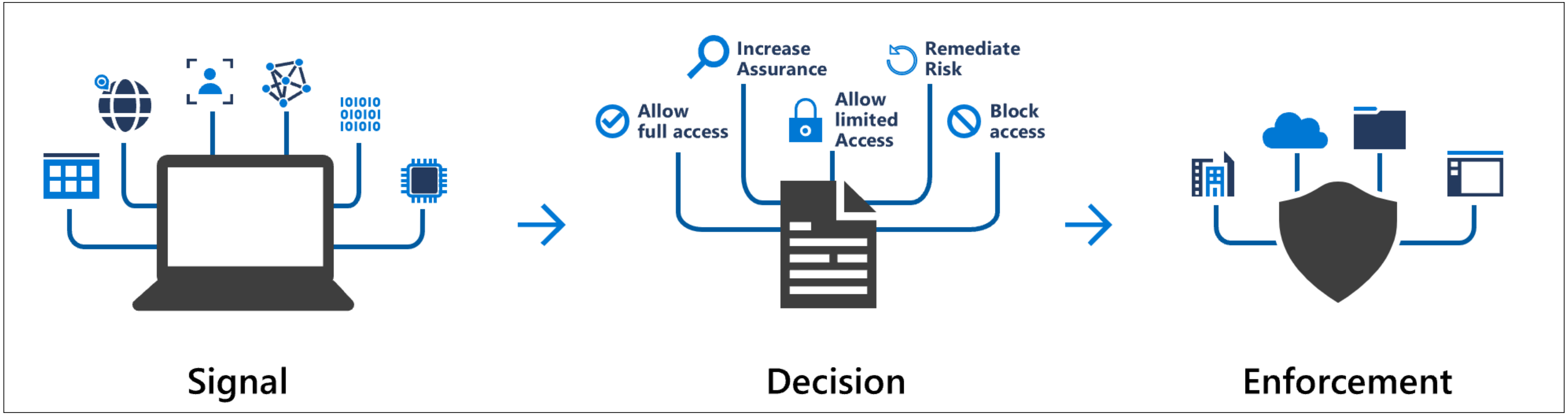
Herbsttagung 2020
Demo: Conditional Access in Azure Active Directory

Thomas Lüthi

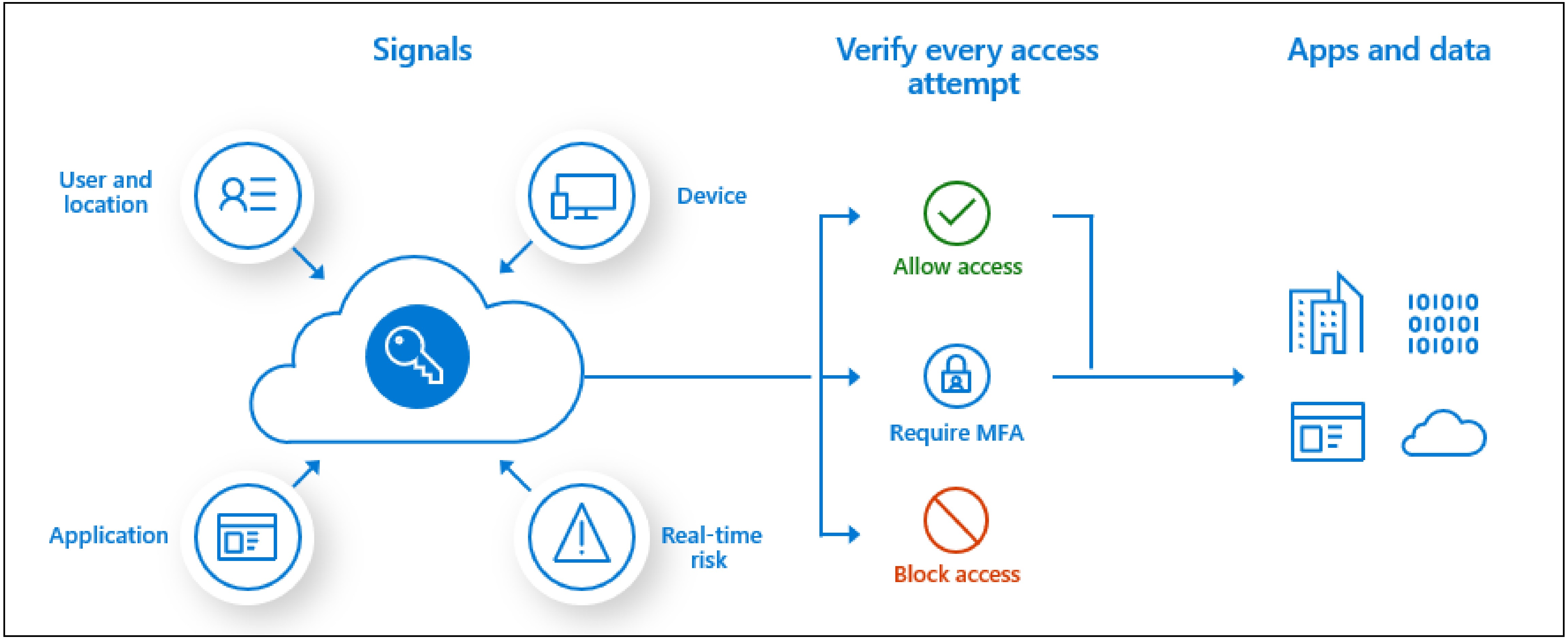
Zürich, 9. September 2020

What is Conditional Access?



https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Conditional Access in Azure Active Directory



Conditional Access – Good to know

- Functionality depends on license
- Conditional Access policies are enforced after first-factor authentication is completed.
- Access is granted by default.
- It is required to disable "Security Defaults" in order to activate Conditional Access policies.
- Security Defaults
  - Requiring all users to register for Azure multi-factor authentication.
  - Requiring administrators to perform multi-factor authentication.
  - Blocking legacy authentication protocols.
  - Requiring users to perform multi-factor authentication when necessary.
  - Protecting privileged activities like access to the Azure portal.

Real time risks

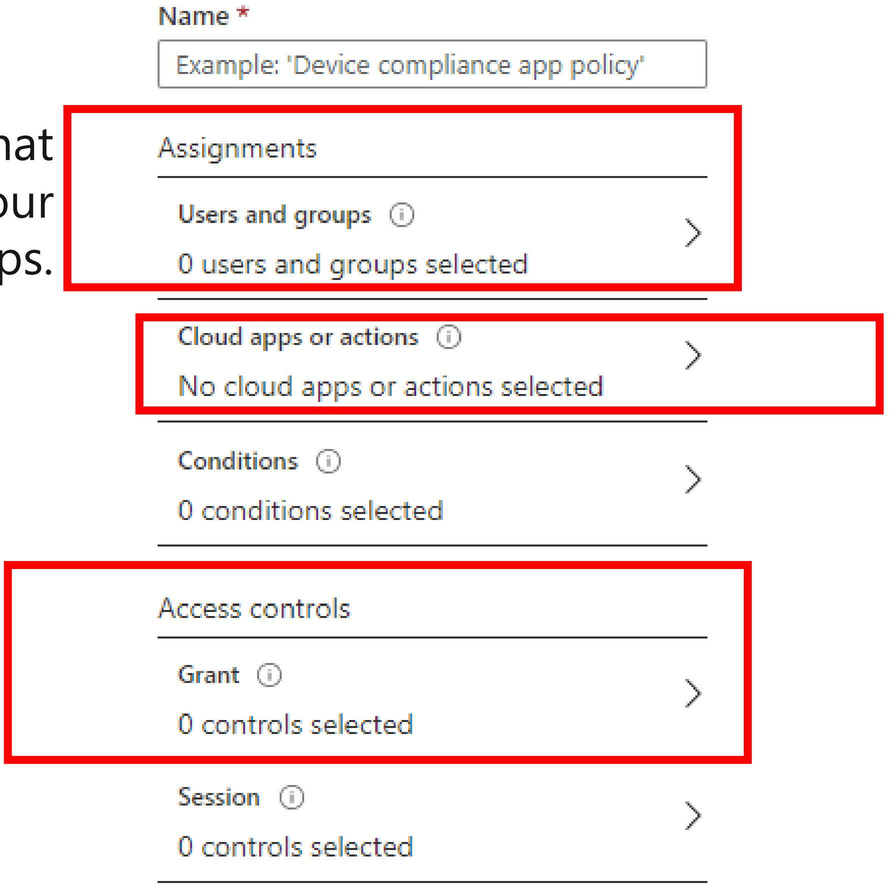
User risk

- the probability that a given identity or account is compromised.
- Detection:
  - Leaked credentials
  - Azure AD threat intelligence

Sign-in risk

- the probability that a given authentication request isn't authorized by the identity owner
- Detection:
  - Anonymous IP address
  - Atypical or impossible travel
  - ....

What's required to make a policy work?



Name *

Example: 'Device compliance app policy'

Assignments

Users and groups ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

No cloud apps or actions selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

1) At least one user or group that is authorized to access your selected cloud apps.

2) One or more apps or user actions

3) Access control decision and applied policy.

Vielen Dank für Ihre Aufmerksamkeit_

Thomas Lüthi

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland