@indiacloudsec

#ICSS2025

INDIA CLOUD SECURITY SUMMIT

ICSS

India Cloud Security Summit - 2025

SPONSORED BY

Microsoft

PENTHARA TECHNOLOGIES

Adaptive Authentication and Zero Trust

Elevating Data Protection in the Cloud

13:00 – 13:45 IST

Sakshi Nasha

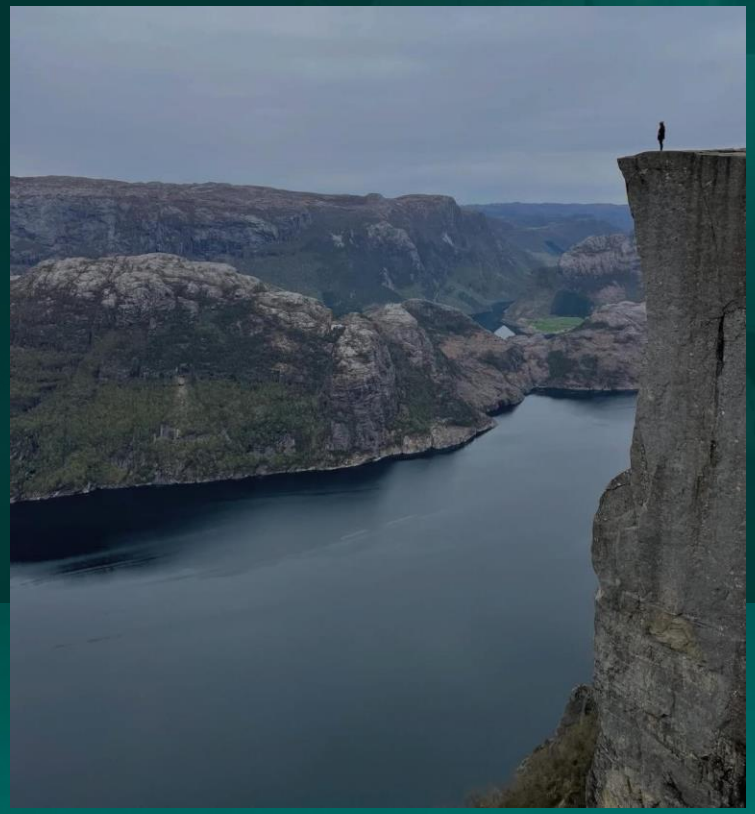
Senior Software Engineer (MTS III)
Cohesity

INDIA CLOUD SECURITY SUMMIT
ICSS

www.indiacloudsecuritysummit.com

$whoami

- ~~Senior s/w Engineer~~ **Learner**
- Community evan·gel·ist
- Innovator
- Opensource Contributor
- Public speaker
- Athlete at heart : 🏃 🏀 ⚽ 🎾



Off the grid? soaking up nature to recharge for the next big idea.

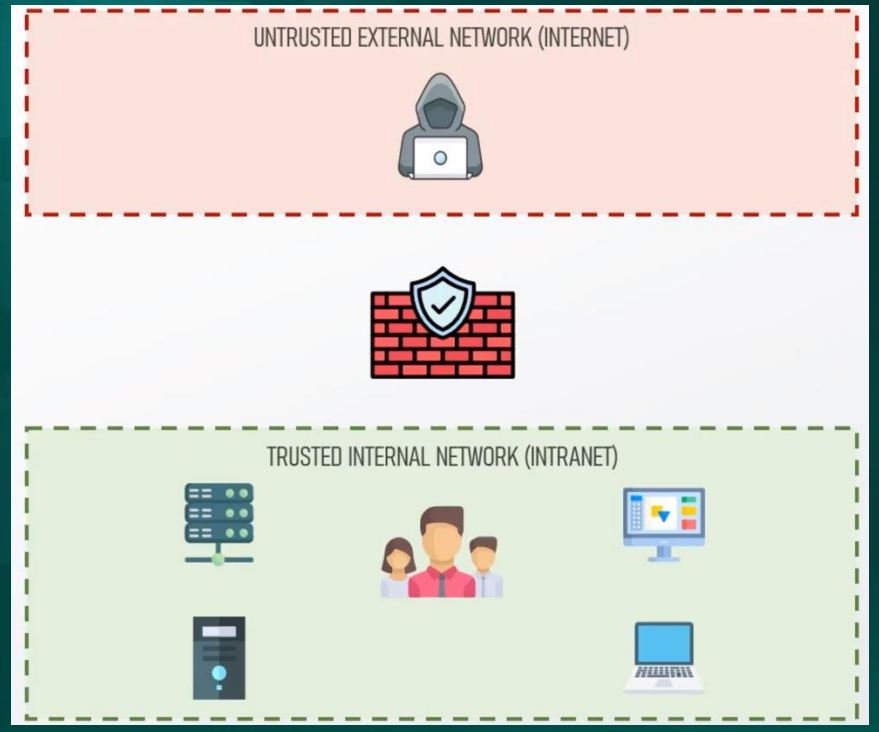
AGENDA

1. Why we need Zero Trust Architecture?
2. What is Zero Trust Architecture?
3. What is Adaptive Authentication?
4. Benefits of Zero Trust Architecture
5. Overview of NIST Zero Trust Architecture
6. Microsoft’s Internal Zero Trust Architecture
7. Microsoft Zero Trust Strategy Step by Step
8. References
9. QnA

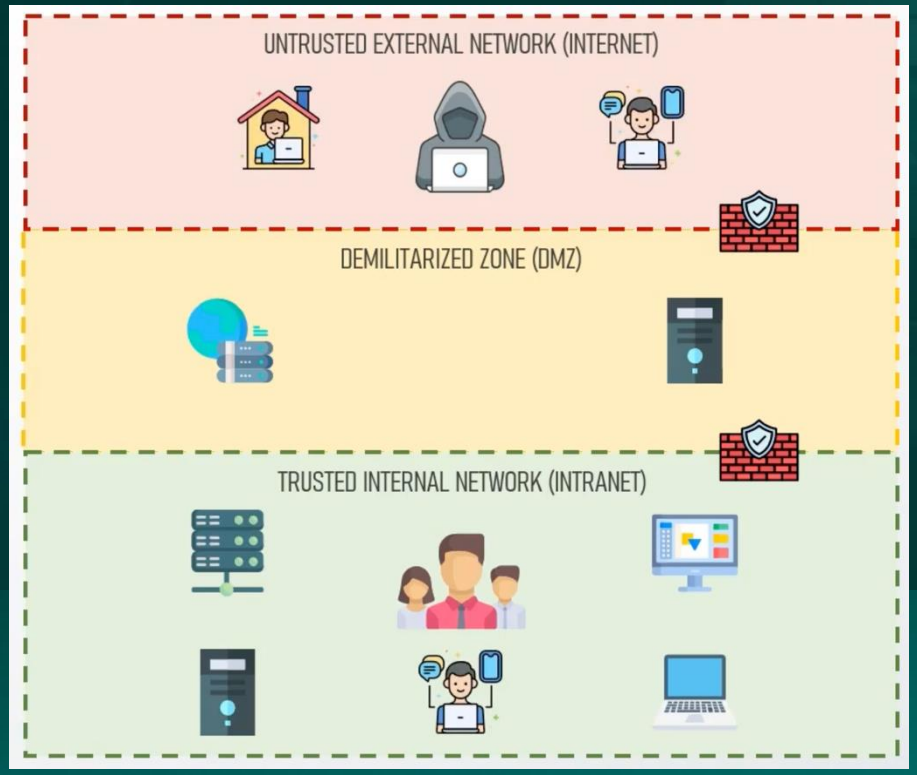
Why Zero Trust Architecture ?

Evolution of IT Infrastructure

1. Started With a Trusted and Untrusted Network



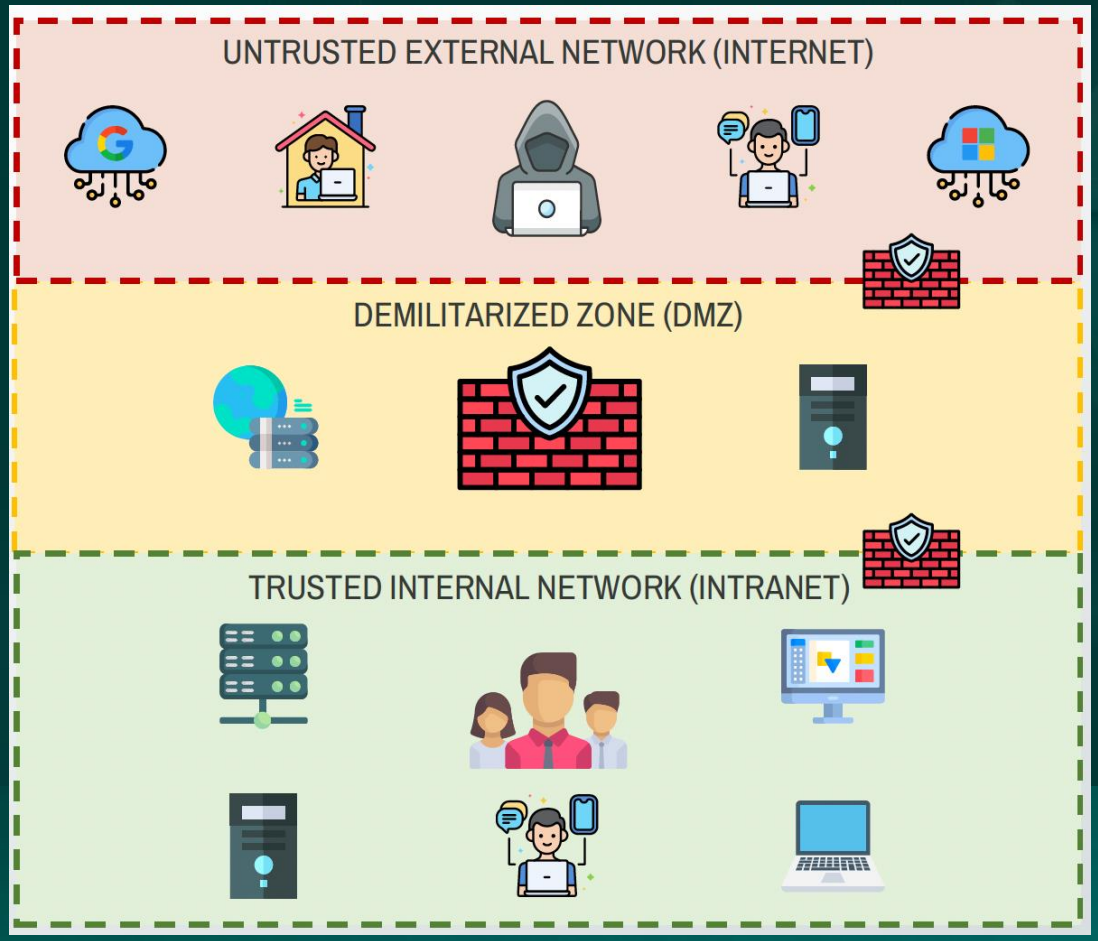
2. Introduced the DMZ for Public-Facing Services



Why Zero Trust Architecture ?

- Working From Home
- BYOD Were Widely Adopted
- Cloud Services Became Highly Leveraged

Effectively **Dissolving the Traditional Network Perimeter**



Why Zero Trust Architecture ?

- Digital Transformation :
  - More than 90% of the organizations use cloud[1]
  - 8 in 10 people are working hybrid or remotely[2]
  - 83% of the companies allow Bring Your Own Device BYOD[3]
  - Moore's Law: Covid19 accelerated digital transformation by 6 years[4]
- Blurred Traditional Network Boundaries
- Created Complex IT infrastructure Environments
- Failed Mindset :
  - Trust by Verify approach
  - Static Policies

1. O'Reilly: The Cloud in 2021: Adoption Continues
2. Gallup: Returning to the Office: The Current, Preferred and Future State of Remote Work
3. Zippia: 26 Surprising BYOD Statistics [2023]: BYOD Trends in the Workplace
4. Twilio: COVID-19 Digital Engagement Report

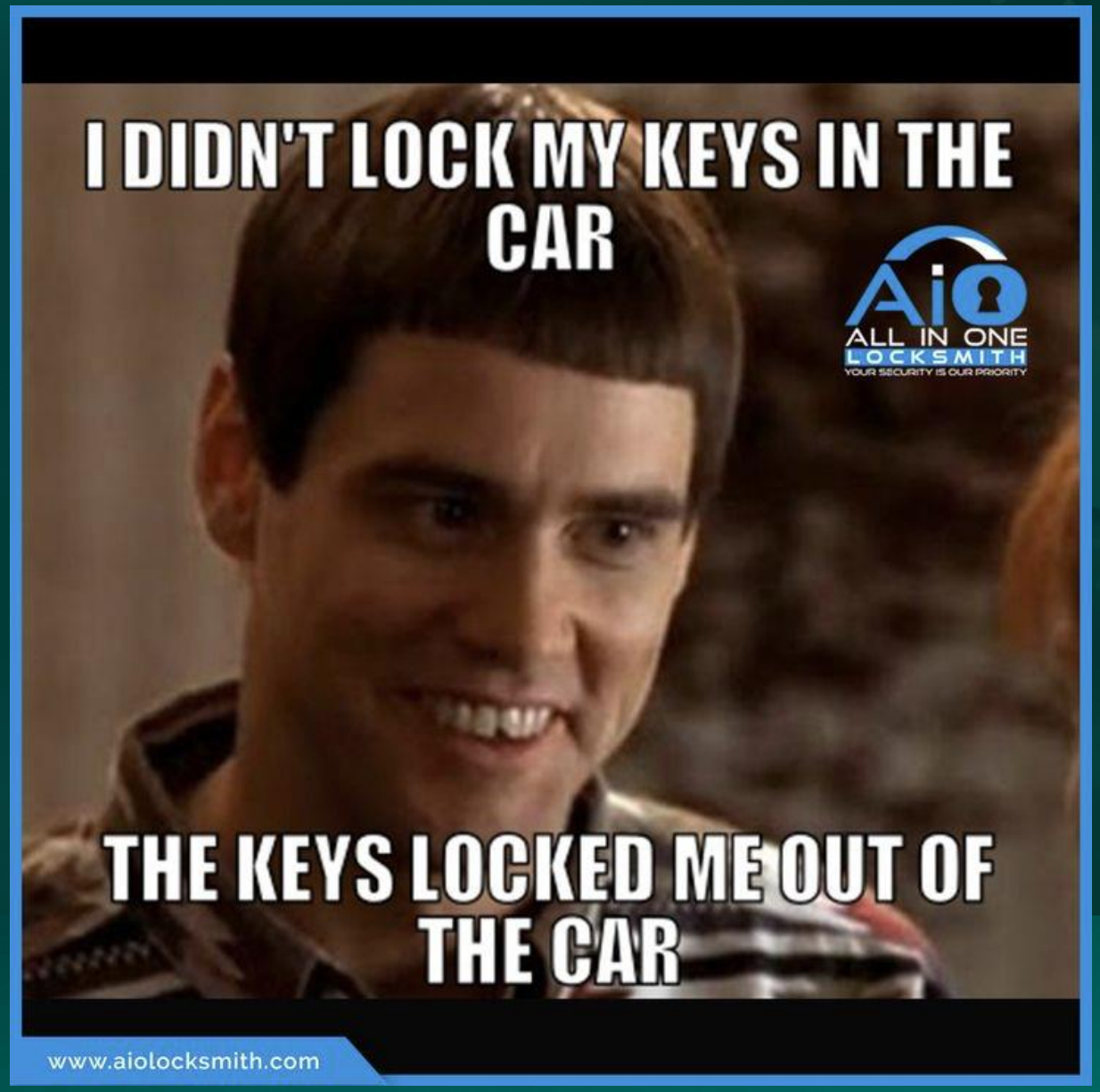
Basic Public Access Rule

Sunburst Attack in Dec 2020

- Hackers injected SUNBURST malware into SolarWinds Orion updates (Mar 2020).
- **Impact**:
  Infected updates reached U.S. government, Fortune 500 firms, and tech giants.
- **Stealth Techniques**:
  Malware evaded detection, disabled security tools, and mimicked legit traffic.
- **Massive Data Theft**:
  Attackers accessed networks, exfiltrated data, and moved laterally.
- **Gov Response**:
  Led to **Executive Order 14028** – mandating Zero Trust, MFA, encryption, logging.
- **Key Lesson**:
  Traditional defenses failed – Zero Trust and supply chain security are now essential.

Reference:

How much security is too much security ?



Colonial Pipeline 2021

- **Ransomware Attack (DarkSide):**
  Shut down 5,500-mile fuel pipeline, causing shortages across the U.S. East Coast.
- **Entry Point**:
  Attackers accessed systems via a compromised VPN account with no MFA
- **Unpatched Software**:
  Exploited known vulnerability (CVE-2019-19781) due to poor patch management.
- **Lack of Network Segmentation**:
  Allowed attackers to move freely within the network.
- **Weak Backup & Response**:
  Inadequate recovery planning led to $4.4M ransom payment and delayed restoration.
- **Zero Trust Could've Helped**:
  MFA, segmentation, and continuous monitoring could have reduced attack impact.

Reference:


Modern problems require modern solutions

What is Zero Trust ?

- Zero Trust is a security model, strategy, and framework that trusts nothing by default.
  - Never Trust, Always Verify
  - Assume Breach
  - Verify Explicitly
  - Least Privileged Access

https://learn.microsoft.com/en-us/security/zero-trust/

https://learn.microsoft.com/en-us/security/adoption/ciso-workshop-module-3

What is Adaptive Authentication?

- Traditional authentication methods: passwords and PINs rely on static credentials
  - Vulnerable to credential stuffing, phishing, and brute-force attacks.
  - Fail to differentiate between low-risk and high-risk scenarios
- Adaptive MFA is a pattern in which the application you're logging into takes into account context about your authentication request.
- Its context-aware security approach

What is Adaptive Authentication?

- Adjusts security measures dynamically based on real-time risk signals
  - What IP address are you making the request from?
  - What geographic location are you making the request from?
  - What client are you making the request from (a specific version of Chrome? Firefox? Android?) Etc.
- Contextual factors such as location, device, or time—related to a user's login or access request feed into adaptive authentication as part of the continuous risk assessment and evaluation process.
  - Geolocation example : User is connected into the network from United States and few minutes later somebody's trying to log in with their credentials in Eastern Europe. That would be an example of a red flag for their geolocation

RBAC vs ABAC

- Role-Based : Uses roles in managing user permissions based on group
- Attribute Based: Access is based on several attributes and information from multiple data sources
- Zero Trust uses a combination of role-based & attribute-based access control, which provides dynamic & contextual information.

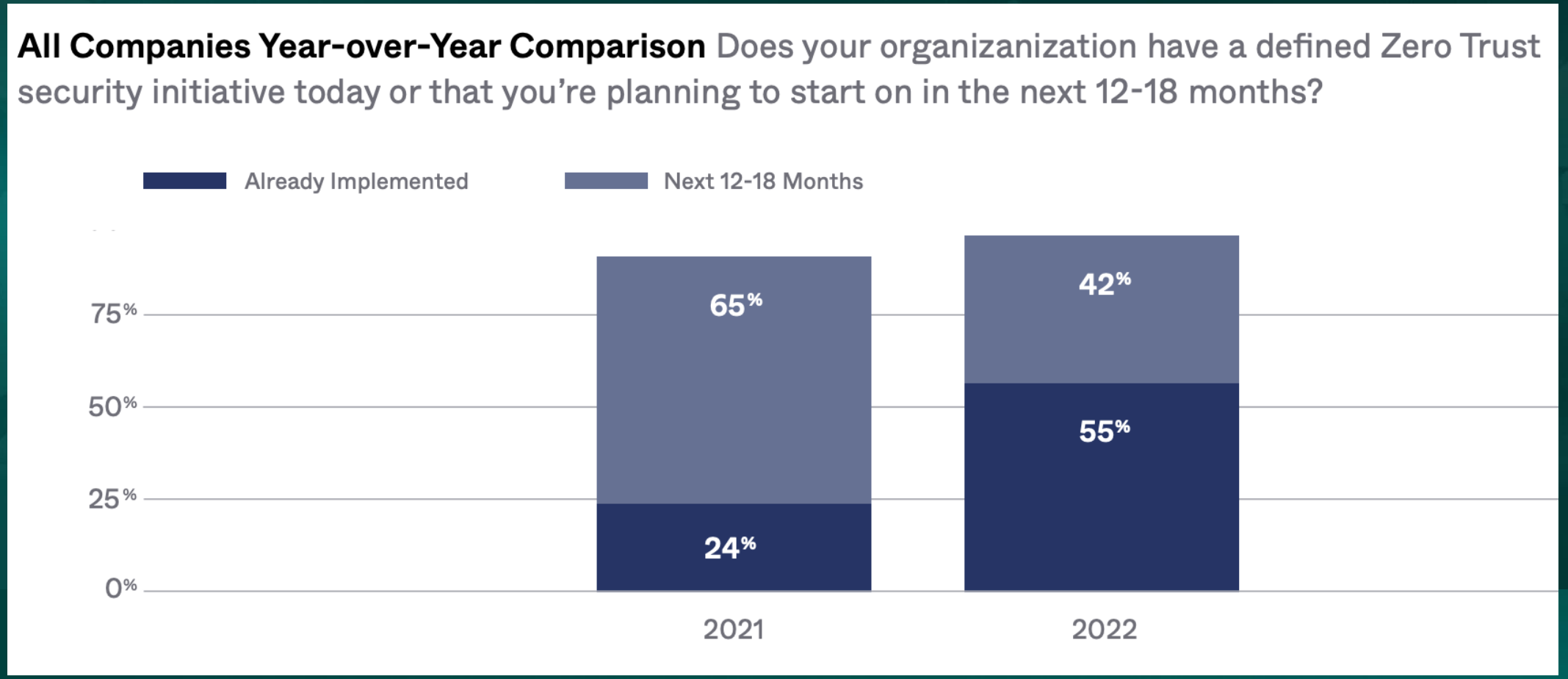
RBAC	**ABAC**
RBAC based on Role, Group Membership	ABAC is based on Time, Location, Authentication and Authorization History, OS, IP and MAC address, System Configuration, Malware Signatures, Communication Method, Resource Policies, Additional Data Sources
RBAC is static in nature	ABAC is dynamic contextual and adaptive in nature

Benefits of ZTA with AA

- 75% Reported Improved Risk Management
- 65% Reported Improved Secure Remote Access
- 41% Reported a Reduced Number of IT Security Incidents
- 34% Reported Reduced Network Complexity
- 26% Reported Lower Overall Security Costs

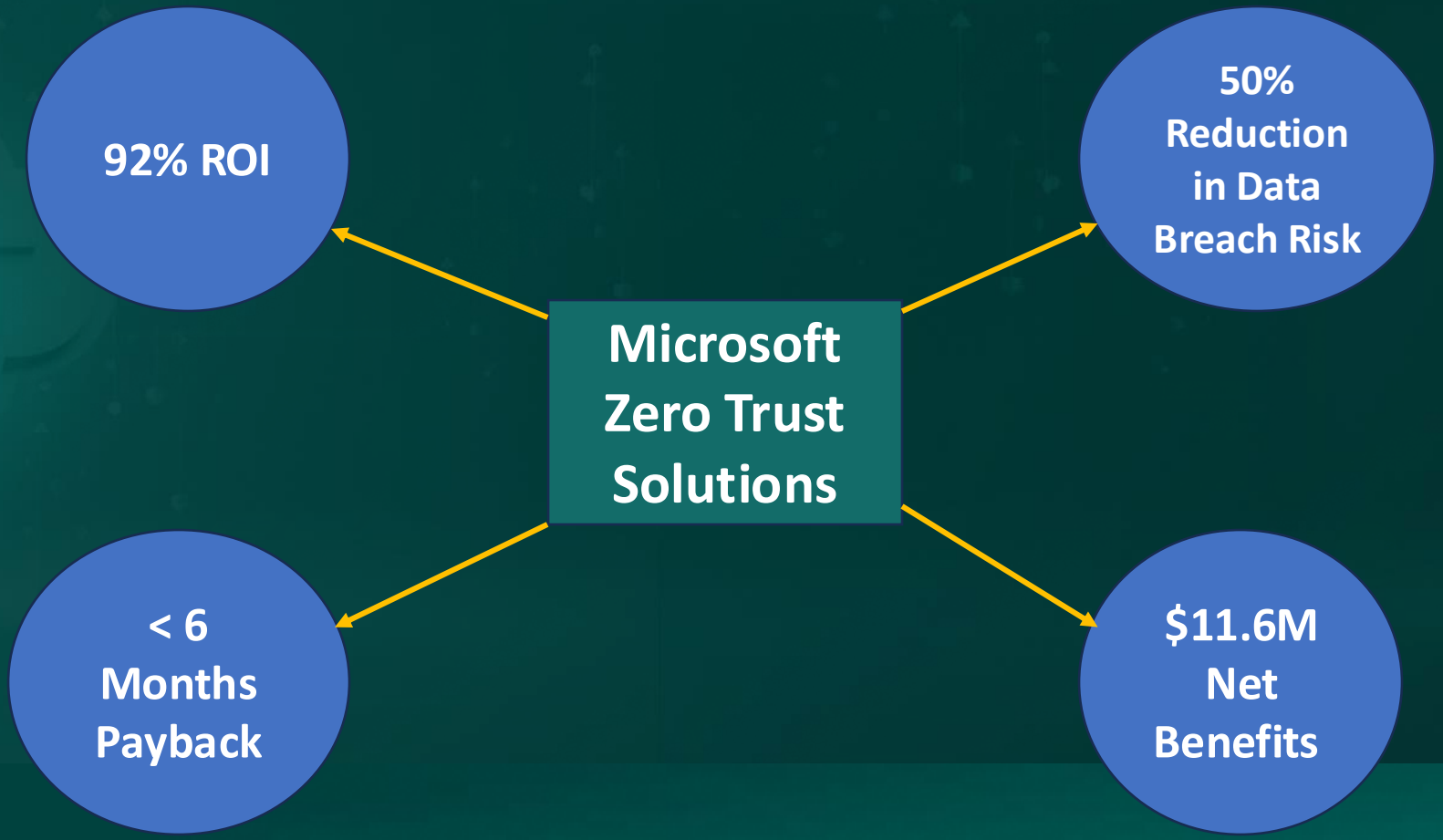
Gartner Peer Insights & WatchGuard: Zero Trust Security Strategy Adoption Survey (2021)

Okta: The State of Zero Trust Security 2022 Report



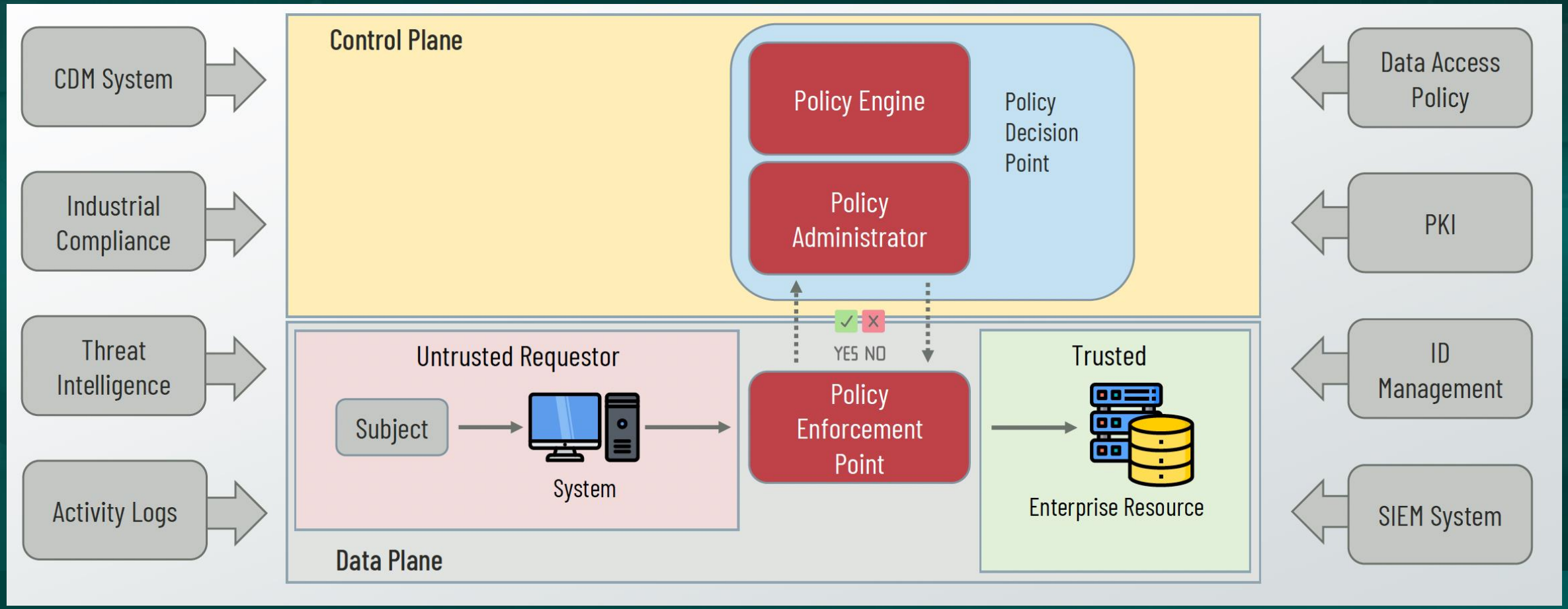
Okta Report

A Forrester Total Economic Impact TEI Study Commissioned by Microsoft



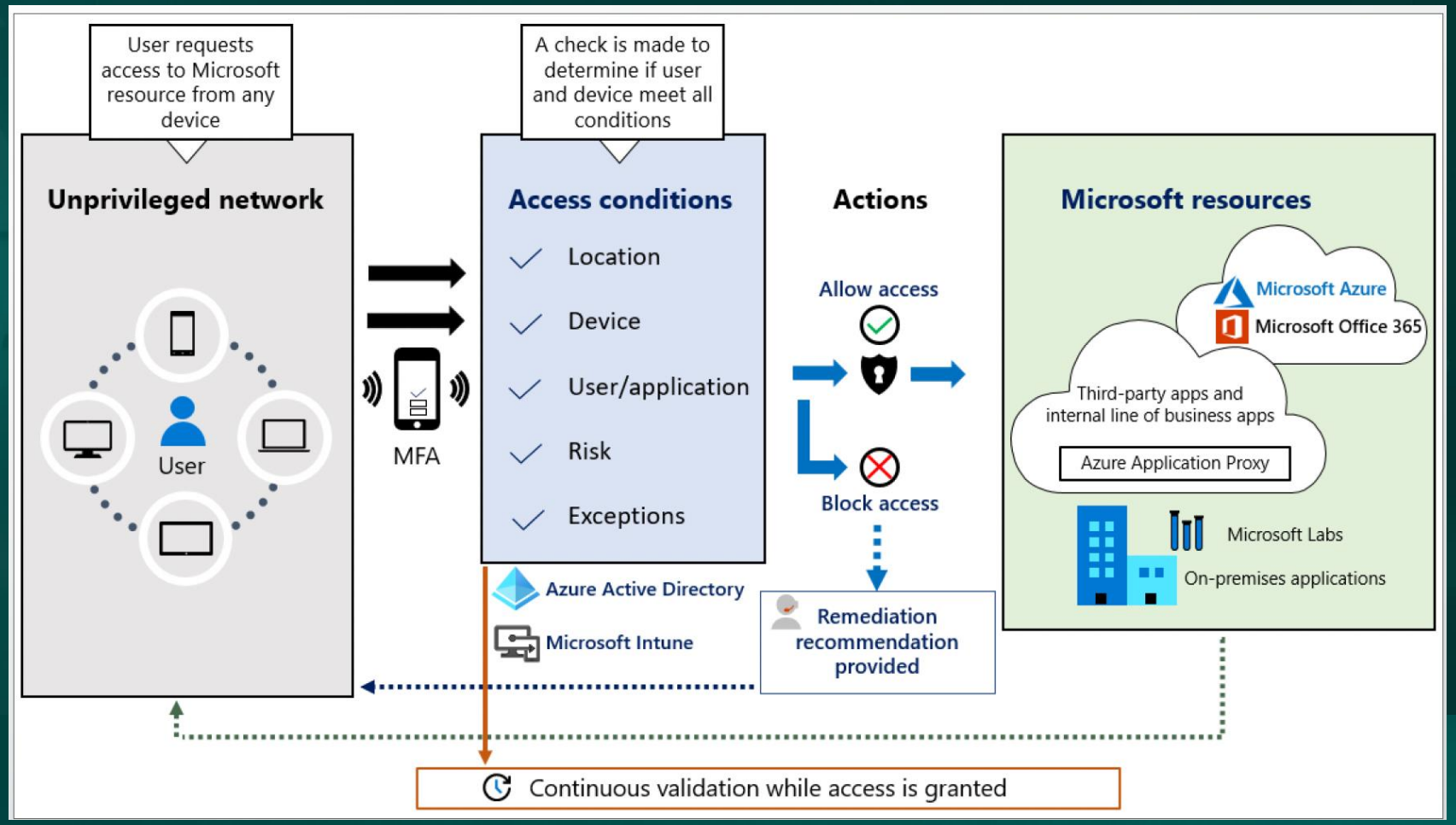
Microsoft Forrester TEI Report

NIST Zero Trust Architectural Model



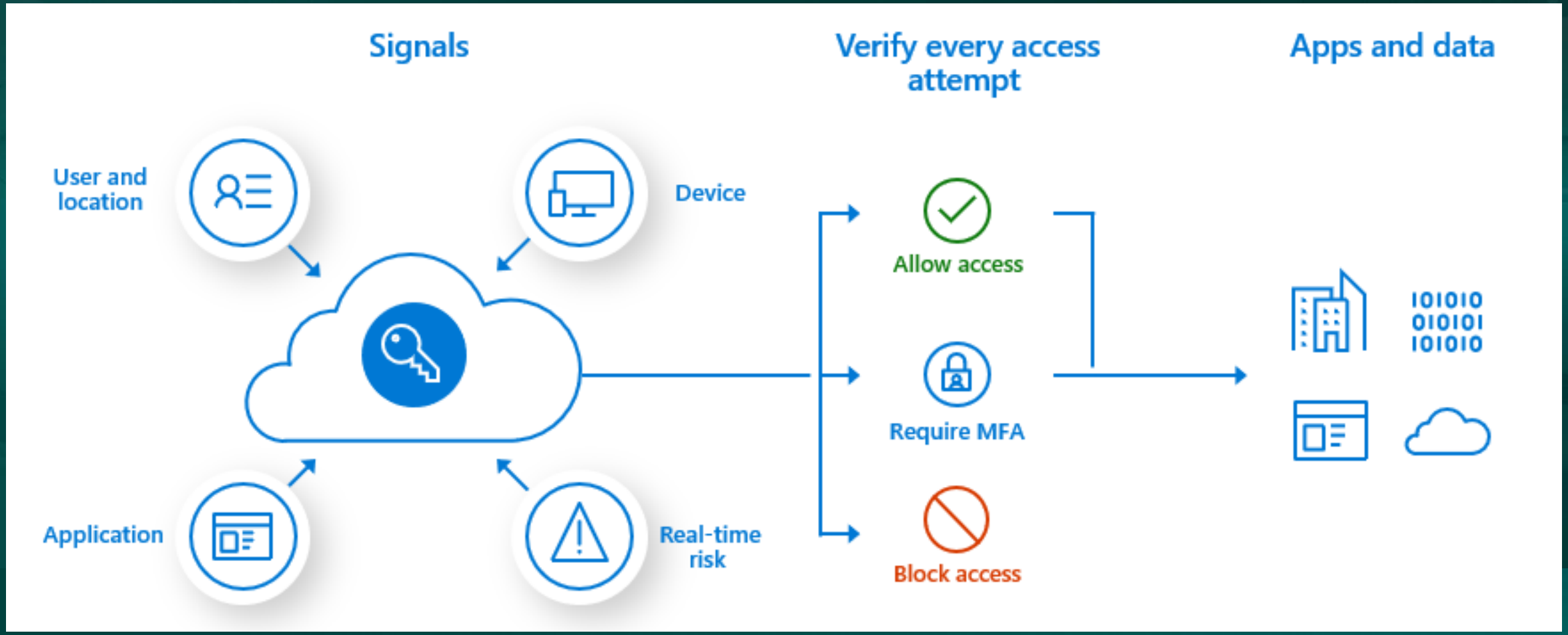
Things are getting out of hand !

Microsoft's Internal Zero Trust Architecture



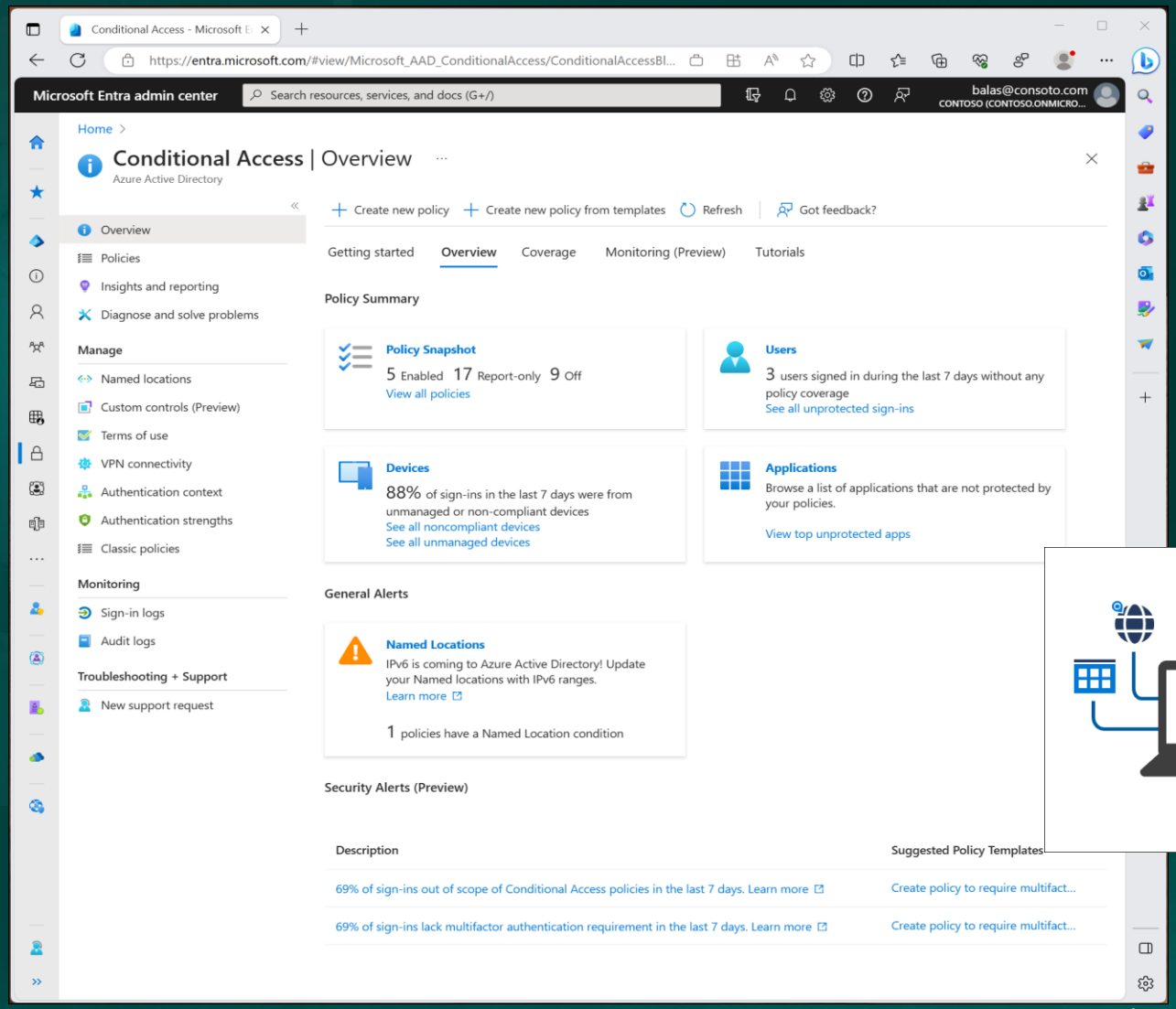
https://www.microsoft.com/insidetrack/blog/microsoft-adopts-proactive-method-for-preventing-and-mitigating-failures/

Microsoft's Internal Zero Trust Architecture

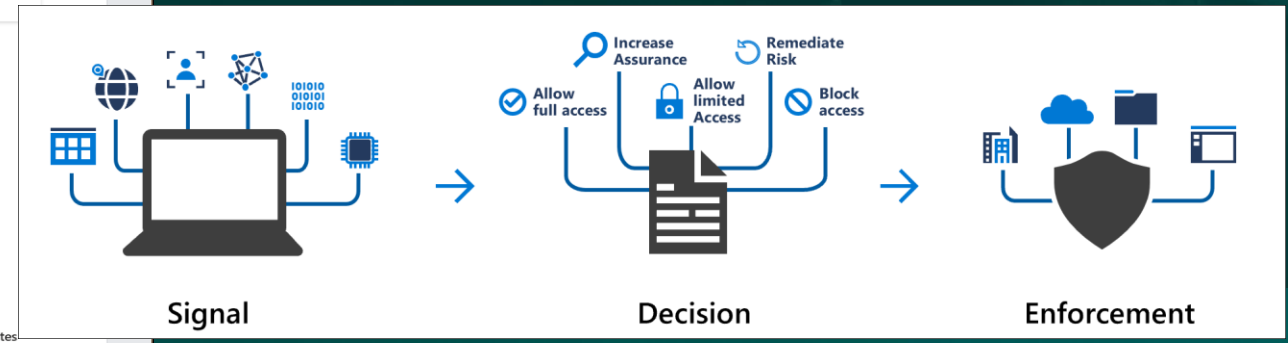


https://www.microsoft.com/insidetrack/blog/microsoft-adopts-proactive-method-for-preventing-and-mitigating-failures/

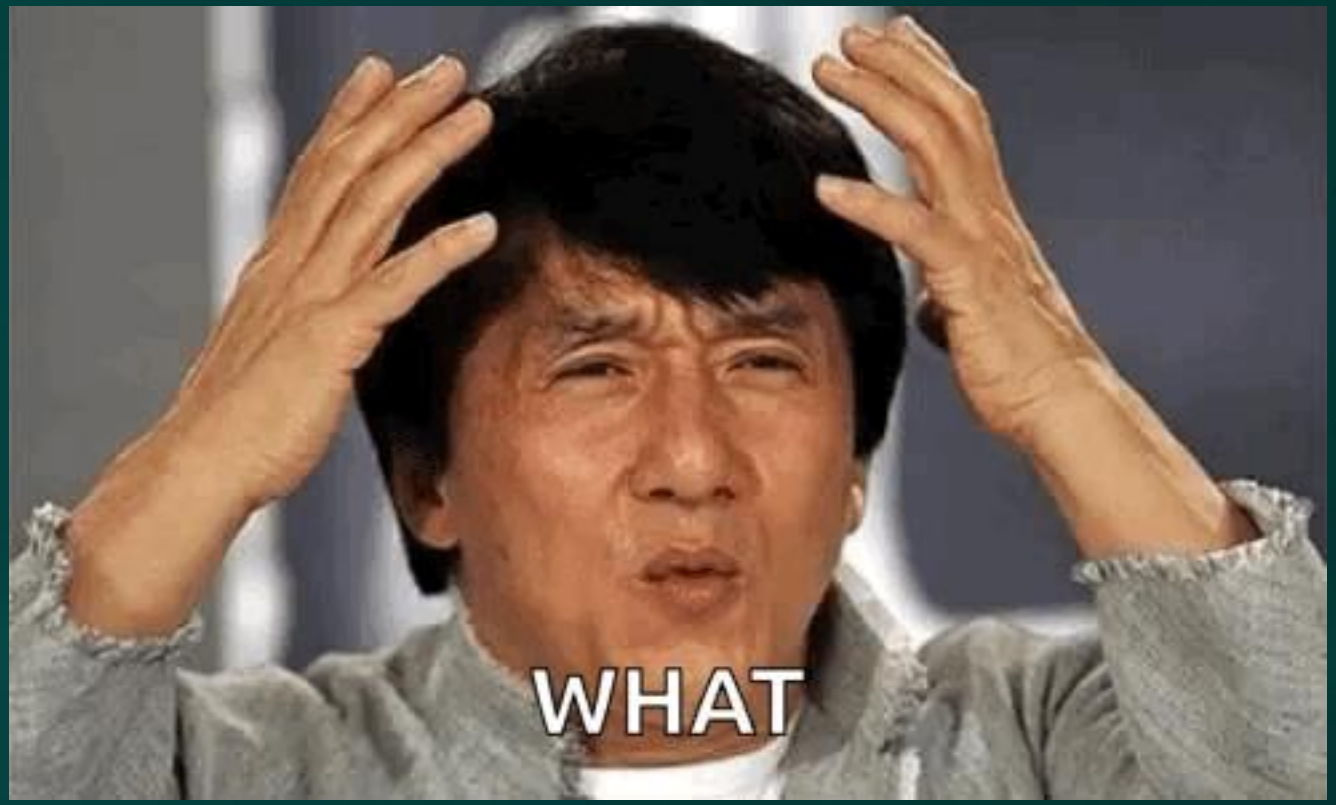
Conditional Access + Adaptive Policies in Entra ID



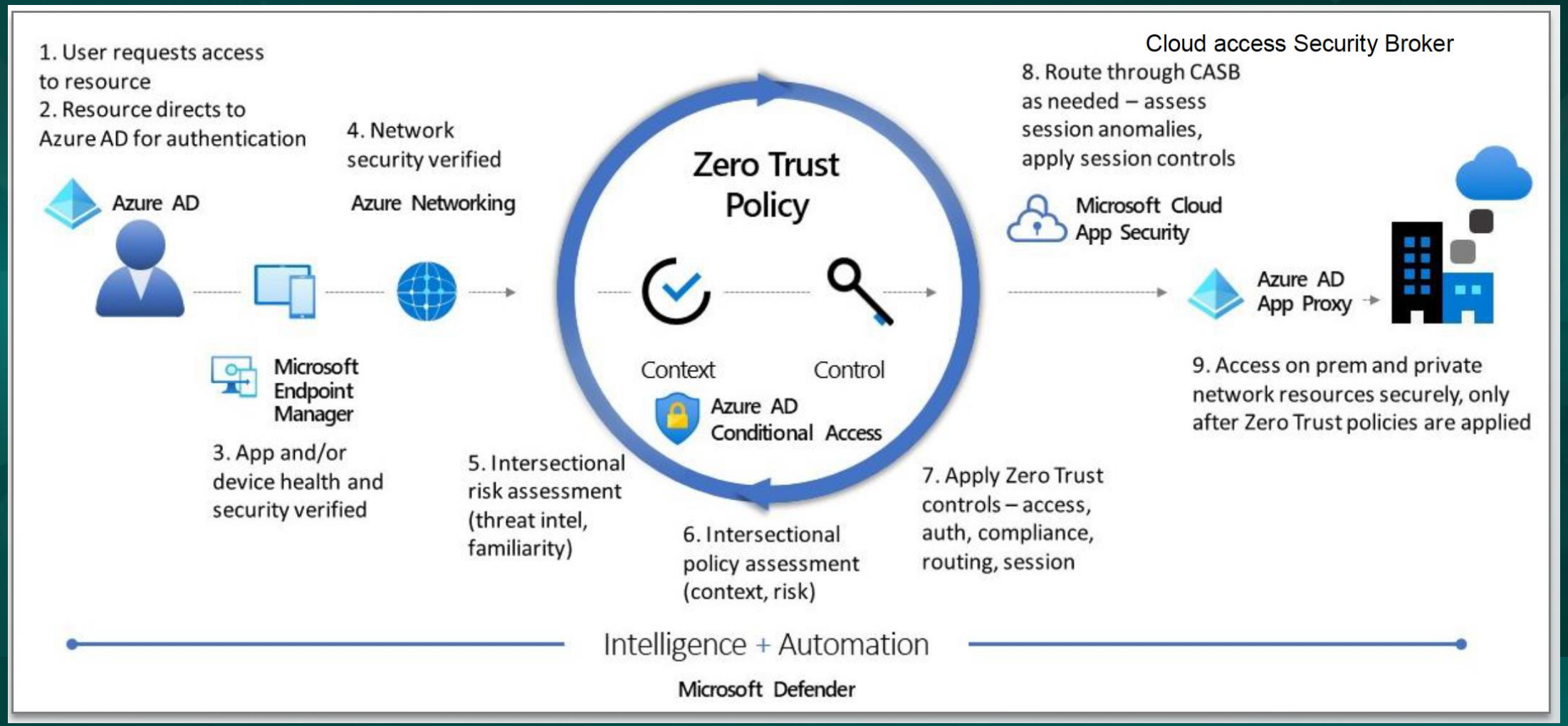
- Microsoft Entra Conditional Access brings signals together, to make decisions, and enforce organizational policies.
- Conditional Access is Microsoft's Zero Trust policy engine taking signals from various sources into account when enforcing policy decisions.



https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-session-lifetime

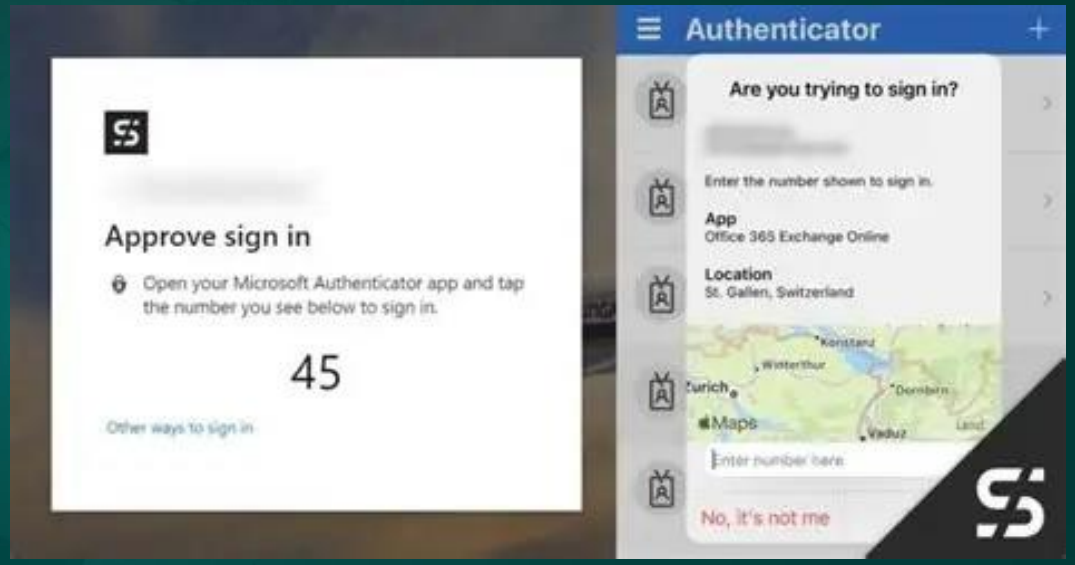

WHAT

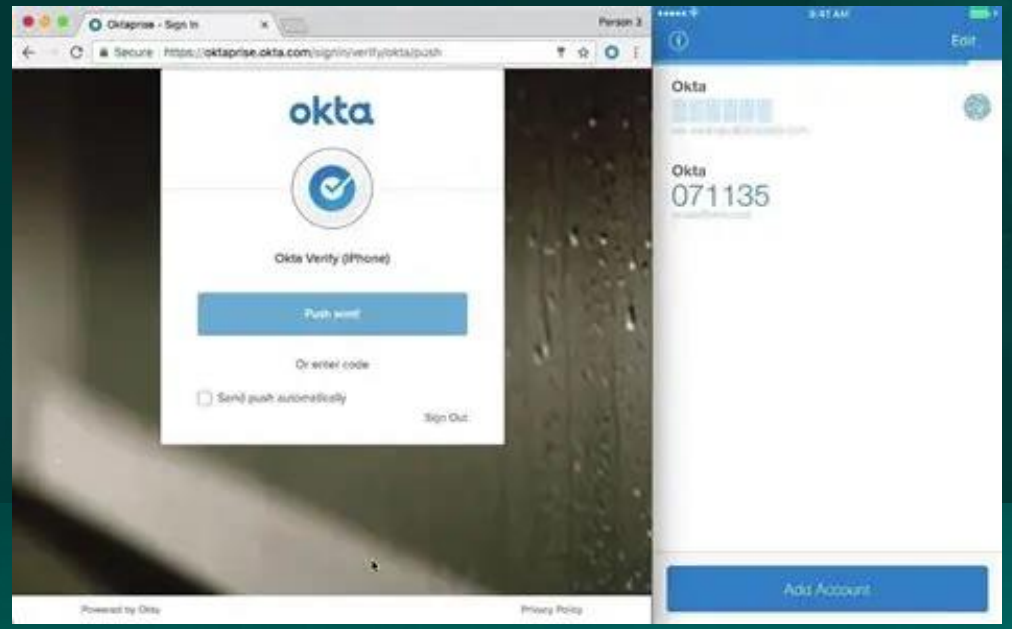
Microsoft Zero Trust Strategy Step by Step

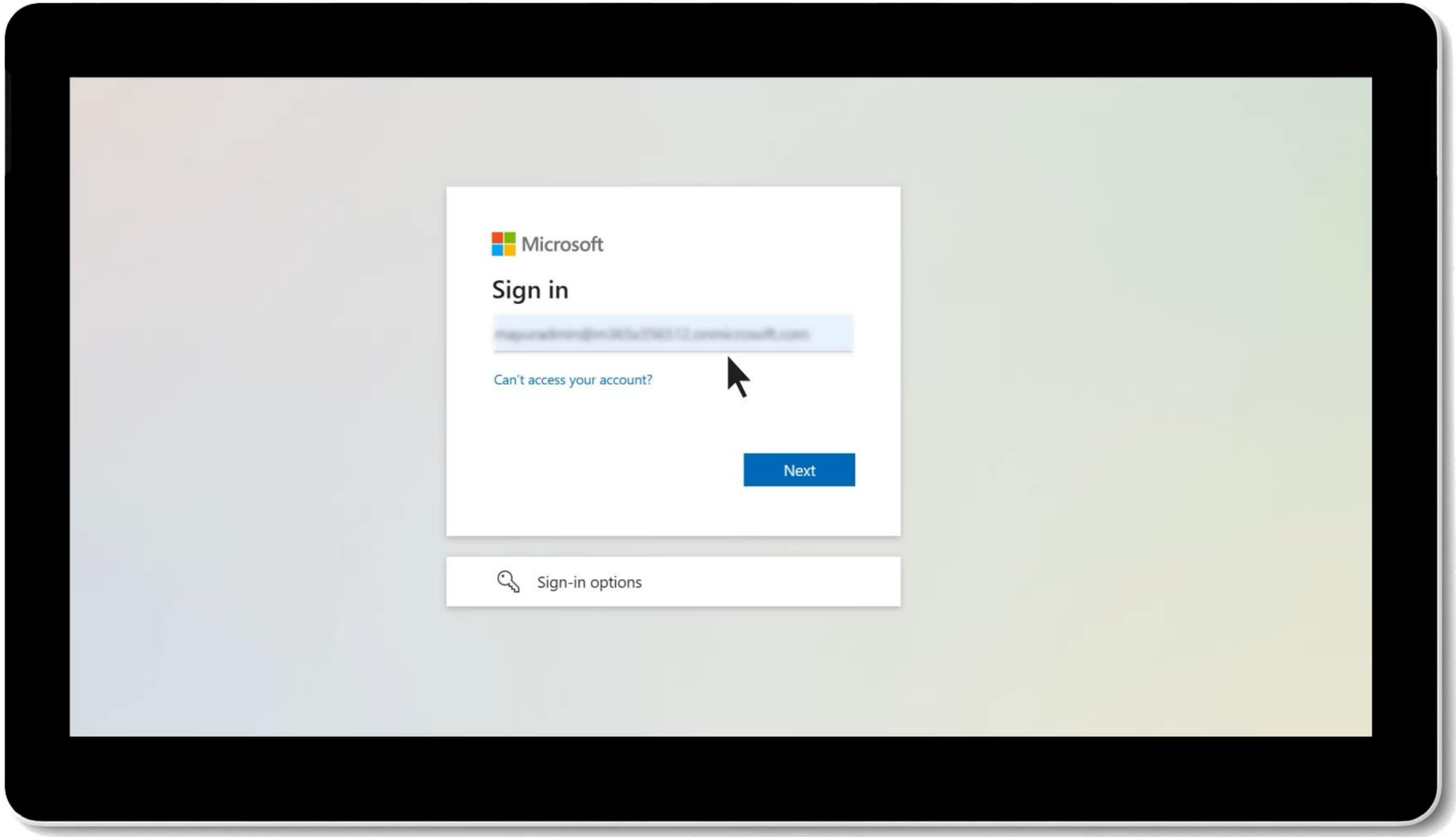


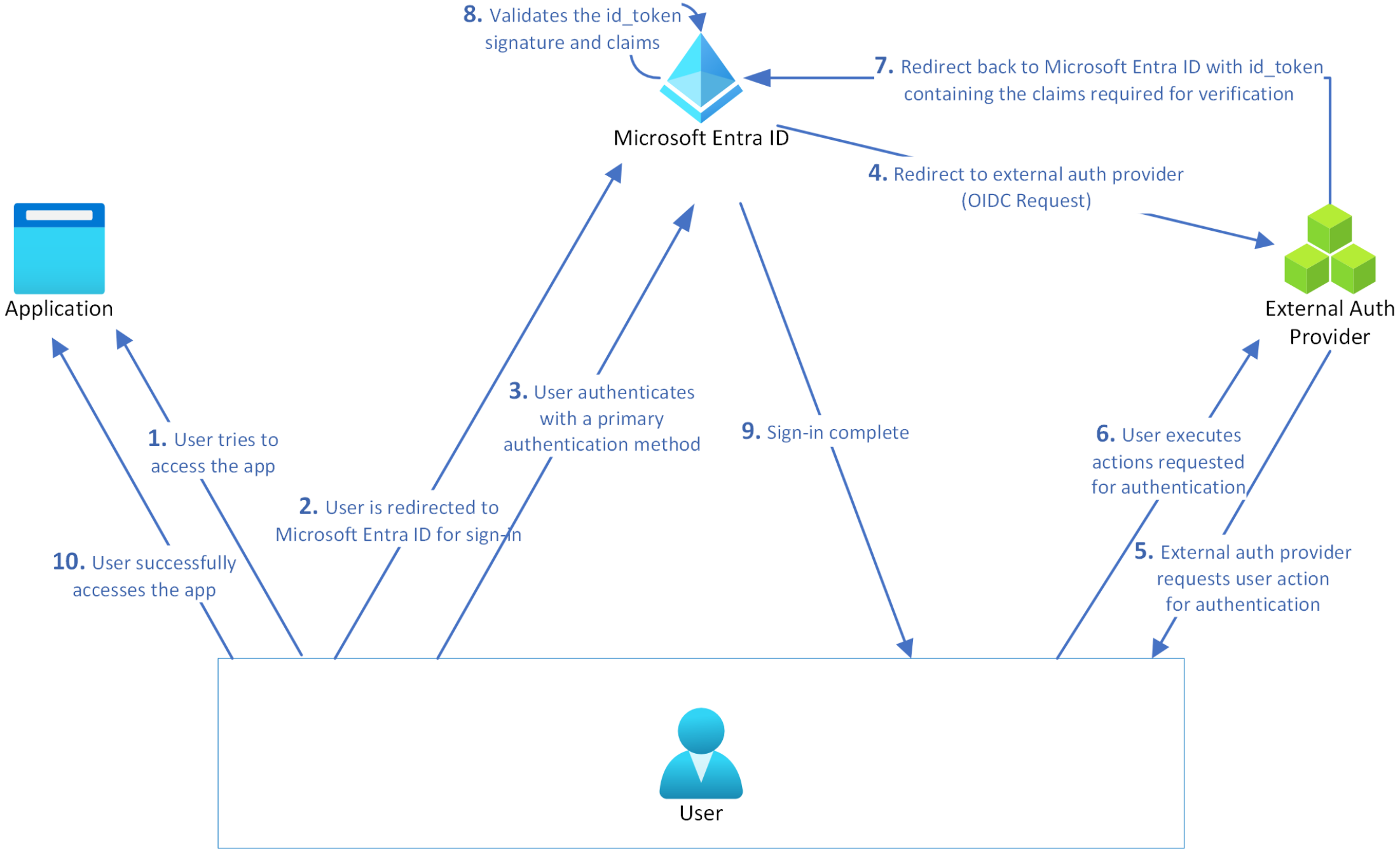
https://learn.microsoft.com/en-us/security/adoption/mcra
https://learn.microsoft.com/en-us/security/adoption/ciso-workshop-module-3

Microsoft Authenticator, Okta Verify






Microsoft
Sign in
Can't access your account?
Next
Sign-in options


8. Validates the id_token signature and claims
7. Redirect back to Microsoft Entra ID with id_token containing the claims required for verification
Microsoft Entra ID
4. Redirect to external auth provider (OIDC Request)
Application
External Auth Provider
1. User tries to access the app
2. User is redirected to Microsoft Entra ID for sign-in
3. User authenticates with a primary authentication method
9. Sign-in complete
6. User executes actions requested for authentication
5. External auth provider requests user action for authentication
10. User successfully accesses the app
User

References

- Whitepapers
  - NIST ZT Architecture : https://csrc.nist.gov/pubs/sp/800/207/final
  - CISA ZT Maturity Model: https://www.cisa.gov/zero-trust-maturity-model
- Courses and Certifications
  - Forrester Adopting ZT Certification Course
  - Cloud Security Alliance ZT Courses
- Compare diff Zero Trust products : https://www.cloudflare.com/lp/ppc/zero-trust-roadmap-x/

BONUS


A Story about a Strategy for Aligning Security and the Business
PROJECT
ZERO
TRUST
GEORGE FINNEY
Foreword by John Kindervag

Connect with me 

Thank You!

INDIA CLOUD SECURITY SUMMIT

ICSS

Sponsors

Microsoft

PENTHARA TECHNOLOGIES

Q&A, Bring it on !!

Until Next time ...