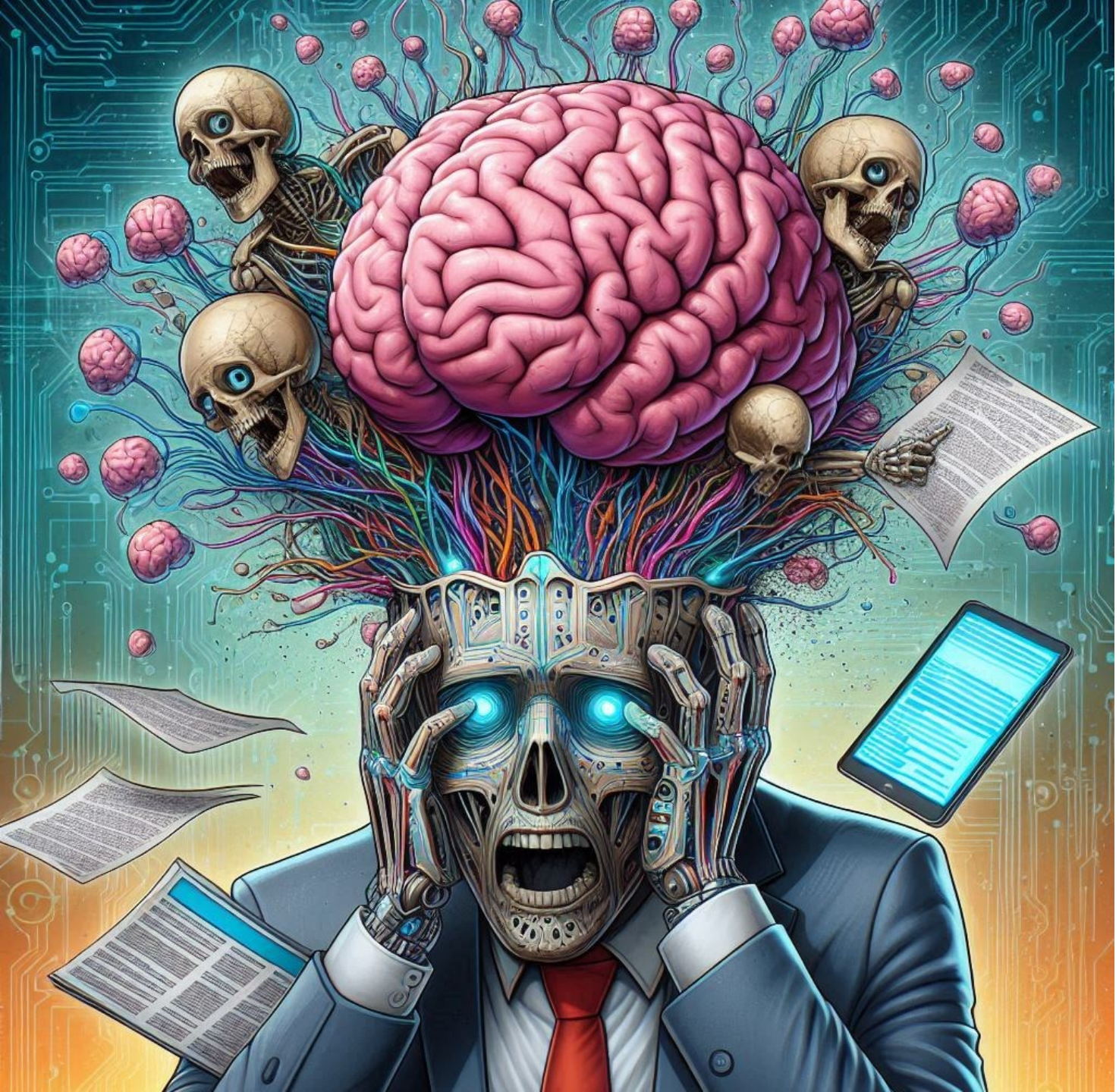
Infrastructure Meets AI: What should security-pro know about AI

MSUG
23.10.2024



Who has AI hype overload?

Markus Lintuala

CLOUD HERO

markus@lintuala.fi | +358 40 585 5531

elisa

- 🫠 Can’t say no for anything new
- 🗣️ Public speaker
- 😋 Gastronomic, craft beer and wine geek
- 🌏 Loves travelling and aviation
- 🚘 Waze map editor

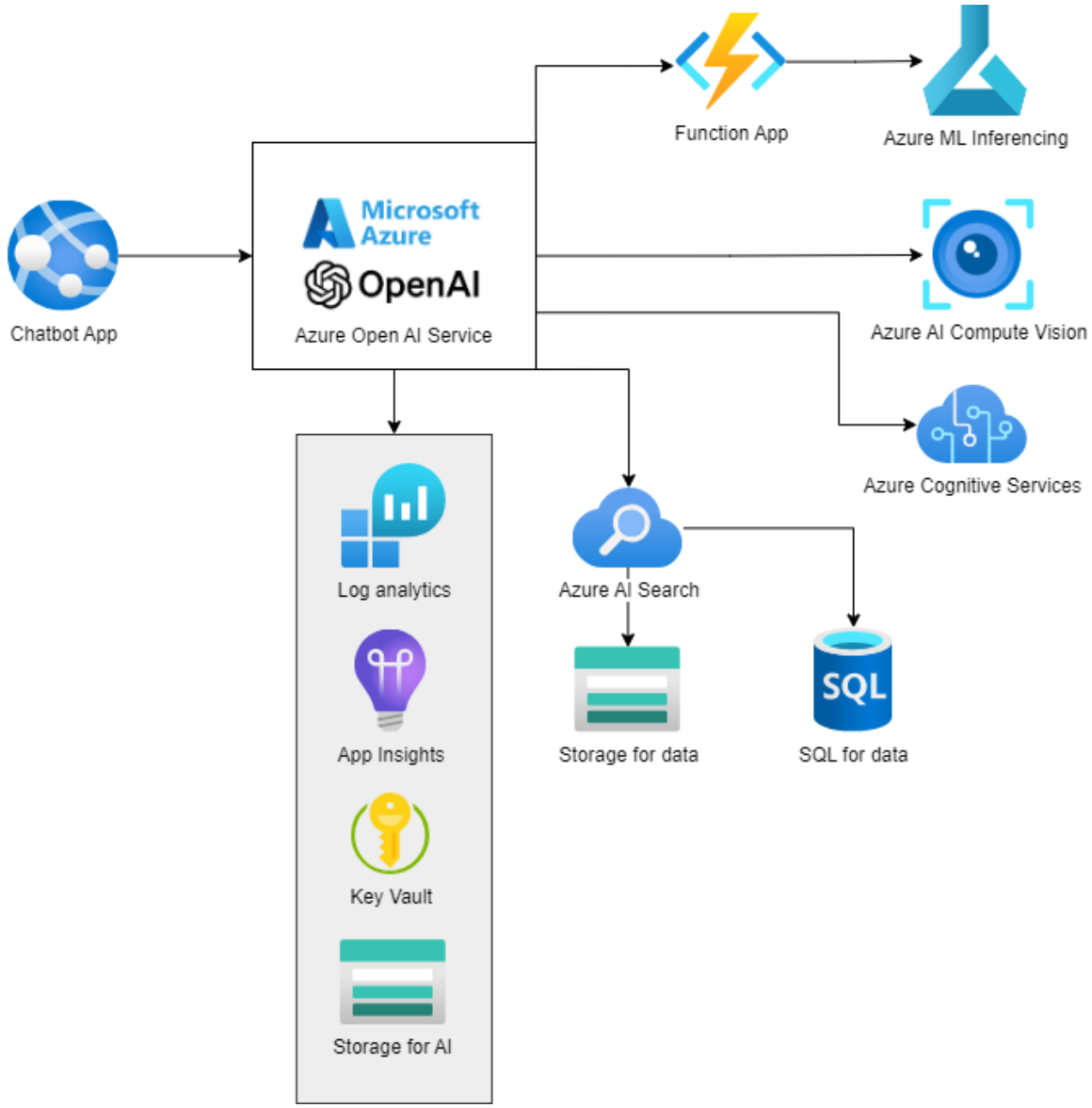
@MarkusLintuala

@mmaraa

What should Azure security-pro know about AI?

- Posture of resources
- Connectivity
- Security
- Published applications
- Published APIs
- Related resources

Posture of resources



Connectivity

- Internal / External connectivity
- Use Web Application Firewall
- Other networks
- Use Zero Trust concept for networking

Security

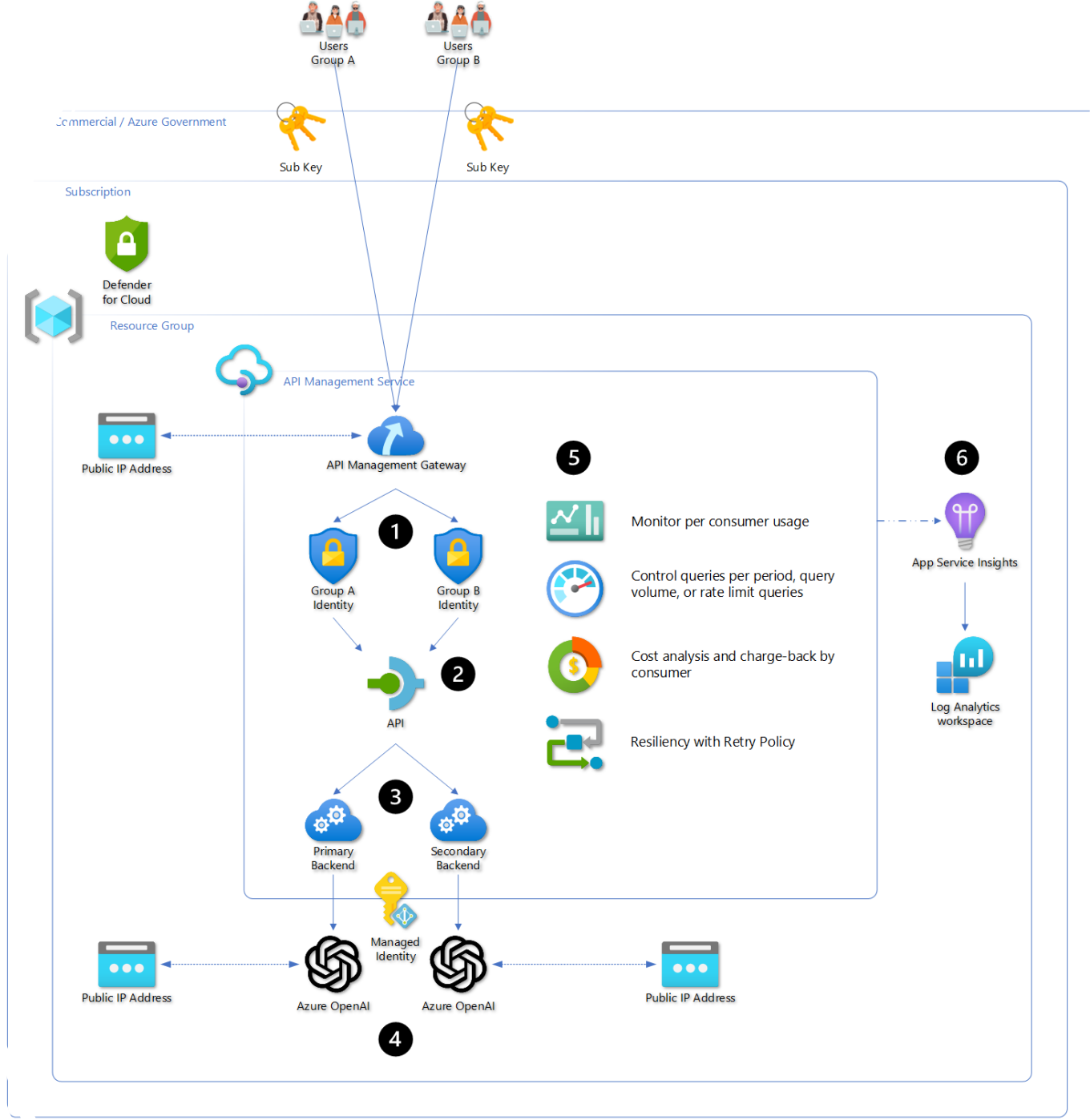
- Authentication for Apps, APIs, between resources
- Application attack vectors
- Use protection features, but do not restrict productivity
- Prefer usage of managed identities
- Use Defender for APIs to tackle OWASP API Top 10 attacks

Published applications

- Authenticated or not
- Rate limits
- Minimize lateral movement
- DOS protection and WAF
- Exposed security endpoints
- Application vulnerabilities

Published APIs

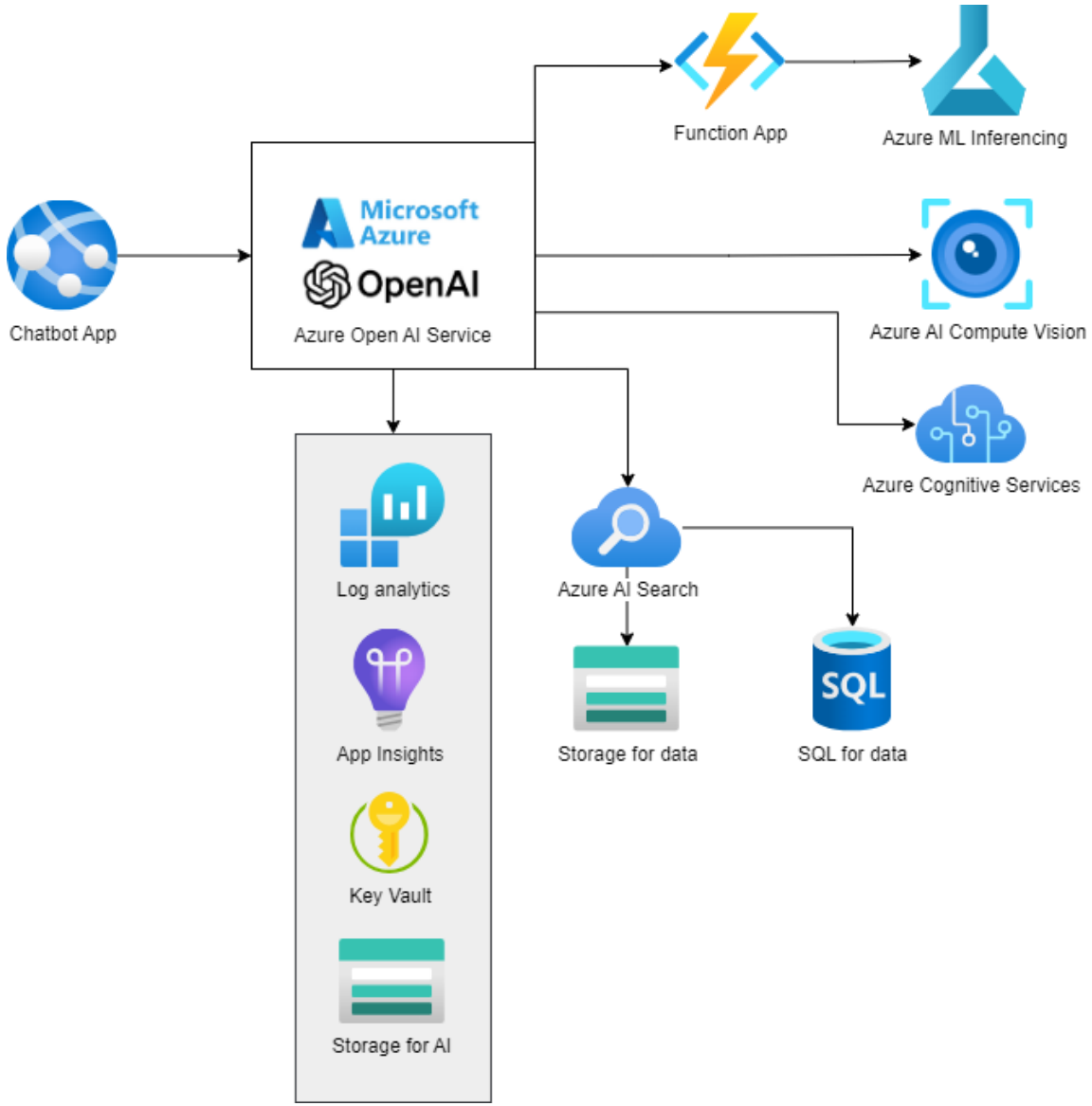
- **No** direct connections
- Use API Management
- Restrict access from network and require authentication
- Disable local authentication



GitHub - microsoft/AzureOpenAI-with-APIM: Deploy APIM. Auto-configure it to work with your Azure Open AI.

Related resources

- Vector databases
- Storage accounts
- Functions
- Other network connected applications and resources
- Azure AI Services



Other considerations

- Entra External ID for better user access management towards API Management
- Remember AI on low-code/no-code solutions
- Is file level labeling and encryption the only solutions for protecting data in future?

Demo

Takeaways

- **Secure** your applications and APIs
- **Disable** local authentication
- **Support** AI developers as much as you can
- Start **labeling** your files and **protecting** those with file level encryption

Q & A