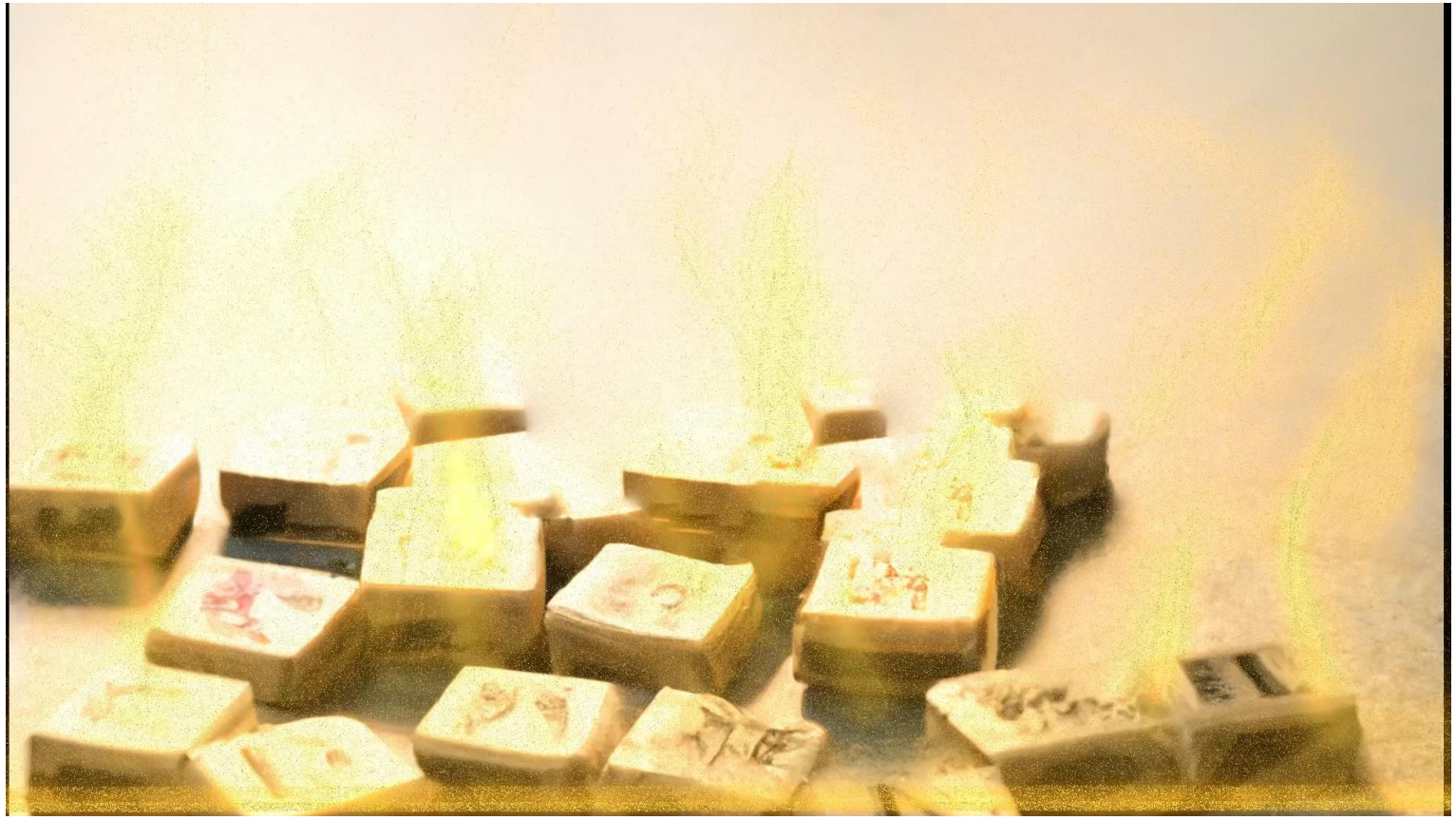
Risk Management

powered by VMWARE

Barbara Steiner
Sr. NSX Account Executive

ITAPA EVENT 2023

Riskmanagement



1st Step- Evalutation

What is “The Ring Of Power”

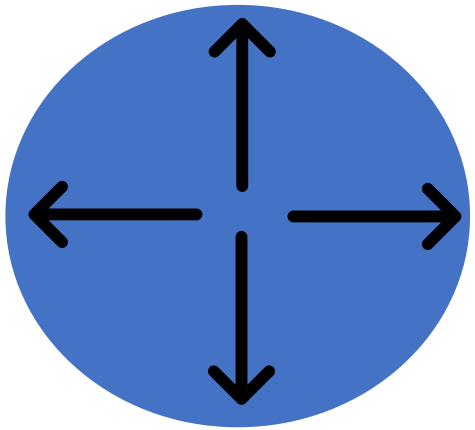
Where is ”The Ring Of Power”

Who needs access to it

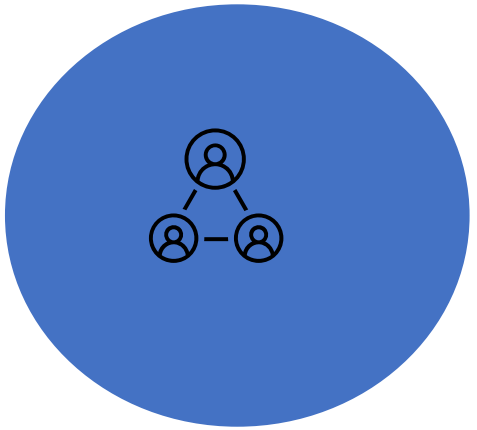
?

3rd Step– Building Security Policies

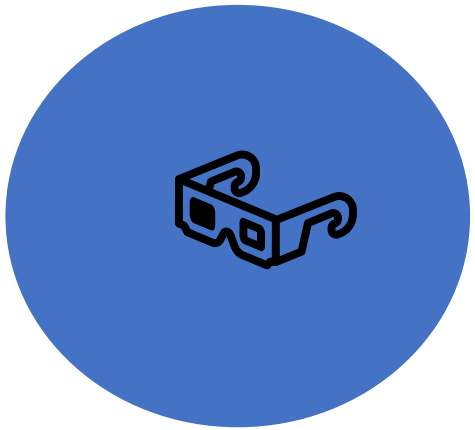
Focus on business outcomes



Desgin from the inside out



Determine who/what needs access



Inspect and log all traffic

4th Step: Implementation of the Rule Sets – but where und how?

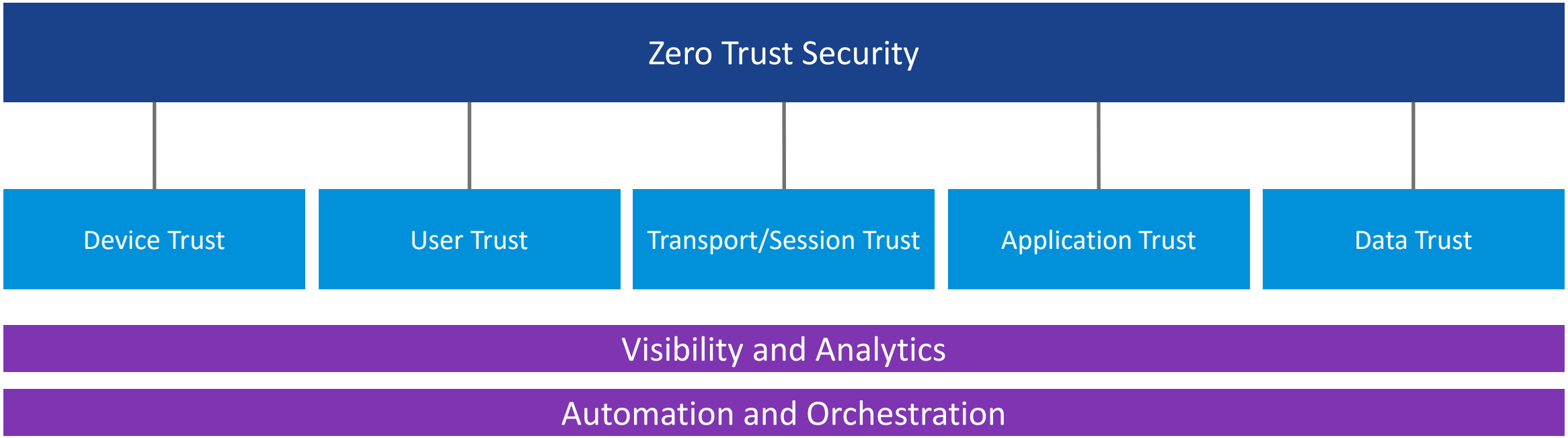
All pictures created with OPEN AI

Preparation

- Create User Awareness in all Departements
- Regular Security Trainings
- Policies about Usage of company owned IT
- Contentfiltering in regards to Usergroups (eg. Young employees etc.)
- Provide secure connections to services (eg Internetbanking for private use)

Zero Trust Security

Multiple layers of trust to be constantly/frequently verified



Device Trust

What devices are our users utilizing?

Are we controlling these devices?

Pic geneated with OPEN AI

User Trust

Are you the person I think you are?

Are you really allowed to do this?

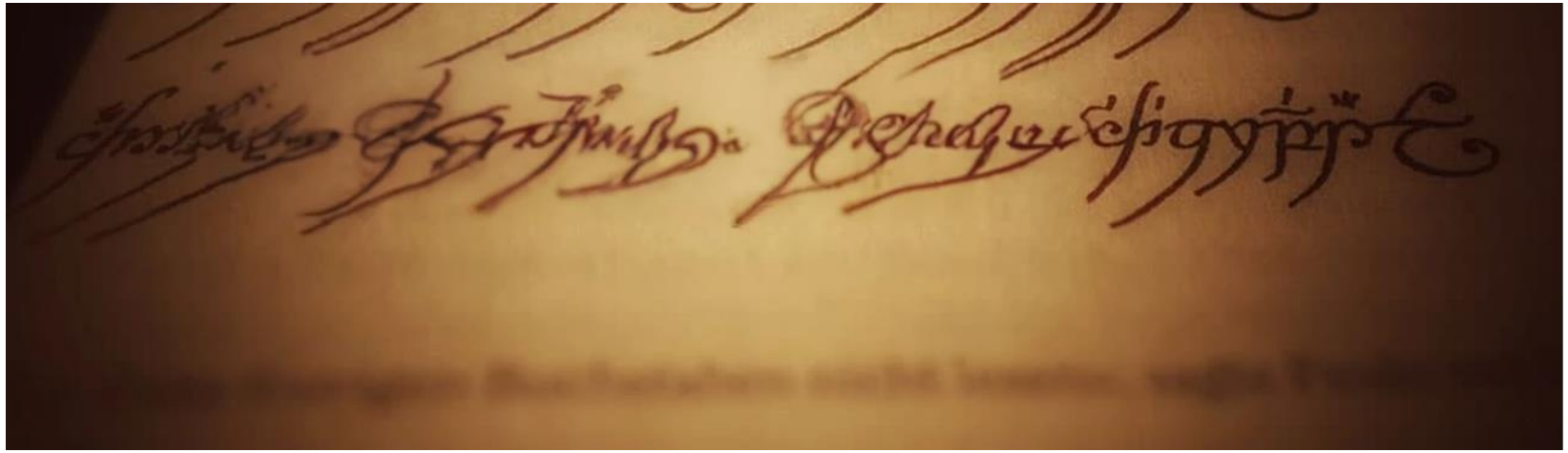
Pic generated with OPEN AI

Transport/ Session Trust

Do I really see everything I need to see?

Application Trust

Data Protection



Can I still trust my data? Also after an attack?

Schritt 5 – Manage & Control

Visibility and Analytics, Automation and Orchestration

Manage

- embedding Policies
- Security as part of the infrastructure
- Identification of new Workloads
- Get transparency

Control

- Evaluation of the Logfiles through SIEM
- Deep Paket Inspection to control traffic in the Datacenter
- Supervision of compliance regarding Security Policies and company guidelines
- Policy Enforcement via East-West Security (Microsegmentation) in the Datacenter

How VMware helps you achieve Zero Trust

Visibility and Analytics, Automation and Orchestration