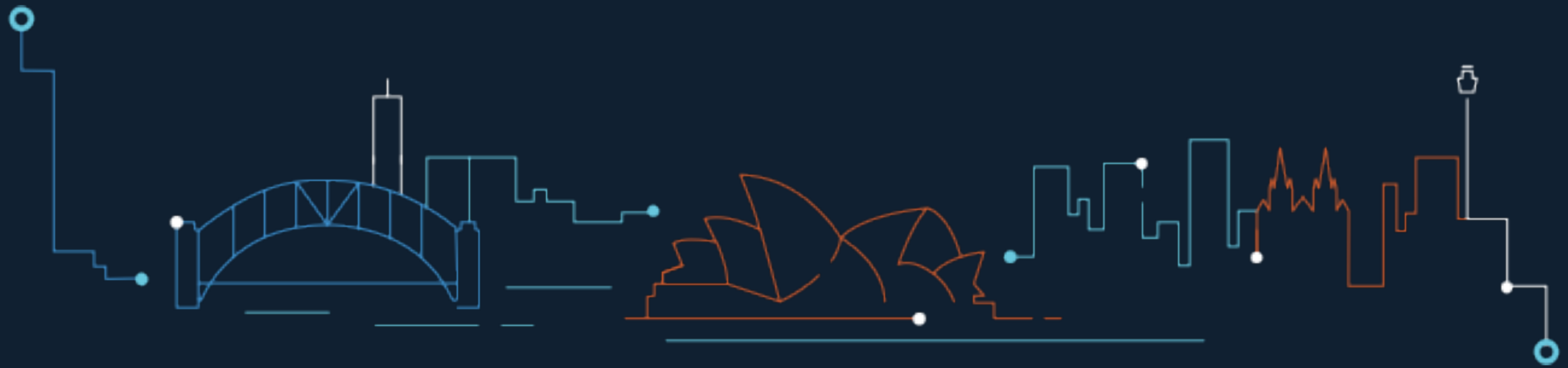
okta

FORUM

Security in the API Economy

D. Keith Casey, Jr. API Problem Solver



Disclaimer

This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, which may include, but are not limited to, statements regarding our financial outlook, product development and market positioning. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms or the negative of these terms and similar expressions are intended to identify these forward-looking statements. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond Okta's control.

In particular, the following factors, among others, could cause results to differ materially from those expressed or implied by such forward-looking statements: the market for our products may develop more slowly than expected or than it has in the past; quarterly and annual operating results may fluctuate more than expected; variations related to our revenue recognition may cause significant fluctuations in our results of operations and cash flows; assertions by third parties that we violate their intellectual property rights could substantially harm our business; a network or data security incident that allows unauthorized access to our network or data or our customers' data could harm our reputation, create additional liability and adversely impact our financial results; the risk of interruptions or performance problems, including a service outage, associated with our technology; we face intense competition in our market; weakened global economic conditions may adversely affect our industry; the risk of losing key employees; changes in foreign exchange rates; general political or destabilizing events, including war, conflict or acts of terrorism; and other risks and uncertainties. Past performance is not necessarily indicative of future results. Further information on potential factors that could affect our financial results is included in our Annual Report on Form 10-K for the year ended January 31, 2018 and other filings or reports filed with the Securities and Exchange Commission that are posted at investor.okta.com.

Any unreleased products, features or functionality referenced in this or other presentations, press releases or public statements are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality. Customers who purchase our products should make their purchase decisions based upon features that are currently generally available.

The forward-looking statements contained in this presentation represent the Company's estimates and assumptions only as of the date of this presentation. Okta assumes no obligation and does not intend to update these forward-looking statements whether as a result of new information, future events or otherwise.

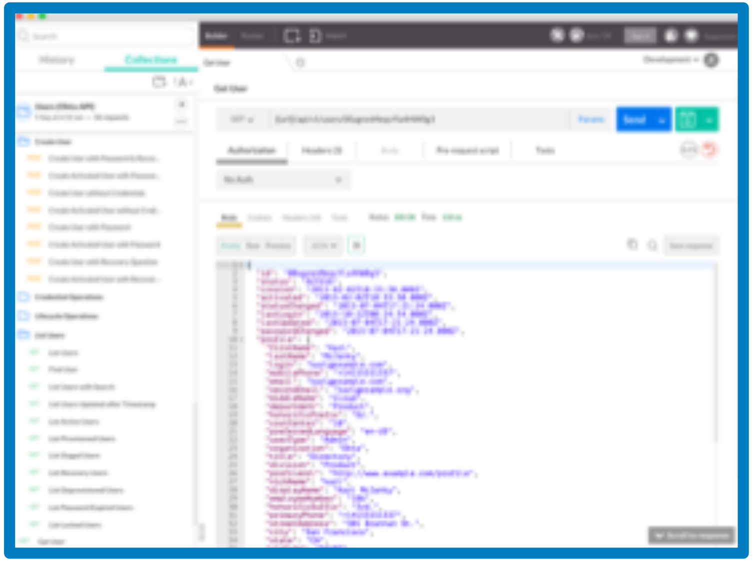
This presentation contains estimates and other statistical data that we obtained from industry publications and reports generated by third parties. These data involve a number of assumptions and limitations, and you are cautioned not to give undue weight to such estimates. Okta has not independently verified the statistical and other industry data generated by independent parties and contained in this presentation and, accordingly, Okta cannot guarantee their accuracy or completeness. Expectations, estimates, forecasts and projections are subject to a high degree of uncertainty and risk. Many factors, including those that are beyond Okta's control, could cause results or outcomes to differ materially from those expressed in the estimates made by the independent parties and by Okta.

D. Keith Casey, Jr.

API Problem Solver

Connected experiences across devices

APIs have enabled this Transformation



APIs drive integrations, opportunities, and revenue

salesforce

APIs drive
50% of
Revenue *

twilio

APIs drive
100% of
Revenue
($540M ARR)

Expedia

APIs drive
90% of
Revenue *

* https://hbr.org/2015/01/the-strategic-value-of-apis

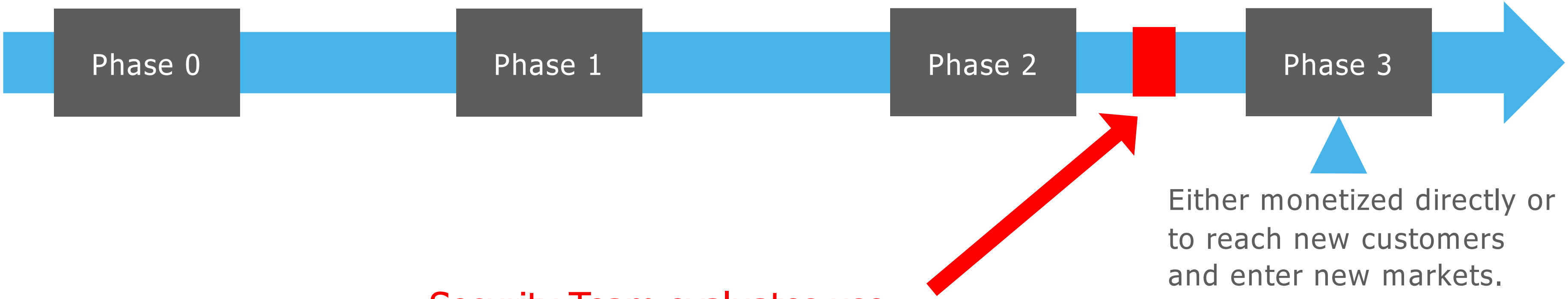
API Journey: A Maturity Model

Integrate internal systems by introducing Private APIs

Internal advocacy & collaboration for internal APIs and CoE/Governance

Limited API access to partners, resellers and suppliers

Grow these APIs as full fledged products with external developer access



Either monetized directly or to reach new customers and enter new markets.

Security Team evaluates use cases, interfaces, authentication, access management, etc, etc

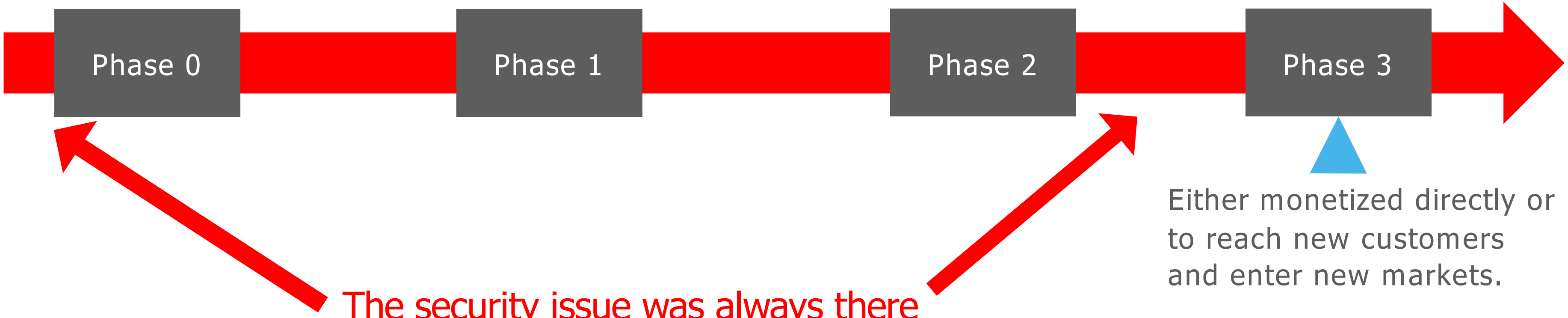
API Journey: A Maturity Model

Integrate internal systems by introducing Private APIs

Internal advocacy & collaboration for internal APIs and CoE/Governance

Limited API access to partners, resellers and suppliers

Grow these APIs as full fledged products with external developer access



The security issue was always there

Either monetized directly or to reach new customers and enter new markets.

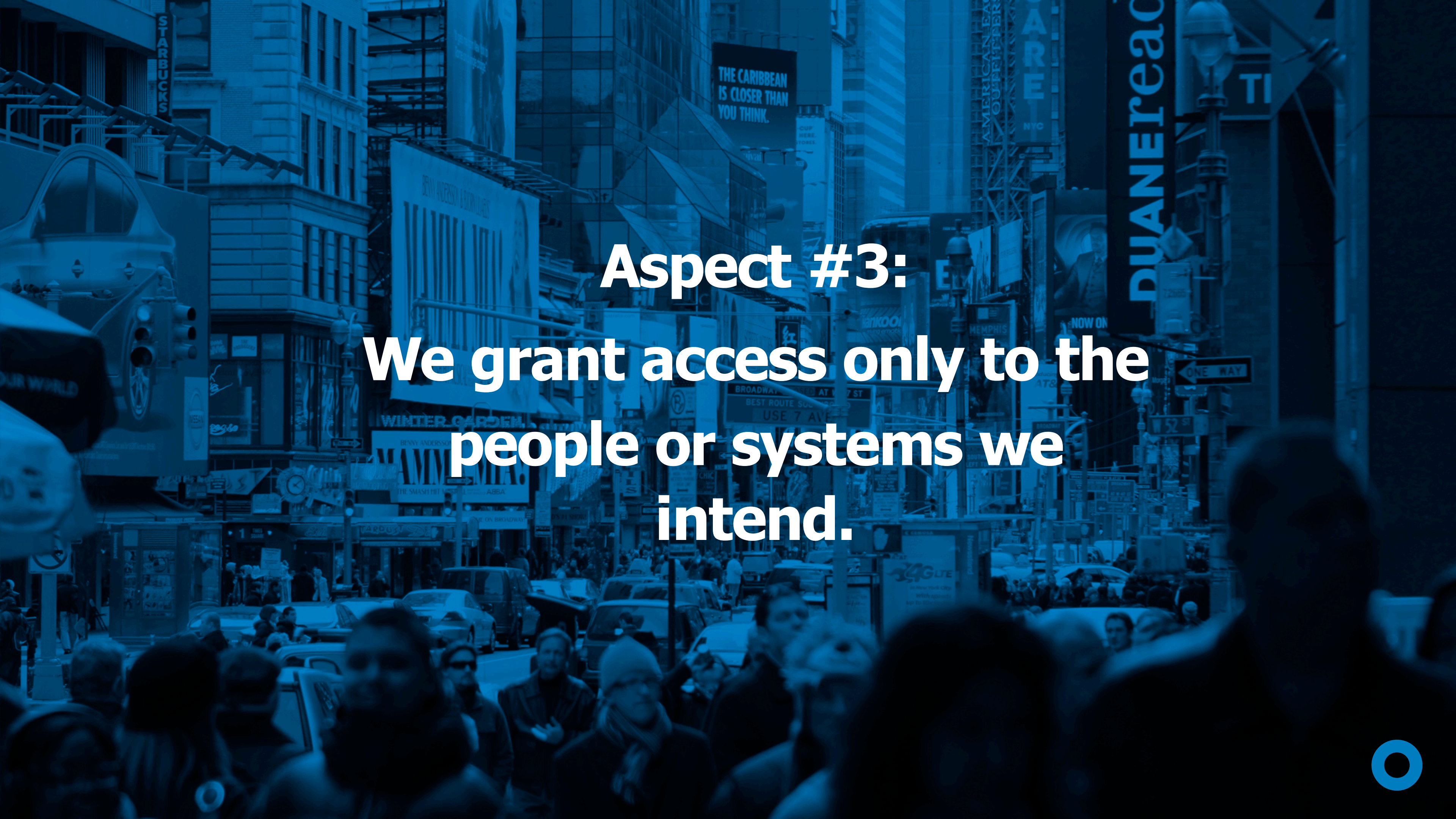
What is API Security?

Aspect #1:

We expose only the interfaces which we intend.

Aspect #2:

We share and accept only the data which we intend.



Aspect #3:

We grant access only to the people or systems we intend.

Approach #1: Trust our End Users

No, I’m kidding.
Unqualified trust is not security.

Approach #2: Use an API Gateway

API Management Capabilities

Full Lifecycle API Management

Lifecycle	Interface	Access	Consumption	Business
What state is it in?	What does it expose?	Who can use it?	How to succeed with it?	How does it drive business goals?
• How was it designed? • How was it built? • Is it deployed? • To which GWs? • Is it live/available?	• Which resources? • Which methods? • Which objects? • Which fields?	• Which users/groups? • How do they authenticate? • Using which clients? • In what contexts?	• API Documentation? • Debugging/errors? • Track usage? • Examples/SDKs?	• Partner CRM • Monetization • Marketing • Business Analytics

API Management Capabilities

Full Lifecycle API Management

Lifecycle	Interface	Access	Consumption	Business
What state is it in?	What does it expose?	Who can use it?	How to succeed with it?	How does it drive business goals?
• How was it designed? • How was it built? • Is it deployed? • To which GWs? • Is it live/available?	• Which resources? • Which methods? • Which objects? • Which fields?	• Which users/groups? • How do they authenticate? • Using which clients? • In what contexts?	• API Documentation? • Debugging/errors? • Track usage? • Examples/SDKs?	• Partner CRM • Monetization • Marketing • Business Analytics

API Management Capabilities

Full Lifecycle API Management

Lifecycle	Interface	Access	Consumption	Business
What state is it in?	What does it expose?	Who can use it?	How to succeed with it?	How does it drive business goals?
• How was it designed? • How was it built? • Is it deployed? • To which GWs? • Is it live/available?	• Which resources? • Which methods? • Which objects? • Which fields?	• Which users/groups? • How do they authenticate? • Using which clients? • In what contexts?	• API Documentation? • Debugging/errors? • Track usage? • Examples/SDKs?	• Partner CRM • Monetization • Marketing • Business Analytics

API Gateways - Drawbacks

- Yet another user database
- Doesn’t have full context on the user
- Designed to manage APIs, not authorization policies

Approach #3: API Keys

An Example

-
  ```
  curl –X POST https://api.company.com/projects
    --header “Authorization: Bearer abcdef012345”
    --data ‘{“name”:”My Project”, “date_due”:”2018-09-14”}’
  ```

-
  ```
  curl –X DELETE https://api.company.com/projects/1234
    --header “Authorization: Bearer abcdef012345”
  ```

API Keys - Drawbacks

- All the joys of passwords
- Rotating at scale is really painful
- Generally all or nothing access

- *The de facto standard for APIs, API gateways, etc.*

Approach #4: OAuth

Hotel key cards, but for apps

OAuth Authorization Server

Access Token

Resource (API)

Compared to API Keys

- All the joys of passwords
- Rotating at scale is really painful
- Generally all or nothing access

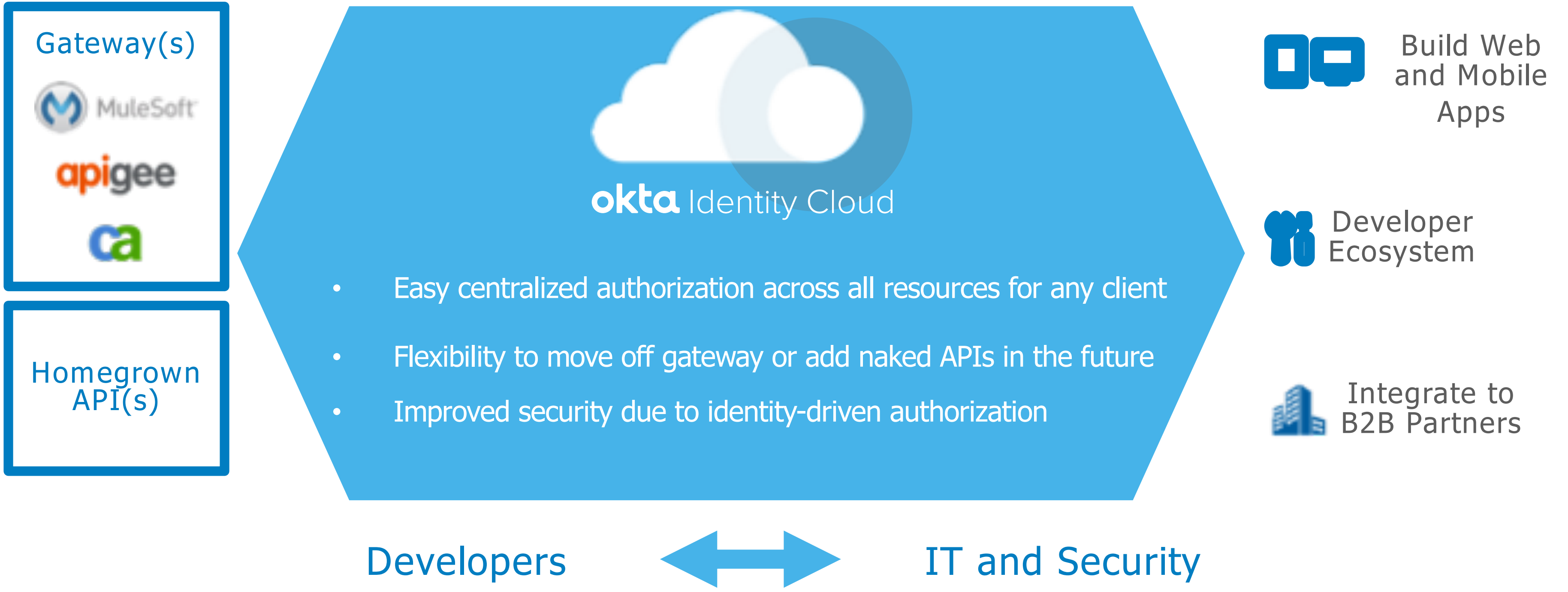
- Tokens expire automatically
- Rotation is part of the spec
- Each application has separate, rotatable credentials
- OAuth is inherently scoped
- Widely & consistently supported in all major programming languages & frameworks

OAuth - Drawbacks

- Not a single specification but a framework
- More complex, more flexible, less standard as a result

- *No, really. Those are the only major drawbacks.*

Okta lets developers focus on development and IT manage policy



Gateway(s)

MuleSoft

apigee

ca

Homegrown API(s)

okta Identity Cloud

- Easy centralized authorization across all resources for any client
- Flexibility to move off gateway or add naked APIs in the future
- Improved security due to identity-driven authorization

Build Web and Mobile Apps

Developer Ecosystem

Integrate to B2B Partners

Developers

Add the Okta SDK and stay focused on core features

IT and Security

Empowered to create, manage, and audit access across all points of access

Closing Thoughts

Questions to Ask Yourself

- Who is responsible for your APIs?
- Who is responsible for security policy & enforcement?
- Who are your users?
- Who will be your users in a year?
- What are their apps: mobile, web backends, IoT, other apps?
- Is their access fine-grained or the same for every user/app?
- What happens when your application is compromised?

okta

FORUM

Thank You