

Cloud Administration Model

-

New paradigms to fly to the moon

Etienne LAFORE

Senior Manager
Etienne.Lafore@wavestone.com
(+33) 6 99 30 95 30



Raymond CHAN

Senior Consultant
Raymond.Chan@wavestone.com
(+33) 6 65 64 38 23

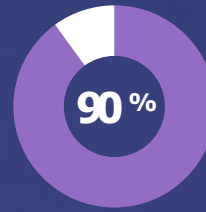


Is your Cloud administration secure ?

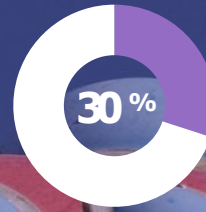


Flash the QR
Code, *or* Go to
www.beekast.live
and enter the
code **492755**

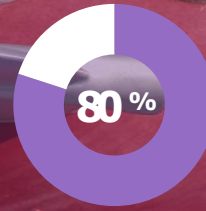
Administration hardening Active Directory



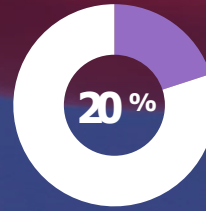
Critical assets hardening (Tier 0)



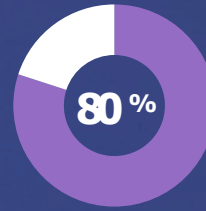
MFA



All administration tools protected



Dedicated PAWs



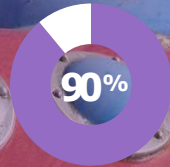
Audit of admin security

Administration hardening

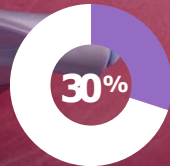
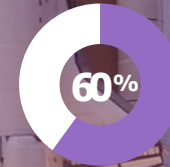
Active Directory

vs

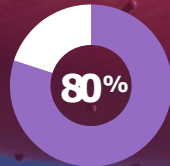
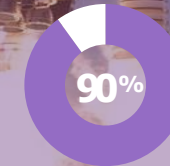
Cloud



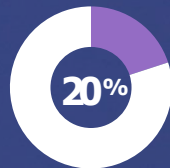
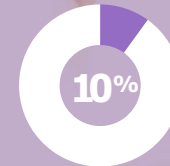
Critical assets hardening



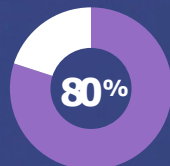
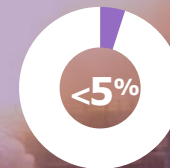
MFA



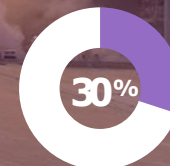
All administration tools protected



Dedicated PAWs

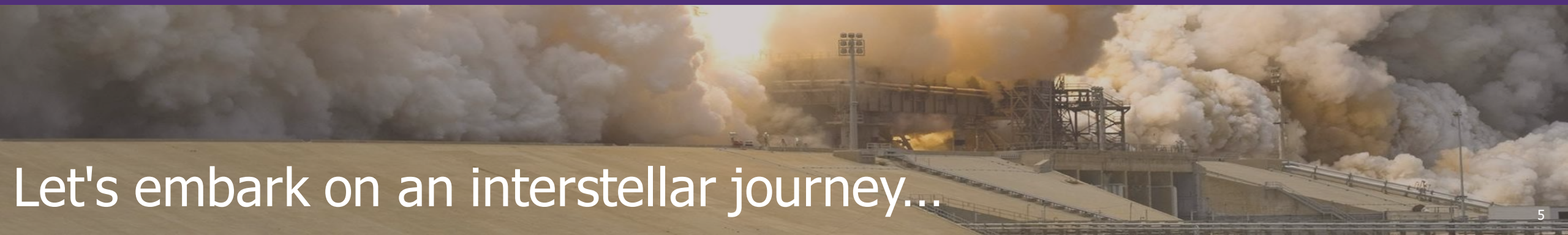


Audit of admin security





Is the compromise of Cloud as critical as the compromise of AD?

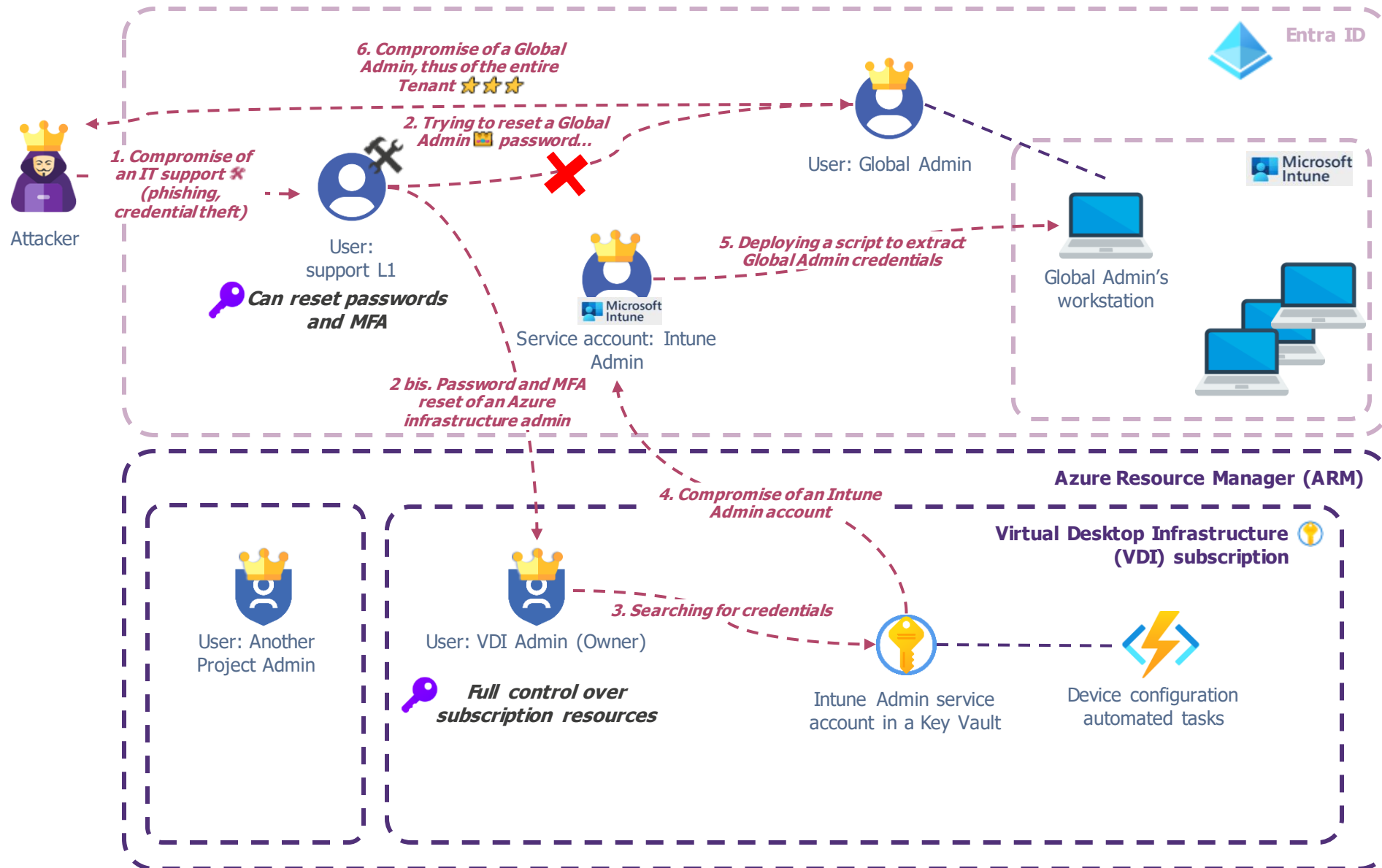


Let's embark on an interstellar journey...

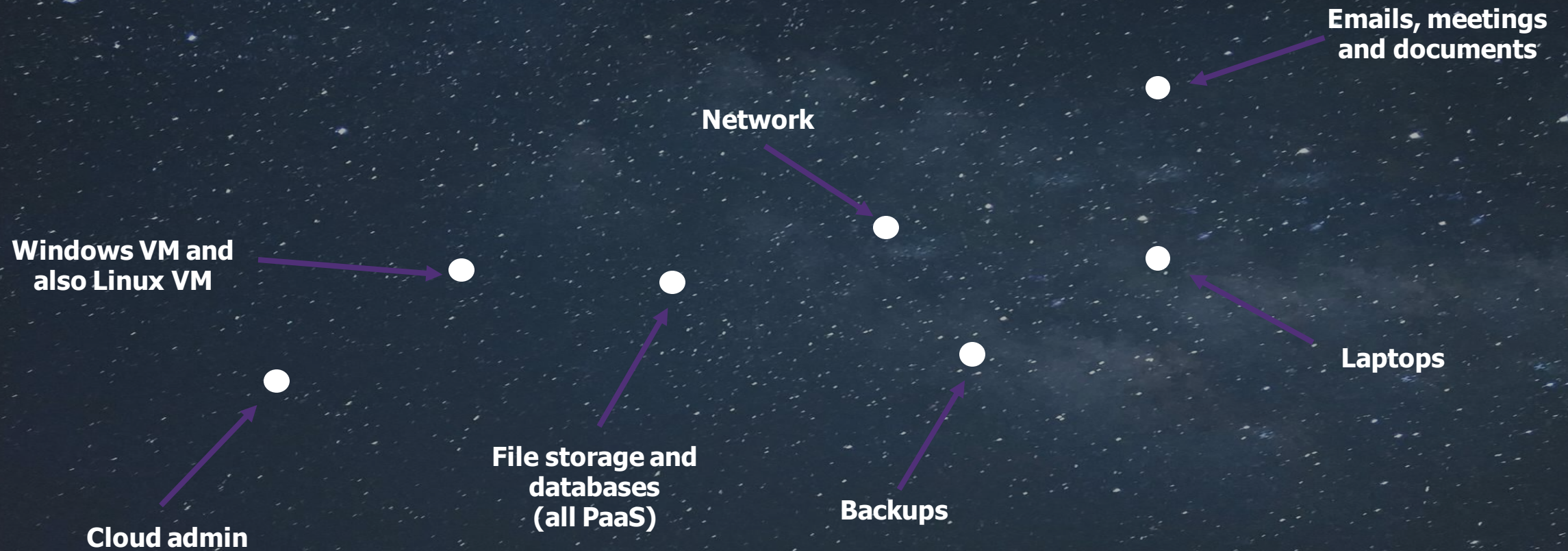
What just happened ?



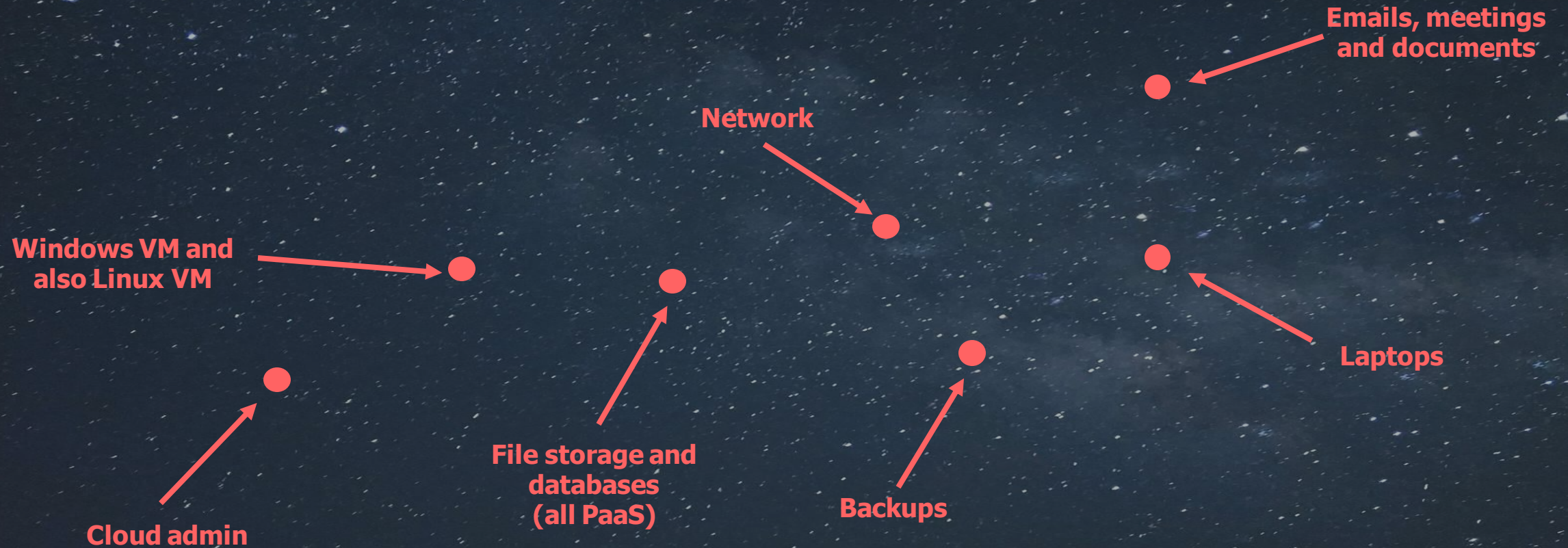
What just happened ?



A Cloud Admin can do *worse* than an AD admin !



A Cloud Admin can do *worse* than an AD admin !



What can we do ?



Let's get back to basics

Why Active Directory 3-tier model ?

On-premise infrastructure

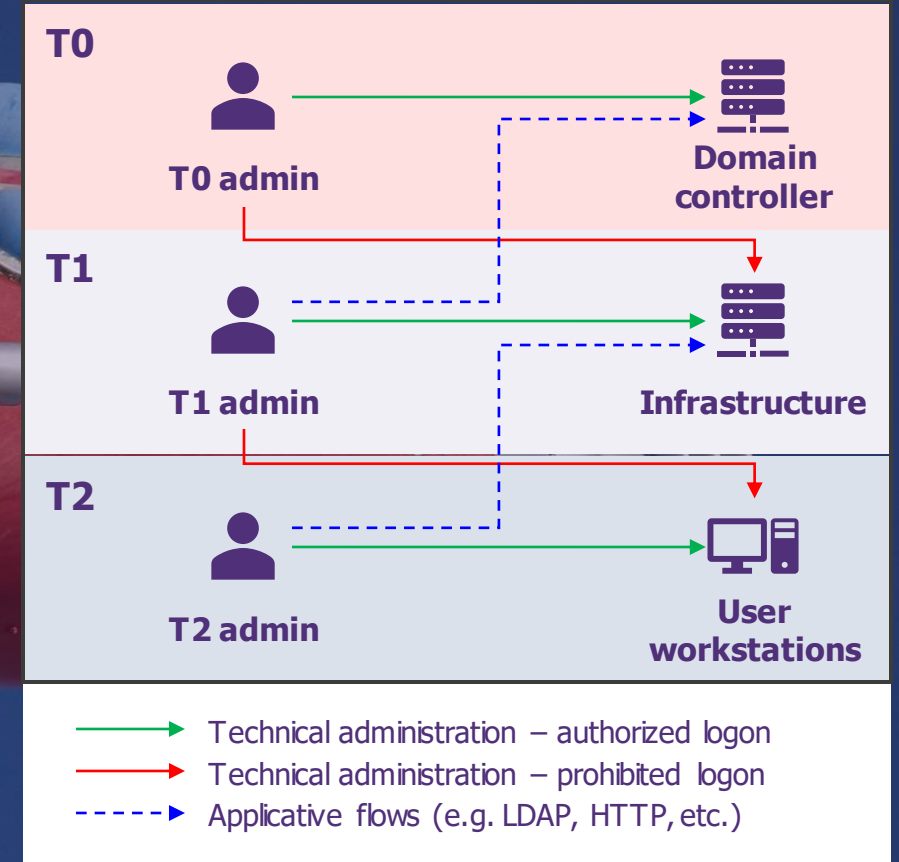
To ensure the **compromise** of a **lower tier (T2)** will not affect a **higher tier (T1, T0)**

Isolation requires

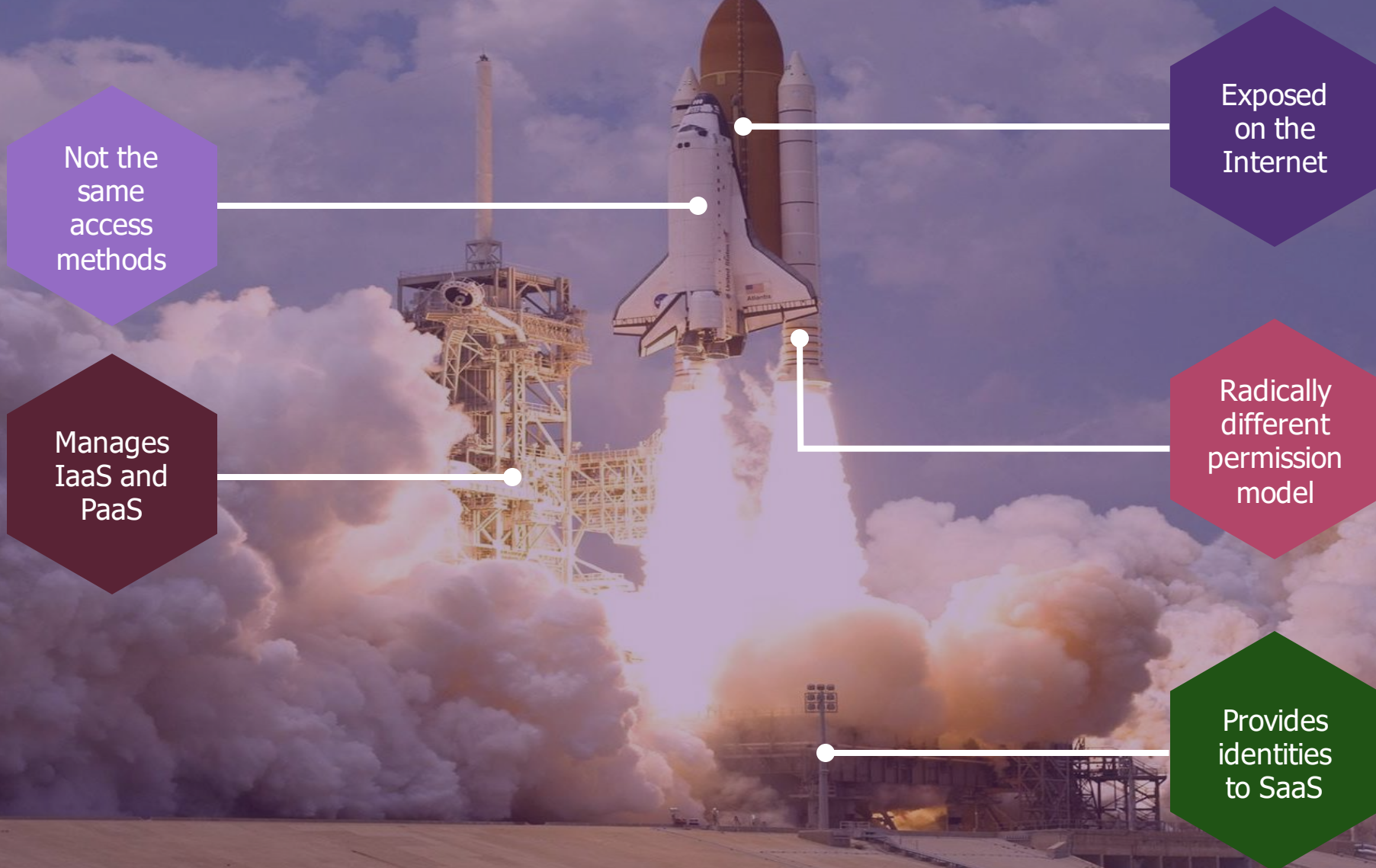
Dedicated admin accounts

Dedicated assets

Dedicated network

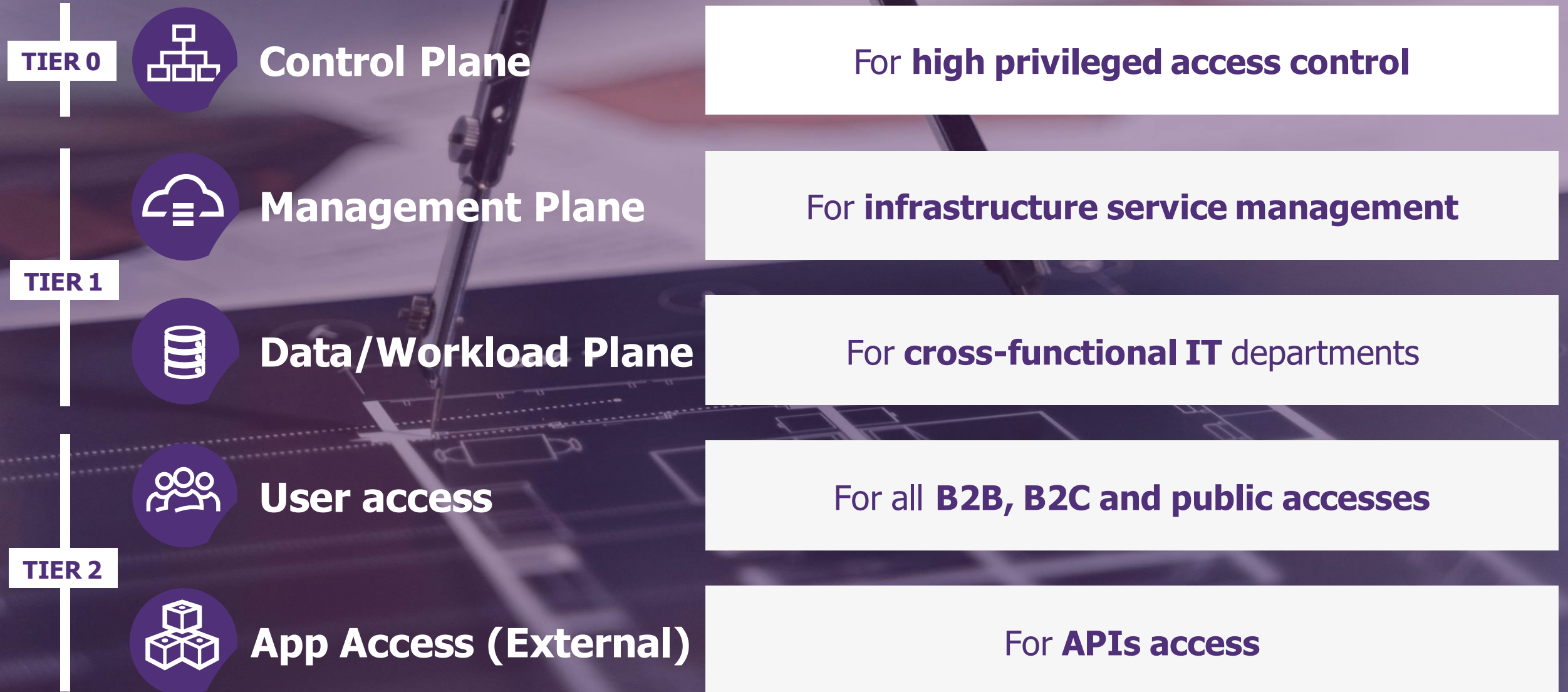


Why is the 3-tier model not applicable as is for the Cloud?



A new model by Microsoft :

Enterprise Access Model



Scope your *Control Plane*

What is *systemic* for your *IS* ?

An aerial photograph of a rocket launch at a space center. The rocket is ascending vertically, leaving a large plume of white smoke and a bright orange flame trail. The launch pad is surrounded by various structures, including a tall water tower labeled 'SPACE' and several buildings. In the background, there is a body of water and a forested area.

Accept to lose a *single rocket*
but not the *whole space center*

Scope your *Control Plane*

Project
Launch to the space/Cloud

Project pipeline
Deploy a single project

IGA
Identity governance

EDR
Detect and respond to security threats

MDM
Device management

IdP
Identity provider

Projects
Other projects in development

AD
Connect to on-premise resources

Bastion
Secure entry point for IaaS administration

CI/CD infrastructure
Set up the landing zone and all projects


Scope your *Control Plane*




Control Plane: High privileged accounts within these tools

Project
Launch to the space/Cloud

Project pipeline
Deploy a single project

 **IGA**
Identity governance

 **EDR**
Detect and respond to security threats

 **MDM**
Device management

 **IdP**
Identity provider

Projects
Other projects in development

 **AD**
Connect to on-premise resources

 **Bastion**
Secure entry point for IaaS administration

 **CI/CD infrastructure**
Set up the landing zone and all projects

Let's prepare our journey

Here are 3 concrete examples
to *retake control*



IT support *compromise*

Isolate Control Plane accounts from the help desk

Prefer **local (Cloud-only) accounts** for the control plane

Separate support accounts for **user workstation administration** from **Cloud administration** (to limit the impact of credential theft)

Control **account lifecycle (IGA, CIEM)**

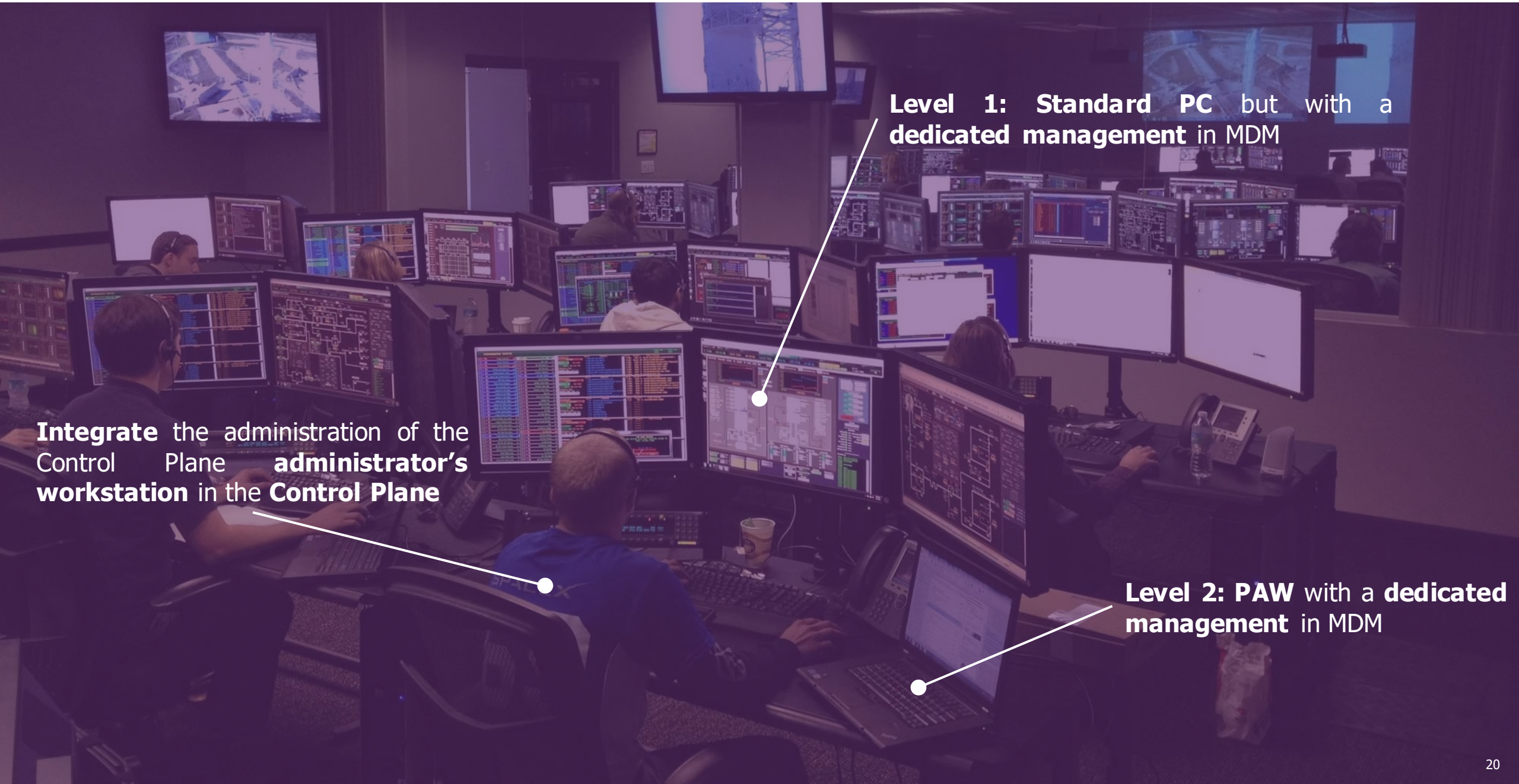
Enforce **conditional access and workstation conformity**

Implement **Just-In-Time admin (JIT)**

Deploy **phishing-resistant MFA**

And the bastion (PAM) ?

Control Plane Admin's Laptop *compromise*



Level 1: Standard PC but with a **dedicated management in MDM**

Integrate the administration of the Control Plane **administrator's workstation** in the **Control Plane**

Level 2: PAW with a **dedicated management in MDM**

CI/CD *compromise*

Apply the **least privilege principle** on accounts used by the CI/CD infrastructure. Make sure they don't have **permission outside of their scope**

Standard development process
Protected branches in Git to reduce human errors and to ensure reviews before deploying to production

Least privilege for runners
Use **OIDC** to adjust the permissions of the runner according to the execution context (project, environment...)

Automate when possible
/ Infrastructure as Code (IaC)
/ Configuration as Code (CaC)
/ Policy as Code

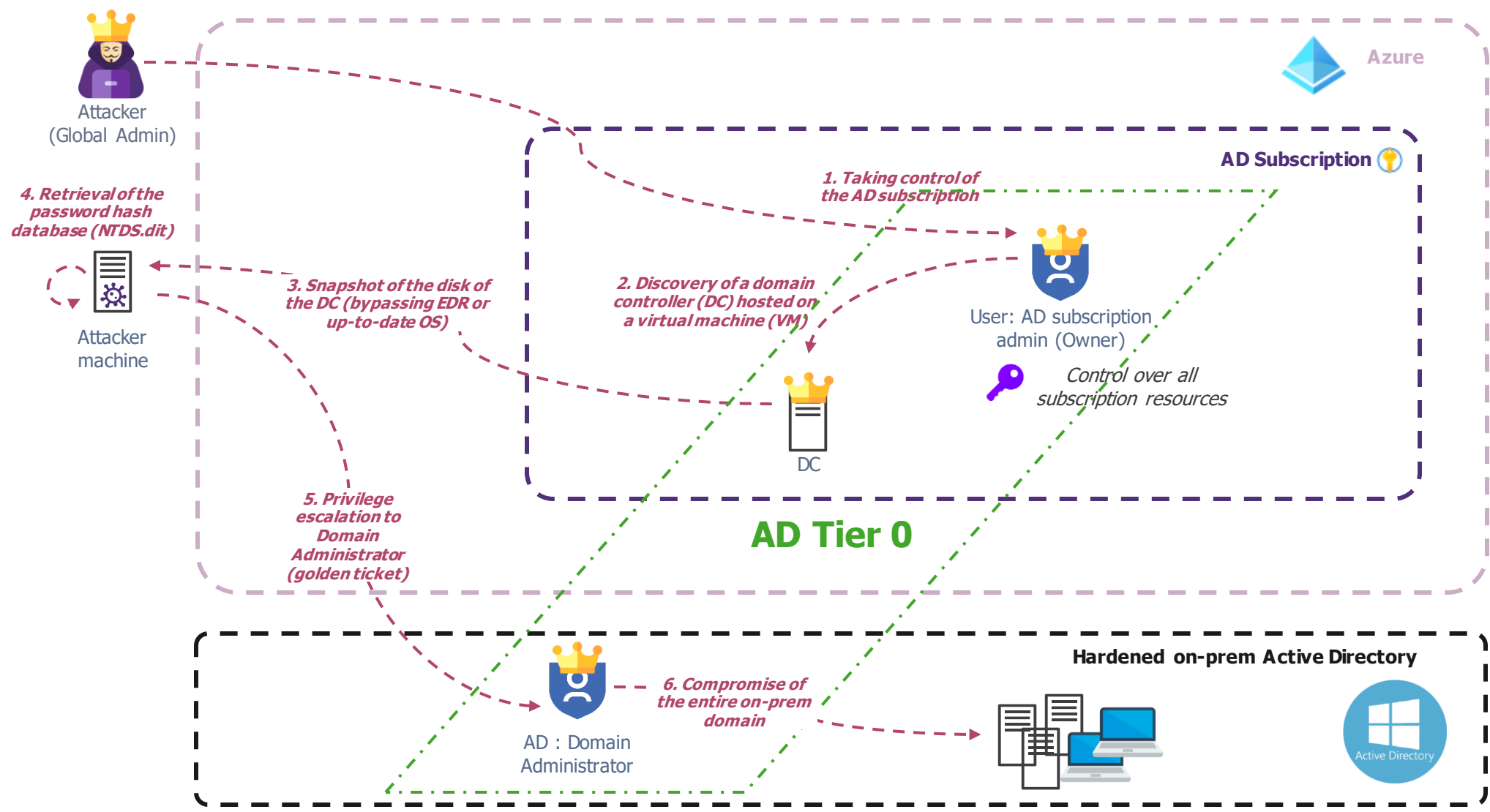
Conduct red team following the hypothesis of a compromised runner to map assets at risk

Wait a minute...


Don't we have a **Domain Controller**
in the **Cloud**?

Oh no...
Our well-secured AD...

Domain Controllers are also hosted in the Cloud for performance and availability



Where do we start our training path ?

- 
- 1 Define what is systemic for your infrastructure
 - 2 Assess your current risk with a security audit
 - 3 Define a roadmap to secure the assets most at risk
 - 4 Prepare for Cloud eraser scenarios

Don't think only of technical solutions

but also, organizational and process solutions



Questions ?

How do you feel about your Cloud administration now ?



Flash the QR
Code, *or* Go to
www.beekast.live
and enter the
code **492755**



*You have completed your first training to
fly to the moon!*

WAVESTONE

Etienne LAFORE
Senior Manager

M +33 (0)6 99 30 95 30
Etienne.Lafore@wavestone.com

Julien MAHIEU
Manager

M +33 (0)7 62 45 74 64
Julien.Mahieu@wavestone.com

Raymond CHAN
Senior Consultant

M +33 (0)6 65 64 38 23
Raymond.Chan@wavestone.com

Louis CLAVERO
Senior Consultant

M +33 (0)6 65 64 45 14
Louis.Clavero@wavestone.com

Christian CHEN
Consultant

M +33 (0)7 60 77 57 13
Christian.Chen@wavestone.com

Rémy UM
Consultant

M +33 (0)6 59 04 75 76
Remy.Um@wavestone.com

Théo RIAILLE
Consultant

M +33 (0)6 48 82 99 36
Theo.Riaille@wavestone.com

wavestone.com
@wavestone_