I am the VIP

Global Azure Meetup #Bergen

Bluescreen Brothers edition

SparebankenVest

Fortytwo.io

WE ARE FORTYTWO

We solve our customers challenges. Problems. We are the solution. We are technology. Using the best tools, we ensure that our customers can rely on their operations, safely, securely, in the cloud.

We`re not just experts

We're like the cosmic hitchhikers of the cloud. Our squad, versed in DevOps, Cloud Native, Security, and beyond, is on a mission to turn challenges into victories across the galaxy.

We`re not just building cloud solutions

We're navigating the cosmic waves of innovation. Step into our realm, where the solutions we craft in the Microsoft Cloud ecosystem are as robust as they are out-of-this-world.

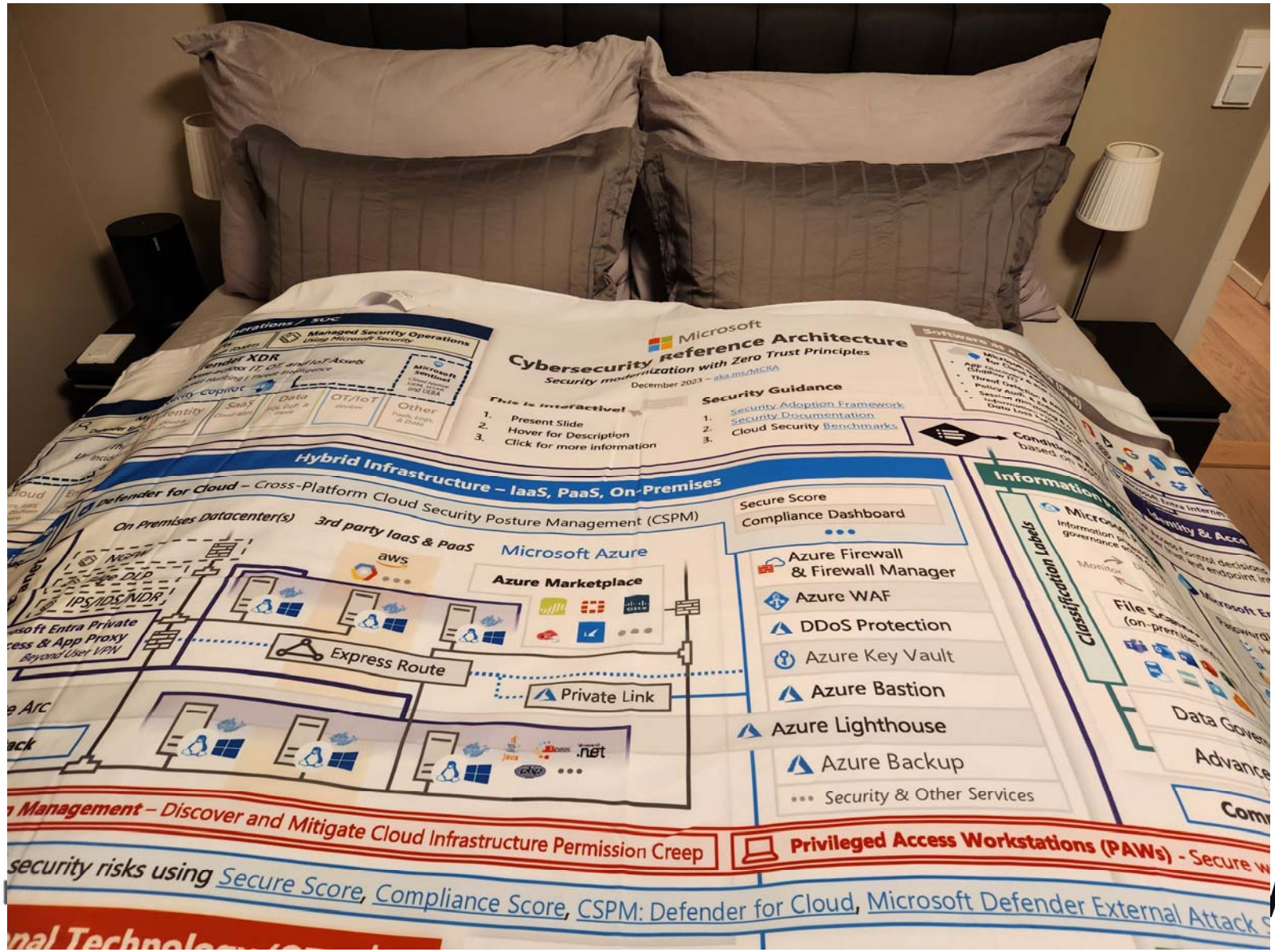
We`re not your ordinary service provider

We're intergalactic partners in your journey to success. Dive into collaboration, and unlock a galaxy of expertise to navigate the cloud with unwavering confidence.

Fortytwo.io

The VIP experience!

Fortytwo.io


Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2023 – aka.ms/MCRA
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1. Security Adoption Framework
2. Security Documentation
3. Cloud Security Benchmarks
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
Azure Marketplace
Express Route
Private Link
Secure Score
Compliance Dashboard
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Classification Labels
Privileged Access Workstations (PAWs) - Secure
security risks using Secure Score, Compliance Score, CSPM: Defender for Cloud, Microsoft Defender External Attack

TLA’s

DNS
JIT
JEA
LOL

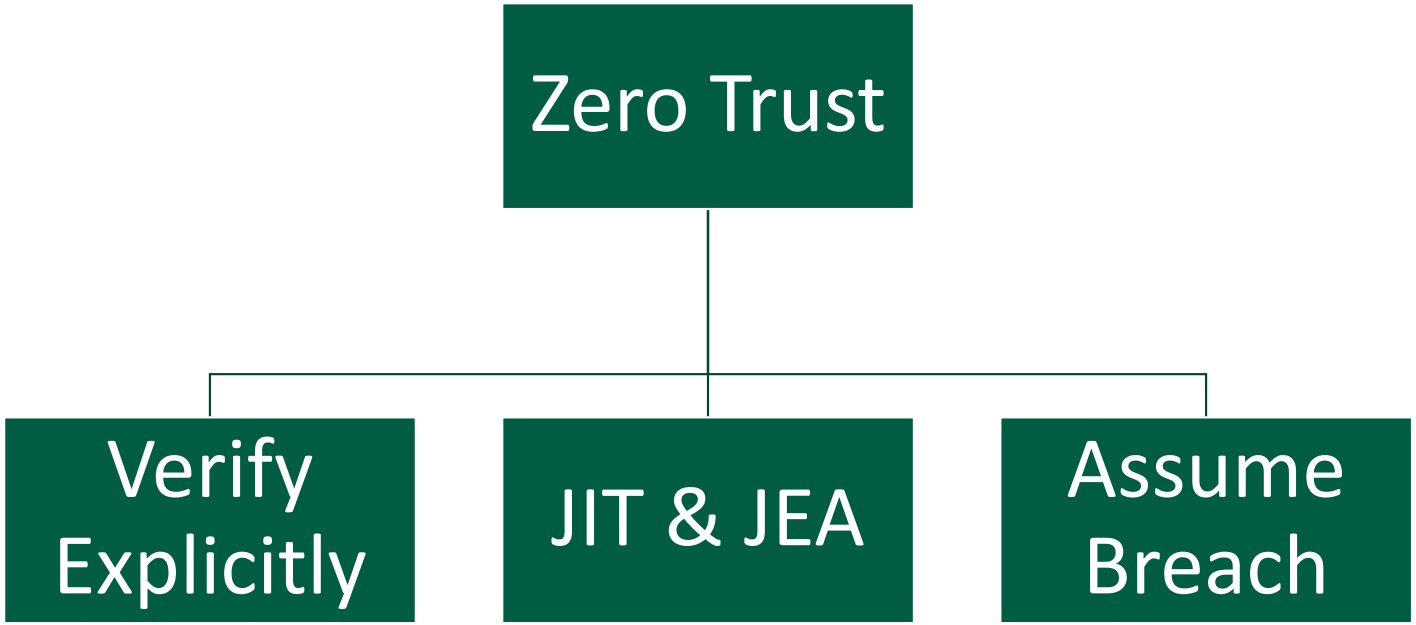
Being geeks, we quickly realized that the problem with TLAs is that there are only 17,576 unique TLAs in a 26-letter alphabet

SOAP
ISDN
ADSL
ROFL

(…)In a 1998 newsletter article, I declared them to be FLAPs. This stands for four-Letter Acronym package, and of course, FLAP itself is a FLAP

Microsoft have used them all up the summer before last.

ZT, VE, JIT, JEA & AB går inn i en bar



SparebankenVest

Fortytwo.io

Who are you?

SparebankenVest

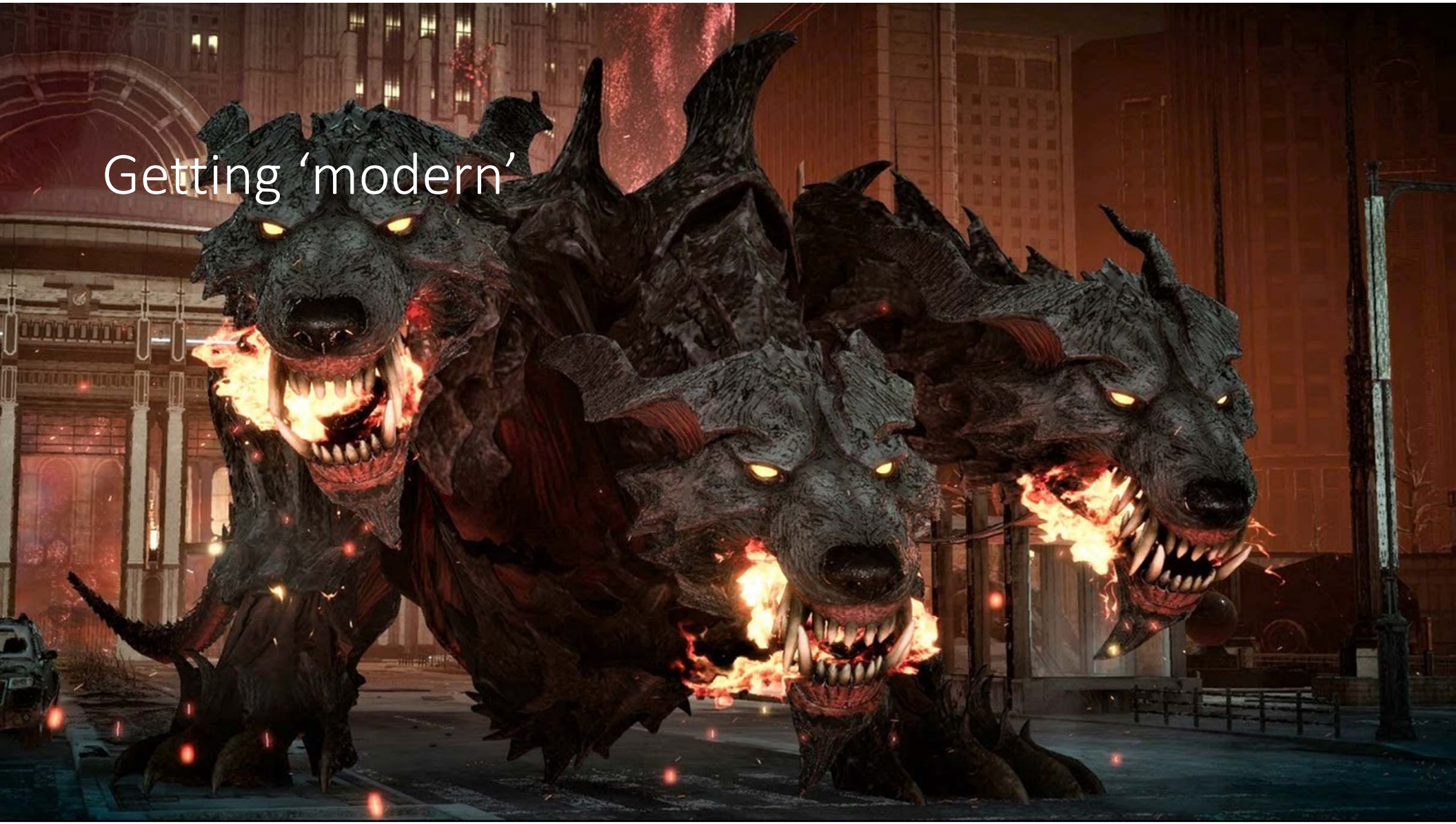
Fortytwo.io

What are you accessing?

SparebankenVest

Fortytwo.io

Getting ‘modern’



Customized or Built-in, spiller det noen rolle(r)?

99

529

SparebankenVest

Fortytwo.io

Azure Resources – Default Owner


```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.",
  "id": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
  "name": "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
  "permissions": [
    {
      "actions": [
        "*"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "roleName": "Owner",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```


SparebankenVest

Fortytwo.io

Azure Resources – Default Contributor


```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Grants full access to manage all resources,but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.",
  "id": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
  "name": "b24988ac-6180-42a0-ab88-20f7382dd24c",
  "permissions": [
    {
      "actions": [
        "*"
      ],
      "notActions": [
        "Microsoft.Authorization/*/Delete",
        "Microsoft.Authorization/*/Write",
        "Microsoft.Authorization/elevateAccess/Action",
        "Microsoft.Blueprint/blueprintAssignments/write",
        "Microsoft.Blueprint/blueprintAssignments/delete",
        "Microsoft.Compute/galleries/share/action",
        "Microsoft.Purview/consents/write",
        "Microsoft.Purview/consents/delete"
      ],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "roleName": "Contributor",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```


Fortytwo.io

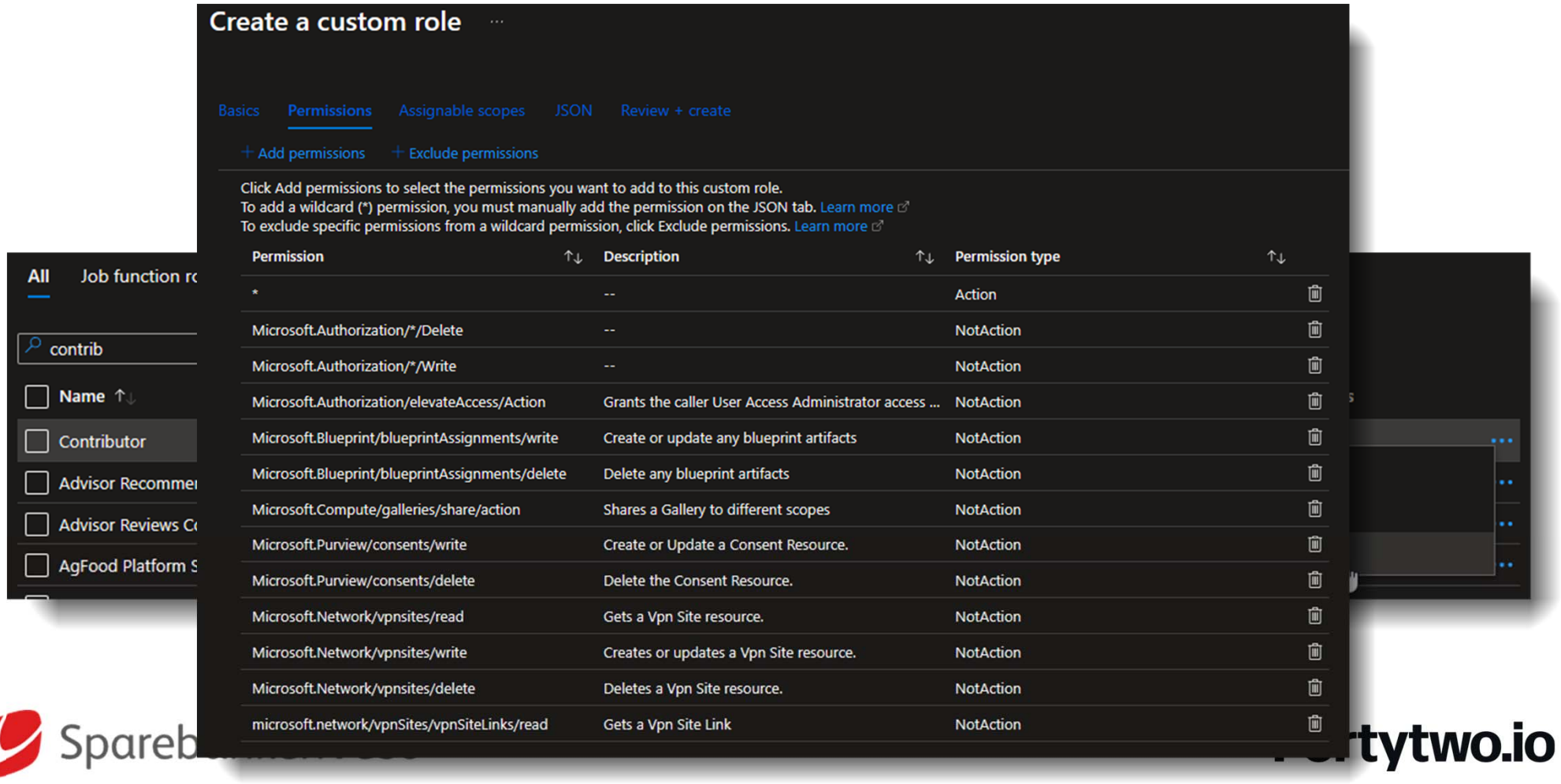
notActions

```
"notActions": [
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/vpnGateways/*",
                "Microsoft.Network/azurefirewalls/*",
                "Microsoft.Network/expressRouteCircuits/*",
                "Microsoft.Network/routeTables/write",
                "Microsoft.Network/routeTables/delete",
                "Microsoft.Network/routeTables/routes/write",
                "Microsoft.Network/routeTables/routes/delete",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete",
                "Microsoft.Network/vpnSites/*“
                ],
```

SparebankenVest

Fortytwo.io

Customizing the Portal way



Spareb rtytwo.io

The missing 

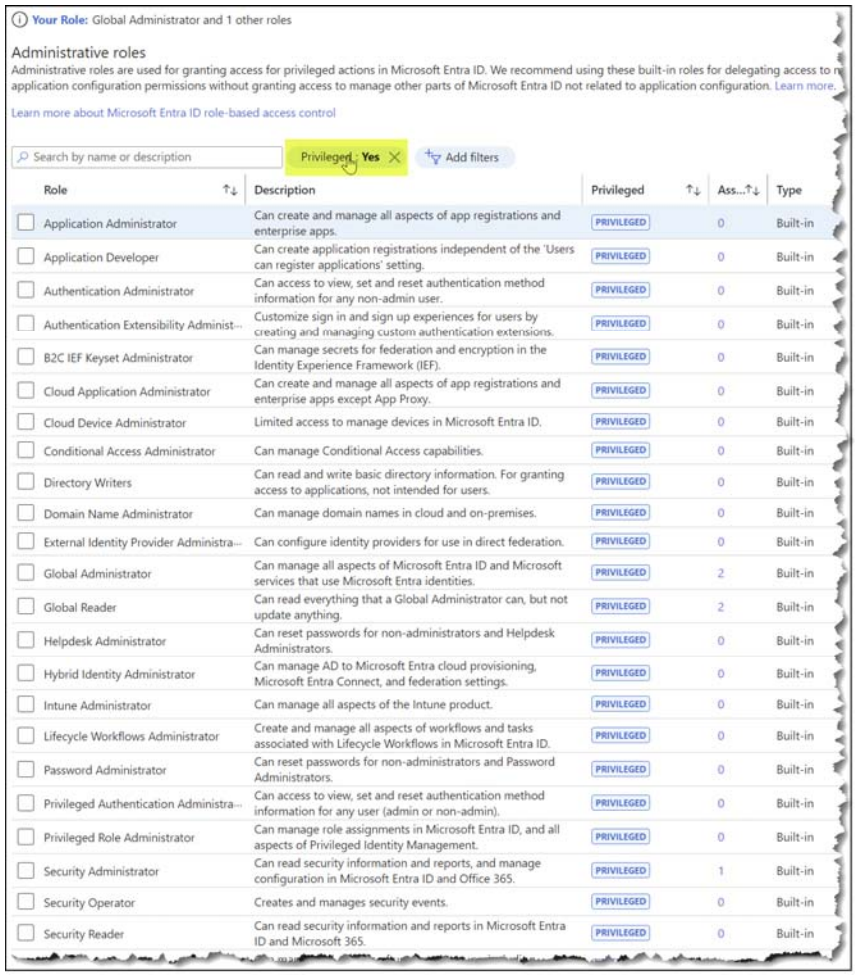

```
Get-AzRoleDefinition Contributor | ConvertTo-Json

New-AzRoleDefinition -InputFile "C:\CustomRoles\Contributor-NoNetwork.json"
```

https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles

SparebankenVest

Fortytwo.io

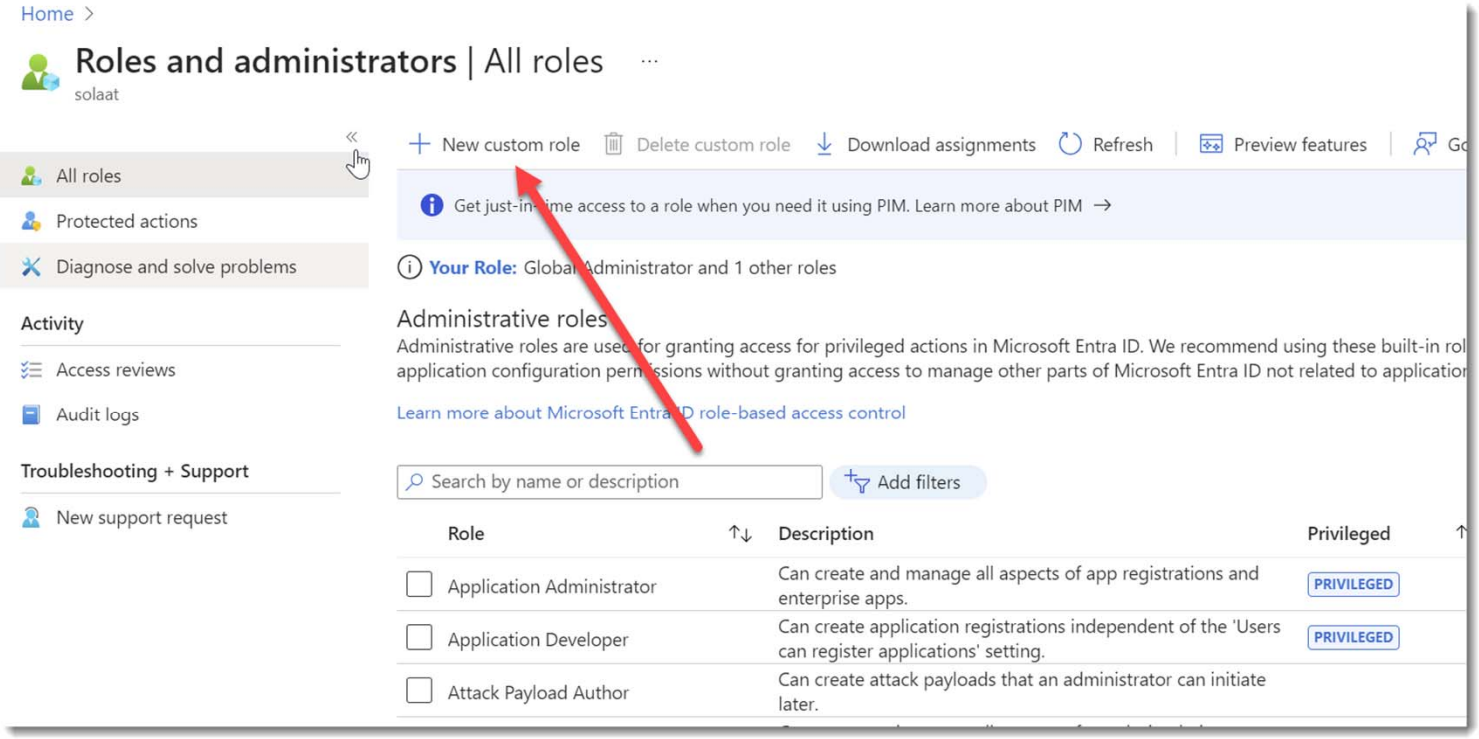
What about Entra ID?



SparebankenVest

Fortytwo.io

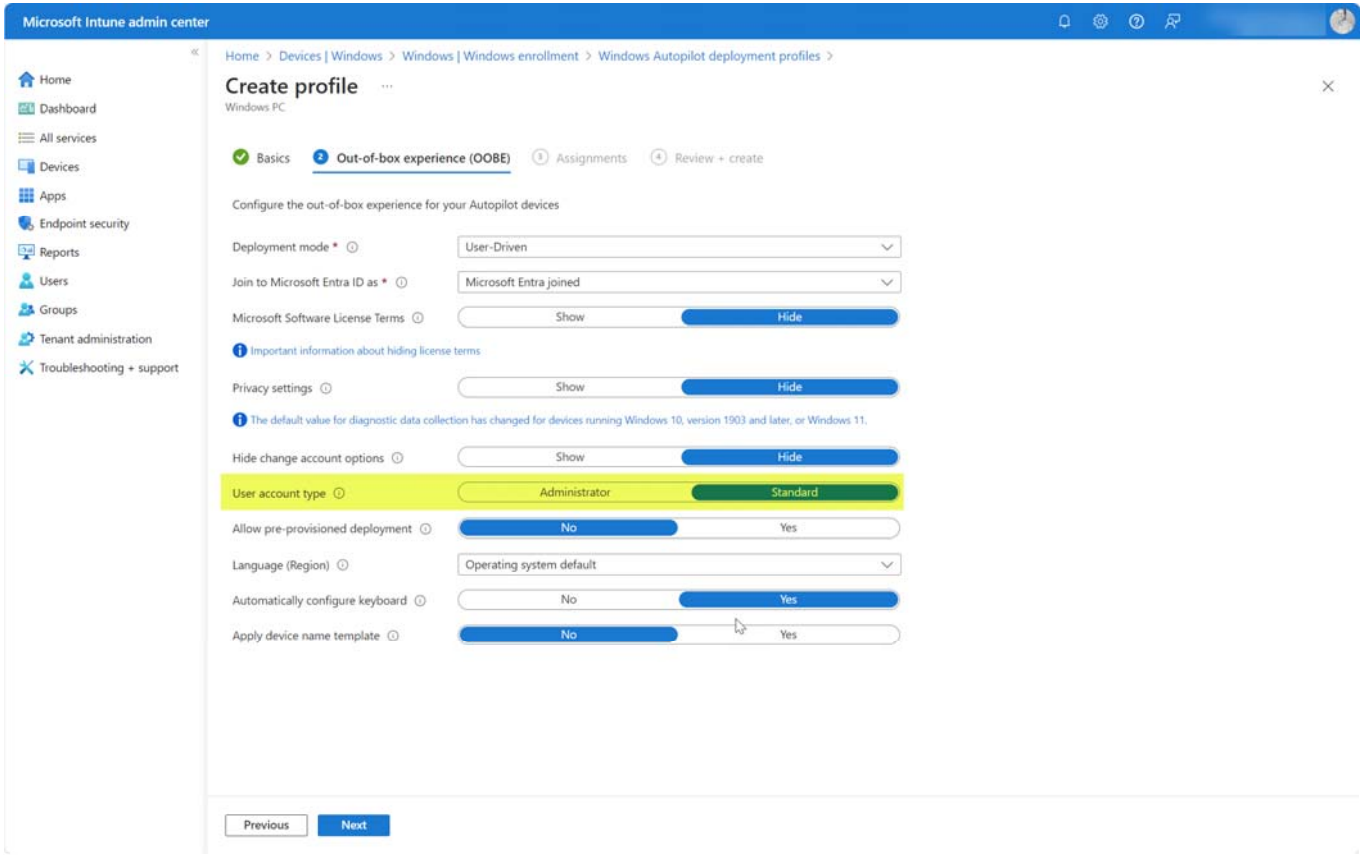
Customize?



SparebankenVest

Fortytwo.io

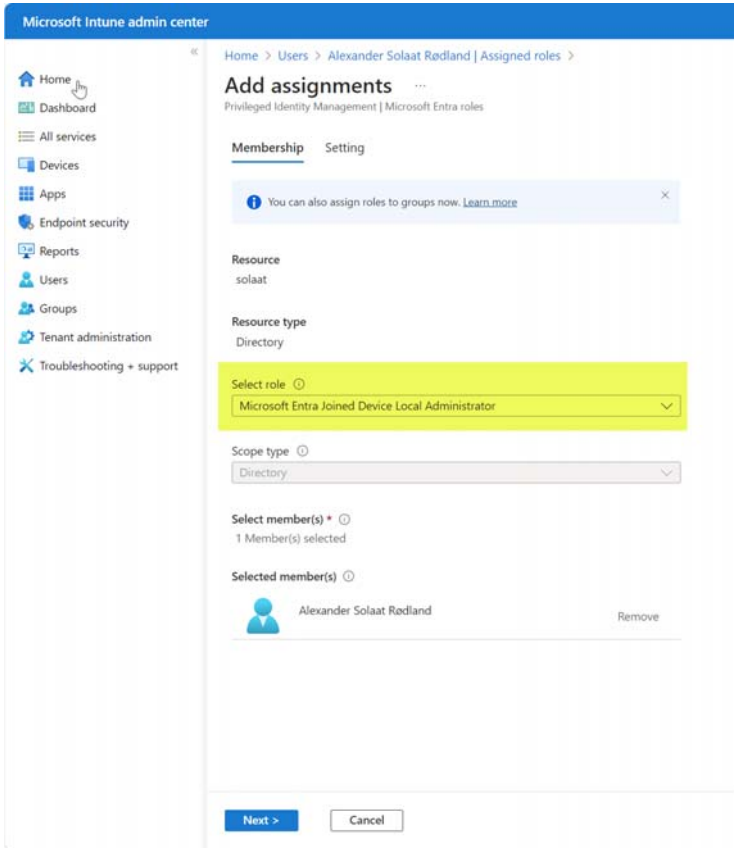
Non-local admin?



SparebankenVest

Fortytwo.io

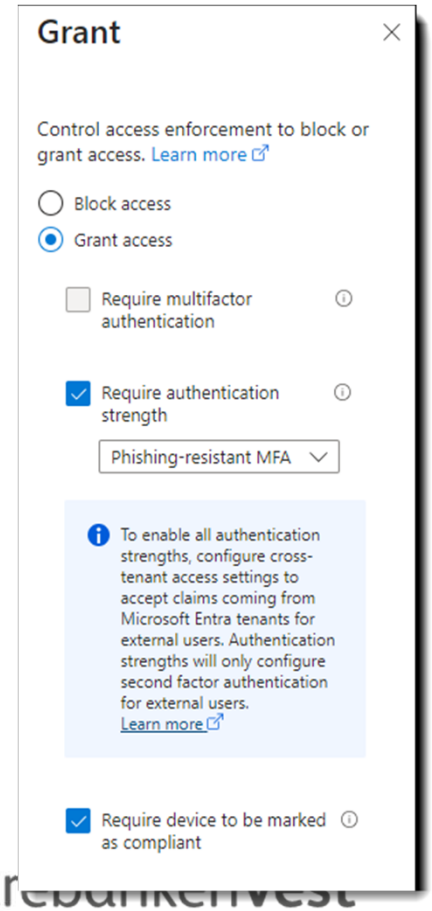
Limitations?

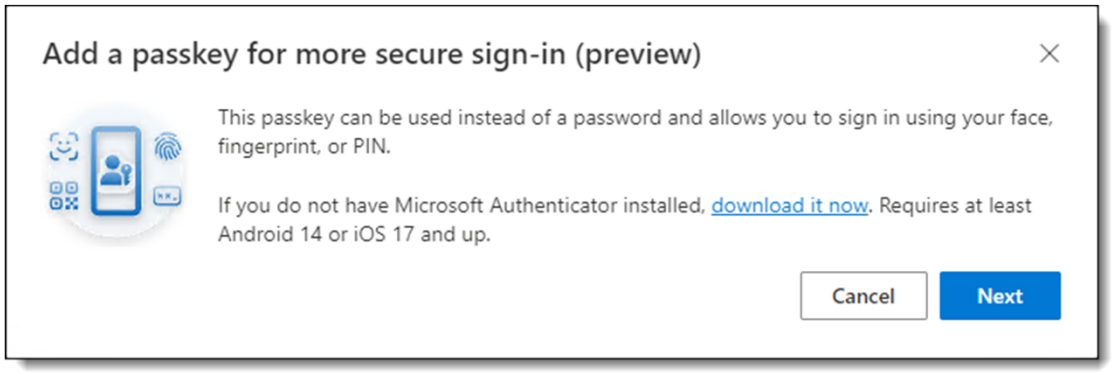


SparebankenVest

Fortytwo.io

Protected actions / Conditional Access

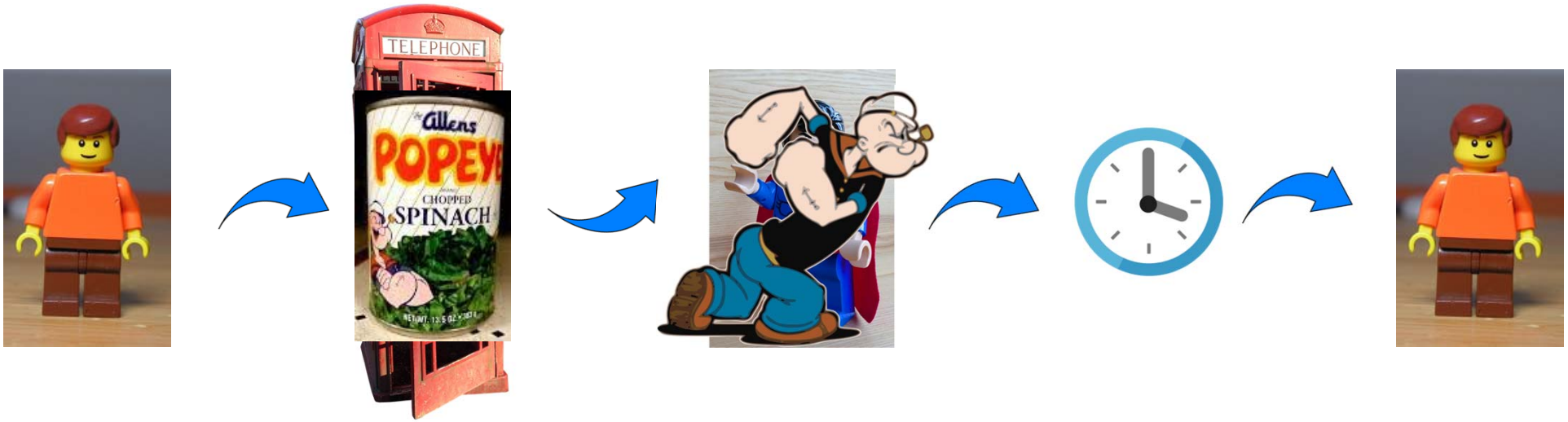




Sparebankenvest

Fortytwo.io

JIT What?

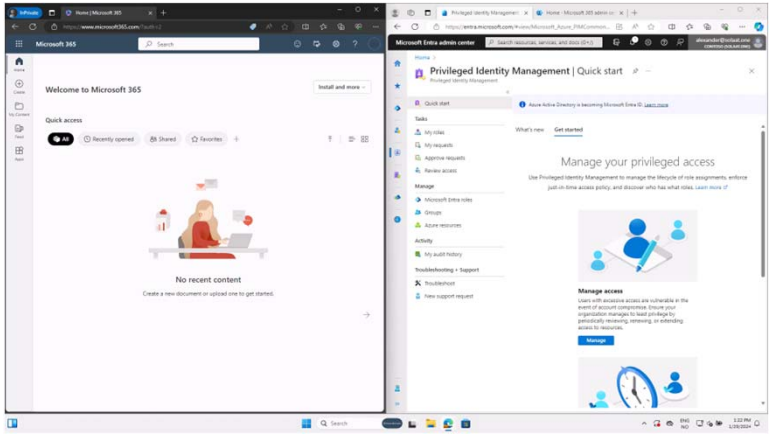


SparebankenVest

Fortytwo.io

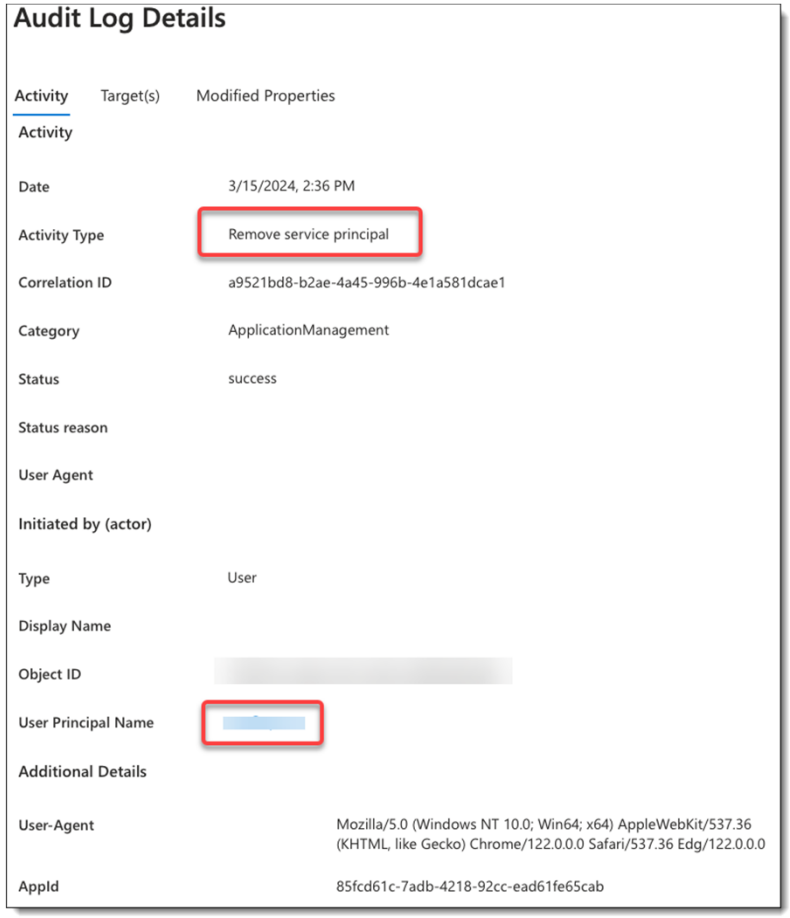
JIT & JEA fundamentals

DEMO TIME



SparebankenVest

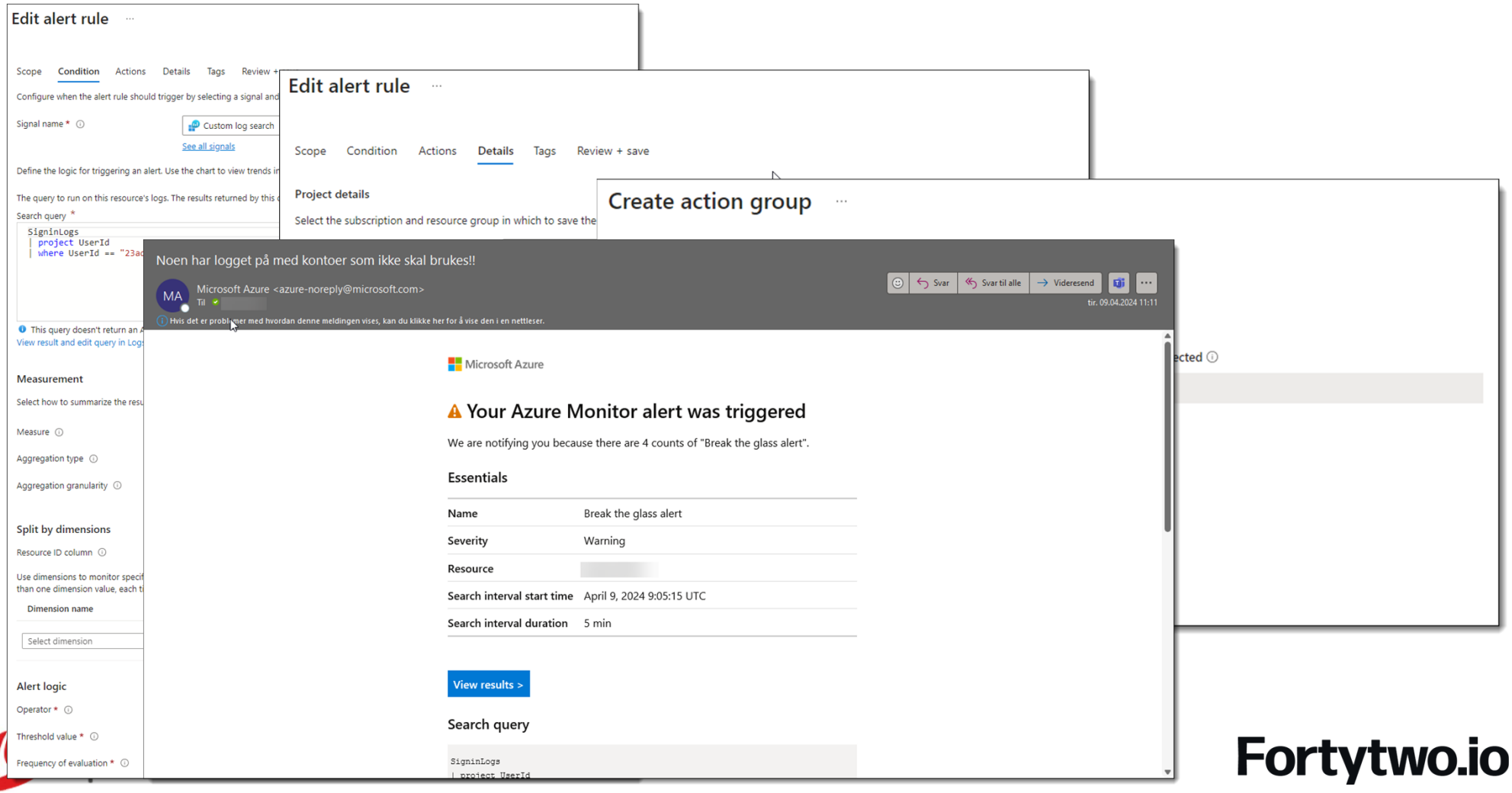
Fortytwo.io



SparebankenVest

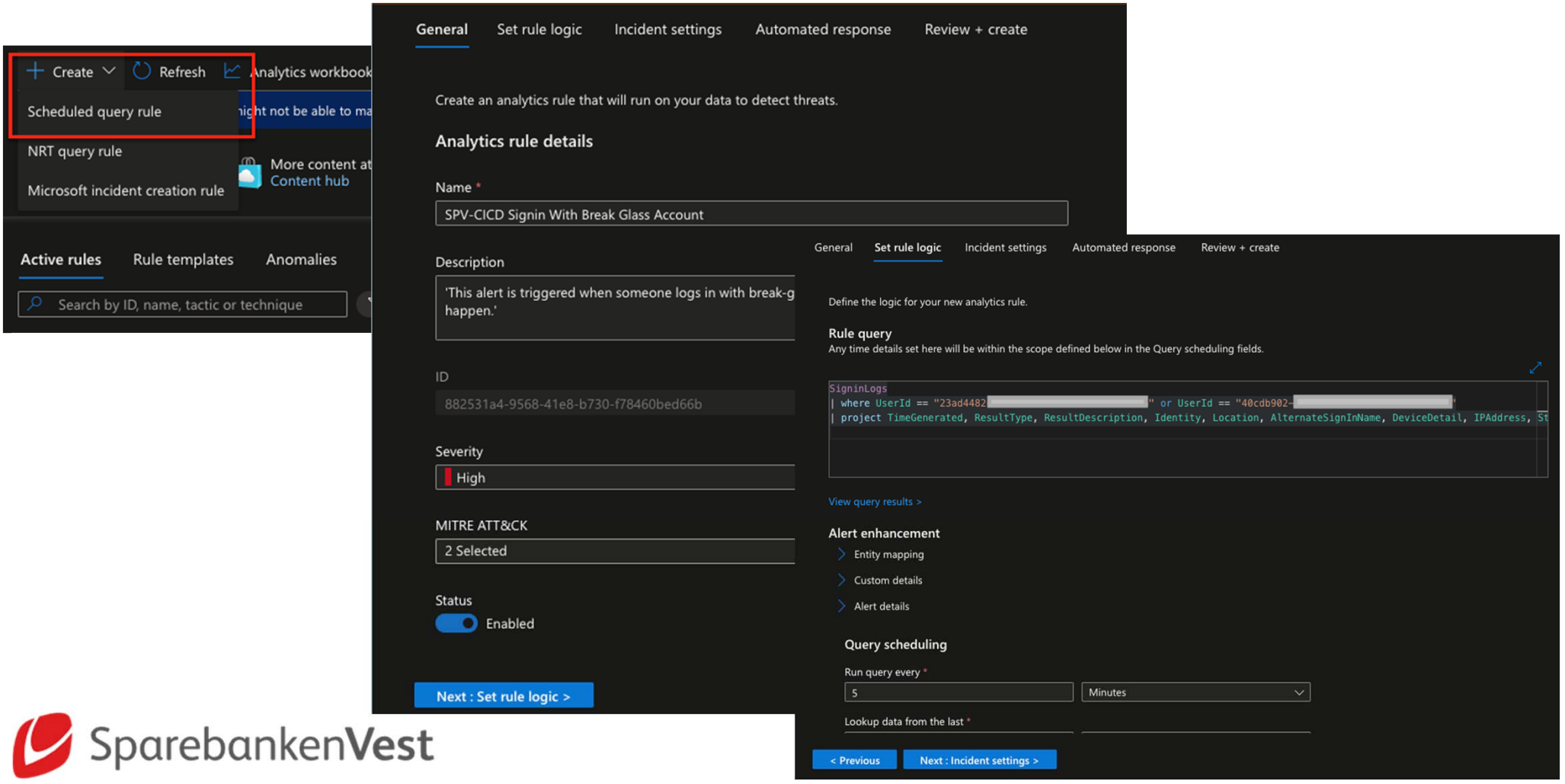
Fortytwo.io

Account monitorering (VIPs / BGA)



Fortytwo.io

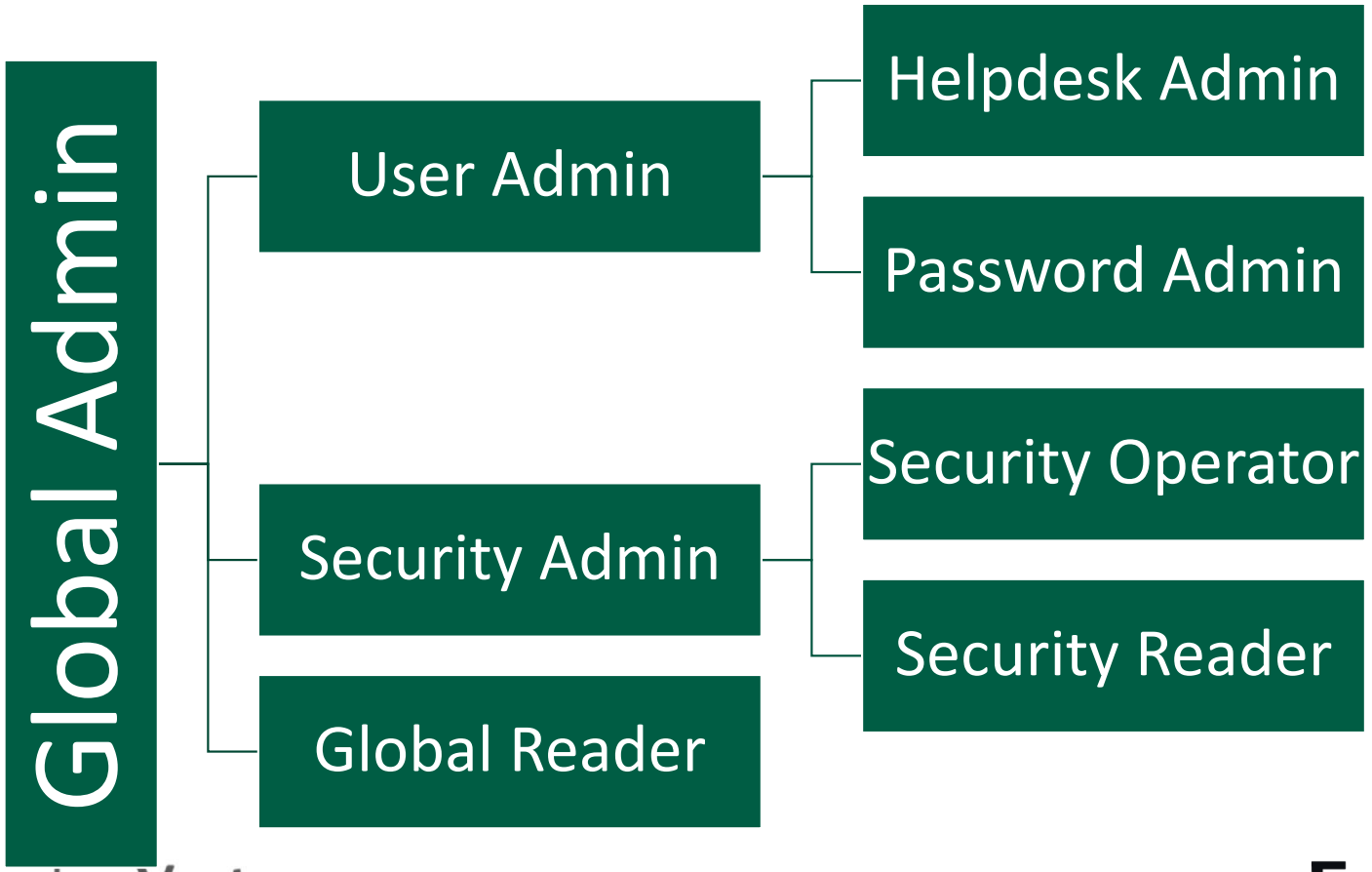
Account monitorering (VIPs / BGA)



SparebankenVest

Too many cooks?

Knowing the many layers of ~~JEA~~ M365- rights



SparebankenVest

Fortytwo.io

Customized or Built-in, spiller det noen rolle(r)?

99

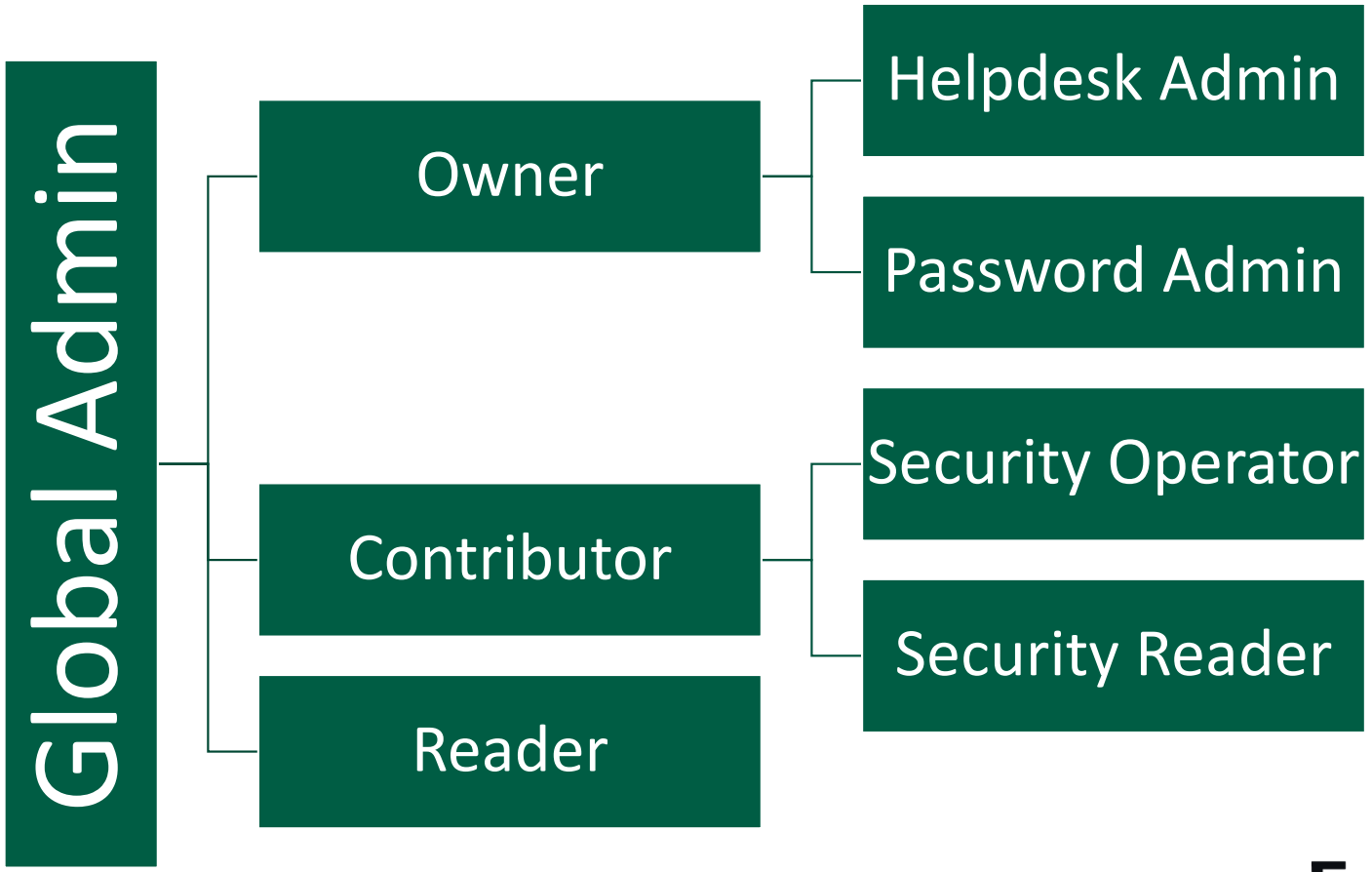
529

SparebankenVest

Fortytwo.io

Too many cooks?

Knowing the many layers of ~~JEA~~ Azure rights



Fortytwo.io

Alexander Solaat Rødland
Principal Cloud Engineer @ Fortytwo

- alexander@solaat.no
- youtube.com/@bluescreenbrothers
- /in/alexsolaat

Microsoft Most Valuable Professional

SparebankenVest

Fortytwo.io

Olav Tvedt
Cloud dude @ Sparebanken Vest

- olav@tvedt.info
- youtube.com/@bluescreenbrothers
- /in/otvedt

Microsoft Most Valuable Professional

SparebankenVest

Fortytwo.io

The BluesScreen Brothers

https://www.youtube.com/@bluescreenbrothers

https://www.linkedin.com/company/blaskjerm-brodrene

https://shows.acast.com/blaskjerm

SparebankenVest

Fortytwo.io