

# Azure OpenAI Security: Best Practice on using Azure OpenAI service

Beata Zalewa

# About me



Security Architect



Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



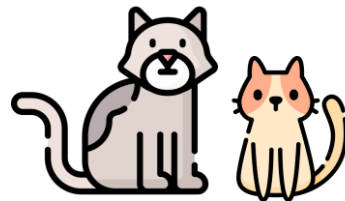
Google Cloud



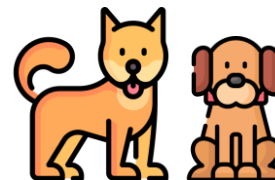
1 Husband



1 Daughter



2 cats



2 dogs



Detective stories



Photography

# Introduction to GenAI Applications

- GenAI applications are those that use large language models (LLMs) to generate natural language texts or perform natural language understanding tasks.
- LLMs are powerful tools that can enable various scenarios such as content creation, summarization, translation, question answering, and conversational agents.

# Introduction to Azure OpenAI

## Artificial Intelligence

### Machine Learning

### Deep Learning

1956

### Artificial Intelligence

the field of computer science that seeks to create intelligent machines that can replicate or exceed human intelligence

1997

### Machine Learning

subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions

2017

### Deep Learning

a machine learning technique in which layers of neural networks are used to process data and make decisions

2021

### Generative AI

Create new written, visual, and auditory content given prompts or existing data.

# The Microsoft Azure AI Portfolio

## Azure AI Studio

The place to test, build and deploy AI solutions

### Azure AI Services

Pre-built models, APIs and SDKs to infuse into custom apps



Azure OpenAI Service



Azure AI Search



Azure AI Speech



Azure AI Vision



Azure AI Content Safety



Azure AI Document Intelligence



Azure AI Language



Azure AI Translator

### Azure Machine Learning

Advanced tools for designing and fine-tuning specialized AI models



Responsible AI Dashboard



Model Catalog



Prompt Flow



MLOps And LLMops

Florence

GPT-4 and GPT-3.5-Turbo

Embeddings

Meta Llama 2

Turing

Whisper

DALL-E

Hugging Face

### Azure AI Infrastructure

State-of-art supercomputing to power AI workloads

# Security Challenges in GenAI Applications

- **Data Protection:** Confidentiality and integrity of training and query data.
- **Service Reliability:** Ensuring availability and reliability of LLM services.
- **Misuse Prevention:** Preventing misuse or abuse by malicious actors or unintended users.
- **Output Monitoring:** Auditing outputs for quality, accuracy, and compliance.
- **Ethical Management:** Managing ethical and social implications of outputs.

# Jailbreak Attack or User Prompt Injection Attack (UPIA)

Intentional attempt by a user to

Exploit the  
vulnerabilities of an  
llm-powered system

Bypass its safety  
mechanisms

Provoke restricted  
behaviors.

# Jailbreak risk detection or Prompt Shields for User Prompts

Unified API that  
analyzes LLM  
inputs and  
detects **user  
prompt and  
document  
attacks**

Model that  
identifies  
anomalies in  
user prompts as  
potential  
jailbreak attacks

Enhances the  
security of LLM  
deployments



## The principle of shared responsibility

- **The principle of shared responsibility** highlights that security in the cloud is a two-way street.
- While Microsoft ensures the security of the Azure OpenAI services, it is the customer's responsibility to secure their end of the interaction.

# Microsoft responsibility

Protecting the  
Azure  
infrastructure

Making sure that  
the Azure  
OpenAI services  
are secure by  
default

Providing  
identity and  
access  
management  
capabilities

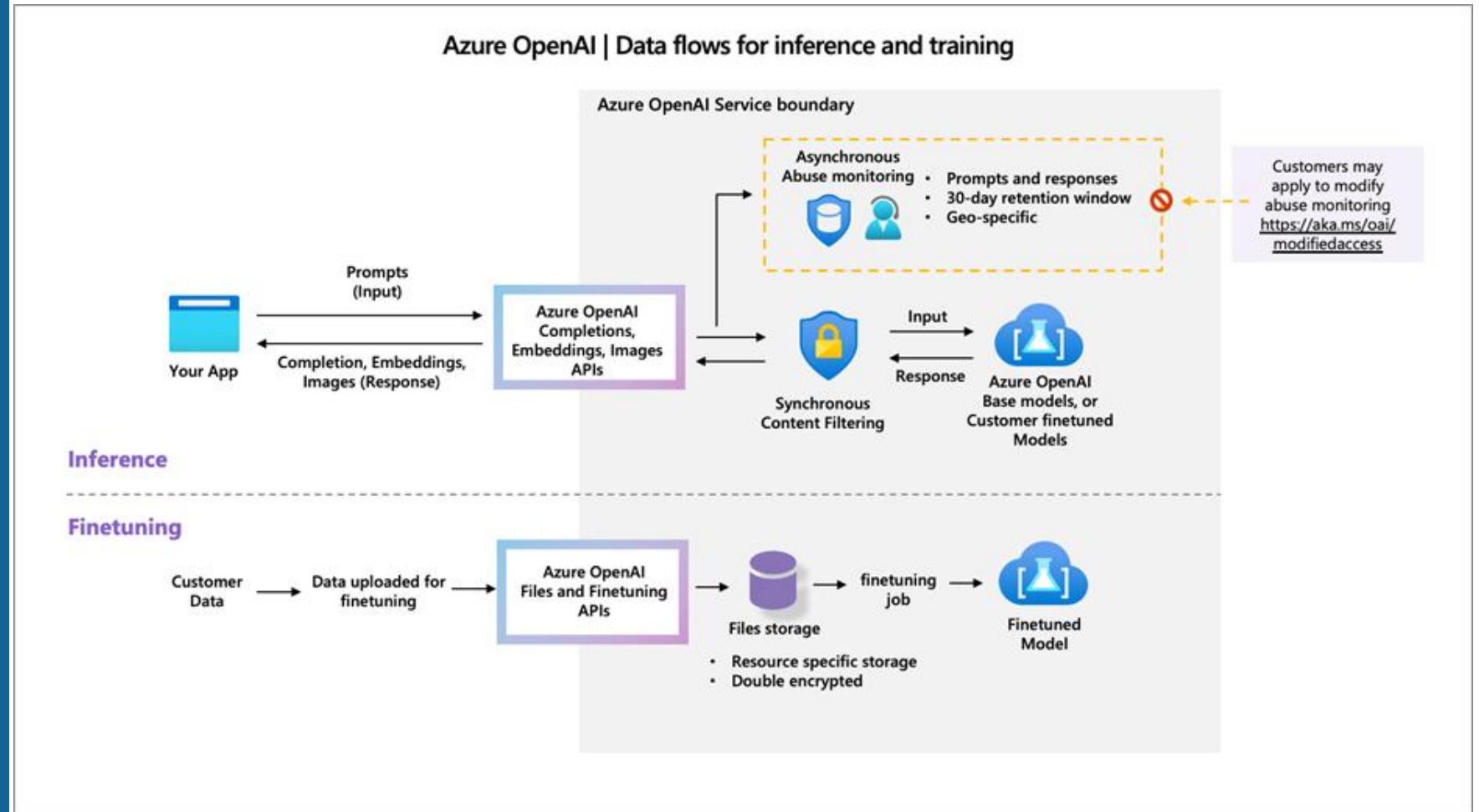
# Customers responsibility

Setting  
appropriate access  
controls and  
permissions for  
their use of Azure  
OpenAI

Protecting their  
Azure credentials  
and managing  
access to their  
Azure subscription

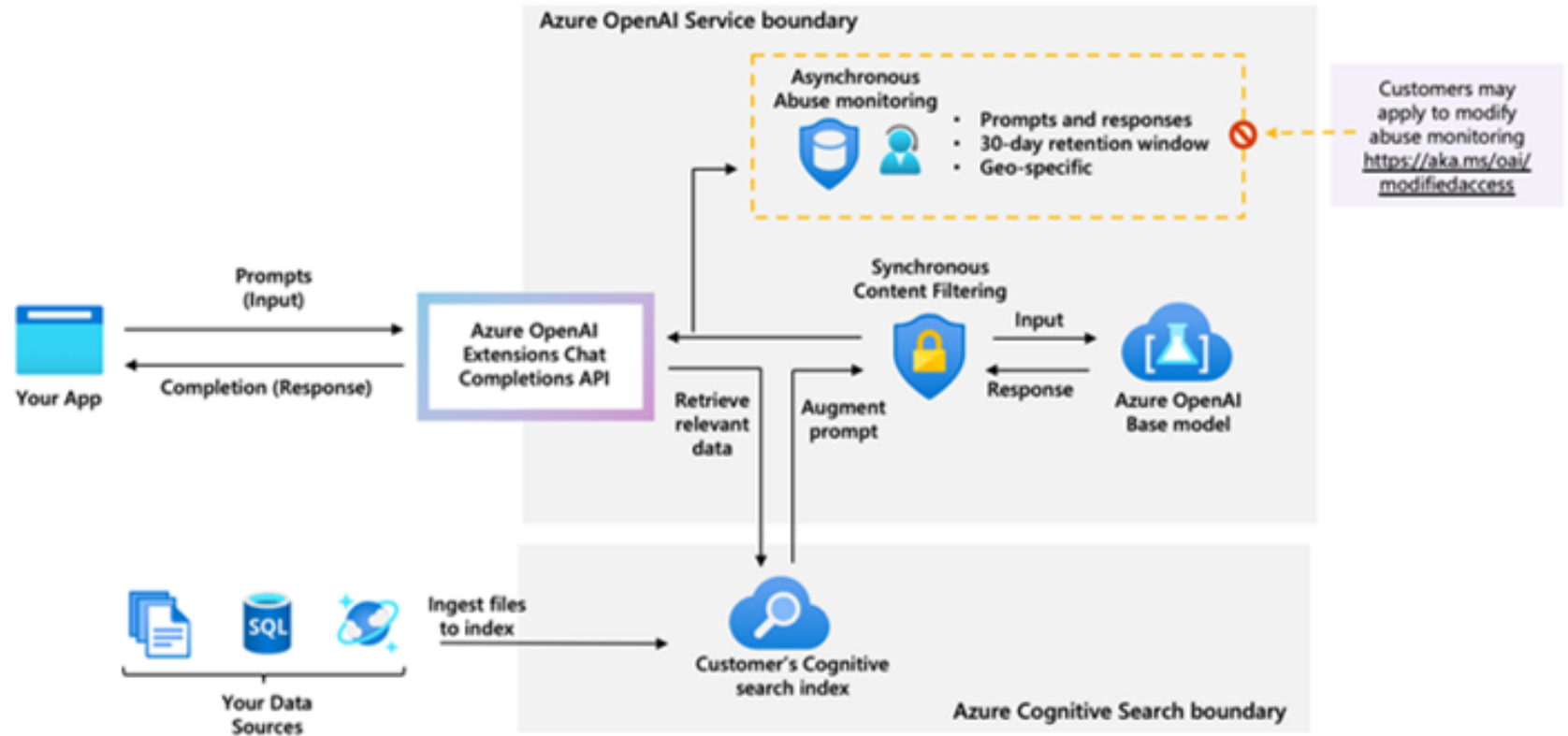
Ensuring that the  
security measures  
around their  
applications are  
adequate, including  
input validation,  
secure application  
logic, and proper  
handling of Azure  
OpenAI outputs

# How does the Azure OpenAI Service process data?



# Augmenting prompts with data retrieved from your data sources to "ground" the generated results

## Azure OpenAI | Data flows for inference 'on your data'



# Data Processing Foundations

Core principles of data processing:

- Secure data processing
- Efficient algorithms
- Real-time processing
- Compliance with standards
- Scalability

## Core principles of data storage

- Azure OpenAI's approach to data storage and processing is built on strong, secure foundations.
- User data is guarded against unauthorized access, ensuring privacy and security in line with Microsoft's data protection standards.

## Core principles of data storage

- Regarding the types of processed data, Azure OpenAI processes your input - prompts and the ensuing AI-generated answers.
- It also processes data submitted for the purpose of training tailored AI models.



# Privacy

- **Privacy** in Azure OpenAI refers to how user data is handled in terms of access and usage.
- It ensures that data such as inputs, interactions, and outputs are used in a way that respects customer confidentiality.
- Azure OpenAI's privacy protocol dictates that Microsoft does not view or use this data for its own purposes, unless explicitly permitted for services like model fine-tuning.

# Privacy Protection

Ensuring user privacy:

- Data anonymization
- User consent
- Data minimization
- Privacy policies
- Compliance with GDPR

## Data privacy

- As for the usage of data, the **principles are simple.**
- The input you provide, along with the AI responses - your data - **remains yours.**
- Microsoft does not use this data to better their own AI offerings. It is kept private unless you choose to use it to train customized AI models.

## Data privacy

- The service's content generation capacity comes with a commitment to safety.
- Input is carefully processed to produce responses, and content filters are in place to prevent the generation of problematic content.

## Data privacy

- Customizing models is a service feature that's handled with care.
- You can train Azure OpenAI models with your data, knowing that it remains secure and for your use only.
- Privacy measures are about control over and the ethical handling of data.

## Data privacy

- To prevent abuse, Azure OpenAI comes equipped with robust content filtering and monitoring systems.
- This is to make sure that the generation of content complies with guidelines and that nothing harmful slips through.

# Privacy Policies

Privacy policies in place:

- Policy overview
- User rights
- Data usage
- Data sharing
- Policy updates

# Compliance Standards

Compliance with industry standards:

- ISO certifications
- GDPR compliance
- HIPAA compliance
- SOC 2 compliance
- Regular compliance audits



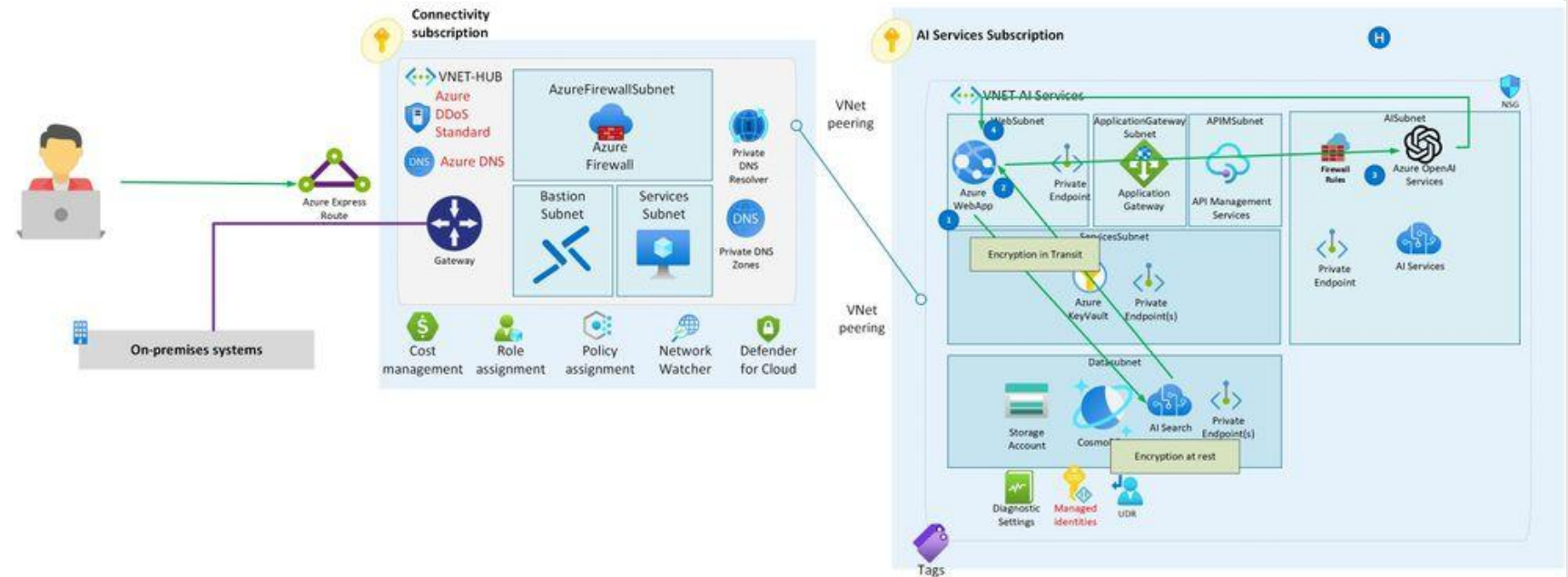
**DEMOS!!!**

Azure OpenAI  
Studio

# Security

- **Security**, on the other hand, is about protecting data from unauthorized access, breaches, and other forms of compromise.
- Azure OpenAI employs a range of security measures, such as encryption in transit and at rest, to safeguard data against threats.
- Microsoft's infrastructure provides a secure environment designed to shield your data from security risks.

# Data security



# Security Measures

Security measures in place:

- Encryption techniques
- Access controls
- Monitoring and logging
- Incident response regular audits

# Access Controls

Managing access to data:

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Least privilege principle
- Access reviews
- User activity monitoring

# Monitoring and Logging

## Monitoring and logging practices:

- Continuous monitoring
- Log management
- Threat detection
- Incident response
- Compliance reporting

# Incident Response

## Handling security incidents:

- Incident response plan
- Detection and analysis
- Containment and eradication
- Recovery and lessons learned
- Communication protocols

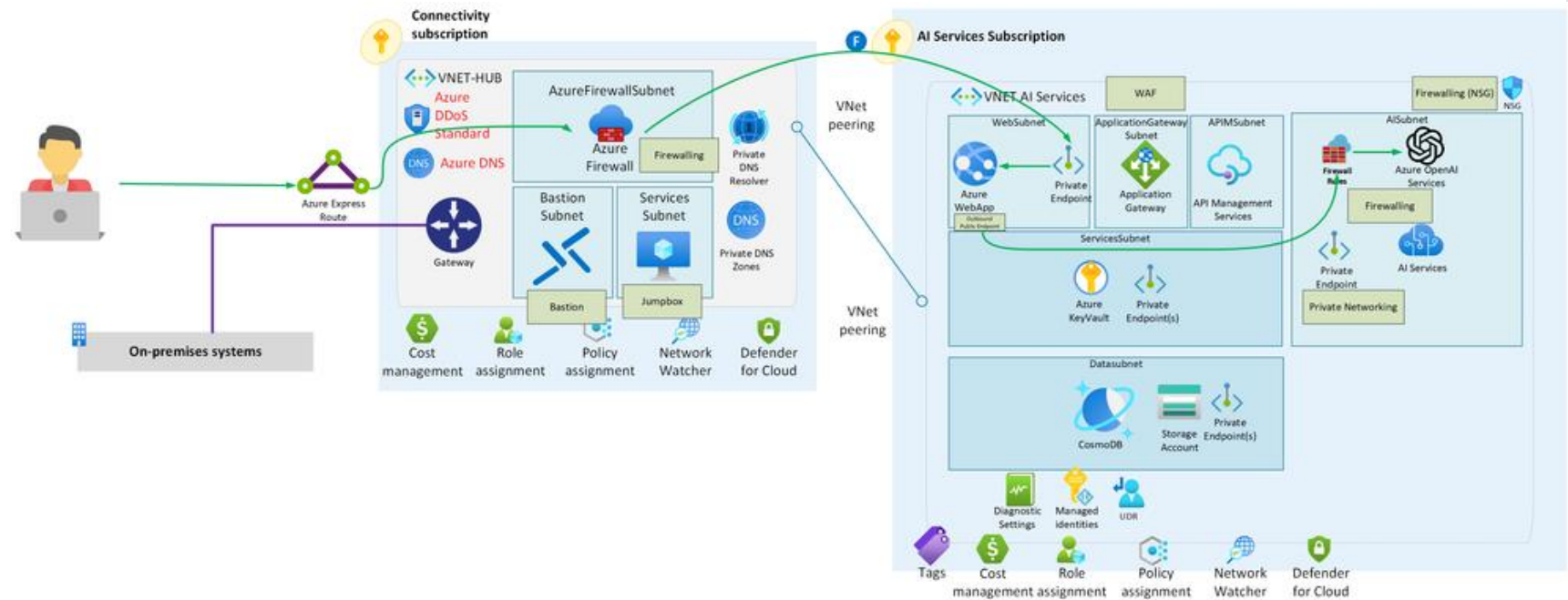
# Data Encryption

Encryption methods used:

- Encryption at rest
- Encryption in transit
- Key management
- Advanced encryption standards
- Data Classification and Sensitivity



# Network security



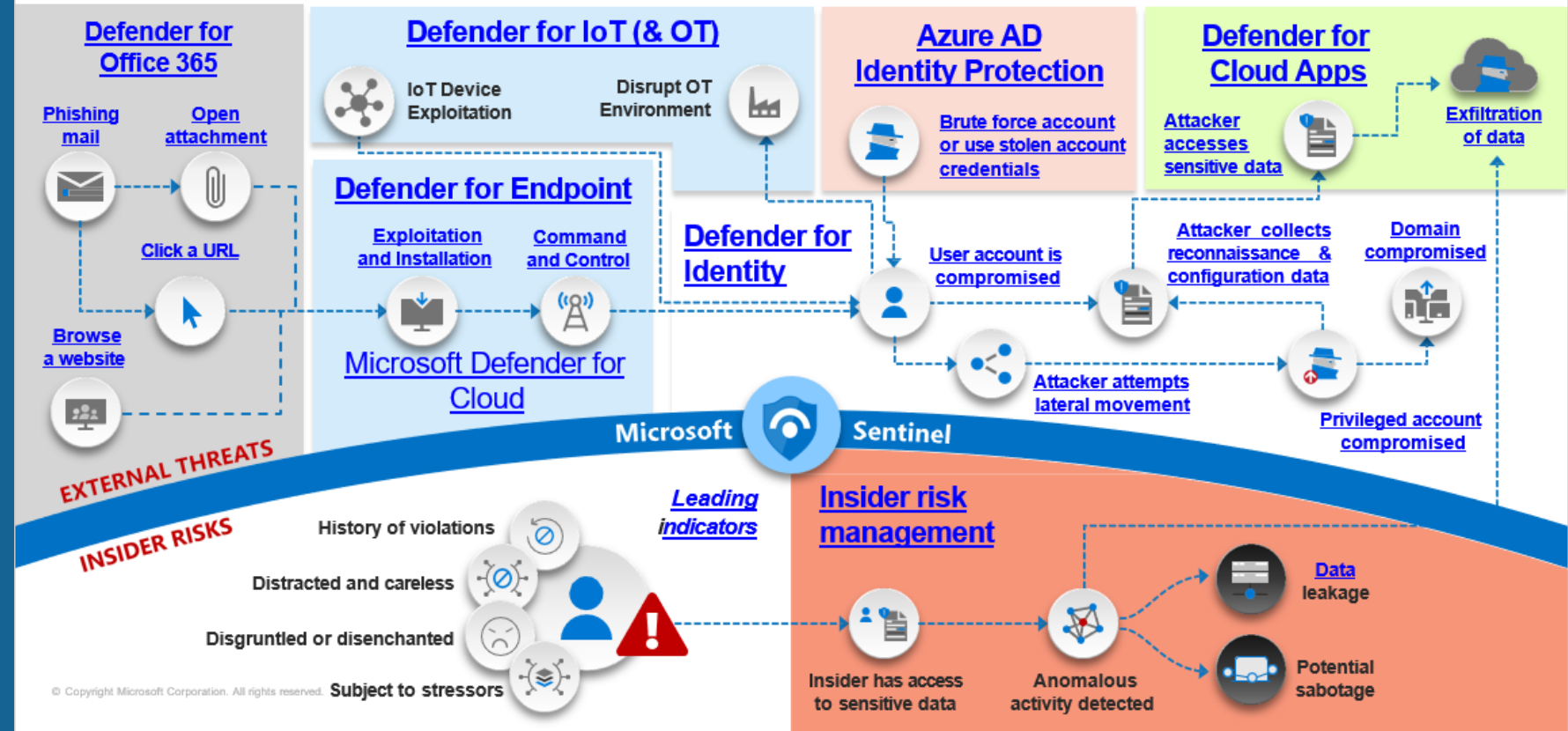
**DEMOS!!!**

Azure  
portal

# Defenders

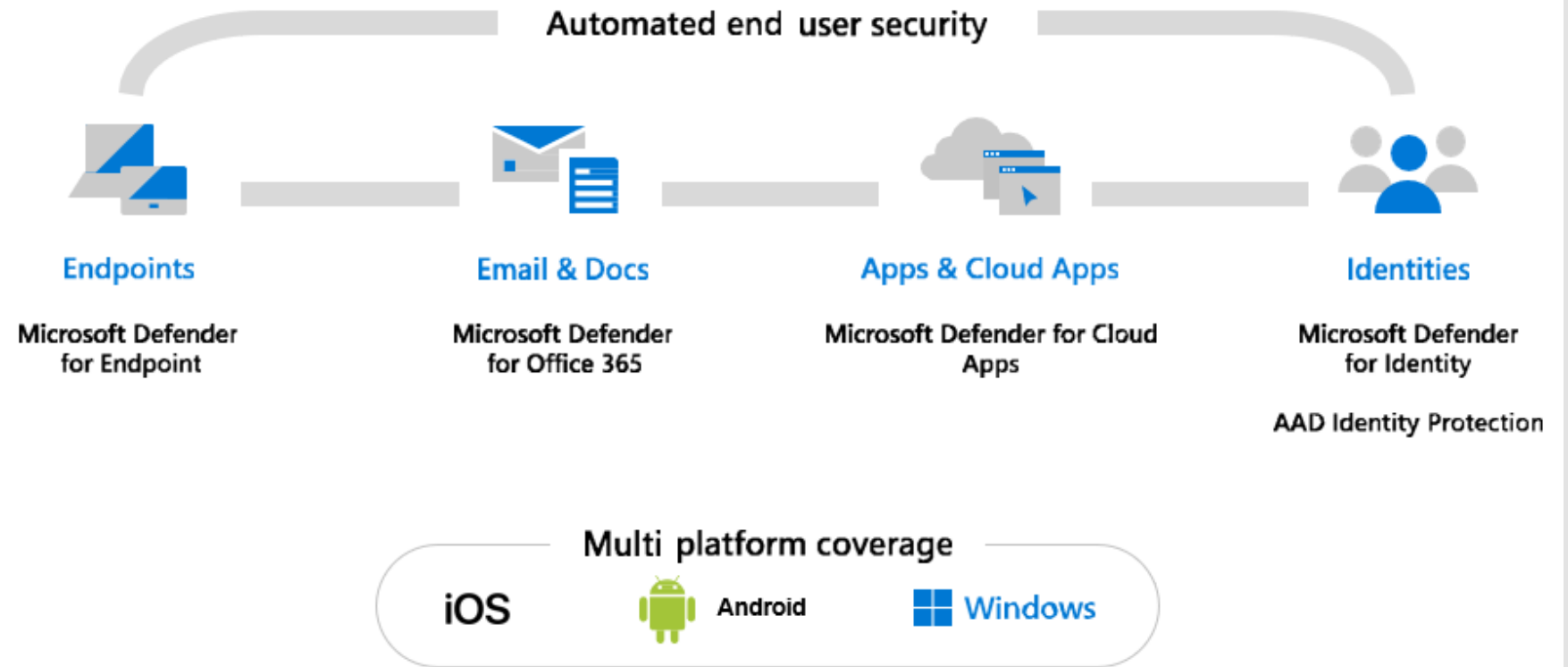
## Defend across attack chain with extended detection and response (XDR)

Microsoft December 2021 <https://aka.ms/MCRA>



# Microsoft 365 Defender

## Microsoft 365 Defender



# Defender for Endpoint

## Microsoft Defender for Endpoint



macOS



iOS



Cisco  
Juniper Networks

HP Enterprise  
Palo Alto Networks

Endpoints and servers



Mobile device OS

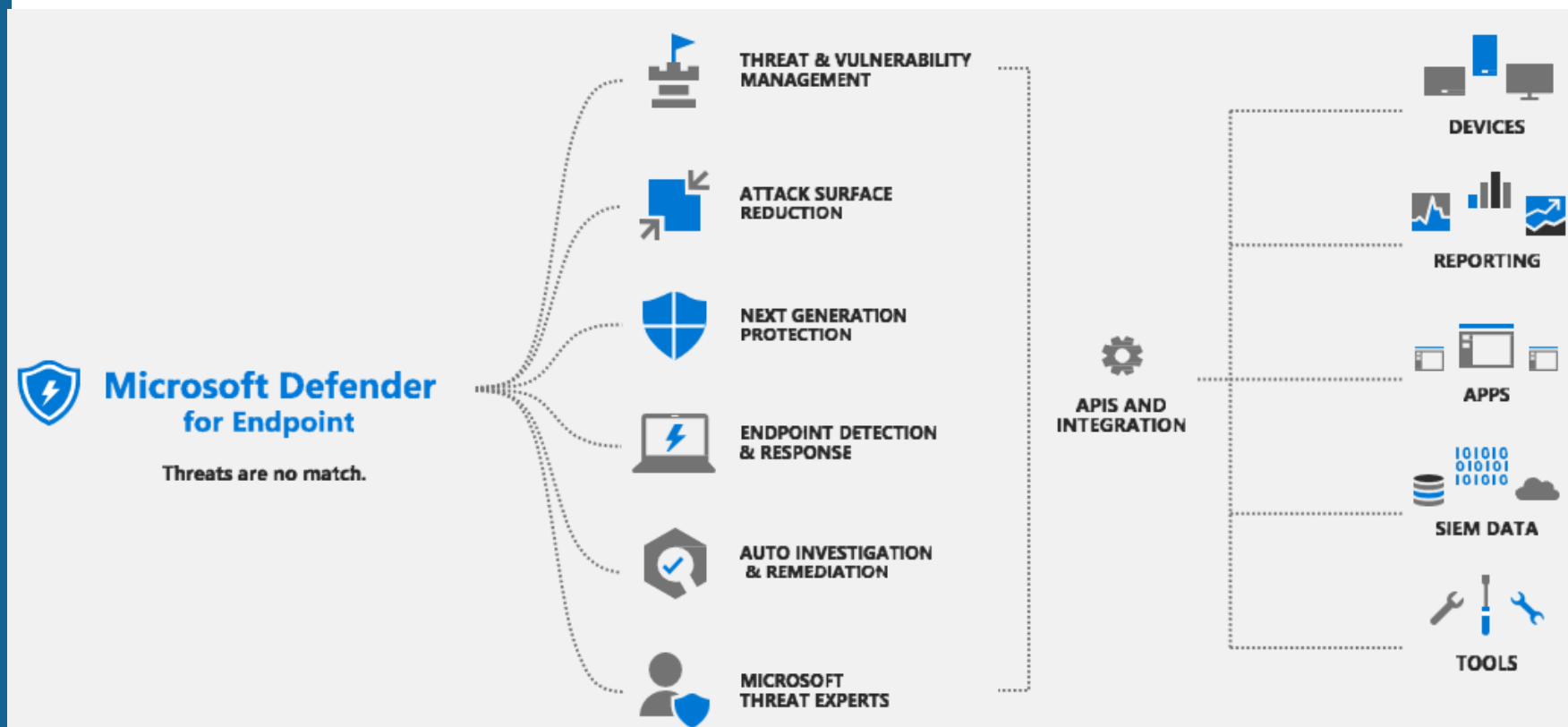


Mobile Threat Defense

Virtual desktops

Network devices

# Connecting with the platform



# Defender for Endpoint

## Microsoft Defender for Endpoint



macOS



iOS



Cisco  
Juniper Networks

HP Enterprise  
Palo Alto Networks

Endpoints and servers



Mobile device OS



Mobile Threat Defense

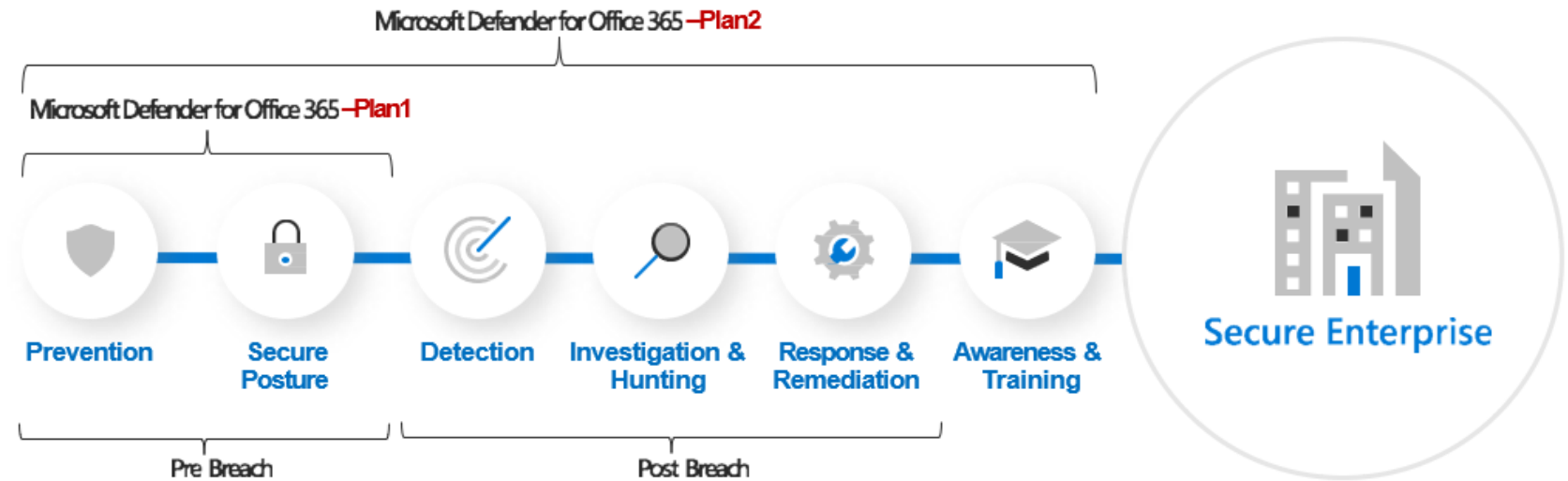
Virtual desktops

Network devices

# Defender for Office 365

## Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention





# Defender for Cloud Apps

Cloud App Security

Cloud Discovery

Dashboard | Discovered apps | IP addresses | Users | Machines

Continuous report Win10 Endpoint Users | Timeframe Last 90 days | Updated on Sep 26, 2018

QUERIES: Select a query...

APPS AND DOMAINS: Apps, domains...

APP TAG: ☒ Sanctioned ☐ Unsanctioned ☐ None

RISK SCORE: 0 to 10

COMPLIANCE RISK FACTOR: Select factors...

SECURITY RISK FACTOR: Select factors...

Browse by category:  Search for category...

- Cloud storage
- Hosting services
- Marketing
- IT services
- Accounting and finance
- Collaboration
- Security
- Online meetings
- Communications
- Web analytics
- Content management
- Content sharing
- News and entertainment
- Social network
- CRM

1 - 20 of 27 discovered apps

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Machines	Last seen (UTC)	Actions
Microsoft OneDrive for Cloud storage	10	98.5 GB	65.8 GB	125K	1109	2540	1110	Sep 20, 2018	✓ ⌚ ⋮
Dropbox Cloud storage	8	3.5 GB	2.5 GB	11.8K	918	1328	919	Sep 24, 2018	✓ ⌚ ⋮
Mozzy Cloud storage	7	1.1 GB	732 MB	1.3K	187	127	188	Sep 24, 2018	✓ ⌚ ⋮
iCloud Cloud storage	7	1.1 GB	689 MB	1.3K	182	132	182	Sep 24, 2018	✓ ⌚ ⋮
iDrive Cloud storage	6	443 MB	272 MB	1.7K	235	174	235	Sep 24, 2018	✓ ⌚ ⋮
Livedrive Cloud storage	6	258 MB	180 MB	1.5K	213	157	213	Sep 24, 2018	✓ ⌚ ⋮
SugarSync Cloud storage	6	1.5 GB	1.1 GB	1.6K	224	169	225	Sep 24, 2018	✓ ⌚ ⋮
BitTitan	6	24 MB	21 MB	1.2K	178	132	178	Sep 24, 2018	✓ ⌚ ⋮

## Used resources

<https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy>

<https://learn.microsoft.com/en-us/azure/ai-services/content-safety/concepts/jailbreak-detection>

<https://learn.microsoft.com/en-us/azure/ai-services/content-safety/concepts/groundedness#groundedness-detection-features>

<https://learn.microsoft.com/en-us/azure/cognitive-services/openai/how-to/monitoring#monitoring-data>

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/monitor-azure-resource#monitoring-data-from-azure-resources>

I am actively seeking new opportunities and exciting challenges. If you would like to get in touch, please feel free to reach out through the following channels:

Email: [beata@zalnet.pl](mailto:beata@zalnet.pl)

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa>

GitHub: <https://github.com/beatazalewa/Conferences/>

