

# Is cyber security getting under your company skin ?

*How to fight online frauds with smoothest UX*

**Michal Antoniak**

Cyber Security Consulting Manager



*Joint Fraud Conference*

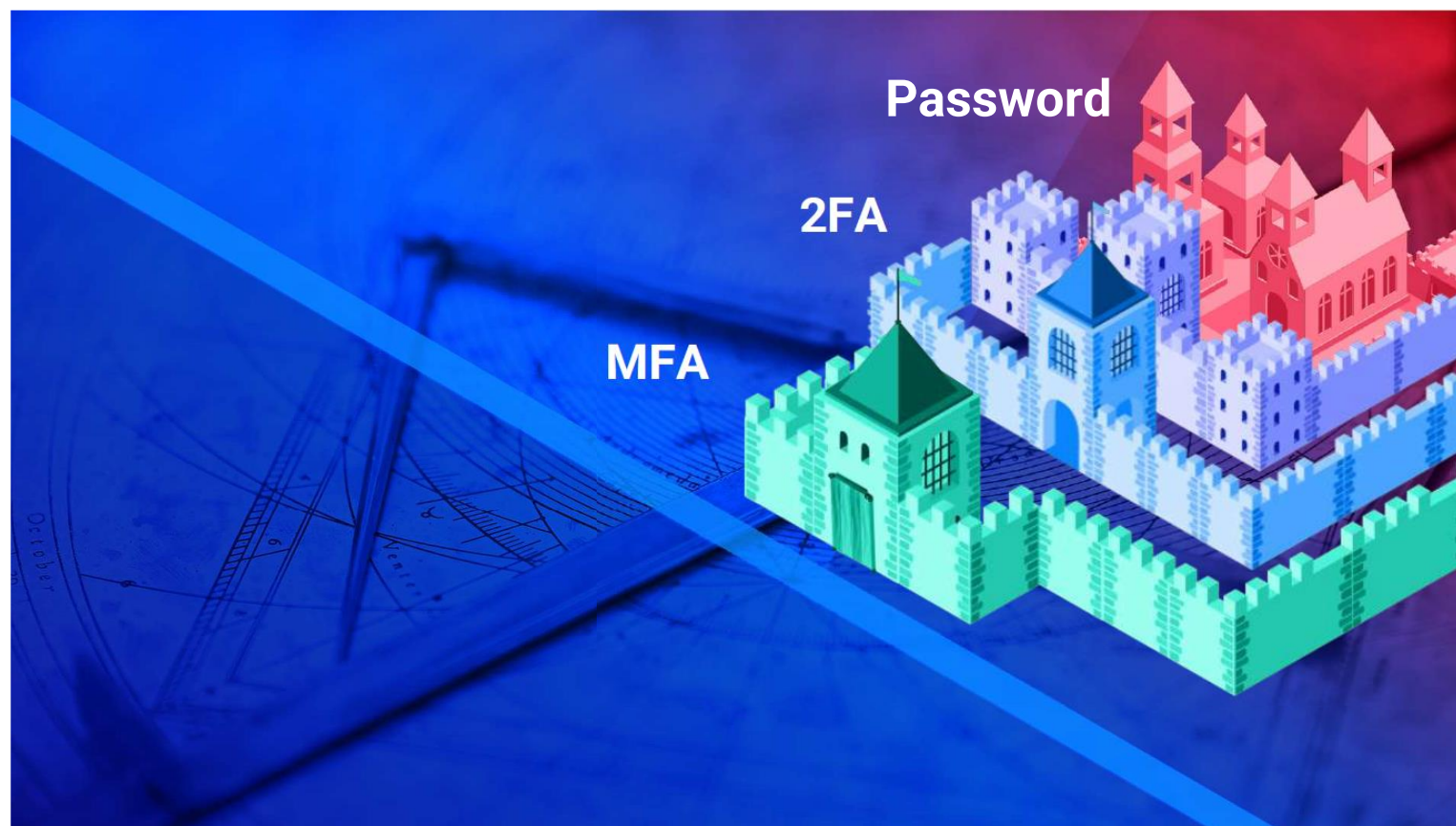


# The Chinese Wall syndrom



*Joint Fraud Conference*

# The Chinese Wall syndrom



*Joint Fraud Conference*

# Why the old concept backfires ?

„The more secure you make something,  
the less secure it becomes.”

Don Norman  
[jnd.org](http://jnd.org)



*Joint Fraud Conference*



# More Security $\neq$ Less Friction

A donut chart with a blue-to-teal gradient, showing 99% completion with a small gap at the top.

**99%**

IT departments believed  
2FA was the best way  
to protect an identity and  
the access to it

A donut chart with a purple-to-pink gradient, showing 74% completion with a larger gap at the top.

**74%**

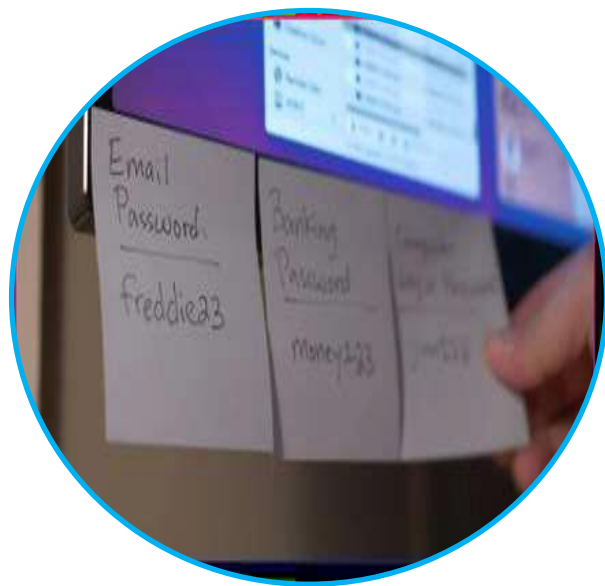
admit that they receive  
complaints about it  
from their users

<https://betanews.com/2017/01/11/2fa-complaints-rise/>

*Joint Fraud Conference*



# When the friction is just too much



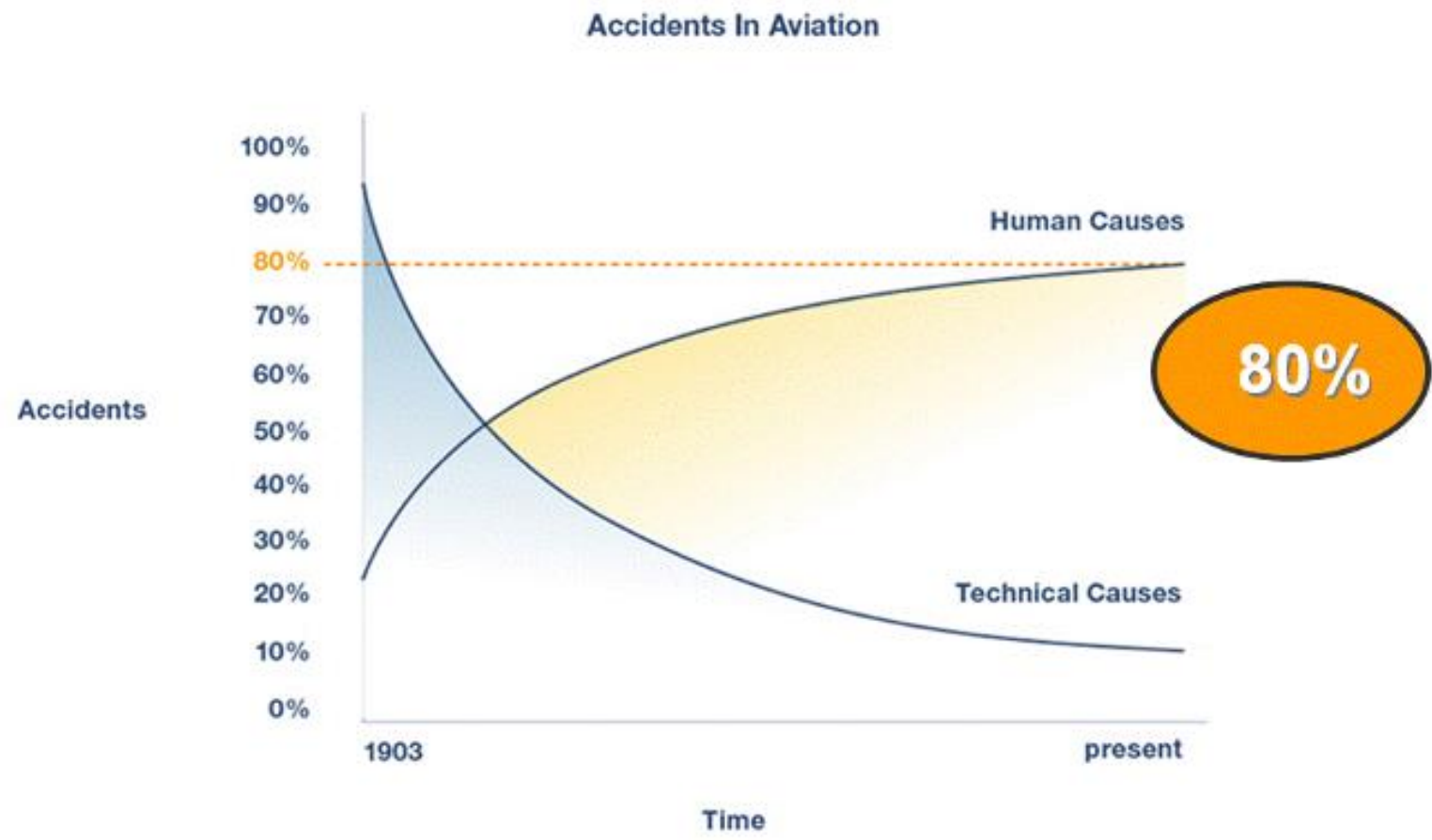
**Too complex  
password  
policies**



**Too many  
Authentication  
factors**

*Joint Fraud Conference*

# The Human Factor



*Joint Fraud Conference*

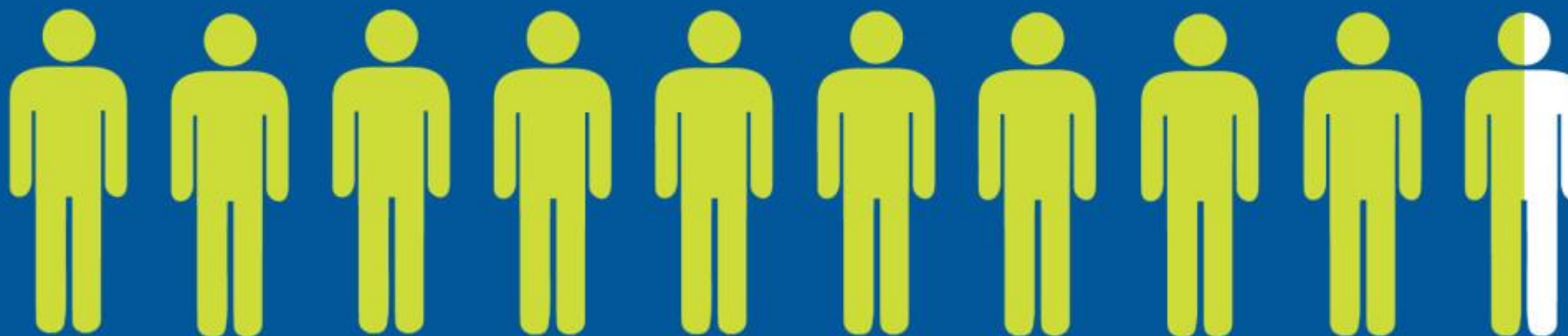


# The Human Factor

# 95%

of all successful cyber attacks  
is caused by human error

Source: IBM Cyber Security Intelligence Index





# The Human Factor

*In 2018 and 2019, the combined threats of phishing and credential stuffing made up roughly half of all publicly disclosed breaches in the United States.*

<https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/2021-Credential-Stuffing-Report-rev.pdf>

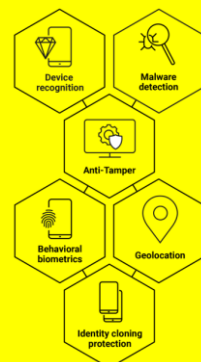


*Joint Fraud Conference*



# More Security & Less Friction ?

## Adaptive Authentication



## Passwordless MFA



AI/ML Analytics

*Continuous adaptive trust (CAT)*

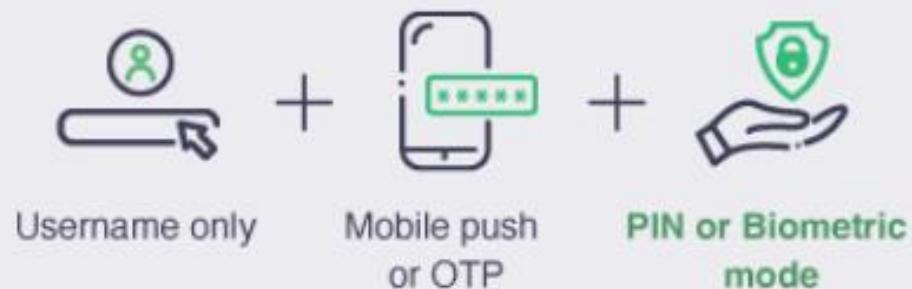
*Joint Fraud Conference*

# Passwordless MFA – better UX

## NOW

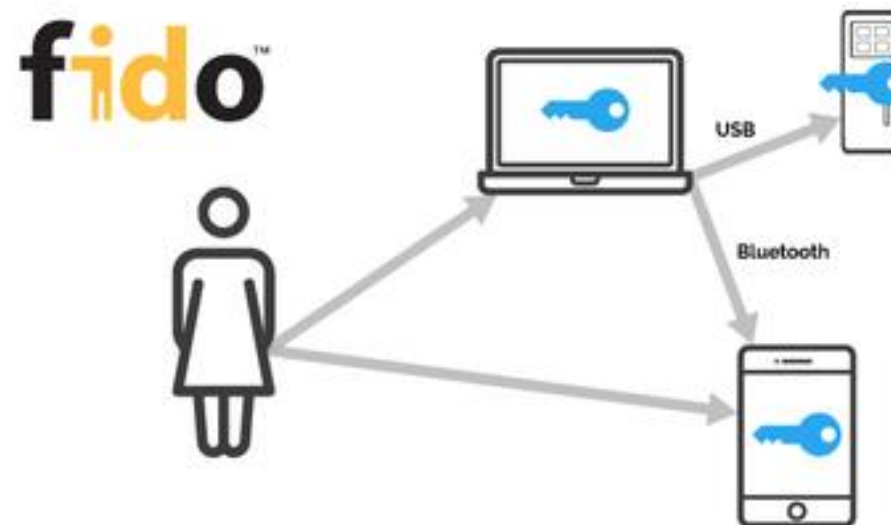
- Phone-as-a-token and mobile MFA

### PASSWORDLESS MFA WITH PHAAT



## Coming SOON

- FIDO2



# Adaptive Authentication – more Security

## CREDENTIAL STUFFING (ATO)



- Device recognition – identifying changes in device unique fingerprint
- Geolocation feature – comparing users geolocation from GPS with the one from IP address
- Behavioral biometrics – distinguishing between man and machine and verifying typical user activities

## MALWARE INFECTION



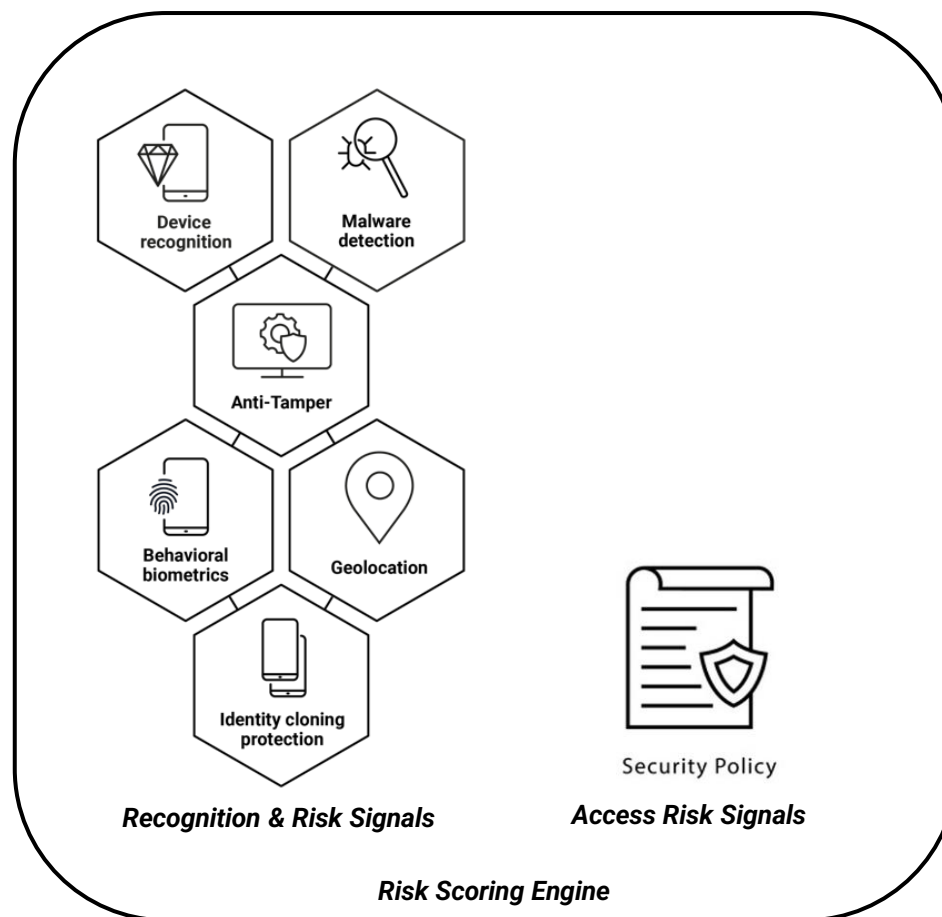
- Malware detection (even if it was installed during users session)
- Untrusted sources application detection
- Root or jailbreak mode detection
- Webpage integrity check

## IDENTITY CLONNING



- Detecting cloned email addresses

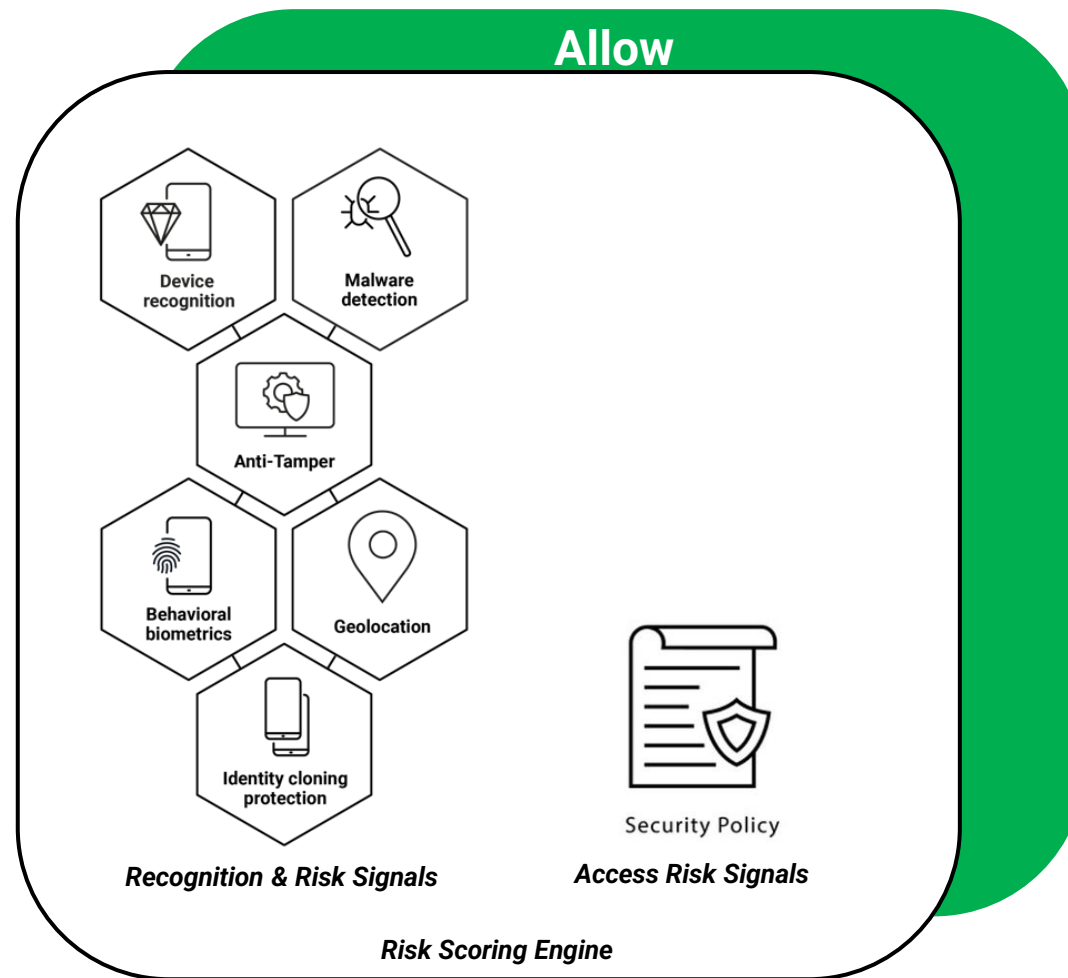
# Adaptive Authentication - more Security & better UX



*Joint Fraud Conference*

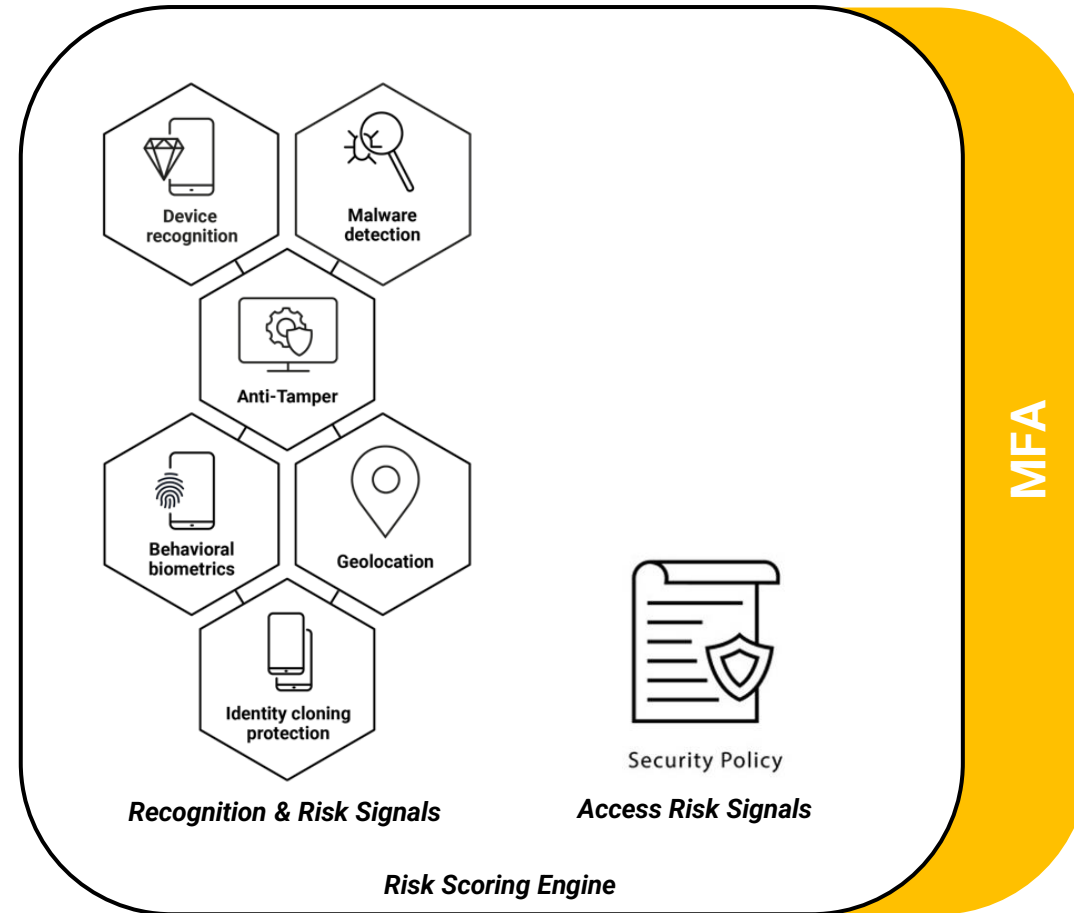


# Adaptive Authentication - more Security & better UX



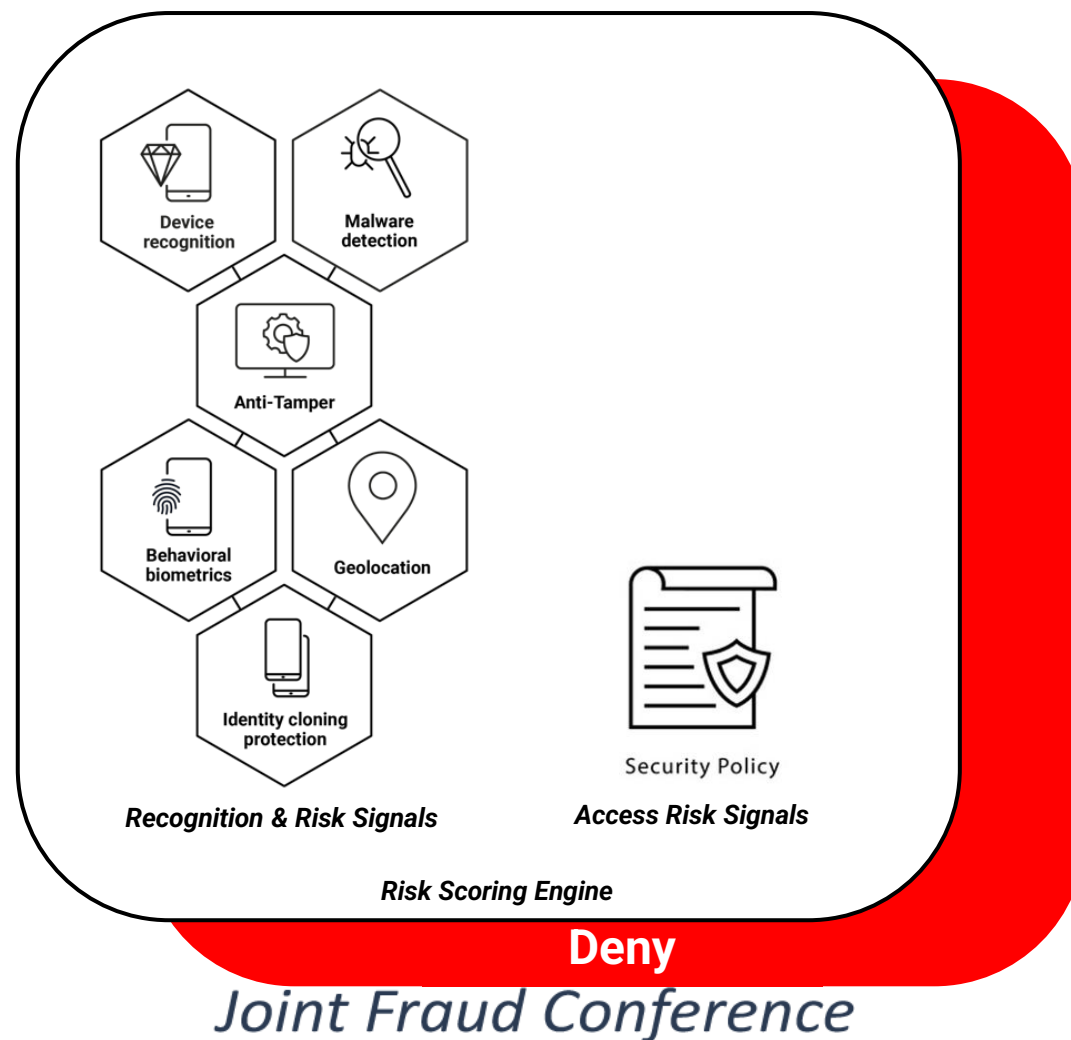
*Joint Fraud Conference*

# Adaptive Authentication - more Security & better UX

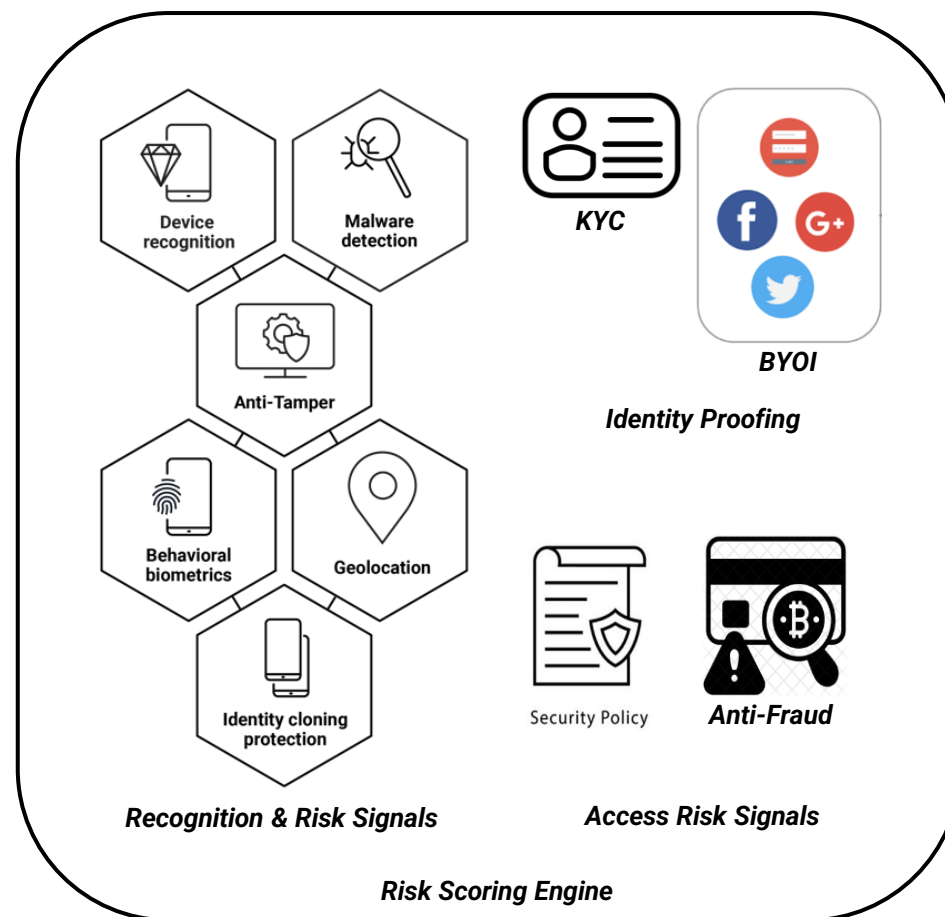


*Joint Fraud Conference*

# Adaptive Authentication - more Security & better UX

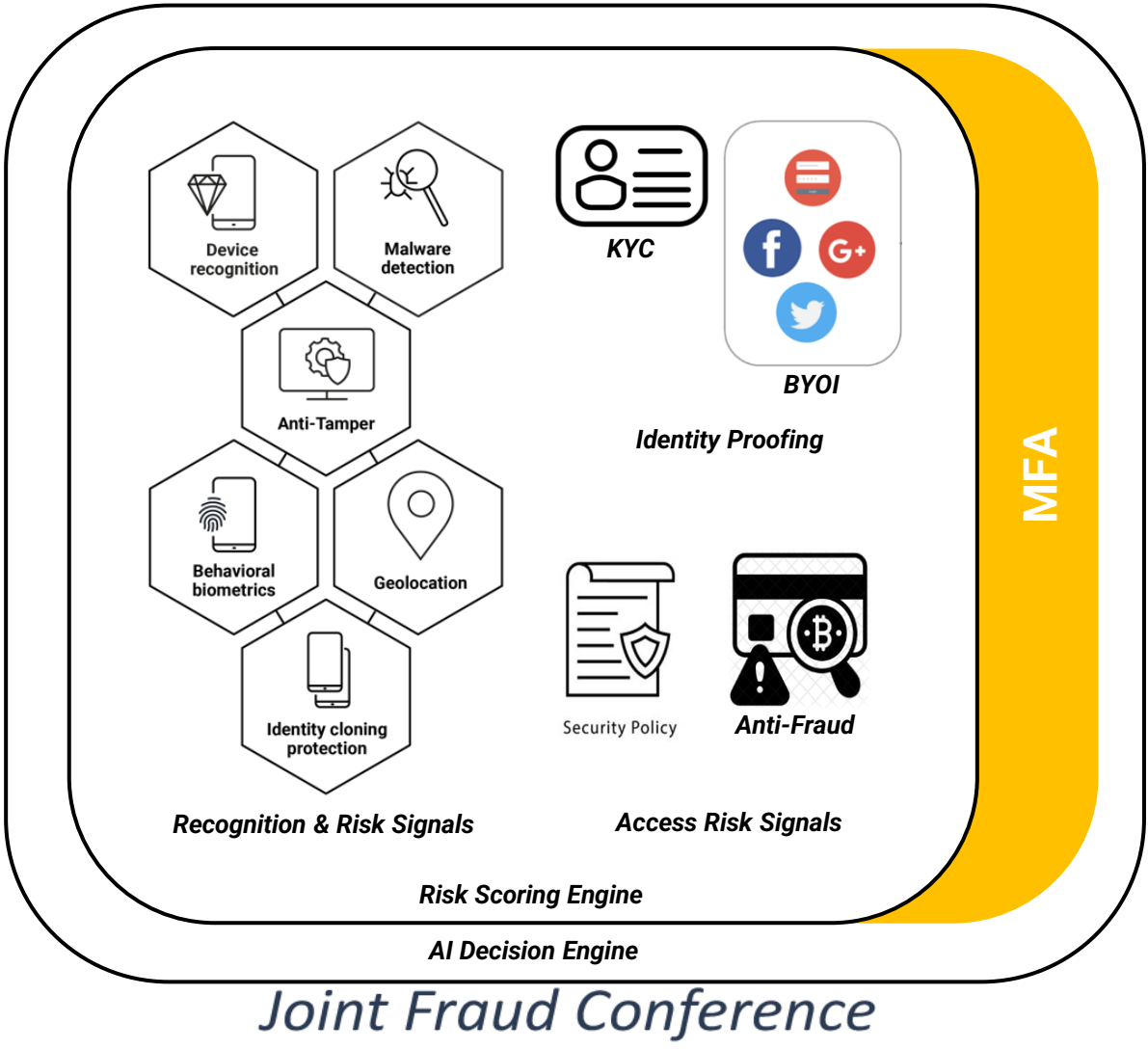


# Adaptive Authentication - more Security & better UX



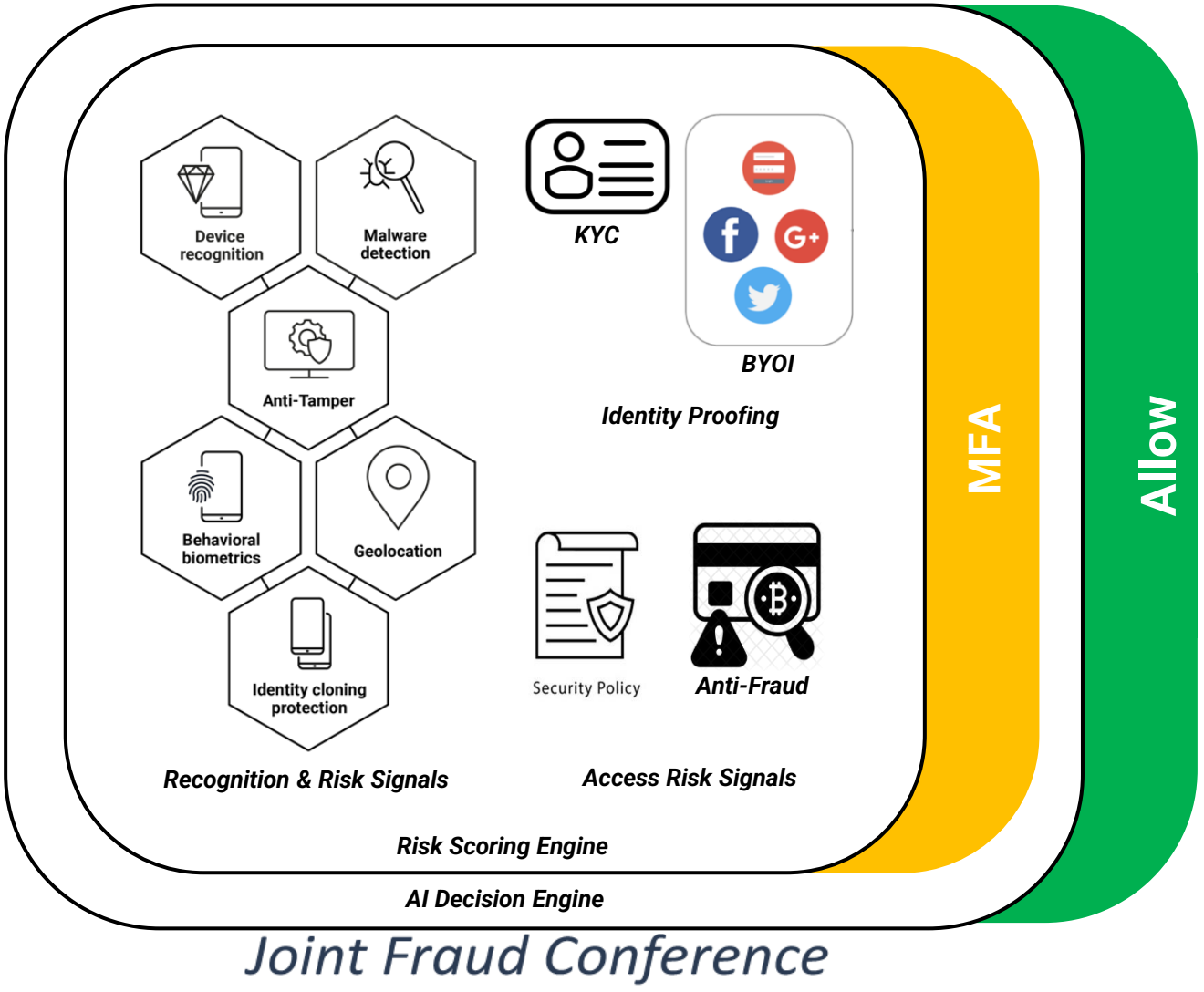
*Joint Fraud Conference*

# Continuous Adaptive Trust concept

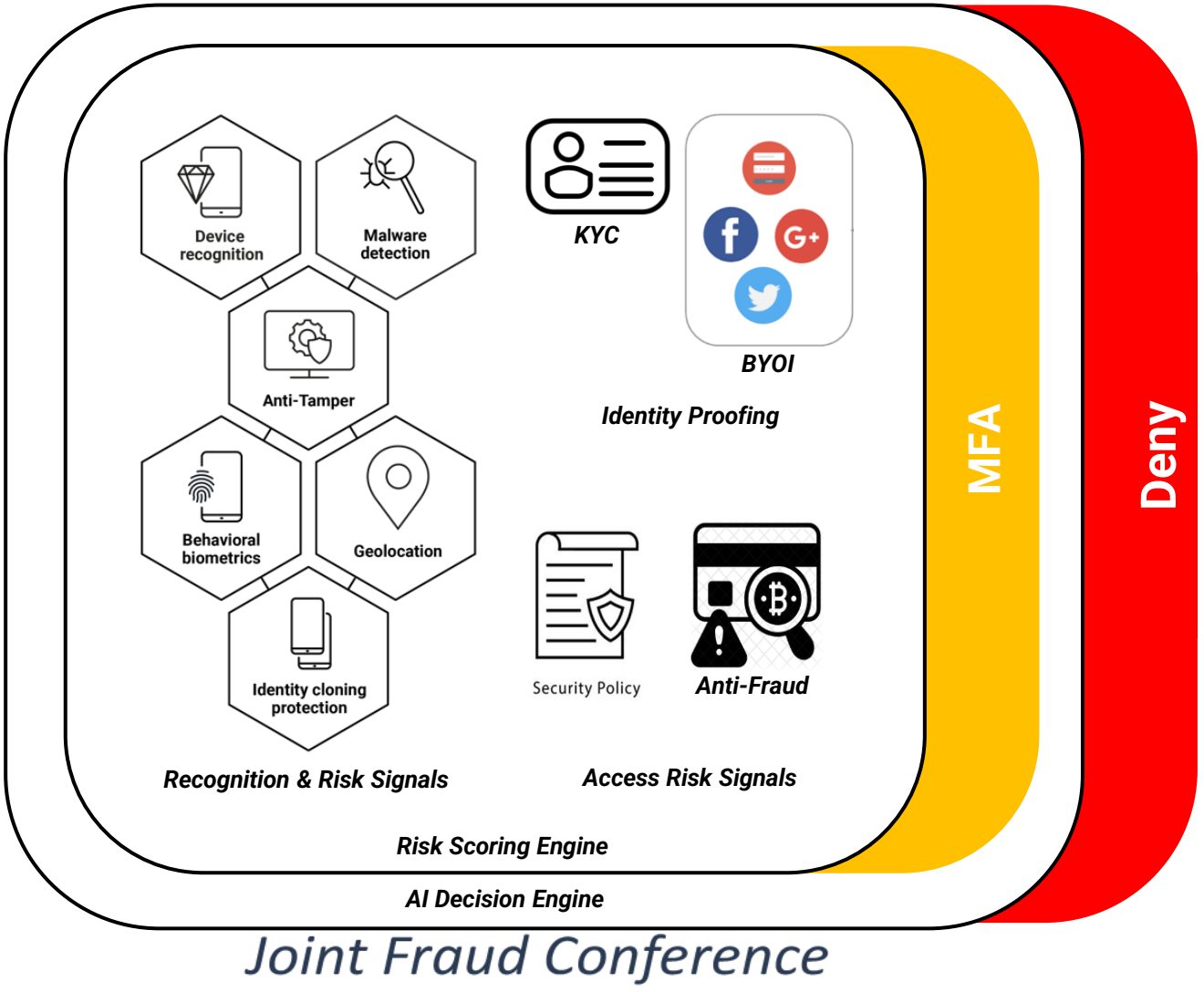




# Continuous Adaptive Trust concept

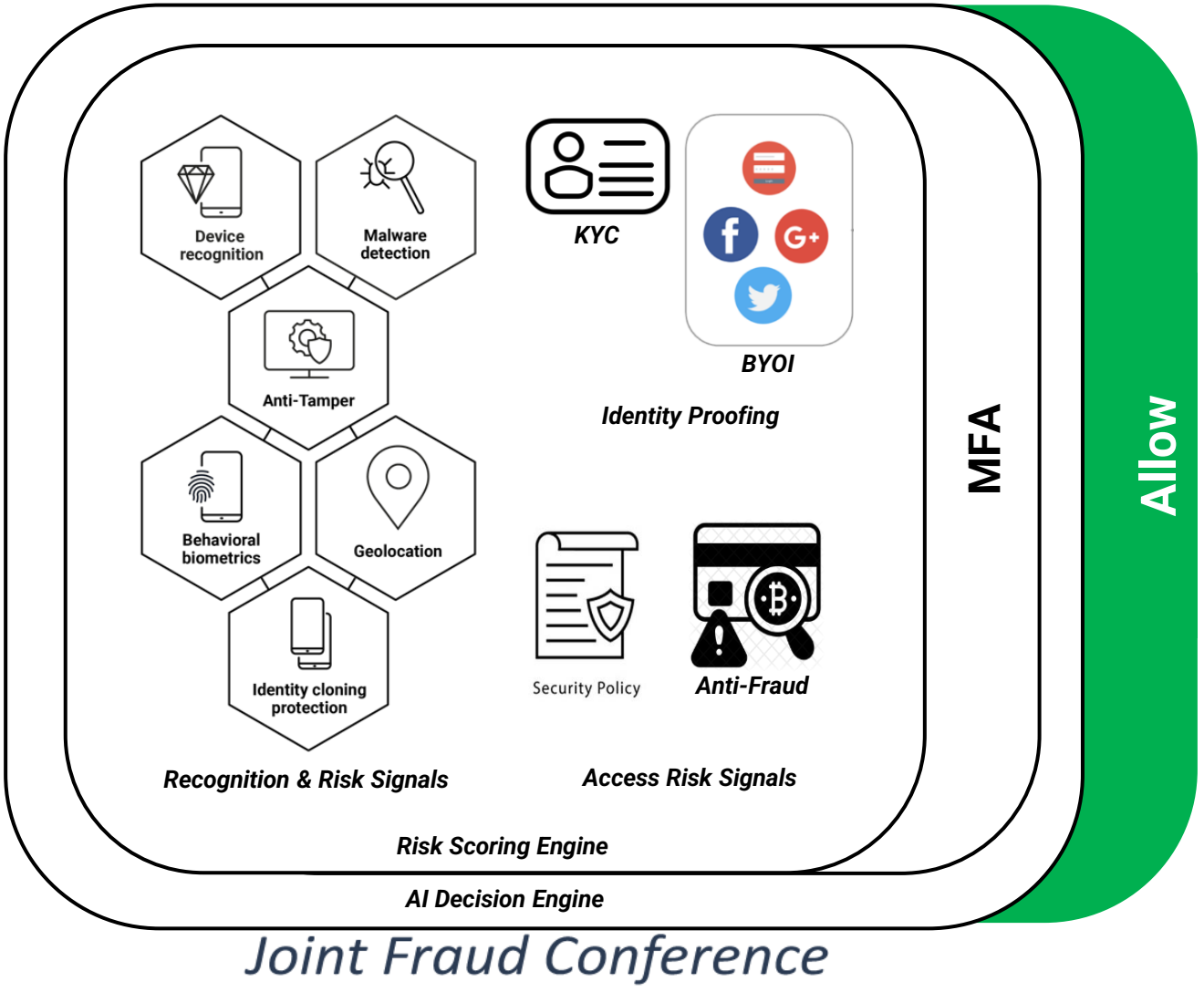


# Continuous Adaptive Trust concept

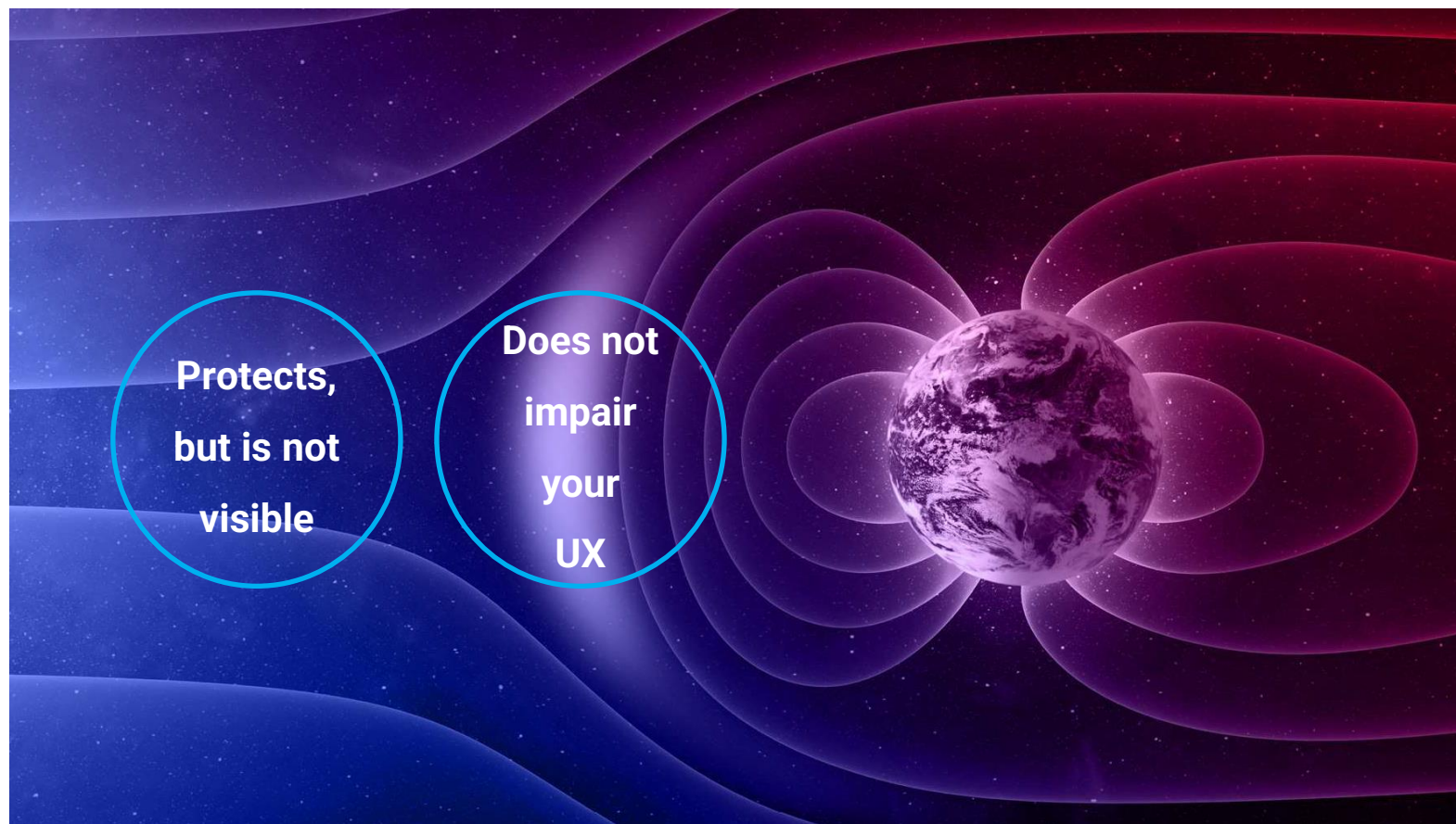


*Joint Fraud Conference*

# Continuous Adaptive Trust concept



# CONCEPT change



# Thank You



<https://www.comarch.com/cyber-security/>

*Joint Fraud Conference*

