TRUESEC

Backup/Restore/Recover

-That works in today's cybersecurity landscape

Mikael.Nystrom @truesec.se

> *"A data backup is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss. Data loss can be caused by many things ranging from computer viruses to hardware failures to file corruption to fire, flood, or theft (etc)."*

Is there a difference between Backup/Restore and Backup/Recovery?

TRUESEC

Your backup is the last line of defence...

Restore and Recover is the first thing that needs to work, otherwise backup is useless

- Time to restore
- Storage Capacity
- Protect the backup
- Worst case scenario

Worst case scenario

- All data needs to be restored
- The existing infrastructure is encrypted
- There are no documents that describe the process
- There is nothing at all

- *And you need to have it up and running within 24 hours…*

Time to restore

- Where is the data?
- How fast is the solution to GET the data
- How fast is the solution to WRITE the data

- *If it takes 23 hours to backup the data, does it mean it takes 23 hours to restore it?*

Capacity

- You need to keep everything you have; they need to find Patient Zero
- You suddenly need the same amount of that that you are currently using
- You might need to get a new SAN
- You might need to get a few servers, like 20-100

- *...before you can start restoring...*

Protection

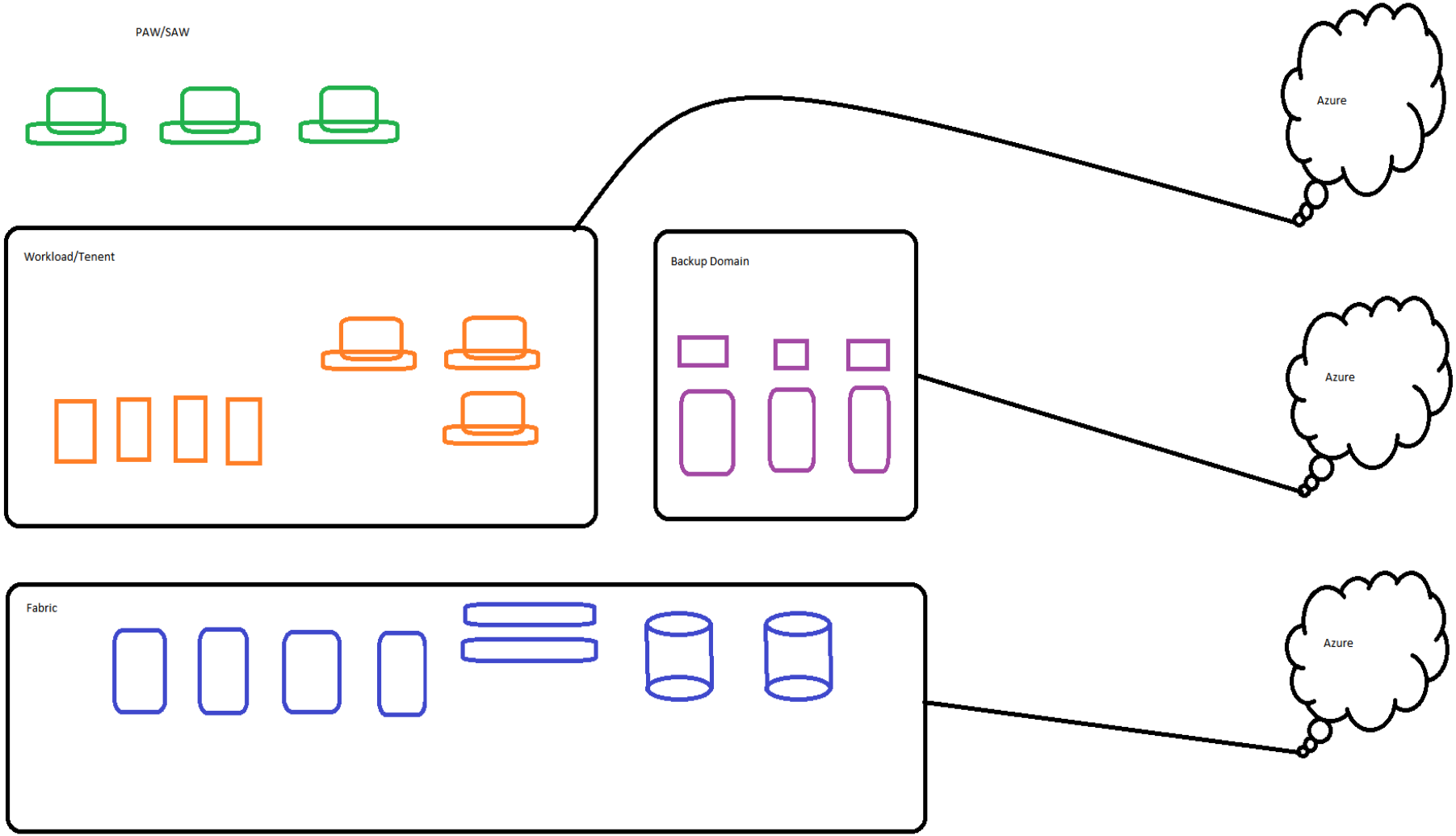
- Hackers are extremely good at
  - Knowing more about backup solutions than you do
  - Backtracking the trails of the backup solution
  - Making sure that whatever you had is wiped before launching the strike
  - Making sure they have all the nice things in the backup so that they can publish it globally

Protection

- Isolated
- Encrypted
- One-way (Diode)
- Separate authentication
- Dedicated storage
- Monitored
- Offsite

What would be the safe way to protect my admin account?

- Never use it, or…
- Use PAW / SAW
- Use Tiering
- Think before you use it
  - I'm I storing this now?
  - Can someone steel the hash?
  - Is this really secure?
  - Why does the dialog box ask for my credentials?


PAW/SAW
Azure
Workload/Tenent
Backup Domain
Azure
Fabric
Azure

Thank you

 www.truesec.com

 x.com/truesec

 linkedin.com/company/truesec