Extending the PAW mentality to the cloud

- Viktor Hedberg
- Cyber Security Consultant @ Truesec
- Twitter @headburgh
- MVP, MCT

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —


NORDIC
– VIRTUAL SUMMIT –
PATCH MY PC
RECAST SOFTWARE
Extending the PAW mentality to the cloud.
Why just enforcing MFA is not enough.

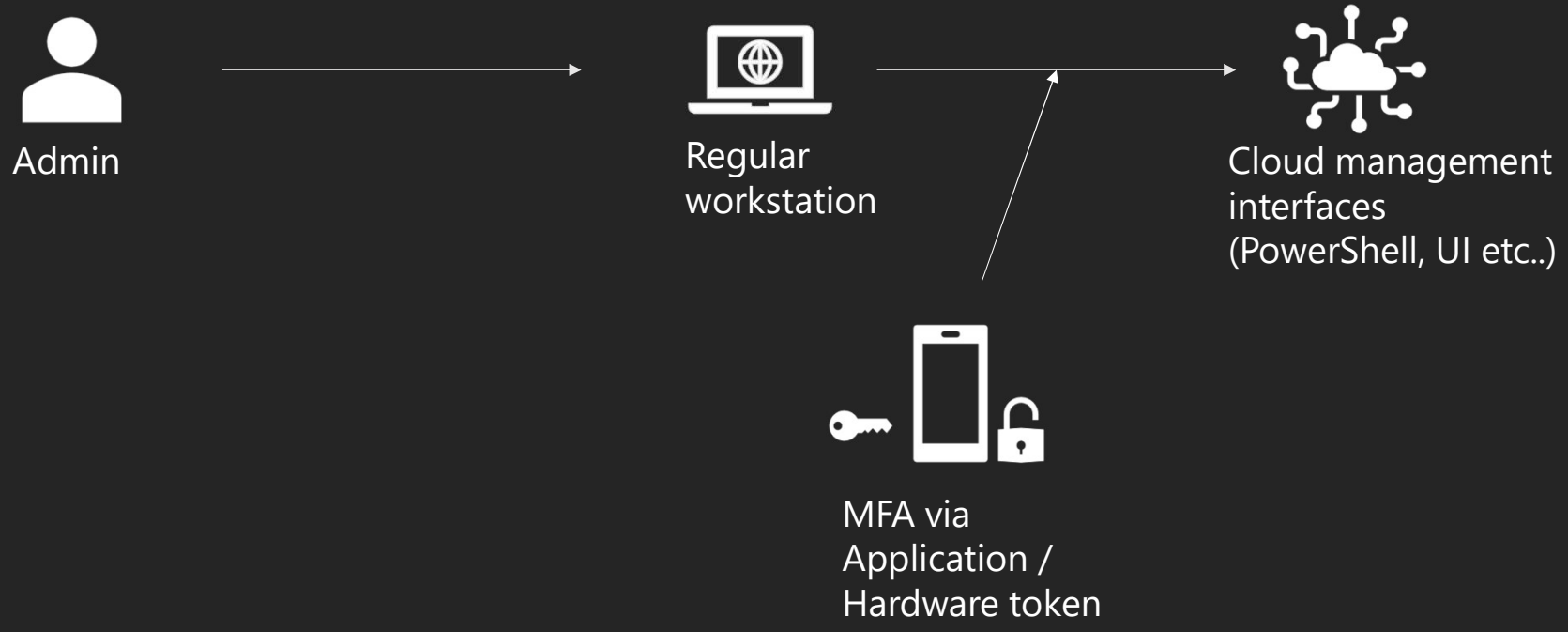
/whoami

- Viktor Hedberg

- Cyber Security Consultant @ Truesec
- Proactive measures
- DFIR
- Advisory

NORDIC
– VIRTUAL SUMMIT –

The current state (for most)

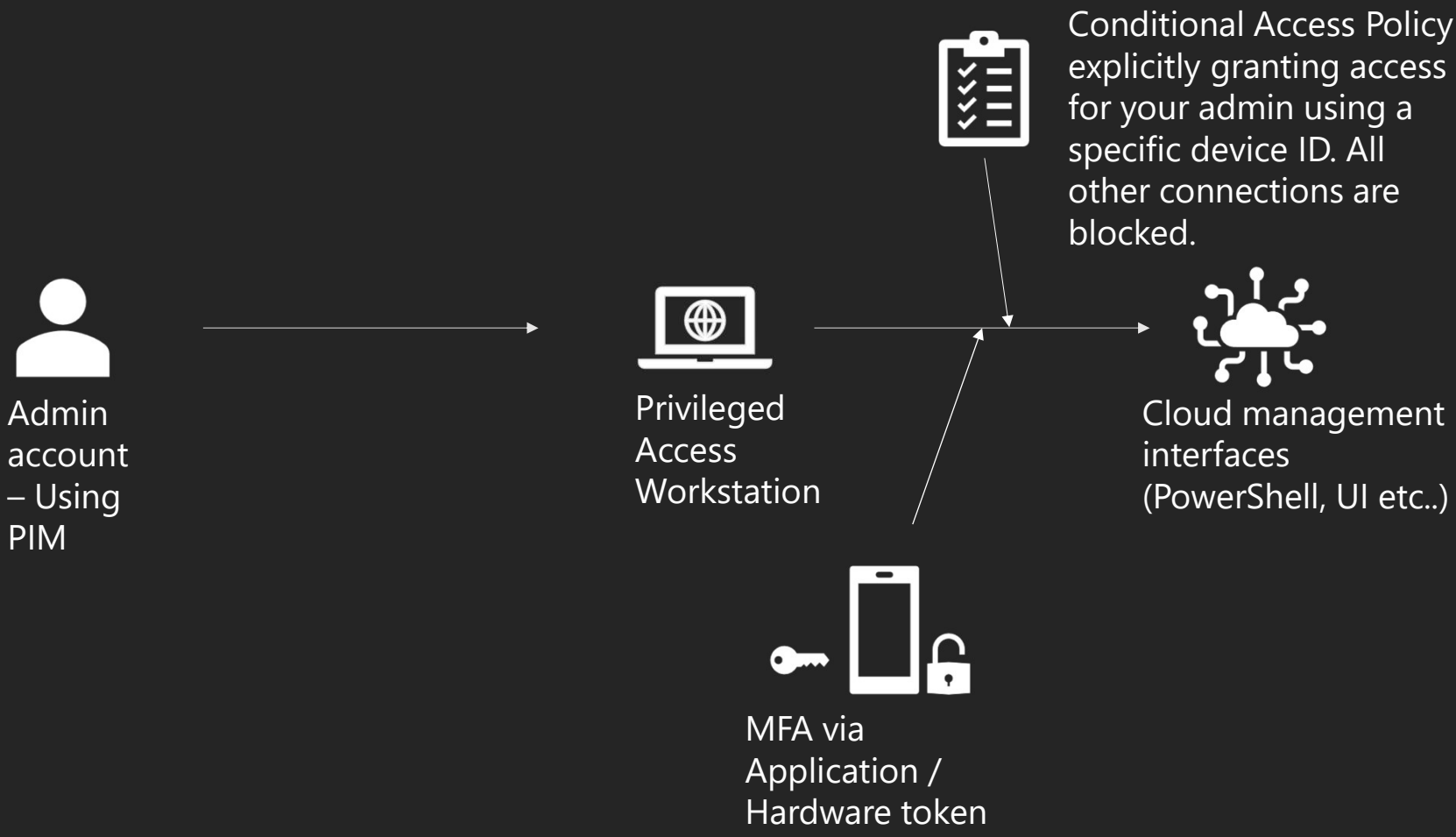


Why the current state is not enough?

NORDIC
– VIRTUAL SUMMIT –

- The sign in can occur from any device.
- Vulnerable to common attack patterns such as:
  - Info Stealers
  - MiTM
  - Prompt Overflow
- What can be done instead?
  - PAW

The preferred state (for ALL!)



Why is the PAW scenario more secure?

NORDIC
– VIRTUAL SUMMIT –

- Sign-in can only occur from a specific device, all other connections are blocked
- A Threat Actor needs to be in possession of all three factors:

Admin account

Privileged Workstation

MFA credential

- This provides for more locking effects, securing our privileged roles and accesses

DEMO

Summary

NORDIC
– VIRTUAL SUMMIT –

- Only use Cloud Native accounts for administrative tasks
- All admin accounts need to have an Azure AD P2 license for PIM/Identity Protection
- Create Device Filter policies to acquire locking effects on individual accounts

A big thanks to our sponsors

NORDIC
– VIRTUAL SUMMIT –

RECAST SOFTWARE

Thank you!

Please remember to fill out the evals!

https://stream.nordicvirtualsummit.com/feedback