

Myths of Modern Management

@pl4nty // tplant.com.au

Sponsors



```
C:\> whoami
```

```
product @ Devicie
```

```
clouds, endpoints, security
```

```
open-source, fancy keyboards
```



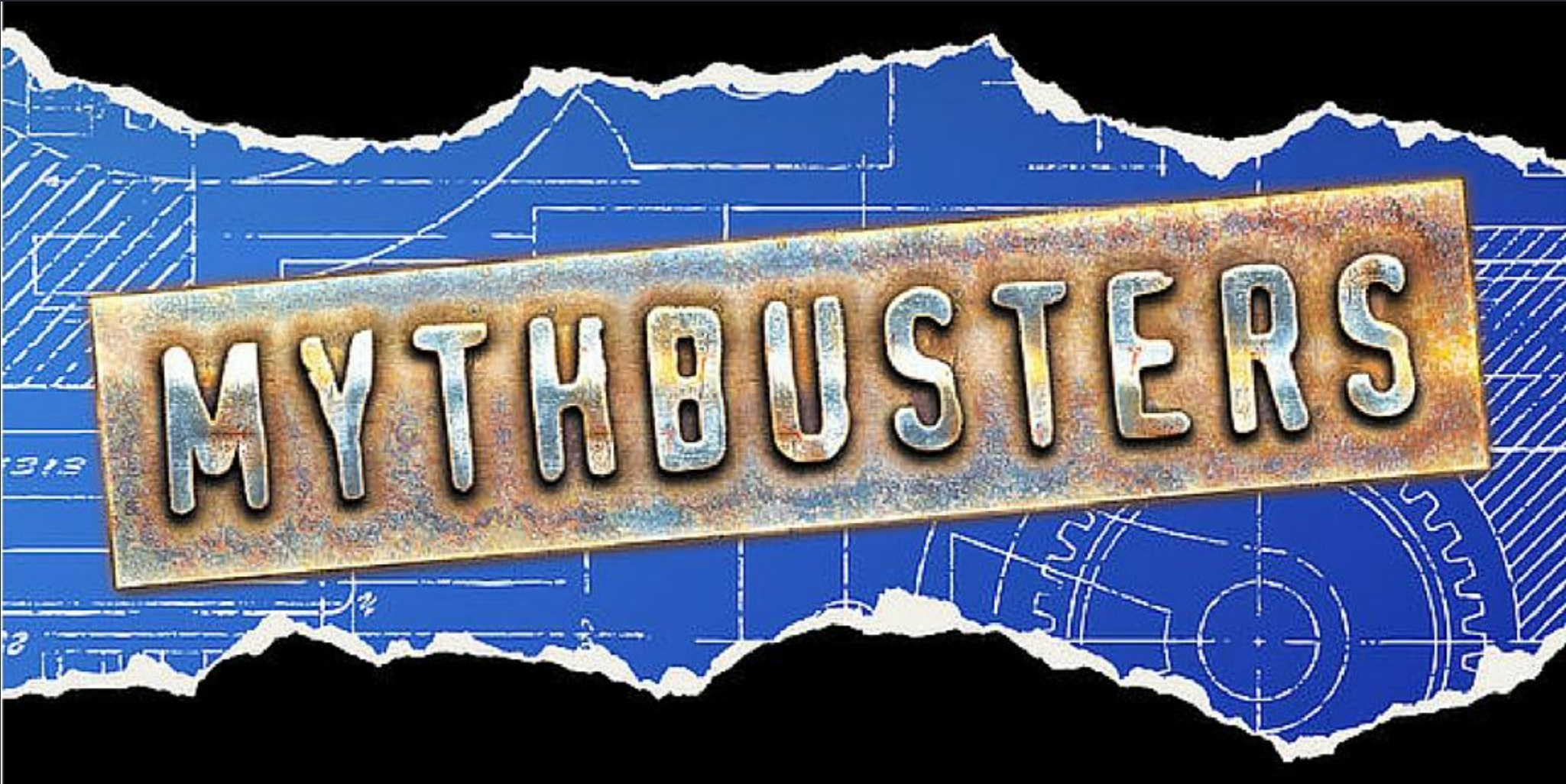
a mythical agenda

trusting Intune – what's under the hood?

on-premises auth in a cloud-native world

filling the gaps in Intune



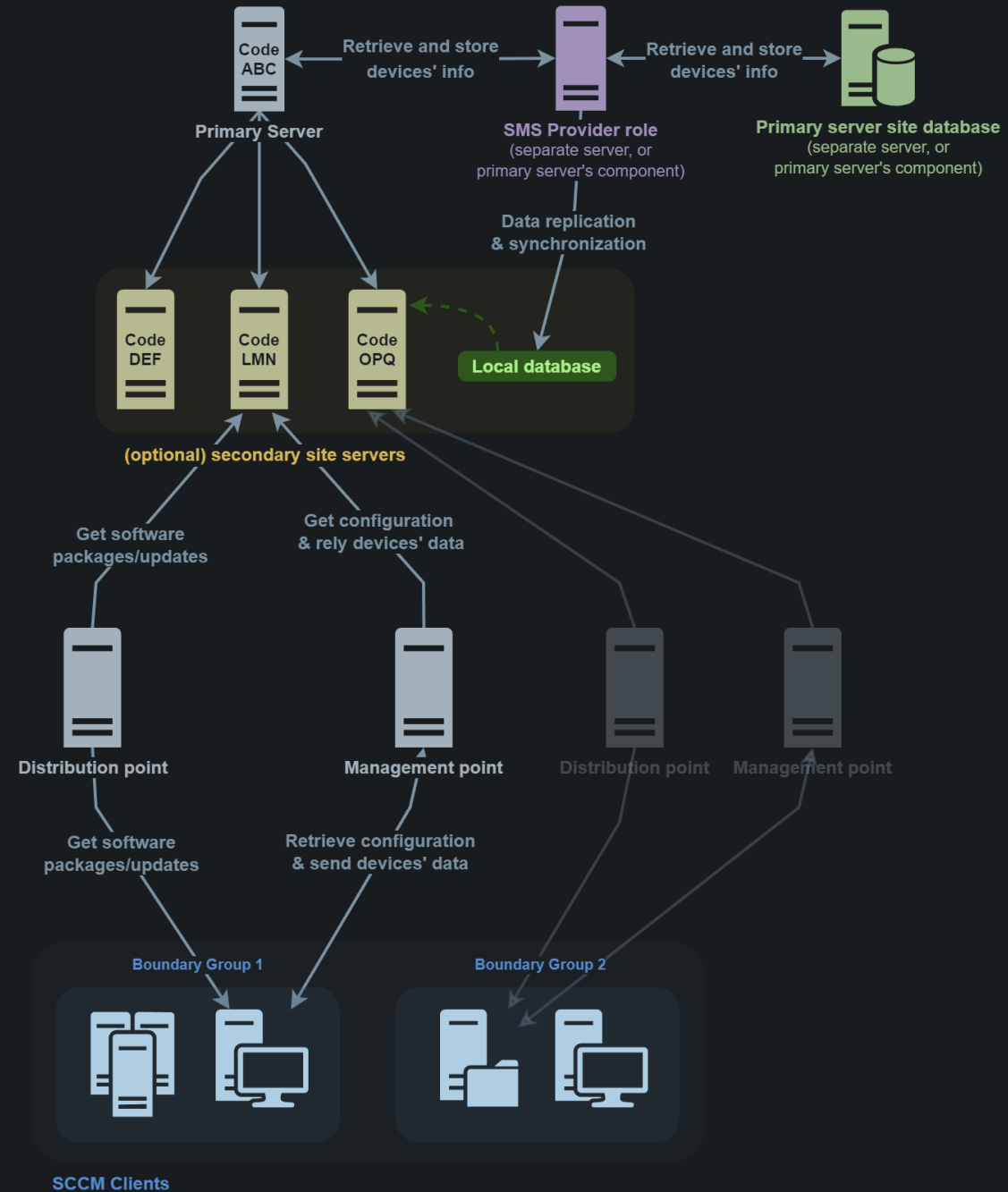


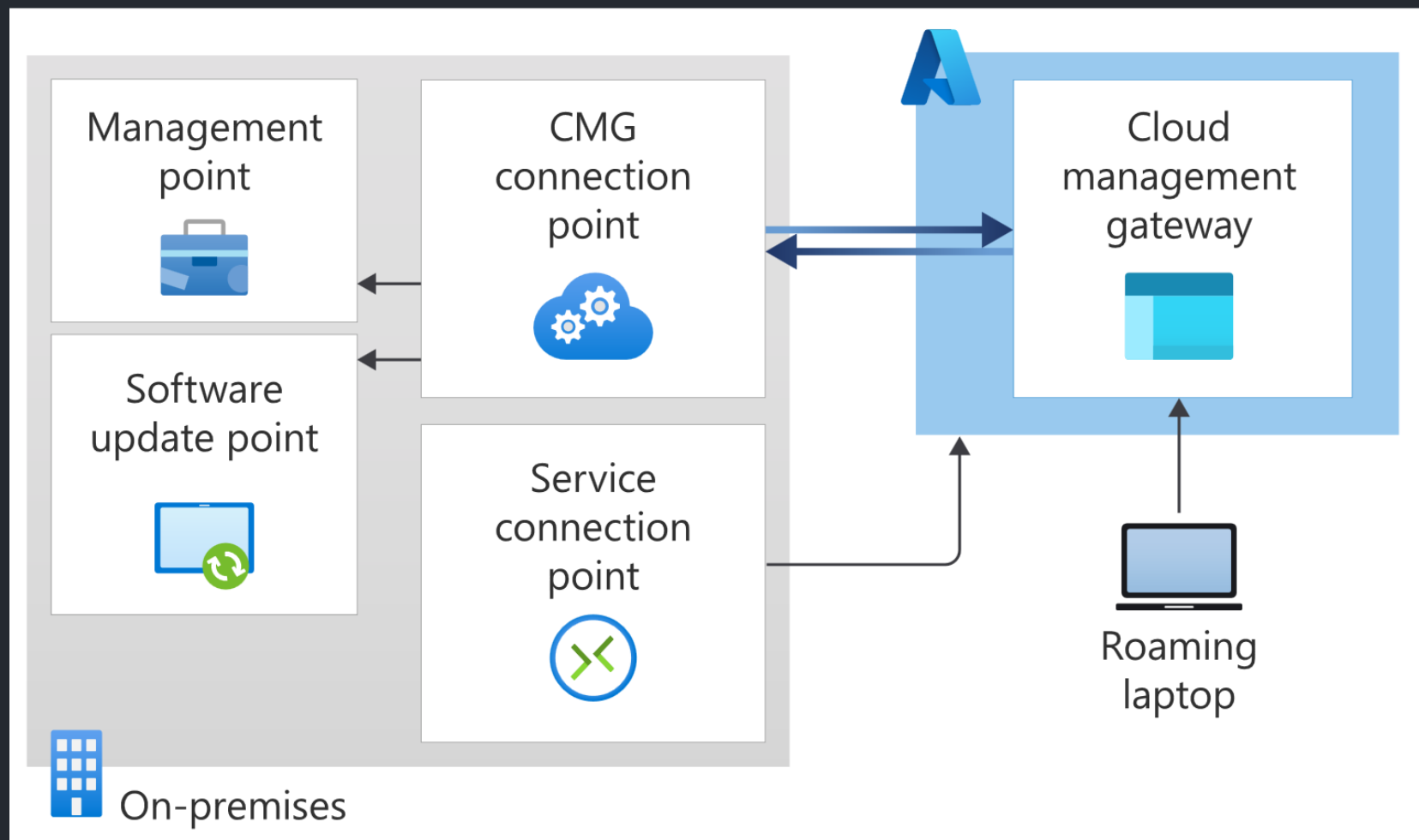
trust

agent-first

self-hosted

limited roaming






(zero-)trust

how to understand, let alone troubleshoot?








still runs in a datacenter


 **Tenant admin | Tenant status** ...

× «

 **Tenant status**

 Remote Help

 Microsoft Tunnel Gateway

 Cloud PKI

Tenant details

Tenant name

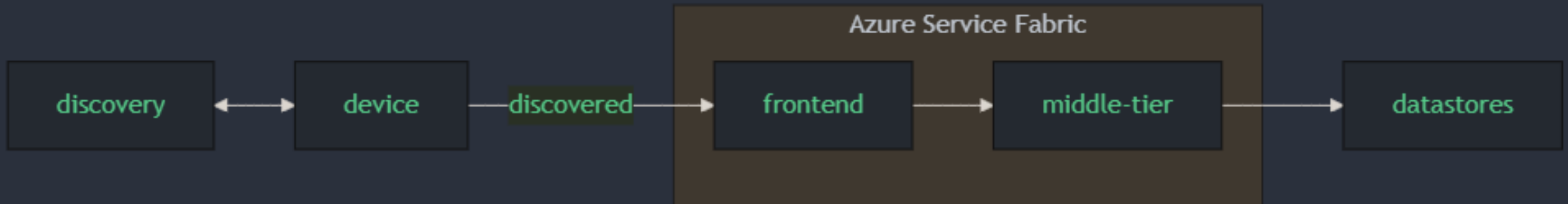
Tenant location
Australia 0101

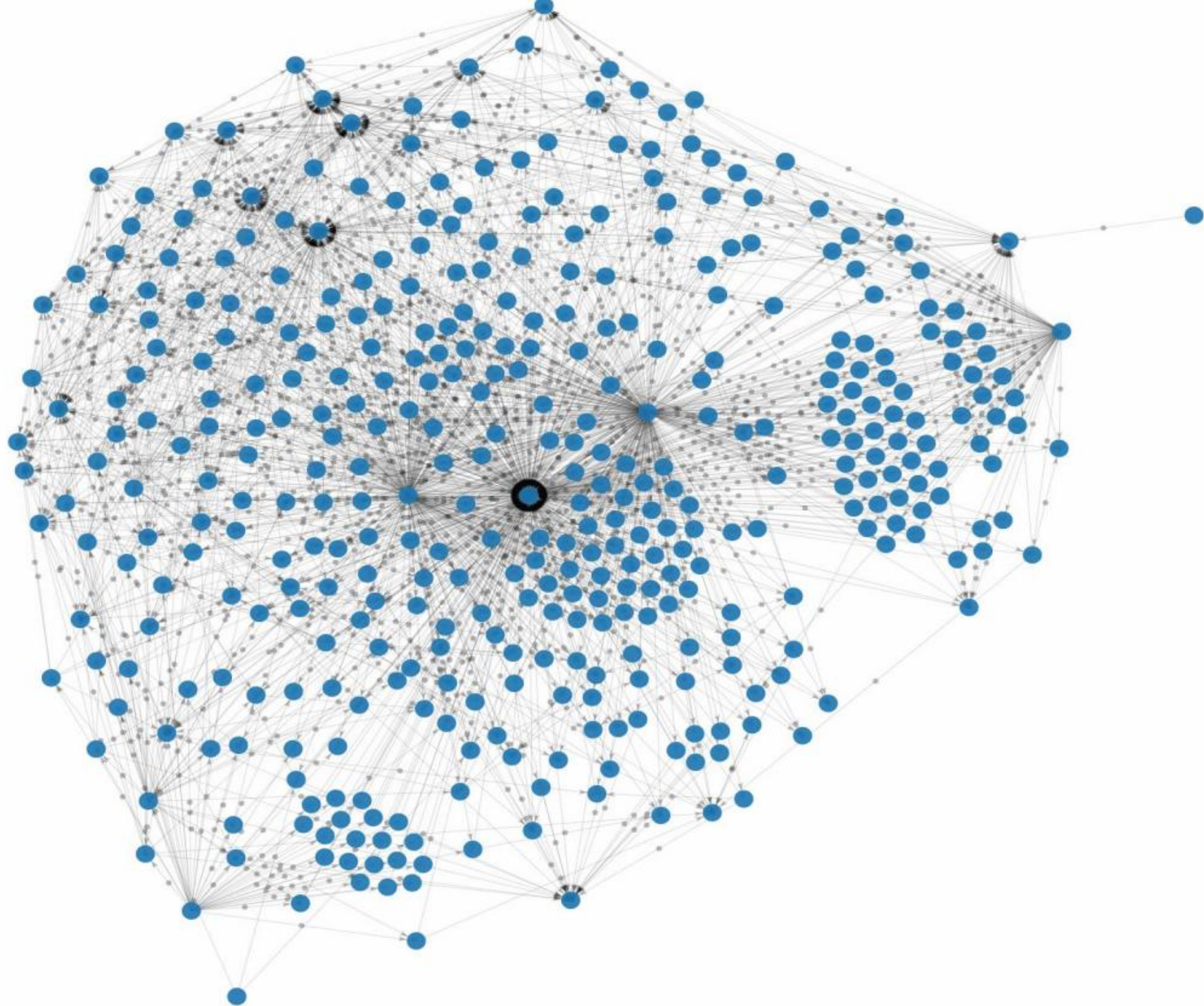
scale units

Australia 0101	North America 0101	CTiP A01
Asia Pacific 0101	North America 0102	CTiP B01
Asia Pacific 0201	North America 0201	CTiP B0102
Asia Pacific 0301	North America 0401	Dogfood A01
Asia Pacific 0501	North America 0402	Dogfood A0102
Europe 0101	North America 0501	Dogfood B01
Europe 0102	North America 0502	USGov Virginia
Europe 0201	North America 0601	SelfHost A0102
Europe 0301	North America 0602	SelfHost A01
Europe 0501	North America 0701	
Europe 0502	North America 0702	



arch





discovery

```
/beta/servicePrincipals  
/appId=0000000a-0000-  
0000-c000-000000000000  
/endpoints
```

```
{  
  "id": "cab303b0-2e9d-45b7-8c49-5364d0f04333",  
  "deletedDateTime": null,  
  "capability": "AADRelayService",  
  "providerId": "0000000a-0000-0000-c000-000000000000",  
  "providerName": "AADRelayService",  
  "uri": "https://fef.msud01.manage.microsoft.com/StatelessAadRelayService",  
  "providerResourceId": "a30e761d-2f4b-425b-82fe-395cc7944873"  
},  
{  
  "id": "c872f021-0403-43c1-be49-f7bfe665f8ce",  
  "deletedDateTime": null,  
  "capability": "ASUName",  
  "providerId": "0000000a-0000-0000-c000-000000000000",  
  "providerName": "ASUName",  
  "uri": "AMSUD0101",  
  "providerResourceId": "2b43d7bc-d485-4626-8073-7005dd4ddb40"  
},  
{  
  "id": "d152c10e-2822-436d-9cfe-dd39418e5448",  
  "deletedDateTime": null,  
  "capability": "AdminExperience",  
  "providerId": "0000000a-0000-0000-c000-000000000000",  
  "providerName": "AdminExperience",  
  "uri": "https://fef.msud01.manage.microsoft.com/AdminExperienceService",  
  "providerResourceId": "97bfd3ed-8726-4e24-aa6e-bc21156d974a"  
},
```



BACK TO THE ENDPOINT



MDM vs agent

Windows CSP/WinDC

Apple MDM/DDM

Android Enterprise

- let's ignore Teams device admin APKs...



MDM

built-in

open protocols

but... tied to OS release cycle



MDM vs agent

Windows CSP/WinDC

- Intune Management Extension (IME)
- Device Inventory, EPM, ...

Apple MDM/DDM

- macOS sidecar

Android Enterprise

- let's ignore Teams device admin APKs...

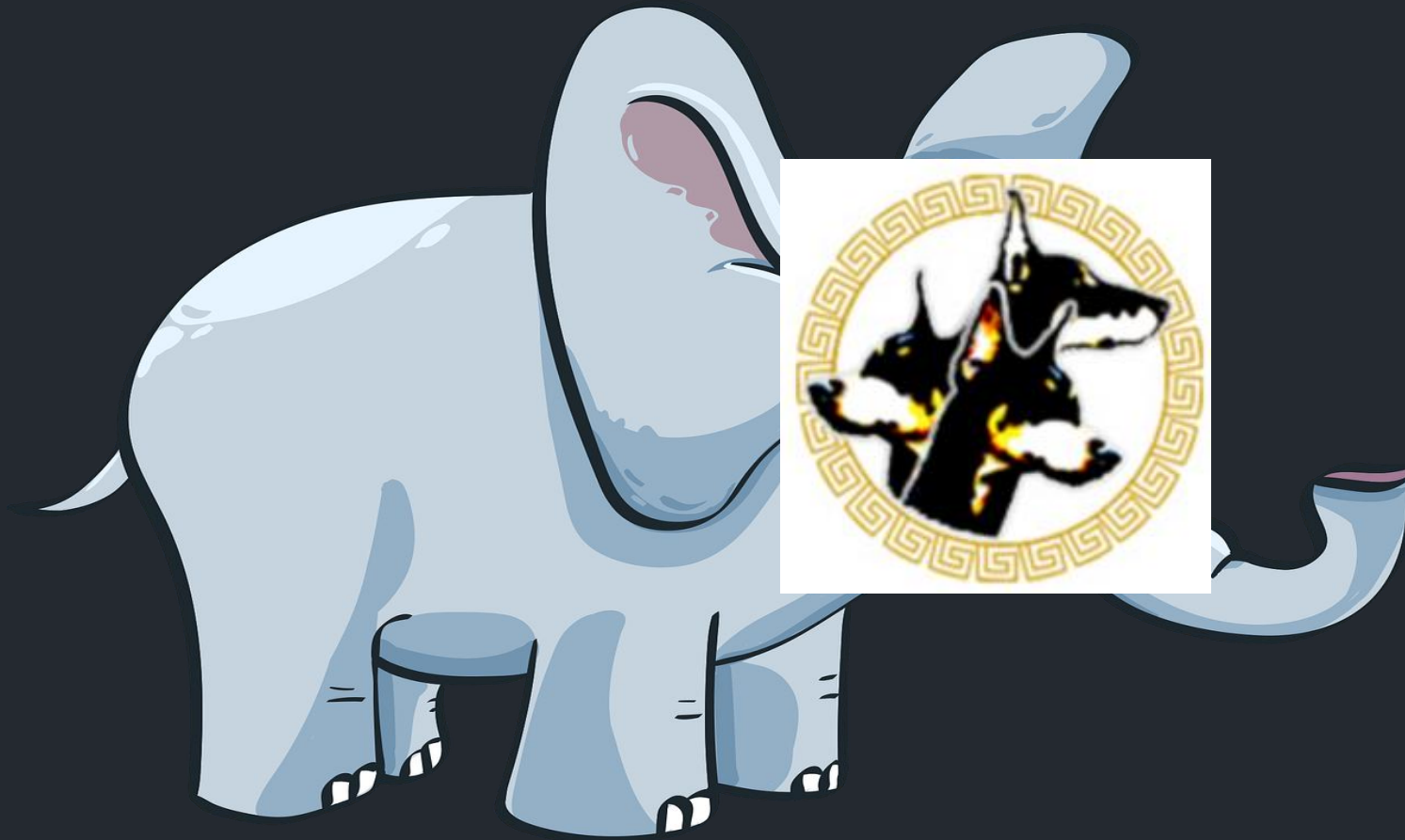


show me the ~~money~~ sync



pause – questions?

what about my on-prem apps?



NTLM...

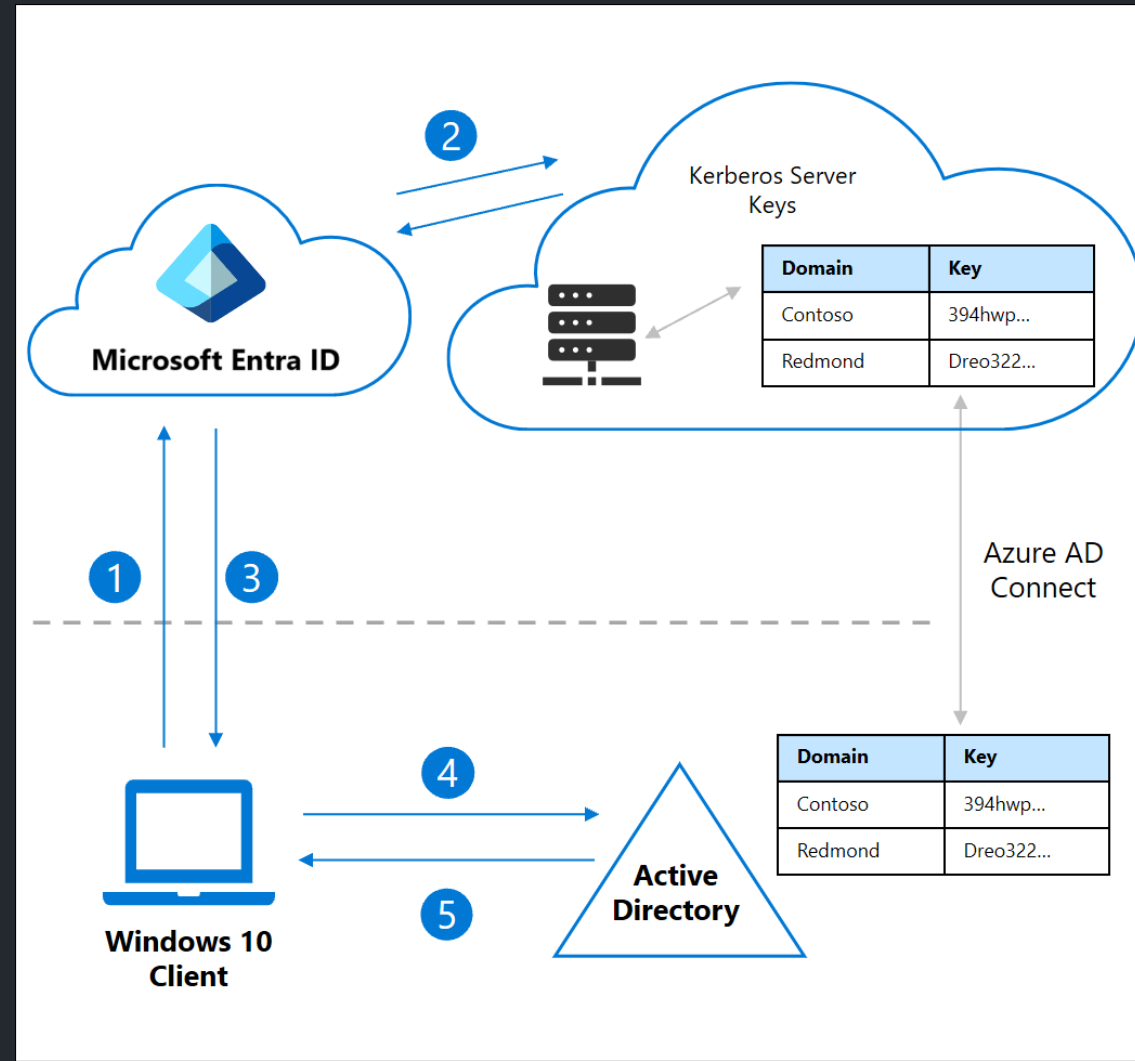
free* SS0!

just like workgroups

but it's deprecated?



Cloud Kerberos Trust



```
▼ Kerberos
  ▶ Record Mark: 1567 bytes
  ▼ tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    ▼ padata: 2 items
      ▼ PA-DATA PA-TGS-REQ
        ▼ padata-type: KRB5-PADATA-TGS-REQ (1)
          ▶ padata-value: 6e82056830820564a003020105a10302010ea20703050000...
        ▼ PA-DATA Unknown:161
          ▼ padata-type: Unknown (161)
            padata-value: 3003020117
      ▼ req-body
        Padding: 0
        ▶ kdc-options: 40810000
        realm: HYBRID.IMINYOUR.CLOUD
        ▼ sname
          name-type: KRB5-NT-SRV-INST (2)
          ▼ sname-string: 2 items
            SNameString: krbtgt
            SNameString: HYBRID.IMINYOUR.CLOUD
          till: 2023-05-30 13:37:47 (UTC)
          nonce: 892760479
          ▶ etype: 2 items
```



Cloud NTLM Trust???

sometimes you really need NTLM

magic KERB-KEY-LIST-REQ



the one downside

entra is authenticating the user...

Active Directory is only authorizing



mitigation

LAPS	Location	Managed By	Object	Security	Dial-in	Attribute Editor
General	Operating System	Member Of	Delegation	Password Replication Policy		

This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Domain Servi...	Setting
Account Operators	hybrid.iminyour.cloud/Builtin	Deny
Administrators	hybrid.iminyour.cloud/Builtin	Deny
Backup Operators	hybrid.iminyour.cloud/Builtin	Deny
Cert Publishers	hybrid.iminyour.cloud/Users	Deny
Domain Admins	hybrid.iminyour.cloud/Users	Deny
Domain Controllers	hybrid.iminyour.cloud/Users	Deny
Domain Users	hybrid.iminyour.cloud/Users	Allow
Enterprise Admins	hybrid.iminyour.cloud/Users	Deny
Schema Admins	hybrid.iminyour.cloud/Users	Deny
Server Operators	hybrid.iminyour.cloud/Builtin	Deny

Advanced...

Add...

Remove

OK

Cancel

Apply

Help



Intune can't do what I want

you're not *wrong*... but

all-encompassing product, vs platform



Microsoft Graph

powers the Intune portal

standard REST, easy to use

(usually) well-documented



one API to rule them all



Community



Questions?