence to corporate standard Lucida BETA with Micro-Frontend in Production Eligibility Integrated with Lucida in Production	Lucida with Micro-Frontend in Production Eligibility Backend Buildout Lucida Main Dashboard ECS Integrated with Lucida in Production CTP Integrated with Lucida in Production	Lucida Main Dashboard Continued ECS Benefits Dashboard ECS Benefit Search ECS Benefit Project and Task Queue Screens CTP Dashboard	ECS Project and Task Details Screens ECS Benefit Screens ECS Benefit Plan Type Screens ECS Benefit Components Screens CTP Create Project Screens	CTP Member, Group, Carrier Screens CTP Run Tests Screens CTP Analysis Screens
Business pabilities functions	Authentication and Authorization Portals (Micro-Frontends) Eligibility	Authentication and Authorization	· ·	Benefit Configuration Claims Testing	Claims Testing
oplication Features	Key Scope Items Gravitee API Gateway Production IBM OIDC - Production IBM SVC User Role Sync Process Lucida MFE Container Lucida MFE Navigation Screen Lucida MFE Login Screen Lucida MFE IBM OIDC Eligibility MFE Eligibility Gravitee API Gateway Eligibility MFE IBM OIDC Lucida ECS MFE Integration ECS UX Styling CTP UX Styling	Eligibility - Backend Services Eligibility - UI Backend Integration Lucida MFE Main Dashboard ECS MFE ECS MFE IBM OIDC ECS MFE Gravitee API Gateway CTP MFE CTP MFE IBM OIDC CTP MFE Gravitee API Gateway Lucida ECS MFE Integration Lucida CTP MFE Integration	Lucida MFE Main Dashboard ECS Search and Results Screen ECS New Internal Project Screen ECS Search Results to Project ECS Benefit Dashboard ECS Project and Task Listing Screens CTP Dashboard	ECS Project Detail Screens ECS Project Task Detail Screens ECS Benefit Screens ECS Benefit Plan Type Screens ECS Benefit Components Screens CTP Create Project Screens CTP Production Claim Test Screen CTP Proto Claim Test Screen	Key Scope Items CTP Group Set Screens CTP Member Set Screens CTP Carrier Screens CTP Run Tests Screens CTP Run Tests View Screens CTP Claim Analysis Screens