



API Economy : Managing Security and Legal Risks

Baljeet Malhotra, PhD

OWASP Vancouver

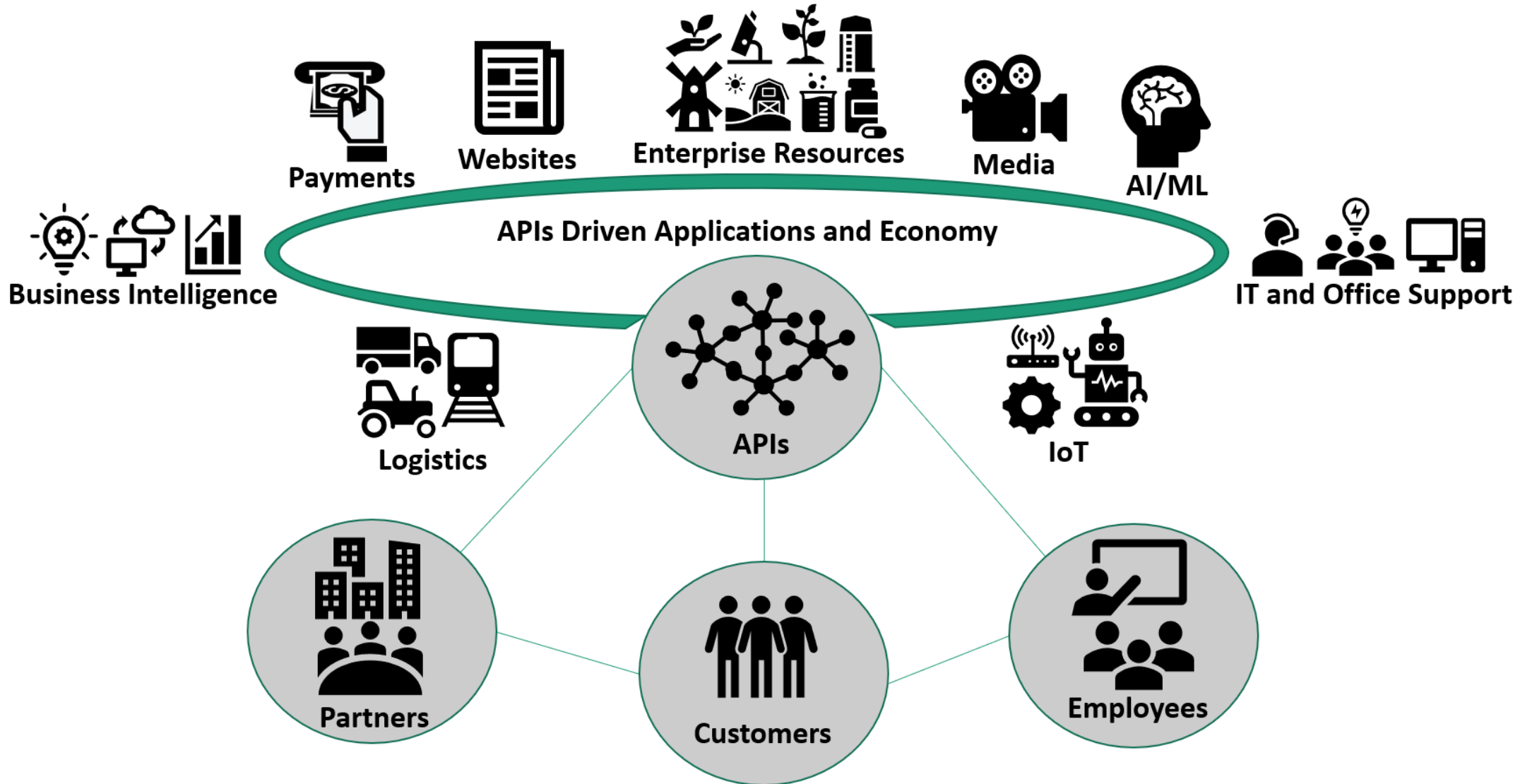
16th July 2020

Visual Intro



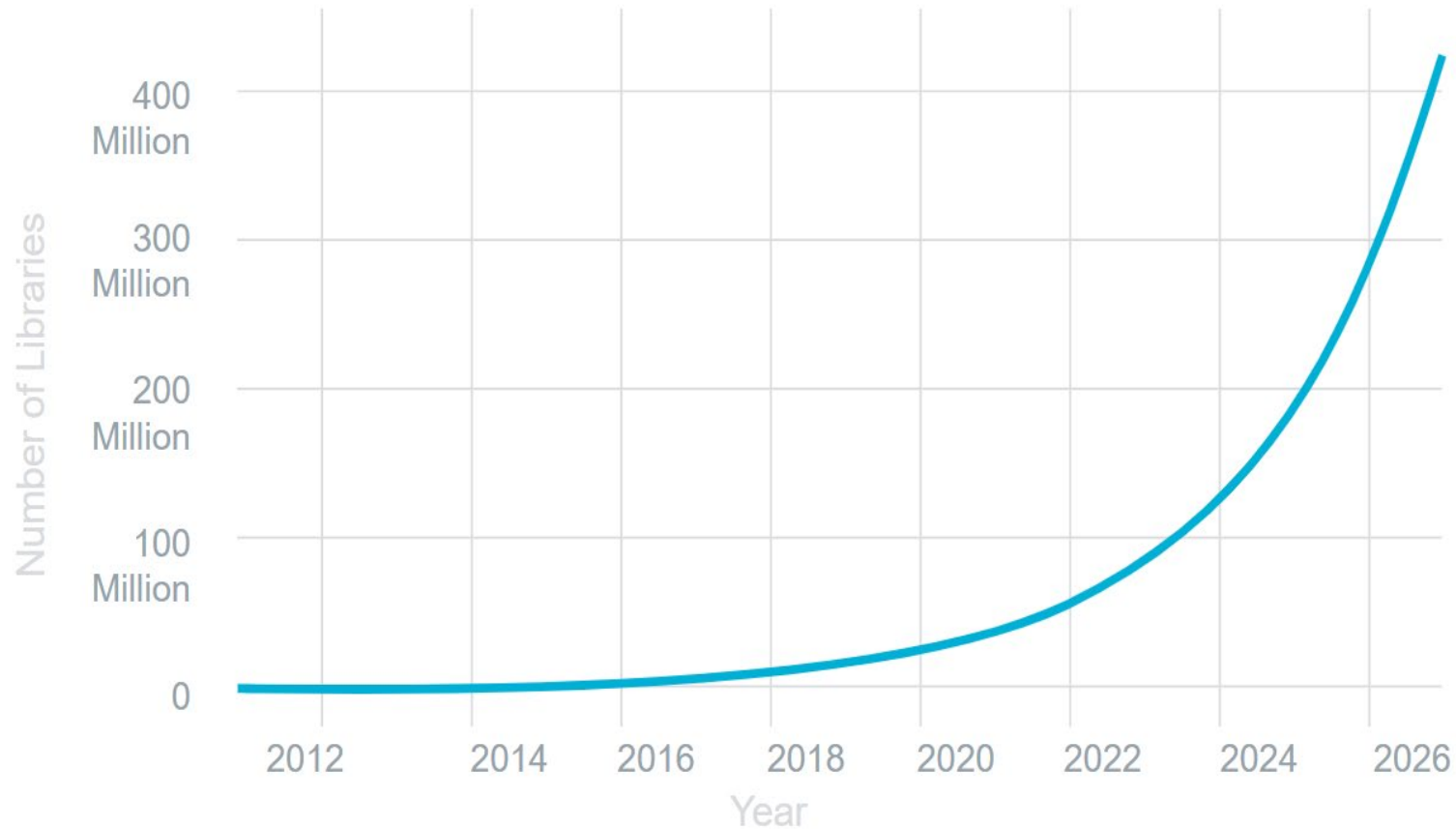
Global Trends: API Economy

Enterprises are depending on more and more third party services (APIs)



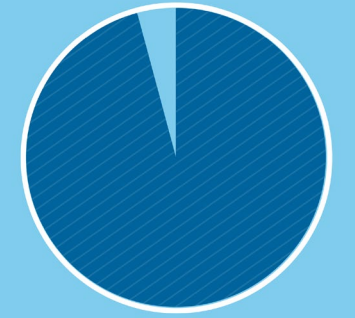
Global Trends: Software

Growth of Software Libraries



Application Challenges

96%
Applications
that contained
open source



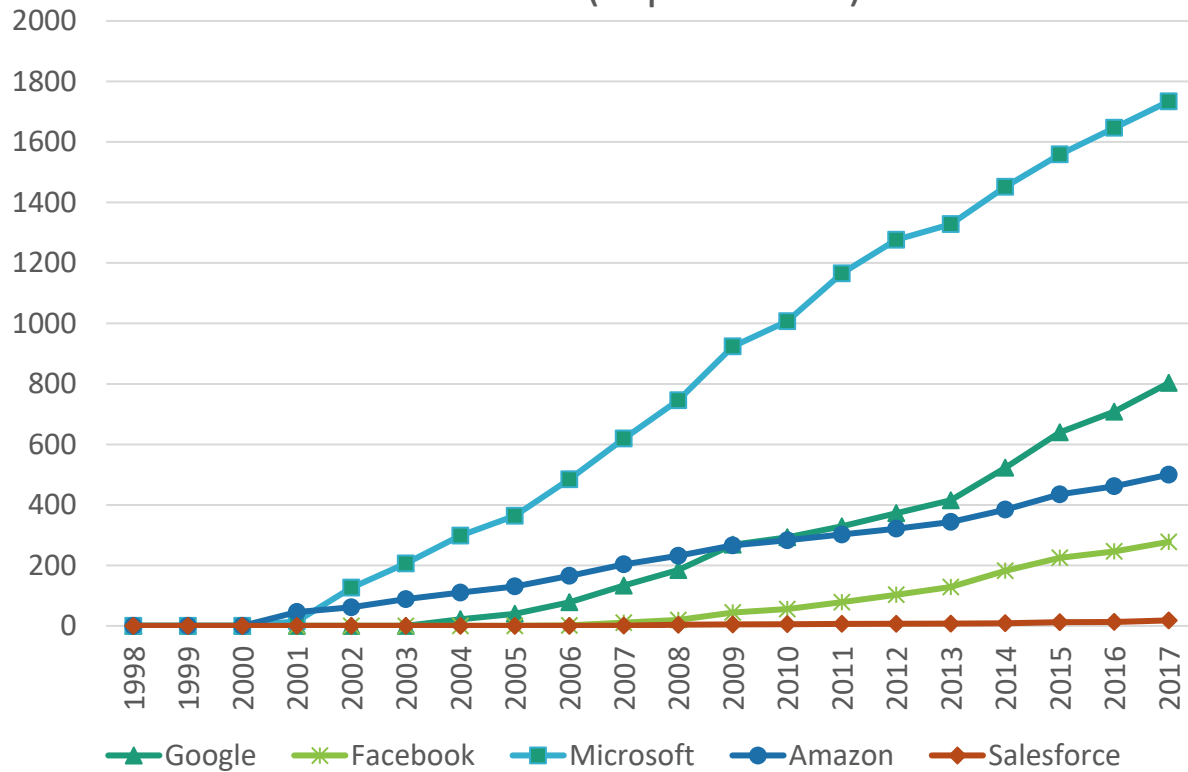
67%
Applications
that contained
known
open source
vulnerabilities



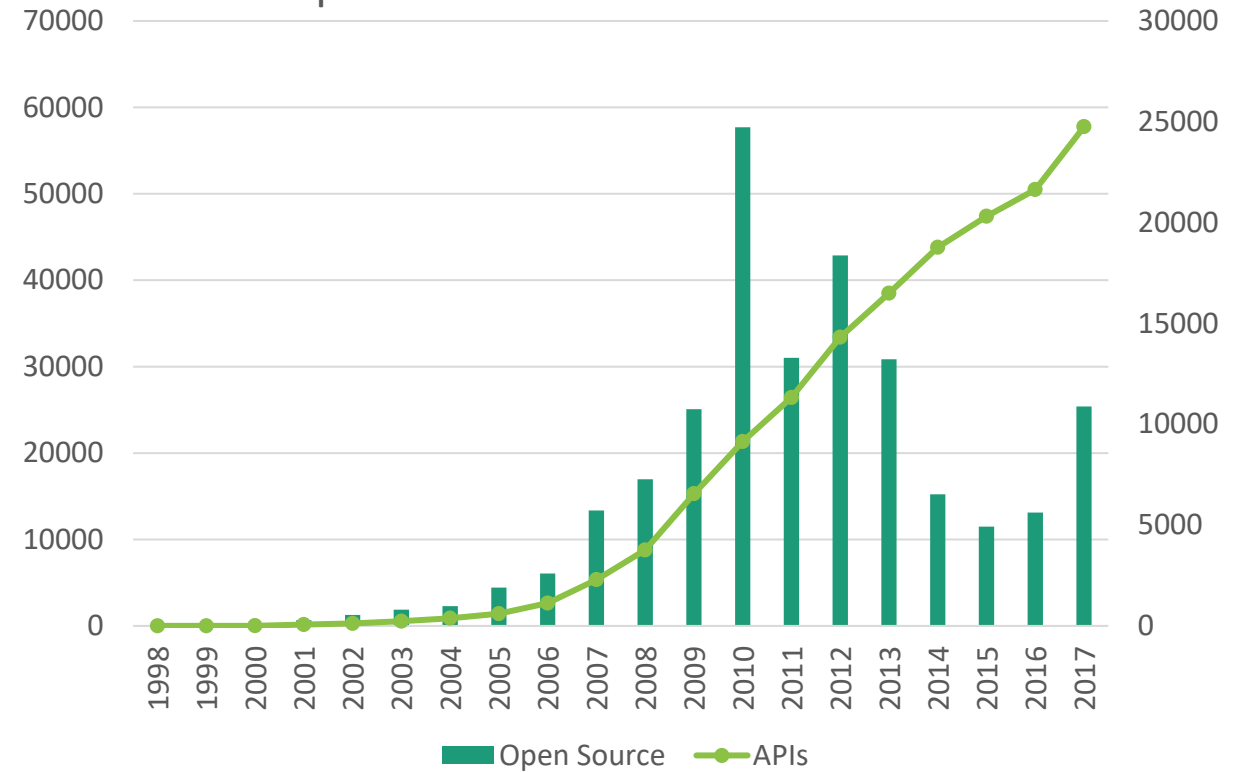
Acknowledgement: Source Clear and Black Duck Software

Global Trends: APIs vs Open Source

Growth of APIs (Top Vendors)



Open Source and APIs



The API Economy: Challenges and Opportunities

APIs are important for digital economy

- Thousands of APIs today and growing at >30%p.a.
- Internal APIs (3rd party integrations)
- External APIs (Open Source and M&A)

Challenges with API management

- Security problems (automation & intelligence)
- Compliance problems (terms of use & regulations)
- Reliability problems (authentication & authorization)

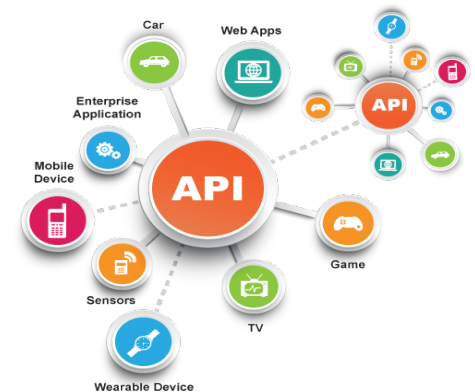
No existing end-to-end solution

- API design solutions: MuleSoft, Apigee, Apiary, etc.
- No programmatic discovery of APIs
- No API consumer centric approaches

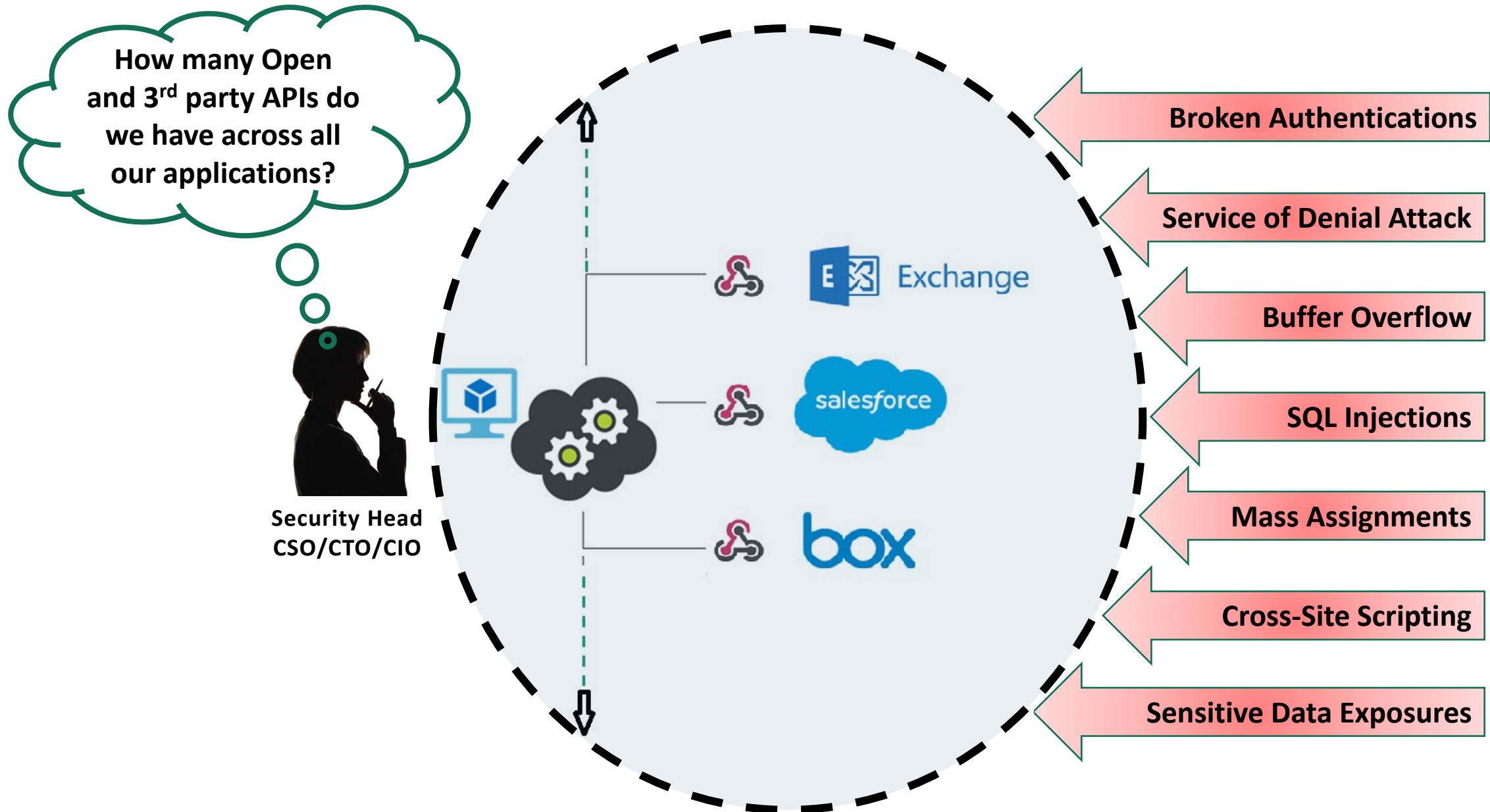
External Open APIs



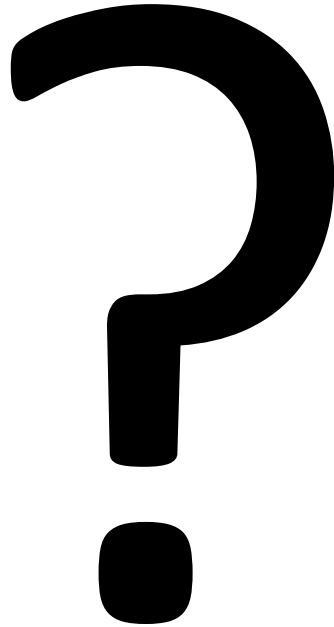
Third-Party Integrations



Why Technical Due Diligence: Managing Risks



Questions



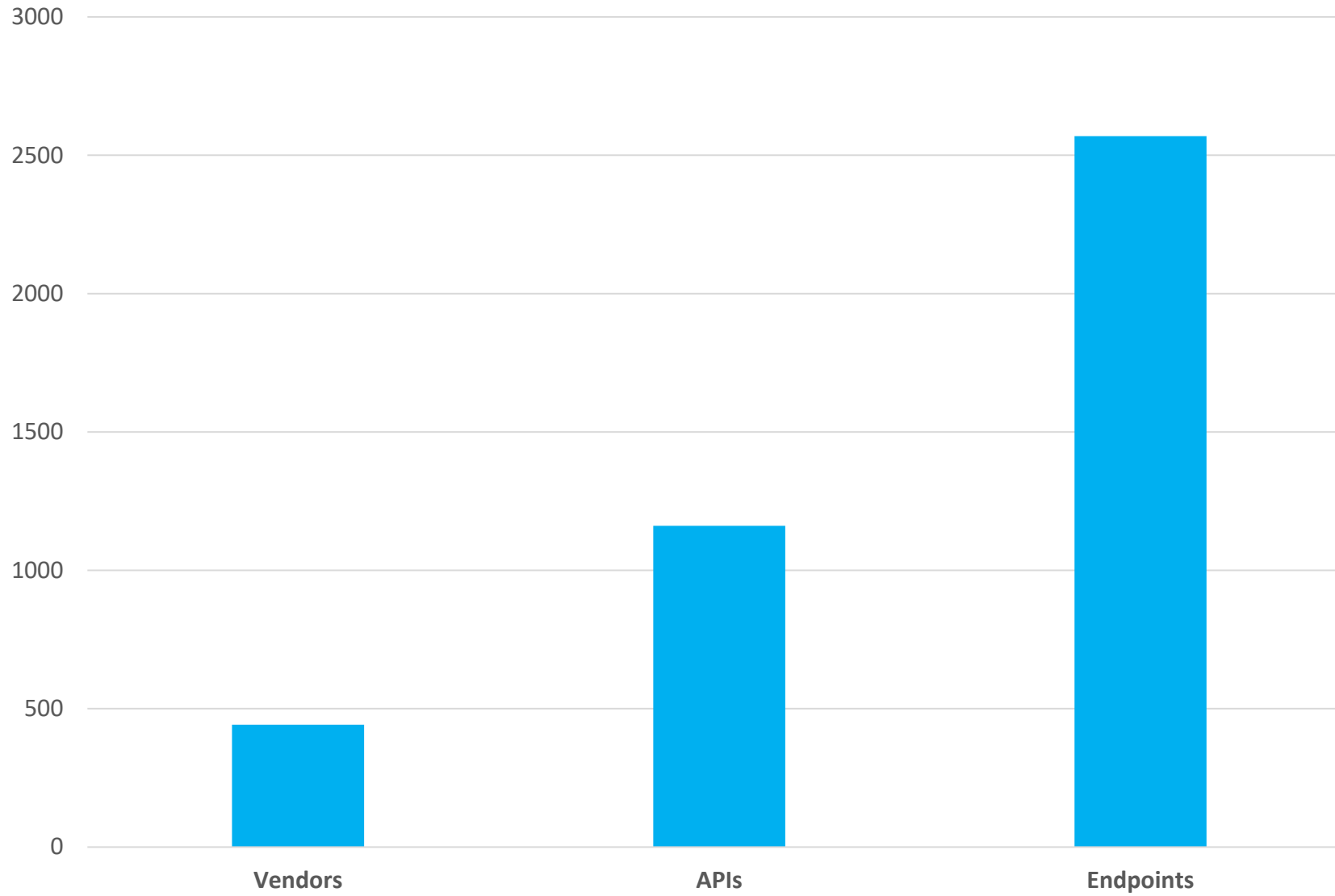
Ecosystem of Open / Public APIs



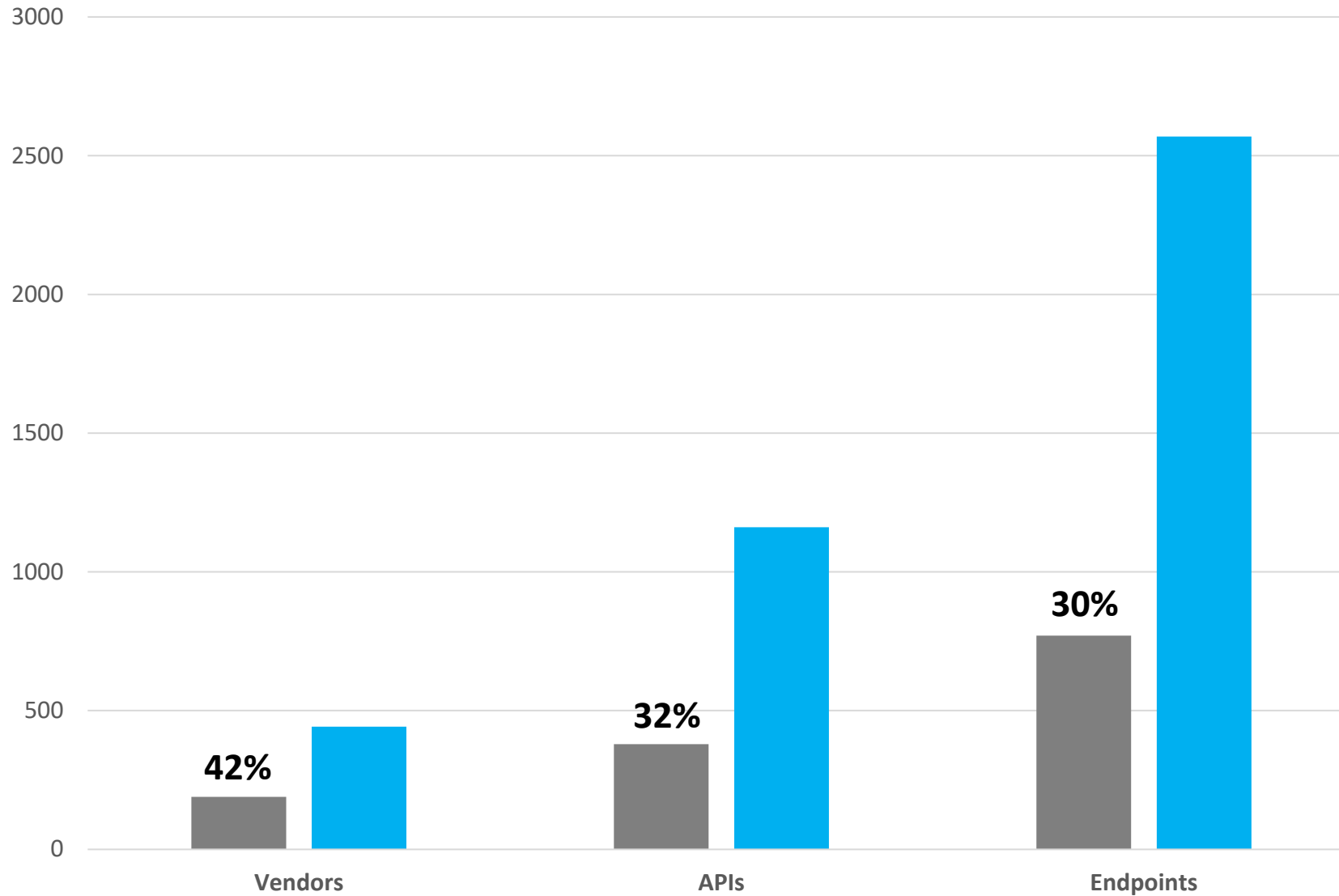
API Discovery™ Tracks:

- ❑ **15000+**
API Endpoints
- ❑ **10000+**
API Providers
- ❑ **50+**
API Frameworks
- ❑ **30000+**
Terms of Services
- ❑ **AI, IoT, etc.**
Growth Drivers
- ❑ **Analytics**
New Innovations

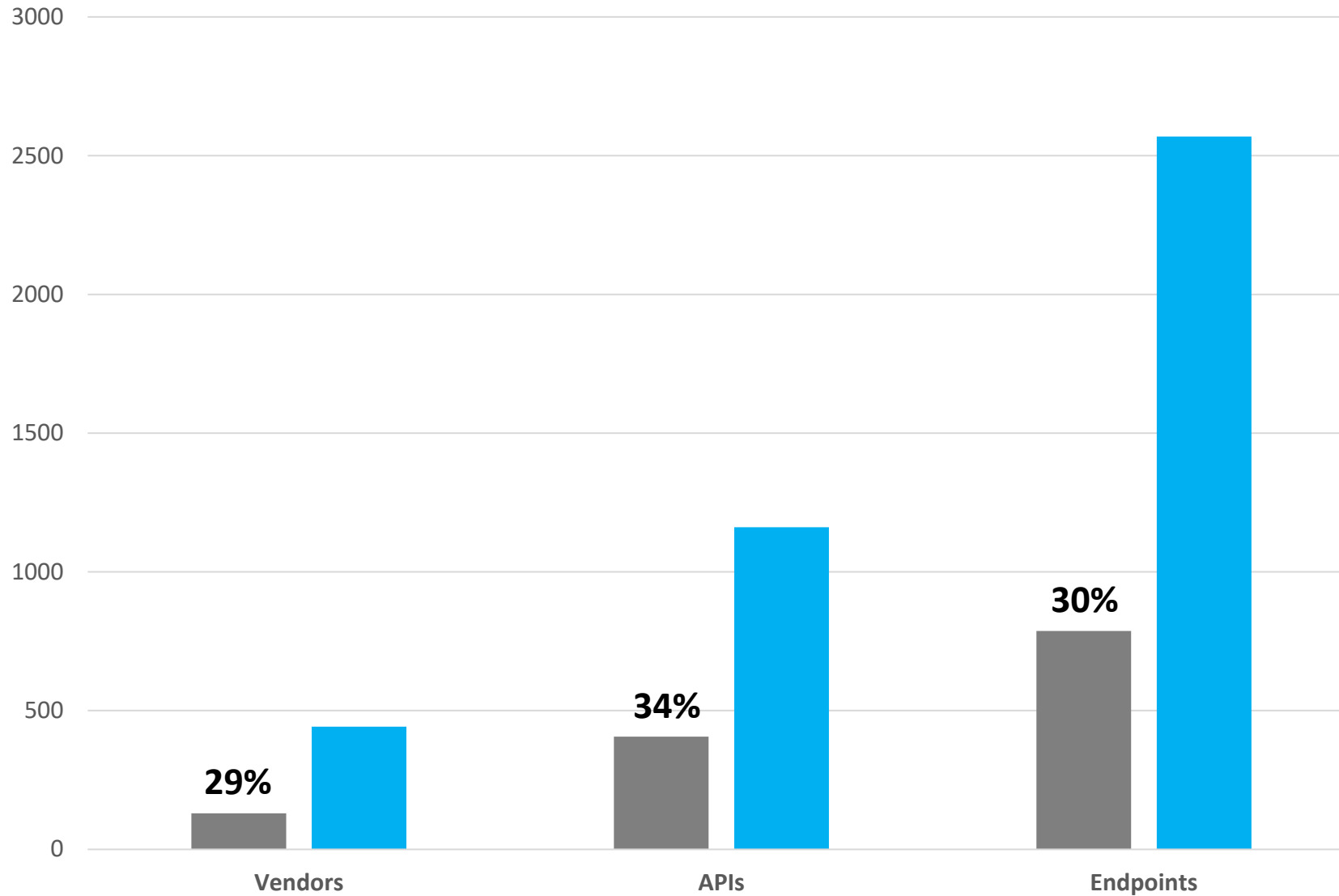
Dataset



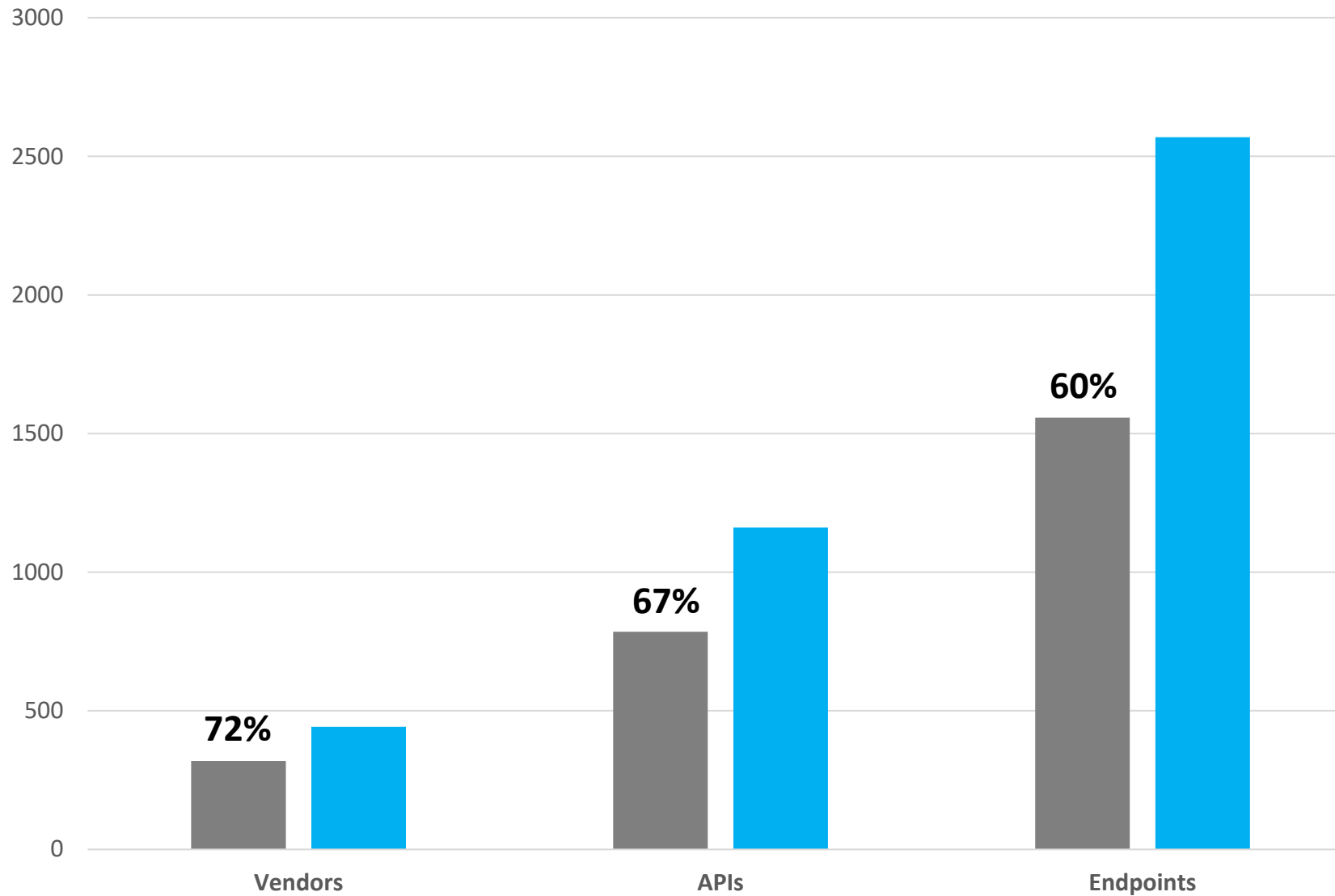
No Access Control (OWASP-1)



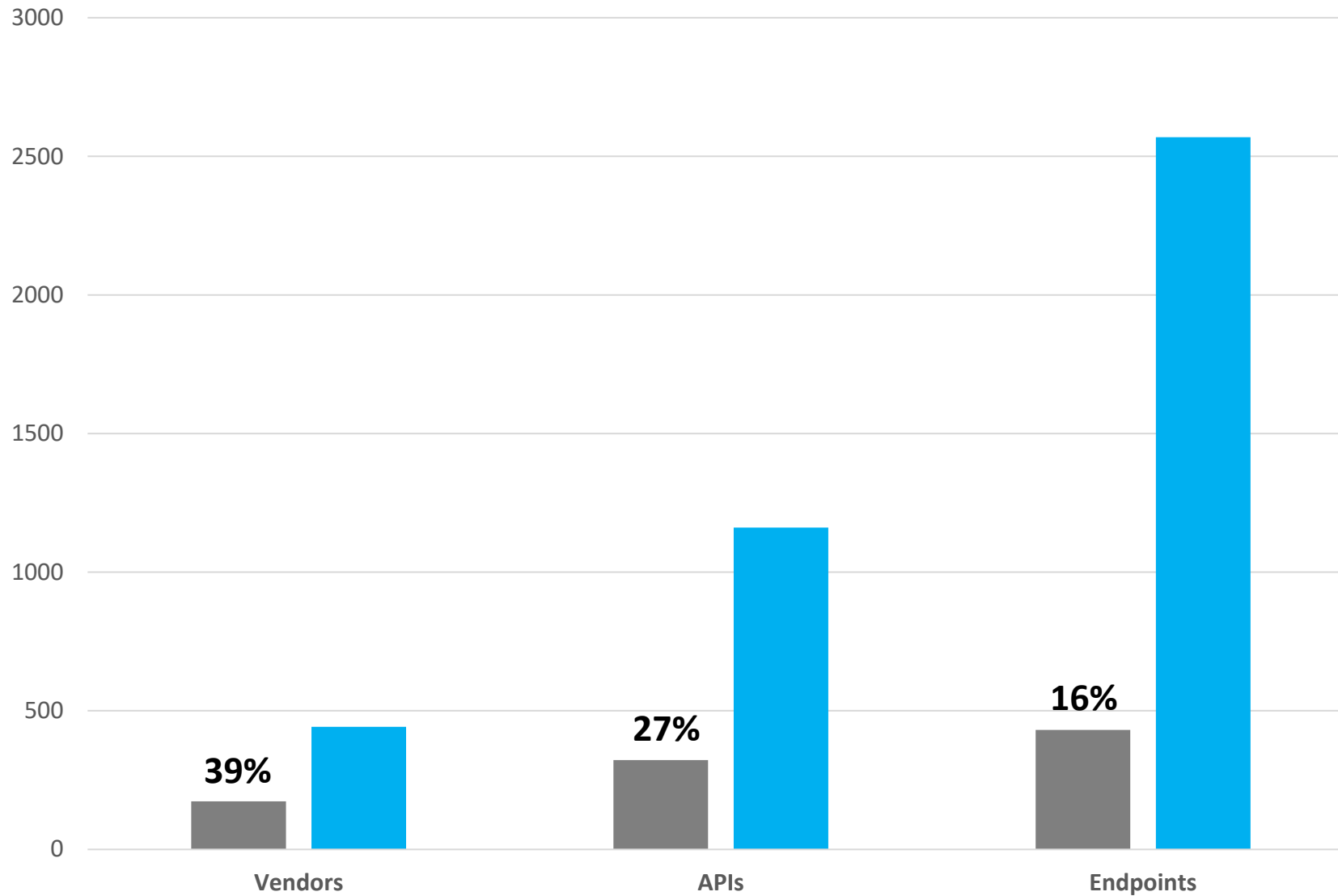
Unsecured Access Control (OWASP-1)



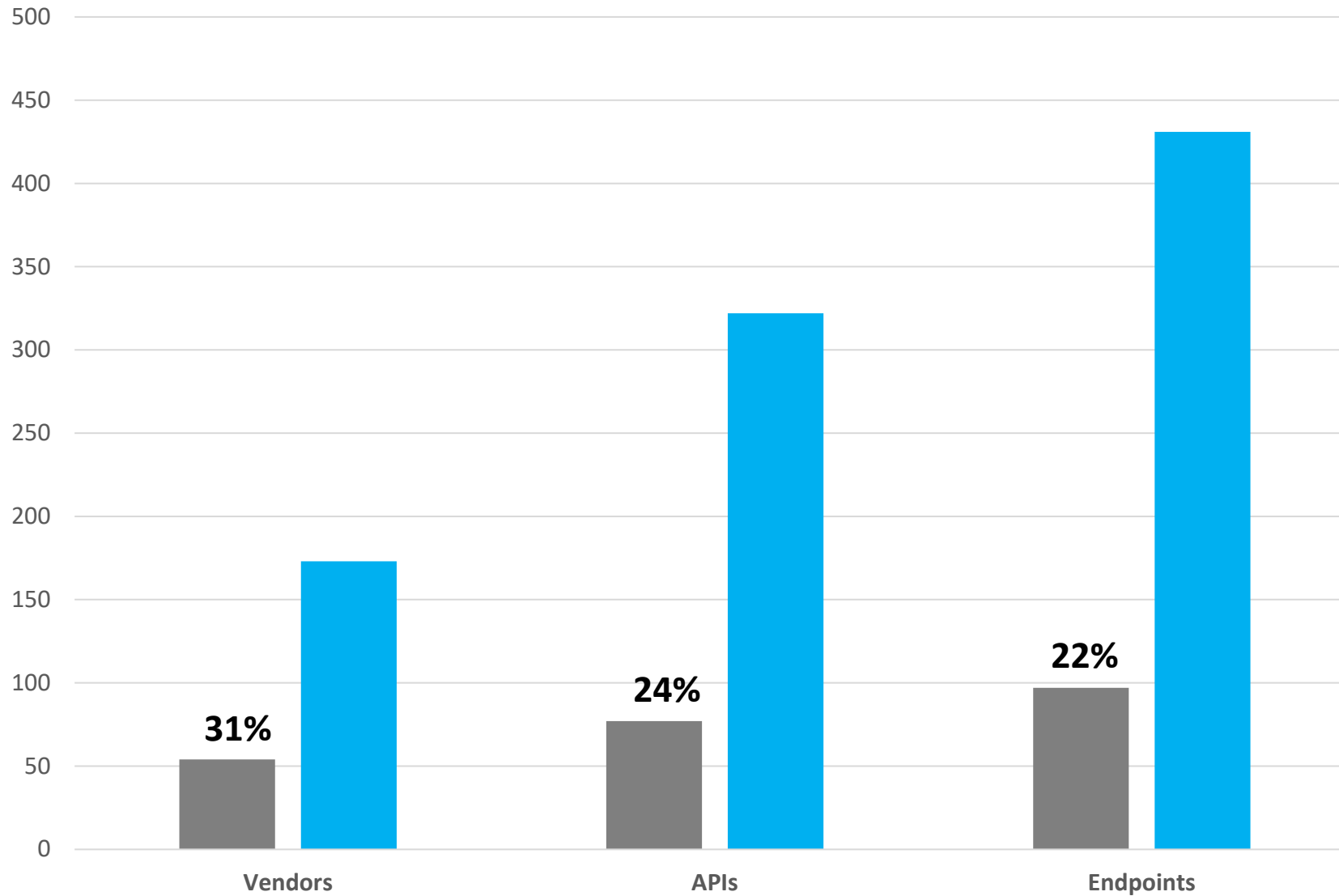
Unsecured/No Access Control (OWASP-1)



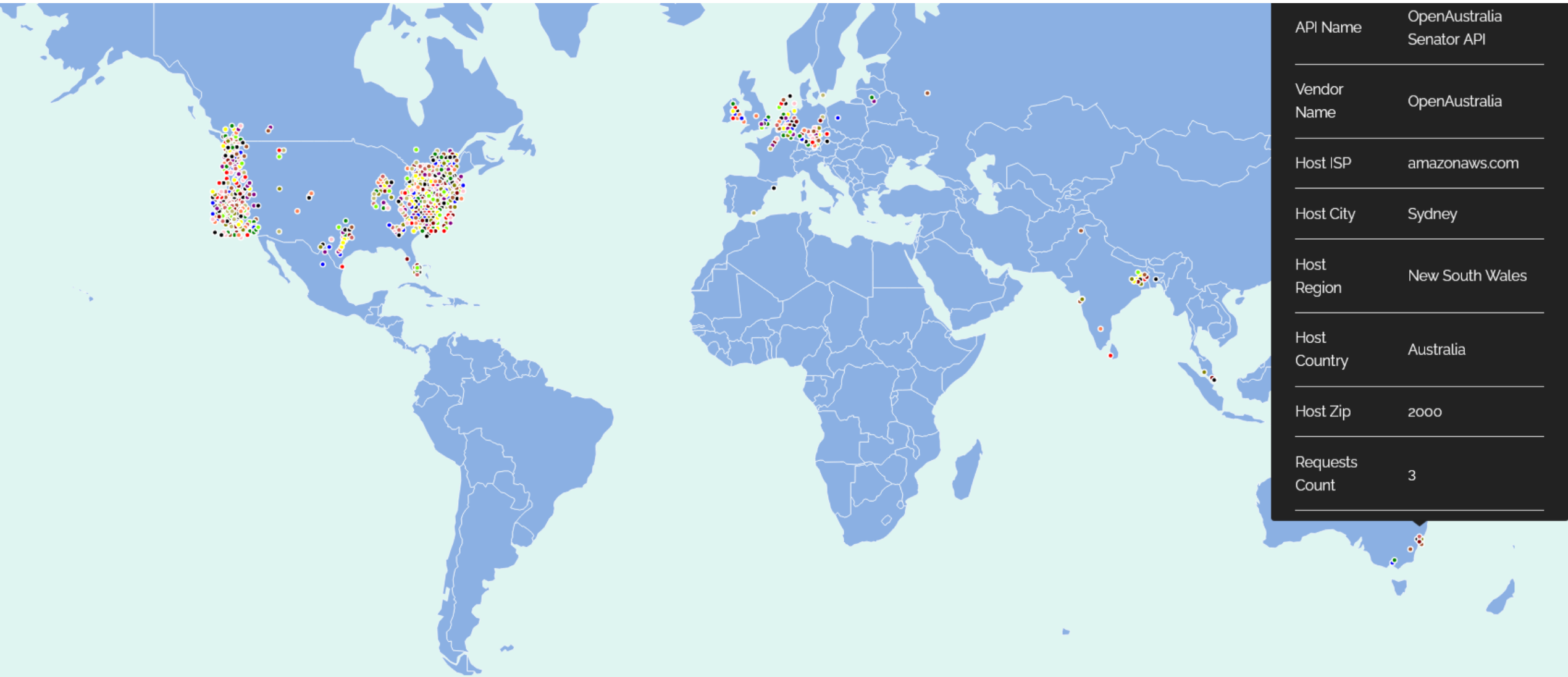
Sensitive Data Exposure (OWASP-3)



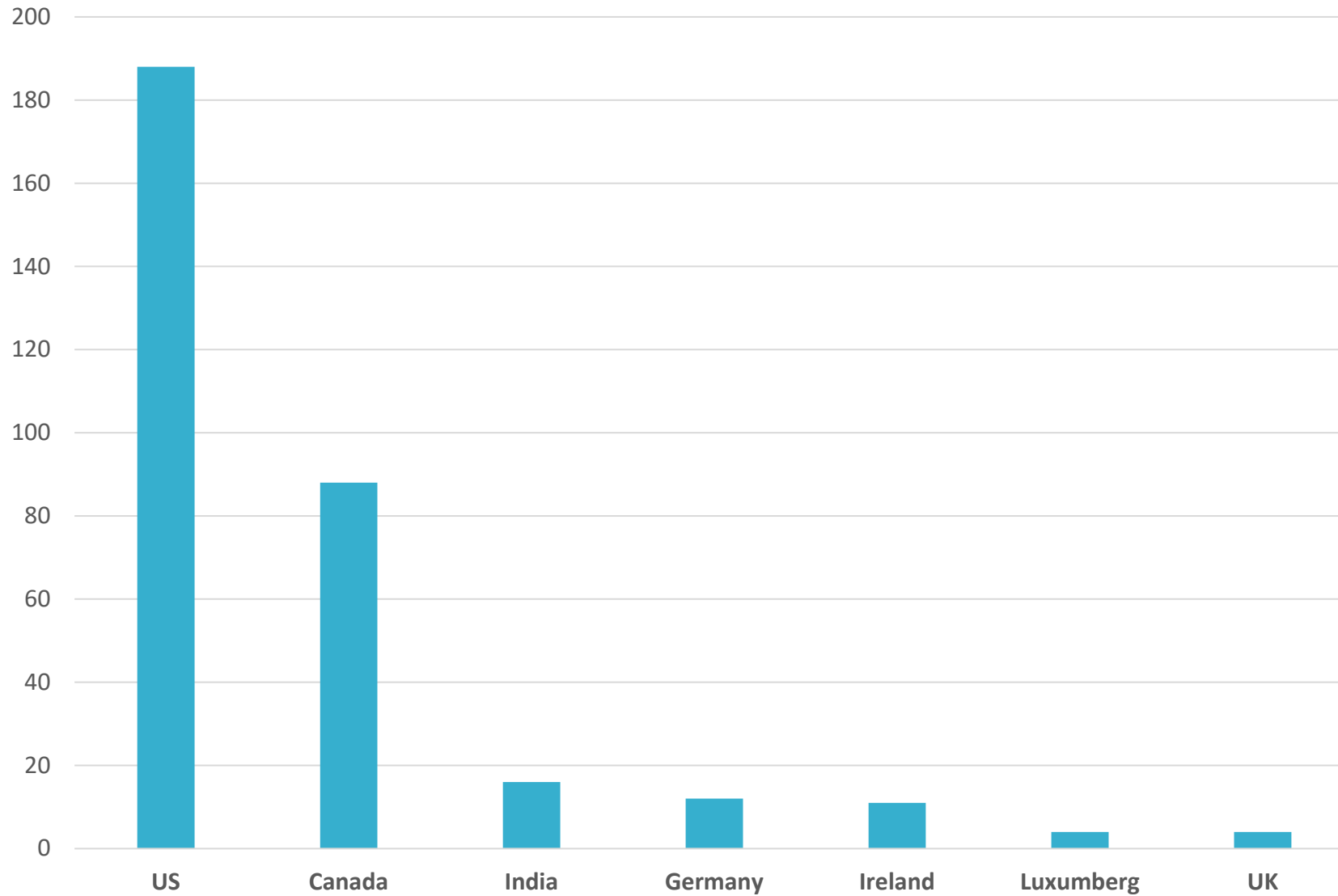
Vulnerable Servers (OWASP-3)



Open API Governance Challenges



Geolocation of API Servers



Summary & Takeaways

Gain Coverage

Discover Open APIs
Cover Attack Surface
Protect Applications

Save Costs

Development Cost
Legal & Security Cost
Fines & Audit Cost

Reduce Risks

PCI, SOC2, HIPPA,
ISO27001 Compliance
Audits and M&A

Build Trust

Team Collaborations
Customer Satisfaction
Enterprise Reputation



API Scan



API Benchmark



API Security



API Monitoring



API Marketplace

How to get involved ?

■ Join API Discovery community

- Signup : <https://apidiscovery.teejlab.com/edsn>
- Explore Open APIs / Upload new Open APIs
- Benchmark Open APIs using OWASP Top-10 and others
- Help community use Open APIs in secure & compliant way

■ Contribute to Open APIs

- Thought Leadership
- Webinars & Fireside Chats
- Contact: info@teejlab.com

Acknowledgements and Contact

Thanks to

OWASP Vancouver Community
Jeevan Singh and Farshad Abasi

Contact

Baljeet Malhotra
info@teejlab.com | https://teejlab.com