®

SECURITY CONSIDERATIONS FOR THE API ECONOMY

Chrysalis Panel Discussion

TECHVISION
CHRYSALIS

Your Presenters

- Nathaneal Coffing, CSO & Co-Founder, Cloudentity
- Doug Simmons, Principal Consulting Analyst, TechVision Research, author or co-author of TechVision's API-centric Reports

What is This Session About?

- APIs are key conduit of an efficient and scalable digital enterprise, but also represent significant security risks.
- This session will focus on API security, key vulnerabilities and developing enterprise strategies and programs to address these risks.
- We'll also get insights about the approaches, strategies and expected future state from some key vendors in this space.

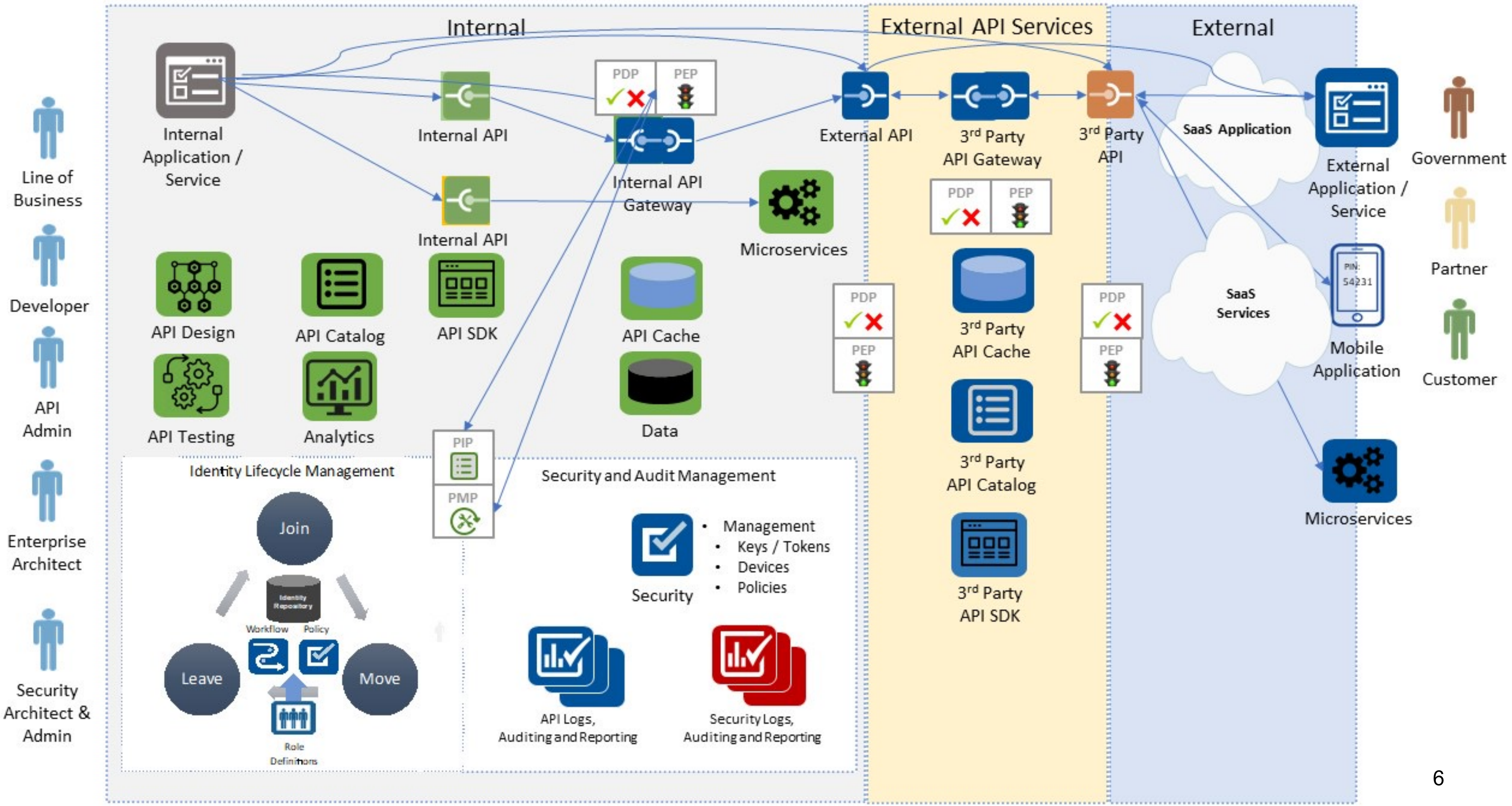
Thesis

- APIs are used as part of the glue across almost all types of application development environments supporting the integration of cloud-native, mobile, enterprise, line of business and consumer applications.
  - While traditionally considered a highly technical discipline supporting Developers, APIs can now support almost functional requirement or role in an organization, with many useful APIs now widely available.
- The movement from monolithic applications to distributed and modular component-based services and the need to integrate/orchestrate these services through APIs, creates large operational and security challenges.

API Security Summary

- The fact that the number of APIs offered and consumed in actual use cases has seen such growth means most organizations must consider comprehensive management and security of APIs to reduce risk to their business.
- Aligning your API security and management with your business priorities in terms of risk, value, and delivery is therefore critical.
- This is a classic security challenge of managing the CIA triangle of Confidentiality, Integrity, and Access: all of which require a level of balance between the requirements to create business value.

API Security Reference Architecture



API Security “Good” Practices

- Incorporate API Management and Security into your standard business processes and functional groups:
  - Security
  - Architecture
  - Development
  - Training
- Audit existing API usage across your organization
  - Internal
  - External/Third-party
- Implement an API Management and Monitoring capability with appropriate tooling
- Apply a Zero Trust security model to API usage for your organization
- Clearly define and publicize your API strategy across the organization

Panel Discussion

- What are the typical obstacles you may be seeing to successful API Management and Security implementation?
- How do you address the hybrid / multi-cloud infrastructure challenges of managing API security, including policies and enforcement points?
- What are one or two of the most significant areas your Product Team is attempting to address?

Questions?

TECHVISION

CHRYSALIS