Entra as the foundation of security

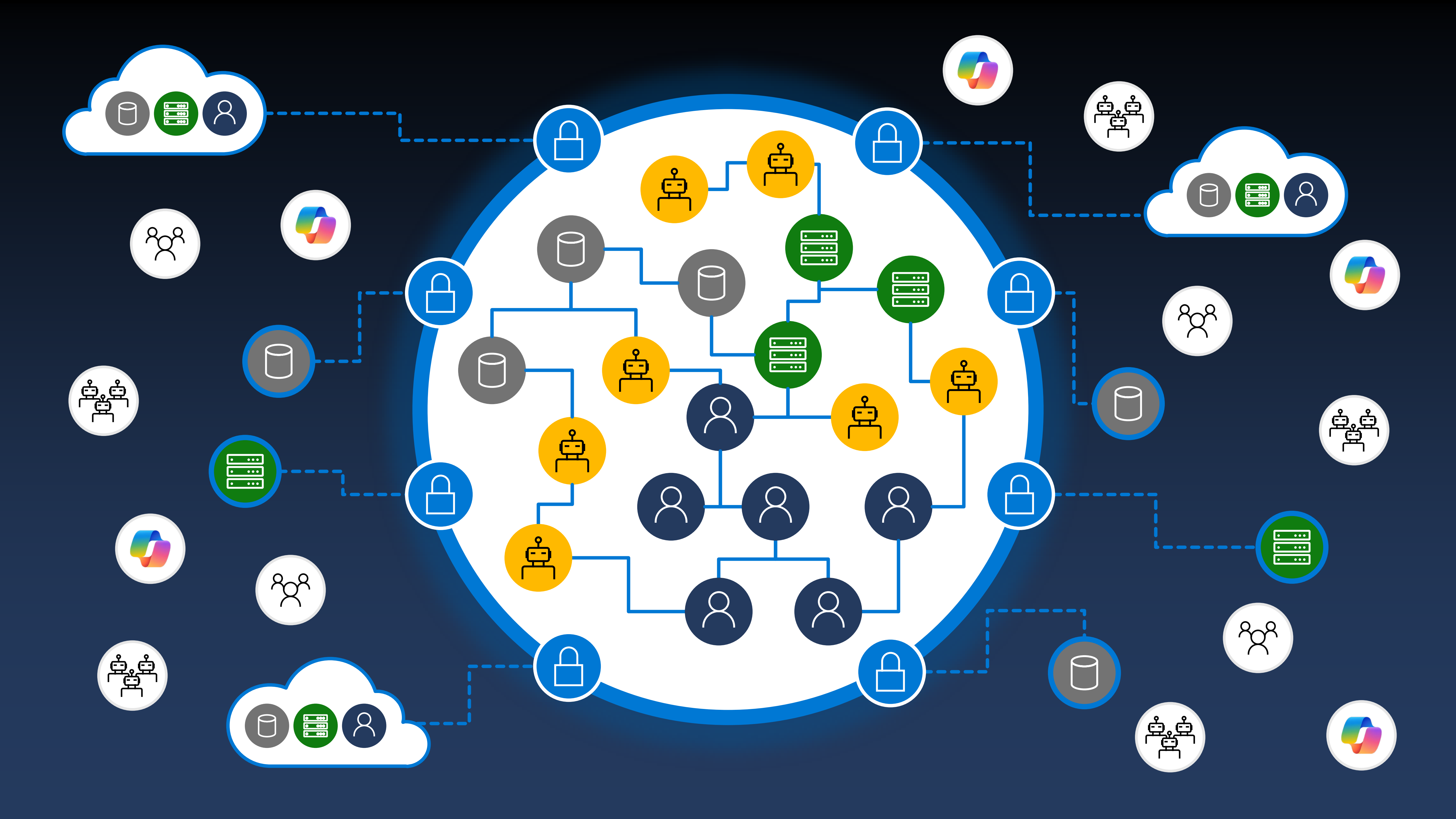
→ David Guest

Solution Architect and Technology

Evangelist

Kocho

BECOME GREATER



Trends in 2024

Proliferation of identities

>300B

passwords in use by humans and machines

Employees access more than

1,500

applications in the average enterprise

Increase in cybercrime

4,000

password attacks per second in 2023

Token Replay attacks

2x

increase since 2023

Cybersecurity Statistics and Trends - 2024 & Beyond (Cybersecurity for me)
2024 State of Multicloud Security Risk Report
Microsoft Digital Defense Report 2023 (MDDR)
How to break the token theft cyber attack chain (2024 Microsoft blog)

Microsoft Entra

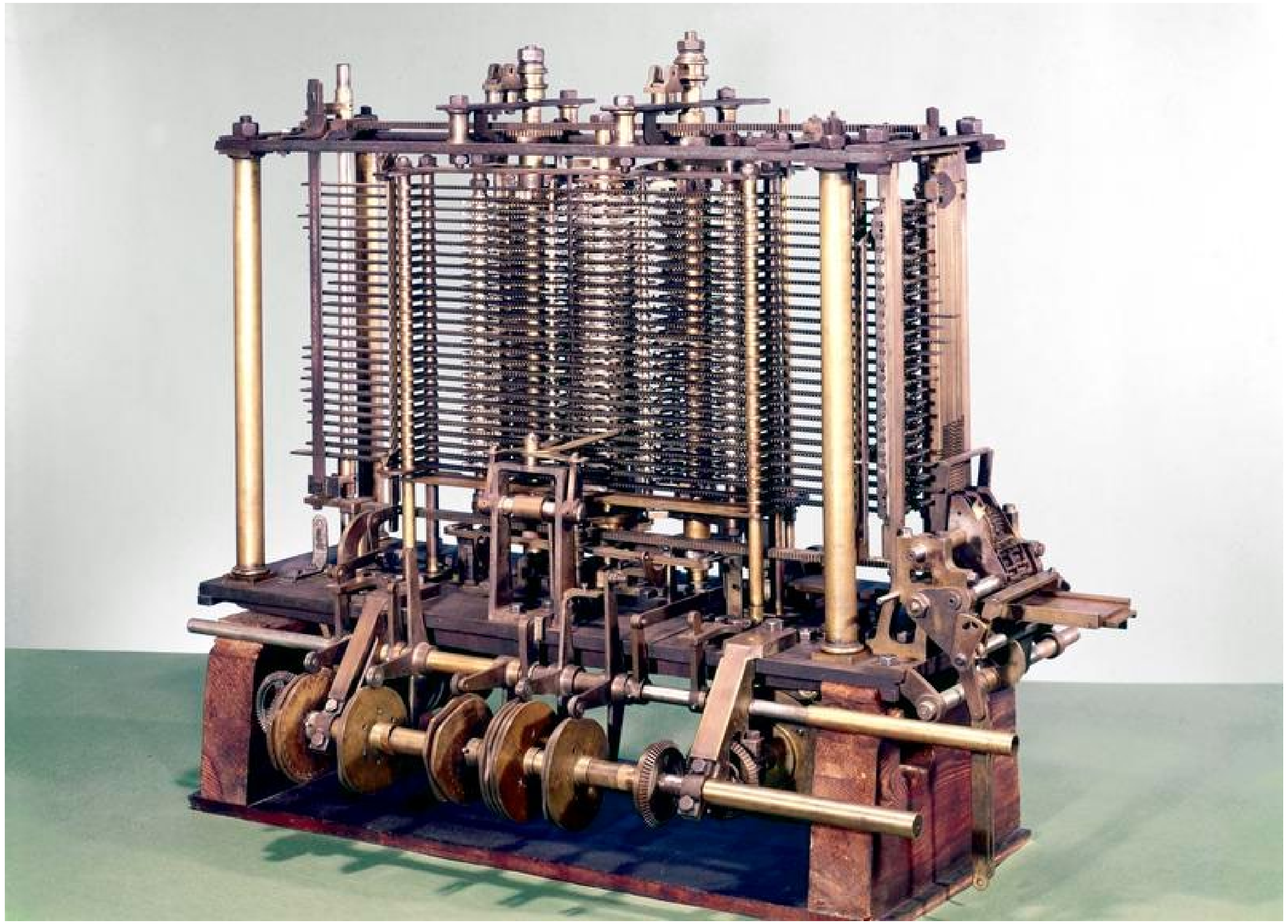
Secure access for any identity,
from anywhere, to any app, AI, or resource

Things have changed

- Changes in technology have changed the way we work
- Changes in society have changed the way we work
- Can security keep up with the devices?

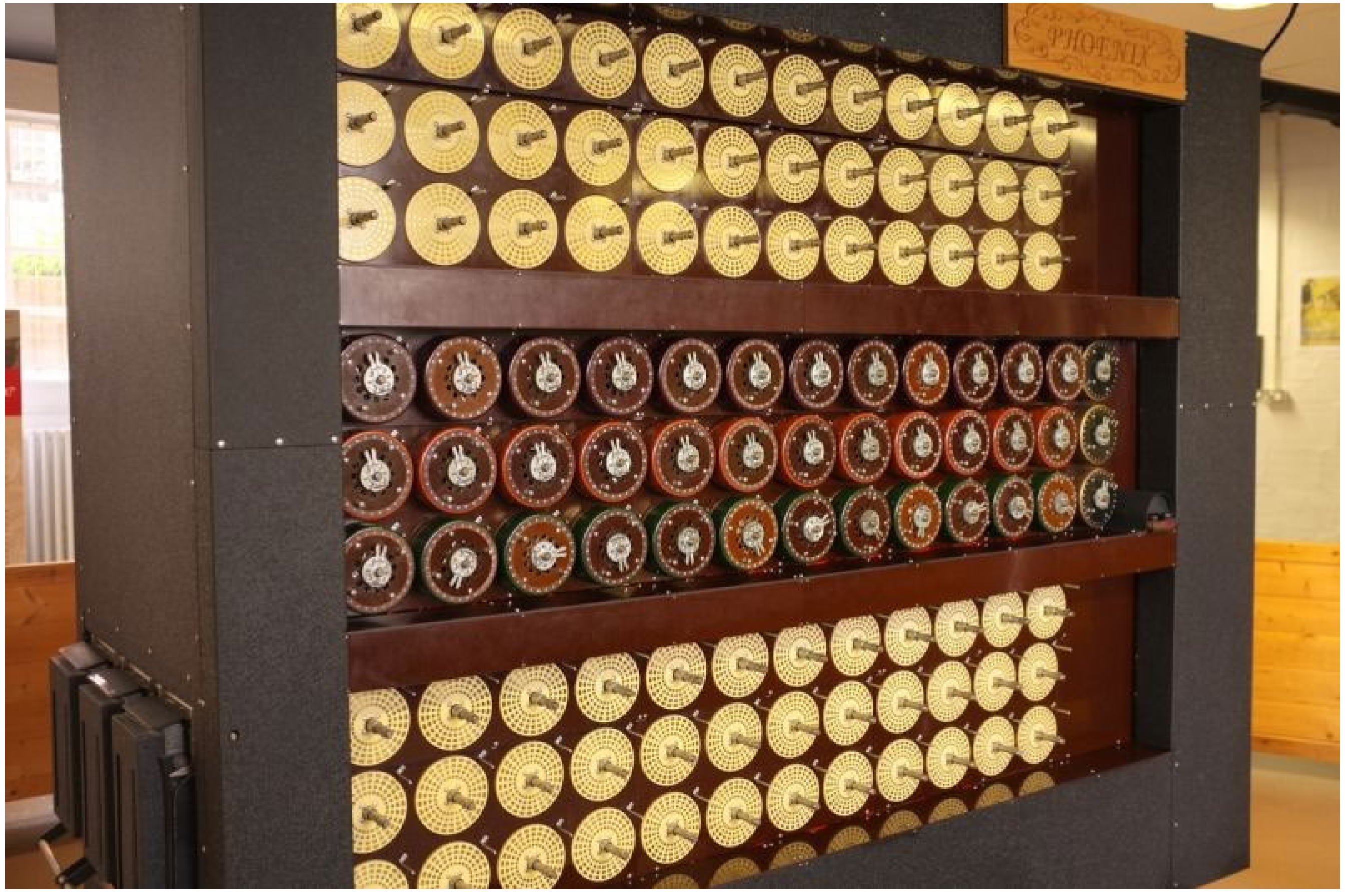
How have things changed

- → 1837
- → Charles Babbage
- → Analytical Engine



How have things changed

- → 1940
- → Alan Turing
- → Bombe



How things have changed

- → 1980s
- → Apple][
- → IBM PC

- → Apple Lisa

- → Networking
  - →Vines, InfoShare, NetWare, PC-LAN

Security

- → How it was

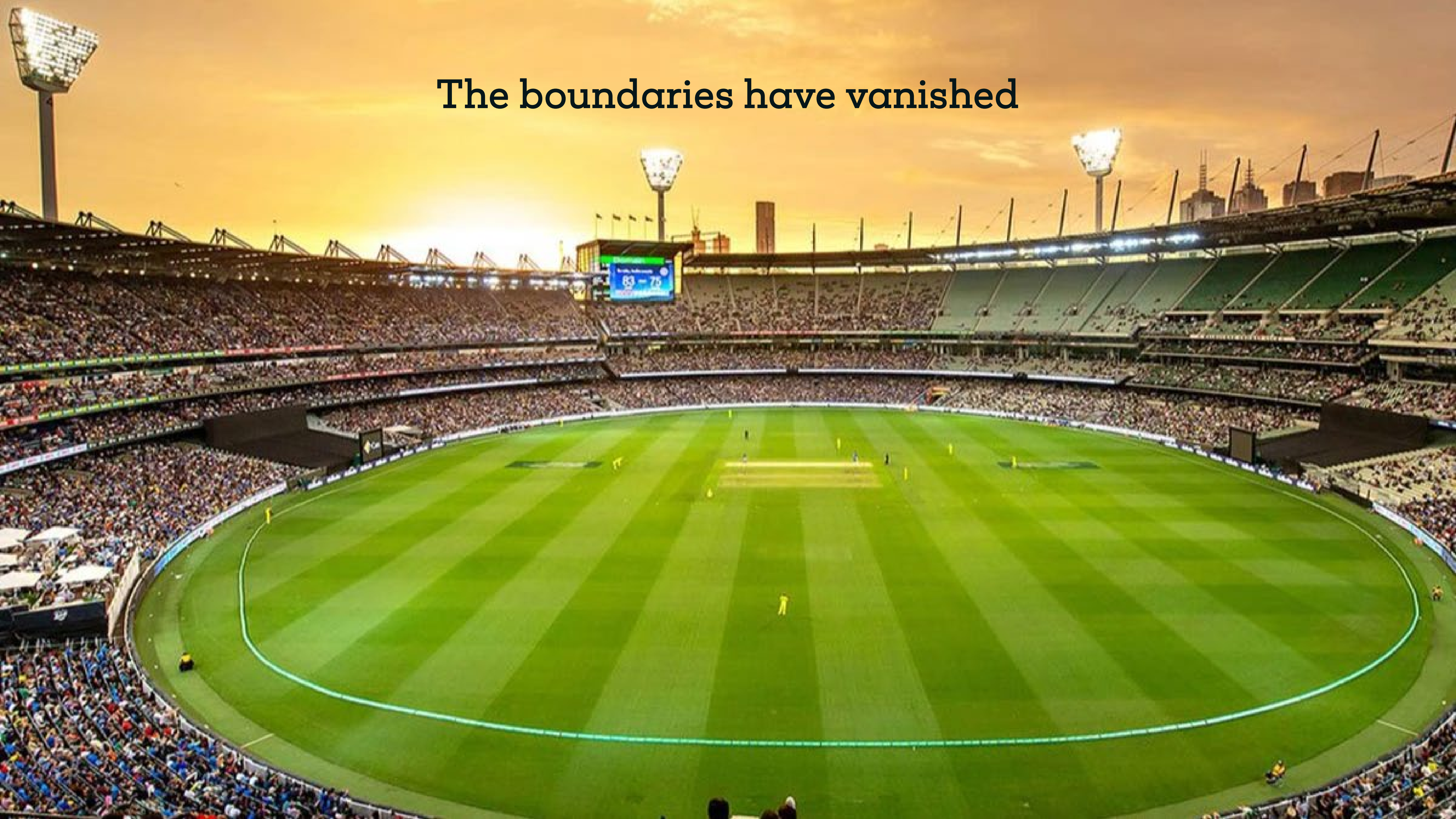
- → Access data
  - → Dial up
  - → 2,400 baud
    - → 2,400 bits per second

The rise of the Internet

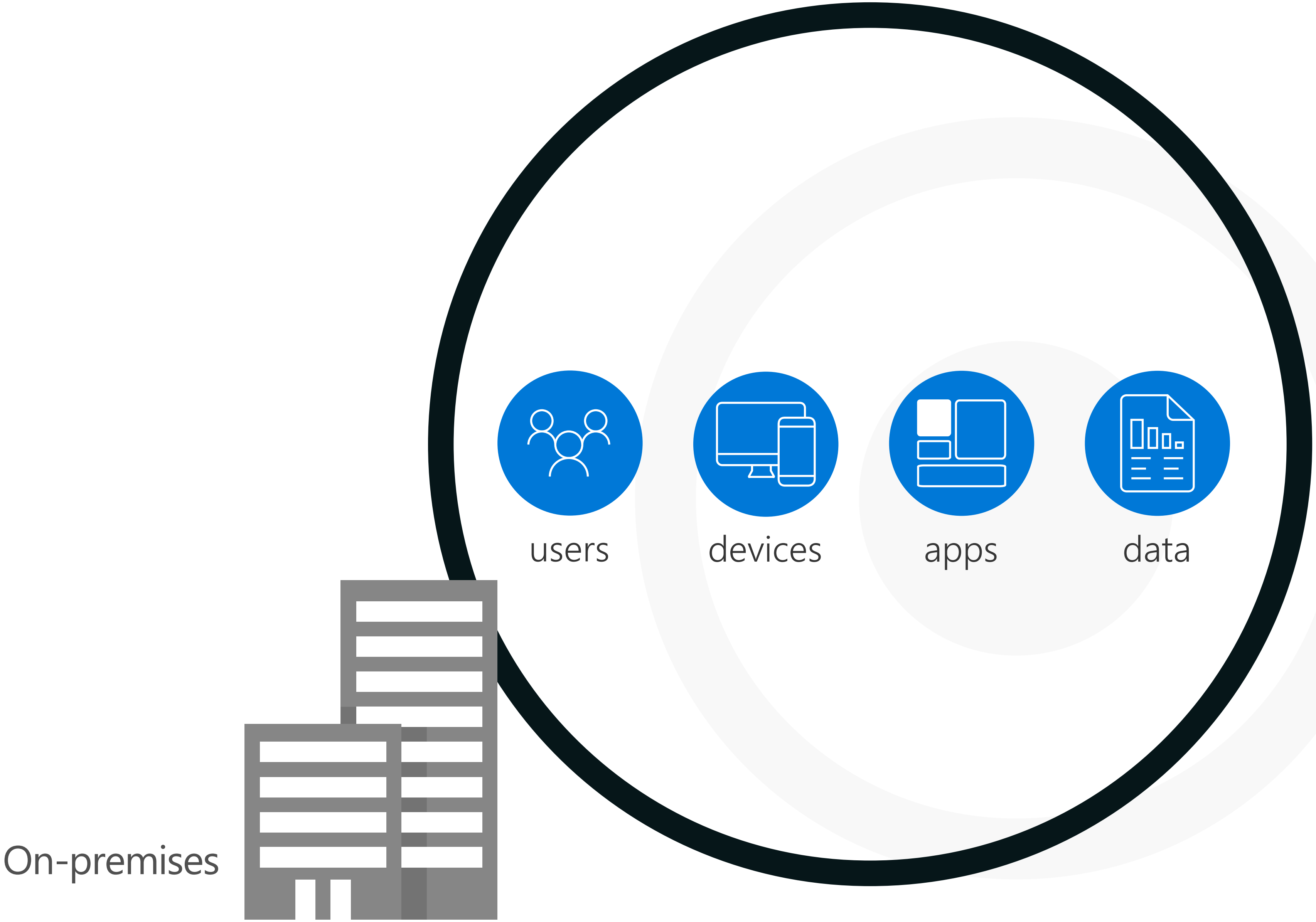
- Laptops
- Mobiles / Tablets / Other devices
- Things
  - Alexa, Siri, Google
  - Fridge
  - Cameras
- Connectivity anywhere

How to stay in control!

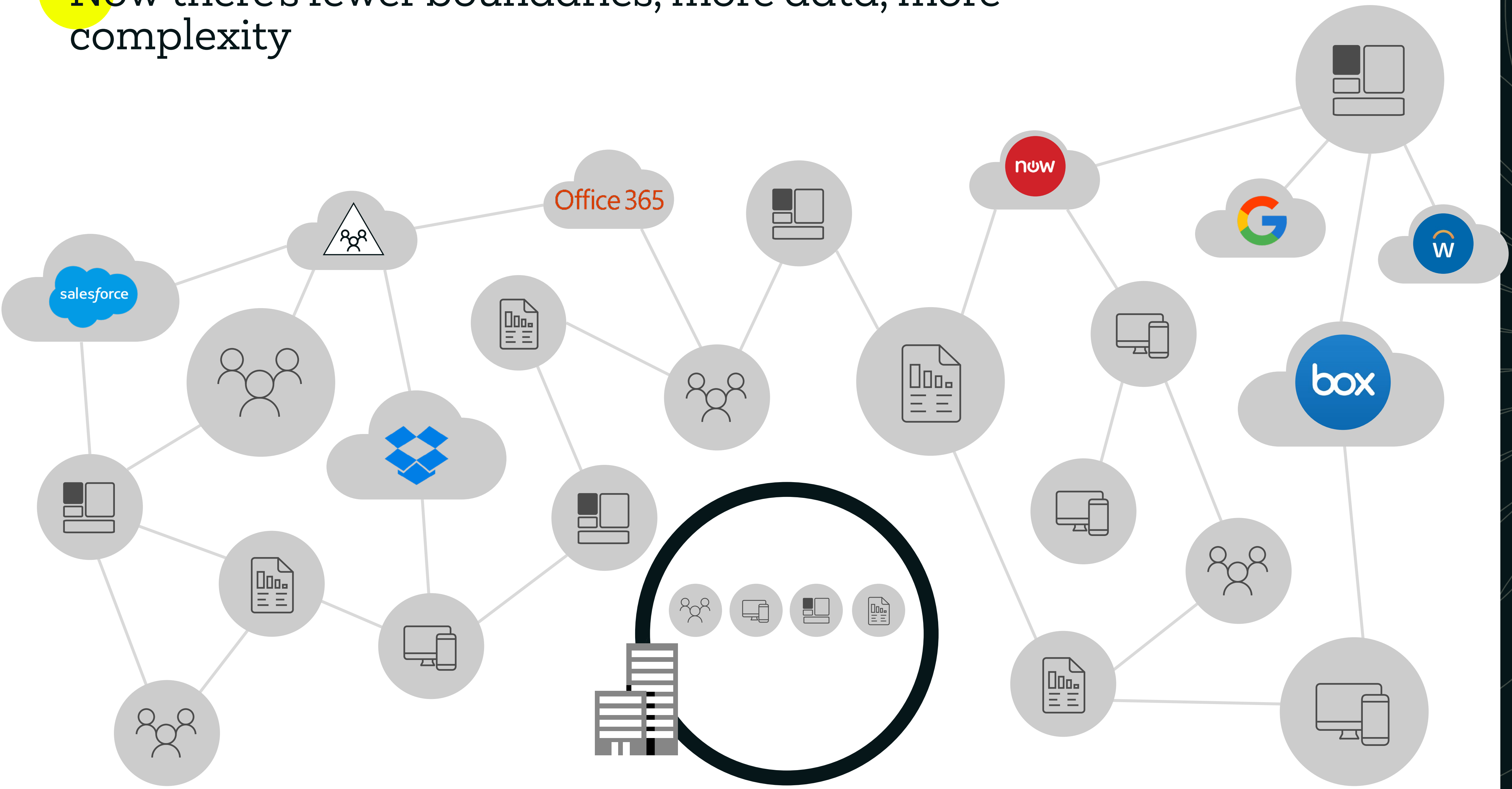
The boundaries have vanished



In the past, the firewall was the security perimeter



Now there's fewer boundaries, more data, more complexity

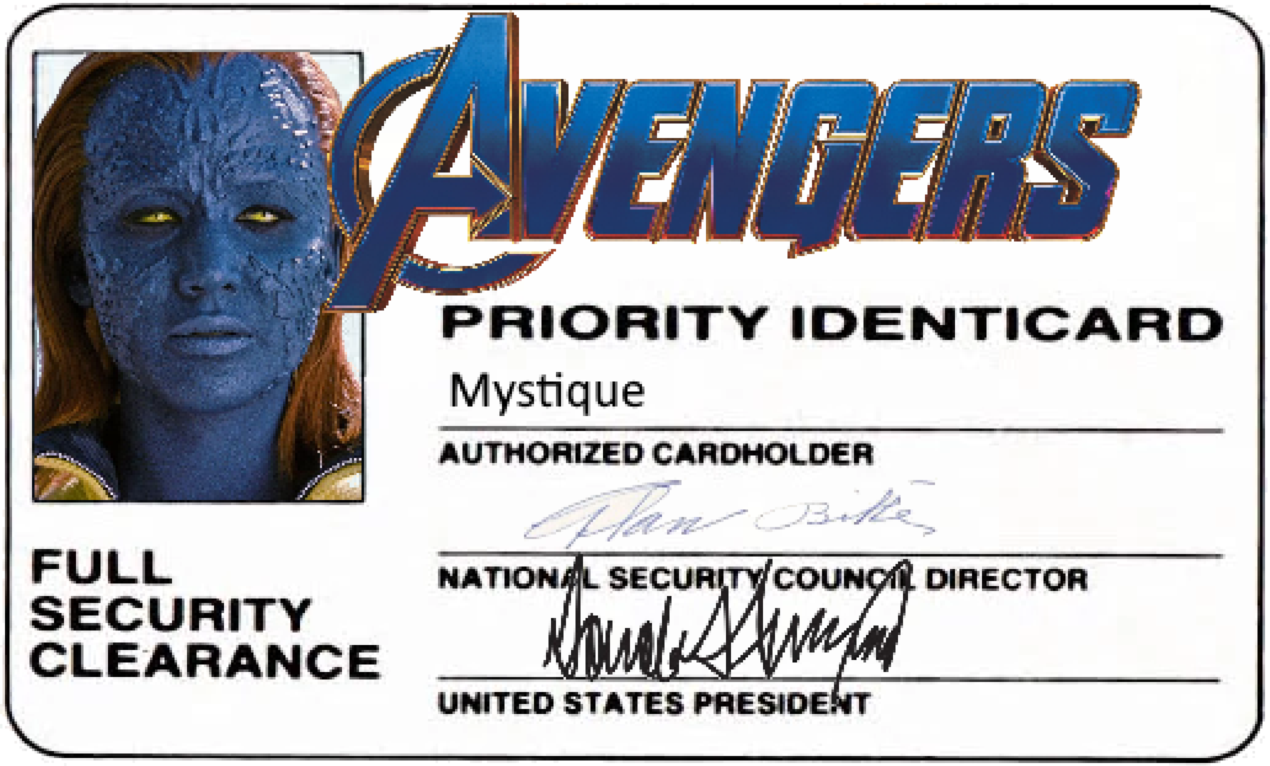


The Rights

- The right people
- The right applications or systems or services
- The right location
- The right time
- The right device

BECOME GREATER
KOCHO.CO.UK

Identity Implementations



AVENGERS

PRIORITY IDENTICARD

Mystique

AUTHORIZED CARDHOLDER

NATIONAL SECURITY COUNCIL DIRECTOR

UNITED STATES PRESIDENT

FULL SECURITY CLEARANCE

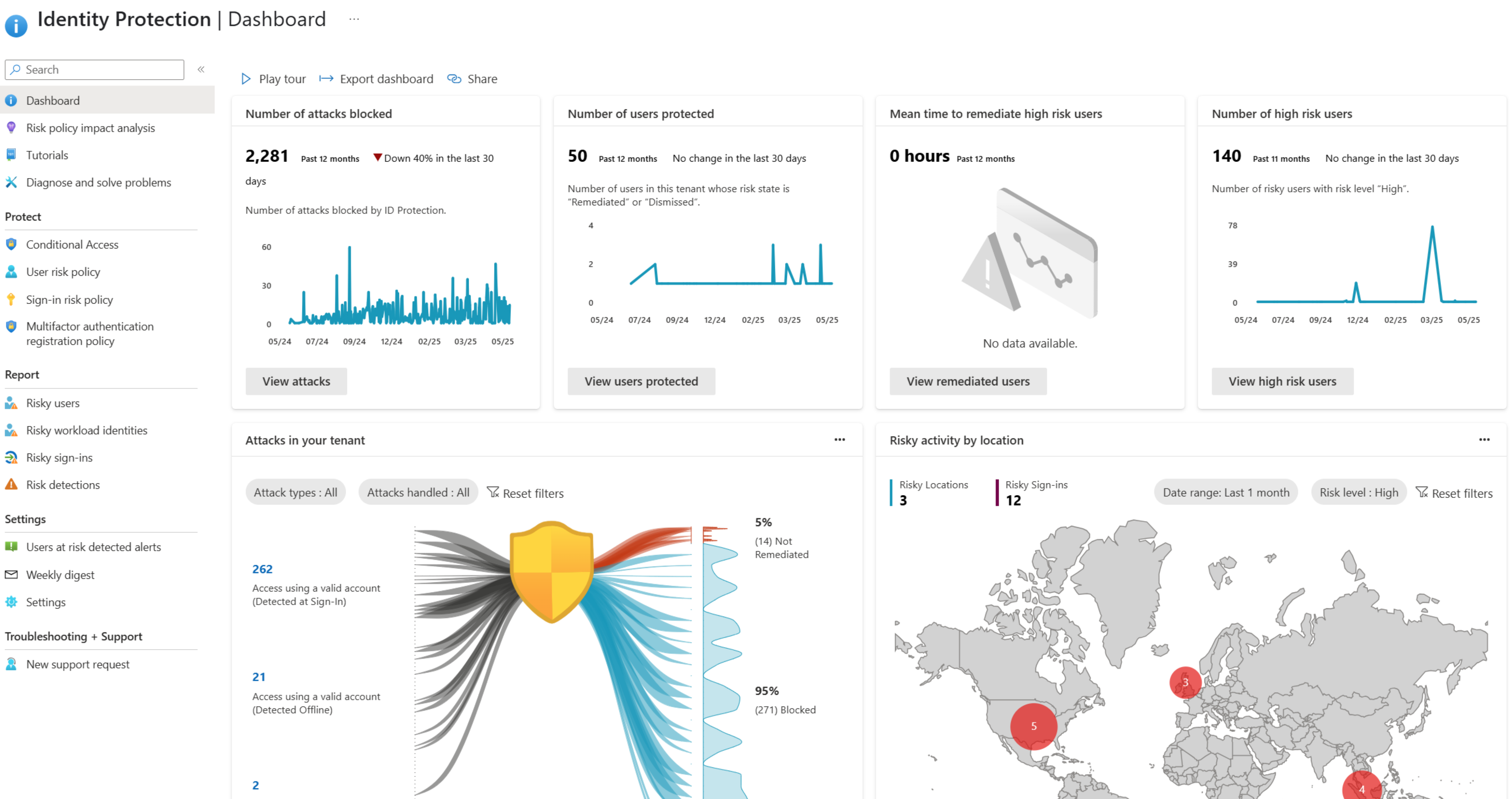
BECOME GREATER

KOCHO.CO.UK

Risky Users

Risky Users

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/IdentityProtectionMenuBlade



Identity Protection | Dashboard ...

Search

- Dashboard
- Risk policy impact analysis
- Tutorials
- Diagnose and solve problems

Protect

- Conditional Access
- User risk policy
- Sign-in risk policy
- Multifactor authentication registration policy

Report

- Risky users
- Risky workload identities
- Risky sign-ins
- Risk detections

Settings

- Users at risk detected alerts
- Weekly digest
- Settings

Troubleshooting + Support

- New support request

Play tour | Export dashboard | Share

Number of attacks blocked

2,281 Past 12 months ▼ Down 40% in the last 30 days

Number of attacks blocked by ID Protection.

View attacks

Number of users protected

50 Past 12 months No change in the last 30 days

Number of users in this tenant whose risk state is "Remediated" or "Dismissed".

View users protected

Mean time to remediate high risk users

0 hours Past 12 months

No data available.

View remediated users

Number of high risk users

140 Past 11 months No change in the last 30 days

Number of risky users with risk level "High".

View high risk users

Attacks in your tenant ...

Attack types : All | Attacks handled : All | Reset filters

262 Access using a valid account (Detected at Sign-In)

21 Access using a valid account (Detected Offline)

2

5% (14) Not Remediated

95% (271) Blocked

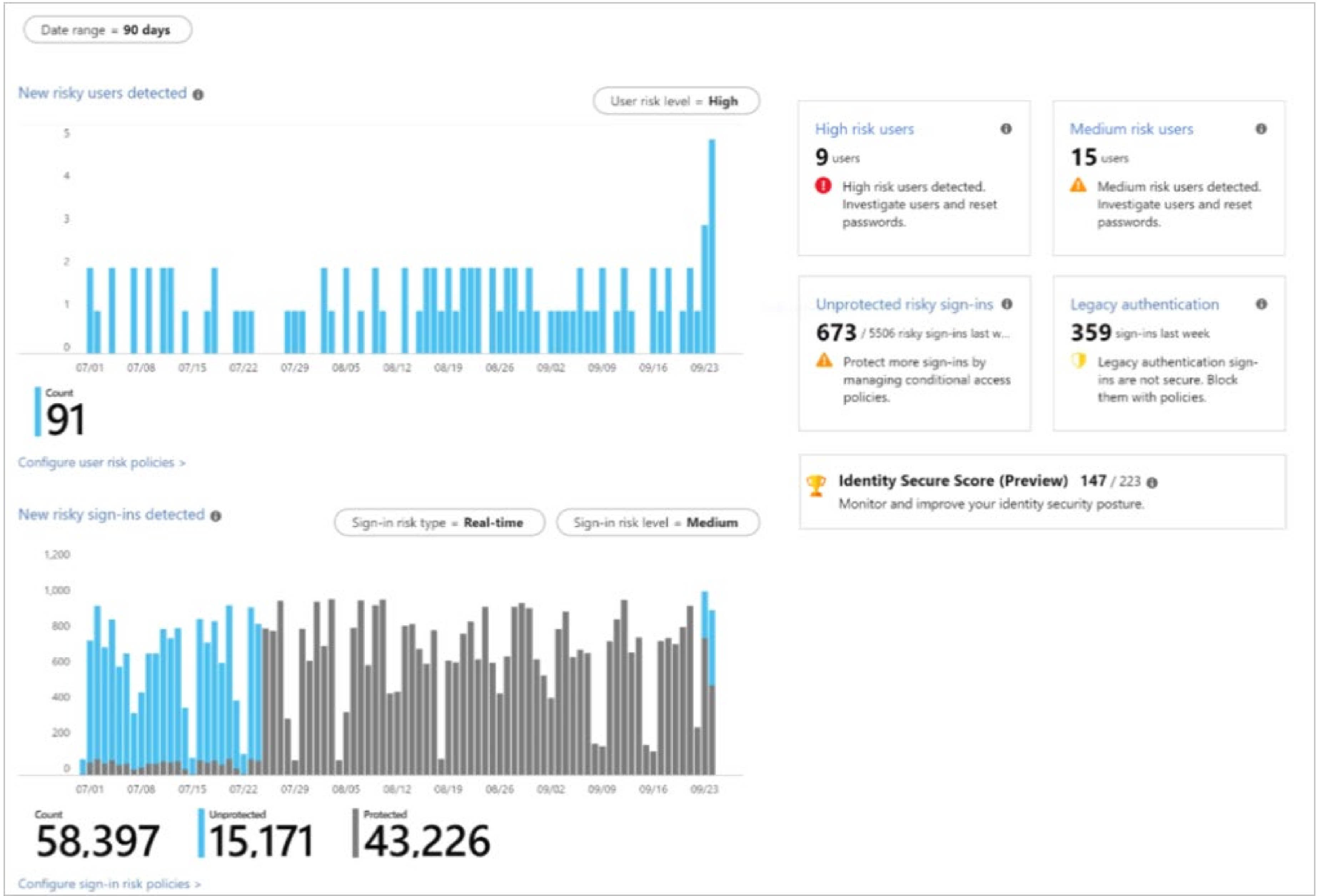
Risky activity by location ...

Risky Locations 3 | Risky Sign-ins 12

Date range: Last 1 month | Risk level : High | Reset filters

BECOME GREATER
KOCHO.CO.UK

Risky Users



Date range = **90 days**

New risky users detected

User risk level = **High**

Count
91

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **Medium**

Count
58,397

Unprotected
15,171

Protected
43,226

Configure sign-in risk policies >

High risk users

9 users

High risk users detected. Investigate users and reset passwords.

Medium risk users

15 users

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

673 / 5506 risky sign-ins last w...

Protect more sign-ins by managing conditional access policies.

Legacy authentication

359 sign-ins last week

Legacy authentication sign-ins are not secure. Block them with policies.

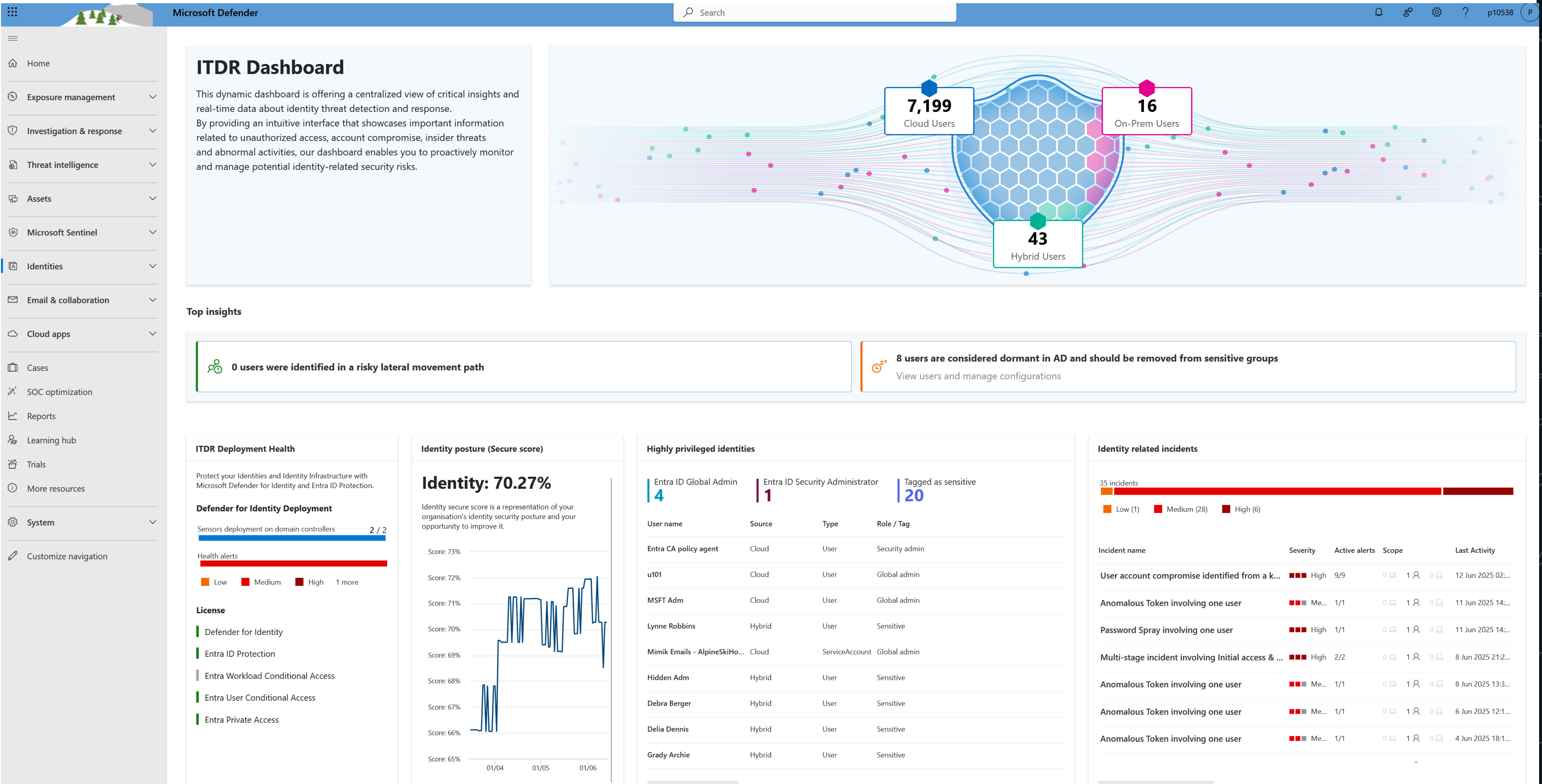
Identity Secure Score (Preview) 147 / 223

Monitor and improve your identity security posture.

BECOME GREATER
KOCHO.CO.UK

Risky Users

https://security.microsoft.com/identities/dashboard



ITDR Dashboard

This dynamic dashboard is offering a centralized view of critical insights and real-time data about identity threat detection and response.
By providing an intuitive interface that showcases important information related to unauthorized access, account compromise, insider threats and abnormal activities, our dashboard enables you to proactively monitor and manage potential identity-related security risks.

Top insights

0 users were identified in a risky lateral movement path

8 users are considered dormant in AD and should be removed from sensitive groups
View users and manage configurations

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

Defender for Identity Deployment

Sensors deployment on domain controllers 2 / 2

Health alerts

🟧 Low 🟥 Medium 🟥 High 1 more

License

- Defender for Identity
- Entra ID Protection
- Entra Workload Conditional Access
- Entra User Conditional Access
- Entra Private Access

Identity posture (Secure score)

Identity: 70.27%

Identity secure score is a representation of your organisation's identity security posture and your opportunity to improve it.

Highly privileged identities

Entra ID Global Admin **4** | Entra ID Security Administrator **1** | Tagged as sensitive **20**

User name	Source	Type	Role / Tag
Entra CA policy agent	Cloud	User	Security admin
u101	Cloud	User	Global admin
MSFT Adm	Cloud	User	Global admin
Lynne Robbins	Hybrid	User	Sensitive
Mimik Emails - AlpineSkiHo...	Cloud	ServiceAccount	Global admin
Hidden Adm	Hybrid	User	Sensitive
Debra Berger	Hybrid	User	Sensitive
Delia Dennis	Hybrid	User	Sensitive
Grady Archie	Hybrid	User	Sensitive

Identity related incidents

35 incidents

🟧 Low (1) 🟥 Medium (28) 🟥 High (6)

Incident name	Severity	Active alerts	Scope	Last Activity
User account compromise identified from a k...	High	9/9	0 1 0	12 Jun 2025 02:...
Anomalous Token involving one user	Me...	1/1	0 1 0	11 Jun 2025 14:...
Password Spray involving one user	High	1/1	0 1 0	11 Jun 2025 14:...
Multi-stage incident involving Initial access & ...	High	2/2	0 1 0	8 Jun 2025 21:2...
Anomalous Token involving one user	Me...	1/1	0 1 0	8 Jun 2025 13:3...
Anomalous Token involving one user	Me...	1/1	0 1 0	6 Jun 2025 12:1...
Anomalous Token involving one user	Me...	1/1	0 1 0	4 Jun 2025 18:1...

BECOME GREATER
KOCHO.CO.UK

Proving Identity

Use Conditional Access

Be aware of location

Be aware of Device

Protecting Users

- → Multi-Factor Authentication
  - → Risk based enforcement

- → Identity Protection
  - → Have I Been Pwned

- → **How do you know?**

But how do we know it works?

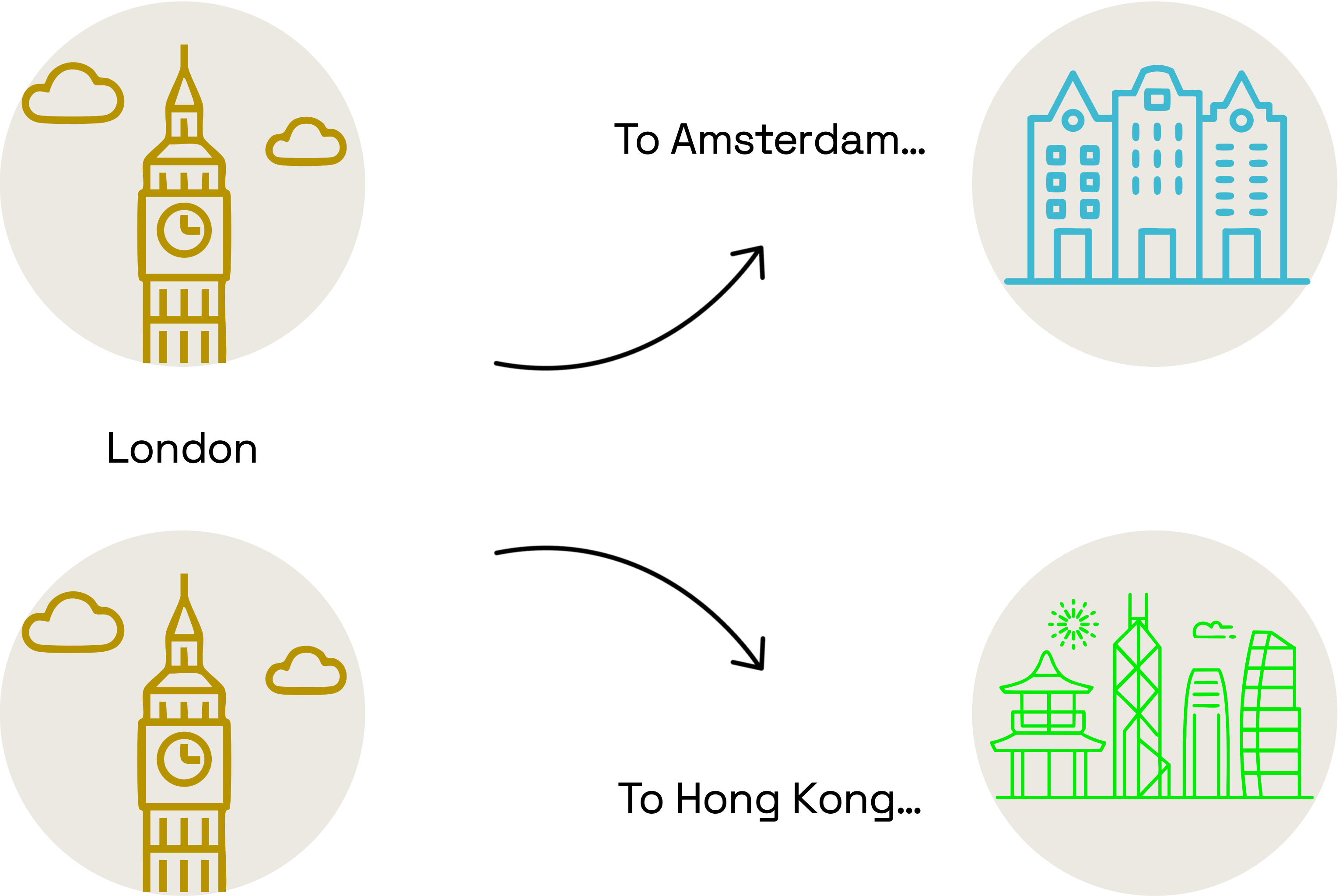
→ MFA ensures that the stolen credentials are not used

→ Conditional Access blocks older/legacy access

  → Spoofing emails

→ B2B Access Risk in source stops access from External locations

Impossible Travel



London

To Amsterdam…

To Hong Kong…

Real or trouble?

Protecting Identity

- → How do we stop identity attacks in their tracks?
- → How do we make sure that we can detect issues?
- → How can we make sure that users are protected?

What is the easiest way to protect an identity?

- → Set a passw[illegible] that is
  - → Long - > 2[illegible]ara[illegible]s
  - → Complex – U[illegible]d lower and Number and Special
  - → Change it [illegible]en

What is the easiest way to protect an identity?

- → Move away from Passwords
- → Passwordless technologies
  - → Authenticator
  - → Passkey
  - → FIDO2
  - → Biometrics
- → Passwords
  - → If you have to
    - → Long (12 characters) – Change it when it is necessary

Detect bad behaviour and verify

- → Unusual country
- → Different device
- → Unusual application
- → Download / upload change
- → Watch risk
- → If in doubt - MFA

What to do ?

- → Force password reset
- → Block activity
- → Control session
- → Validate user
- → [illegible]nb[illegible] t[illegible]n c[illegible]
- → [illegible]not[illegible]g

TAKE ACTION!

BECOME GREATER
KOCHO.CO.UK

Who to attack?

→ Who can I find out about

→ Construct a Phish?

→ When in the LAN what next?

→ What accounts should I aim for ?

Defence

- Education
  - Make sure people know what to do and what not to do
- Scan incoming stuff
- Close off known vulnerabilities
- Patch!

Kocho

BECOME GREATER

Any questions?

Thank you

David Guest

Solution Architect & Technology Evangelist

david.guest@kocho.co.uk