

Control Plane under Control Securing Privileged Access with Managed Red Tenant



Thomas Naunheim

- Cyber Security Architect
- thomas.naunheim@glueckkanja.com

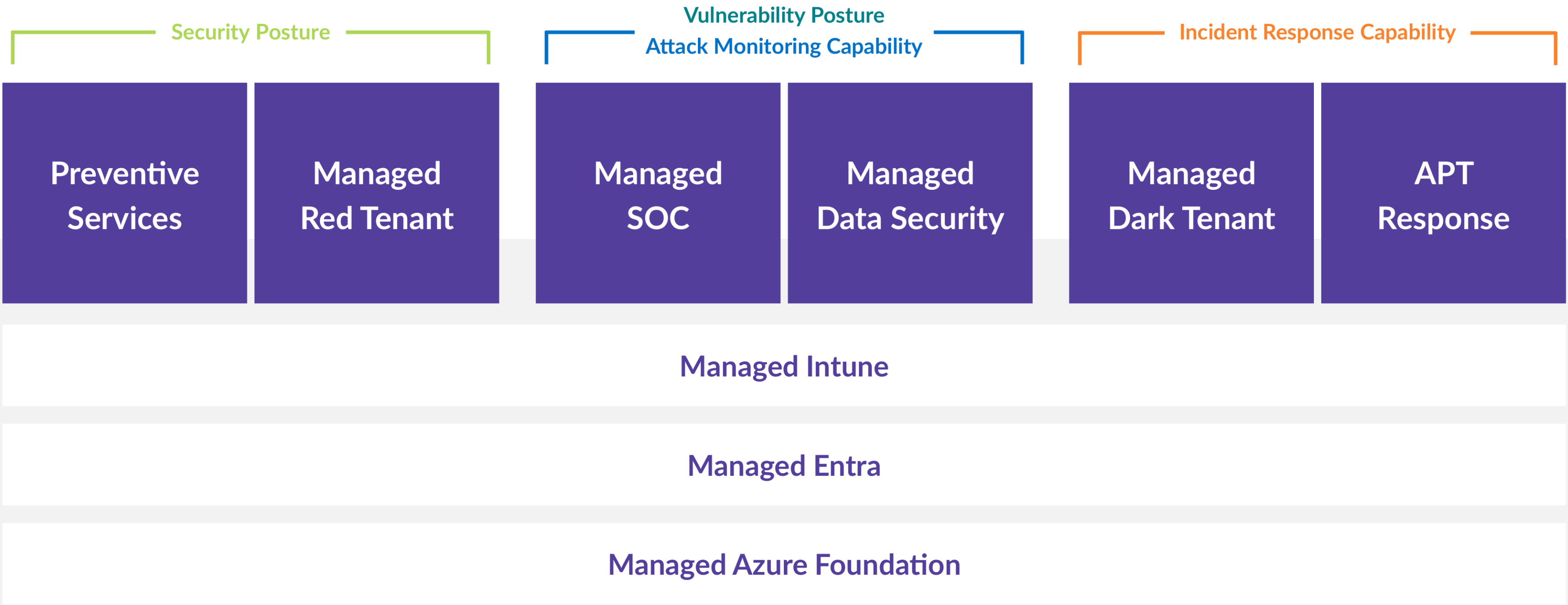
 /thomasnaunheim

 cloud-architekt.net

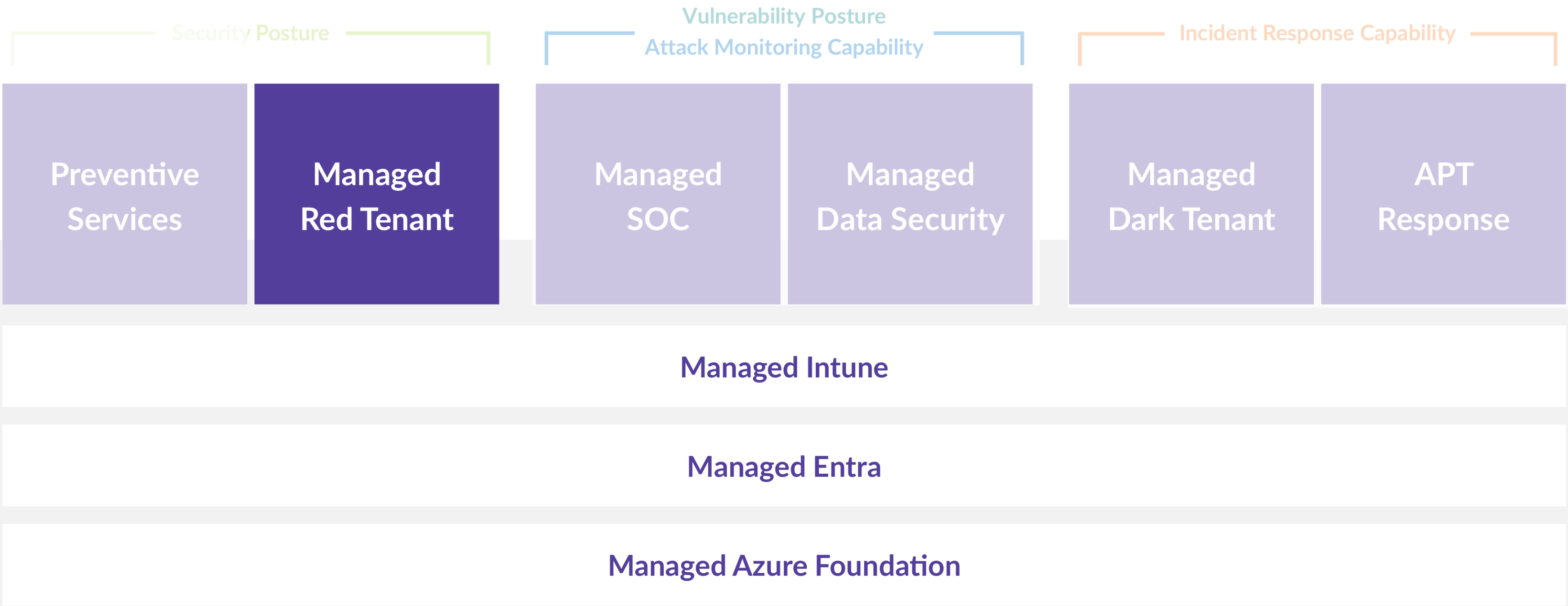
 Thomas_Live



We Have You Covered



We Have You Covered



697 ways in.

Attackers need one.

697 documented techniques to escalate privileges, move laterally and reach your most sensitive assets.

MITRE ATT&CK Enterprise: 222 techniques, 475 sub-techniques

In most incident responses we run, admins were working on the same device they read email on.

How do you make sure a compromised laptop never becomes a compromised domain?

Phish



Foothold



Escalate



Move Laterally

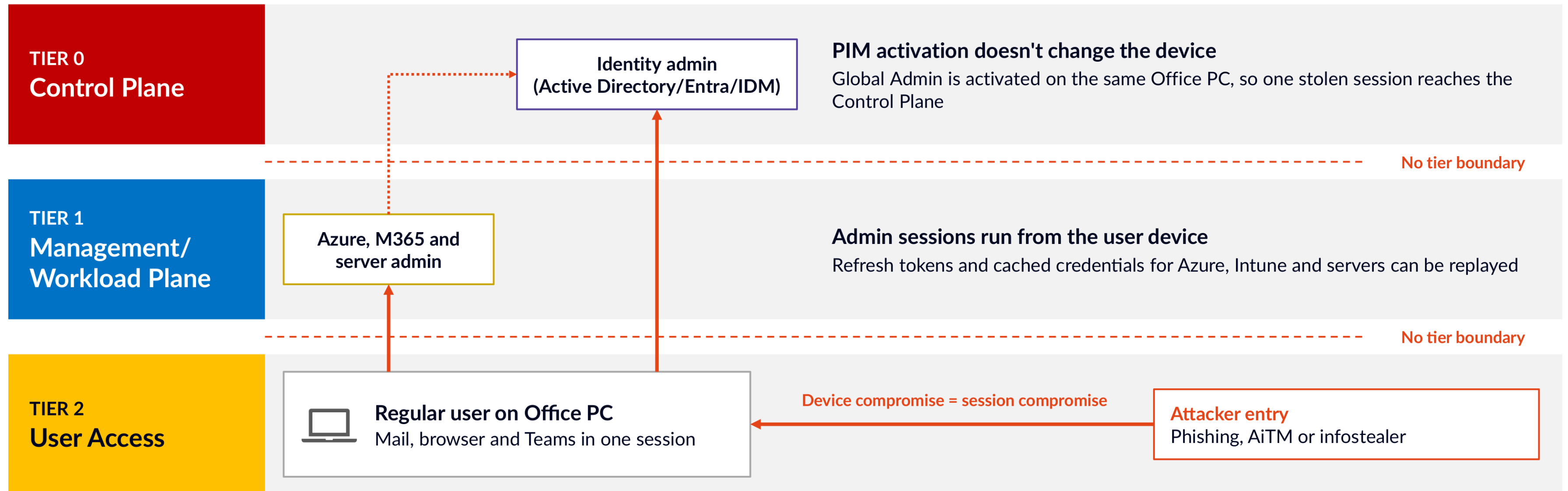


High Privileges



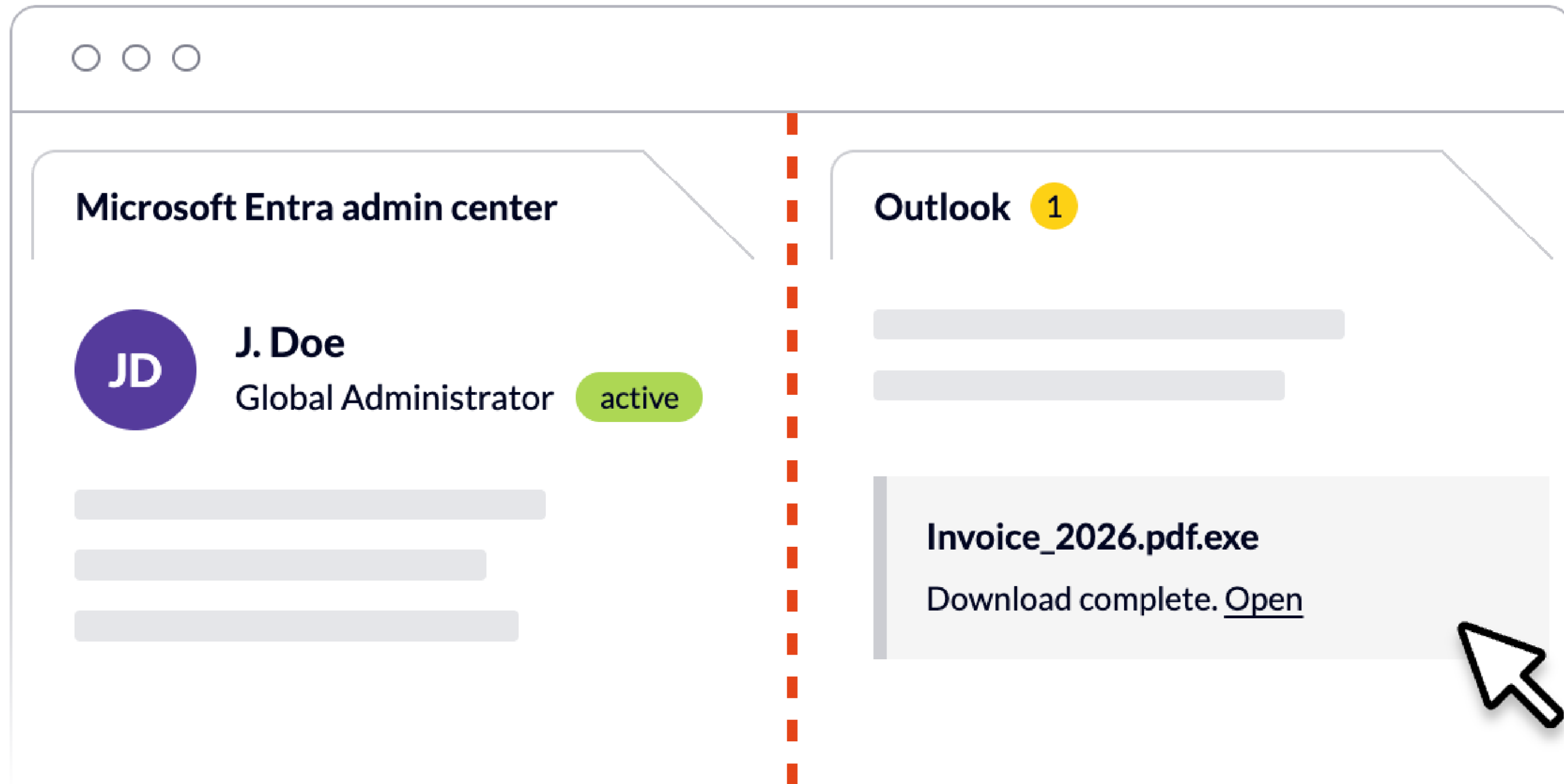
Crown Jewels

One Office PC holds the keys to your privileged assets



One compromised Office PC is a direct path to Tier 0: no exploit and no privilege escalation required.

The Problem: Admin & User Work



The Stryker Attack: When Intune Becomes a Weapon

What happened

- Pro-Iranian group Handala hijacked a single Intune admin account and wiped devices worldwide through the legitimate management console – overnight, with no malware.
- Affected: corporate laptops, company phones and private BYOD devices alike.

Why it worked

- Flat privilege model: admin and everyday work share the same device and identity.
- Phishing, infostealers or AiTM tokens become a direct path to the most powerful controls
 - with no privilege escalation.

CISA response

- High-risk Intune actions such as Wipe require approval from a second admin.
Not an edge case – a pattern.

79

Countries with wiped devices

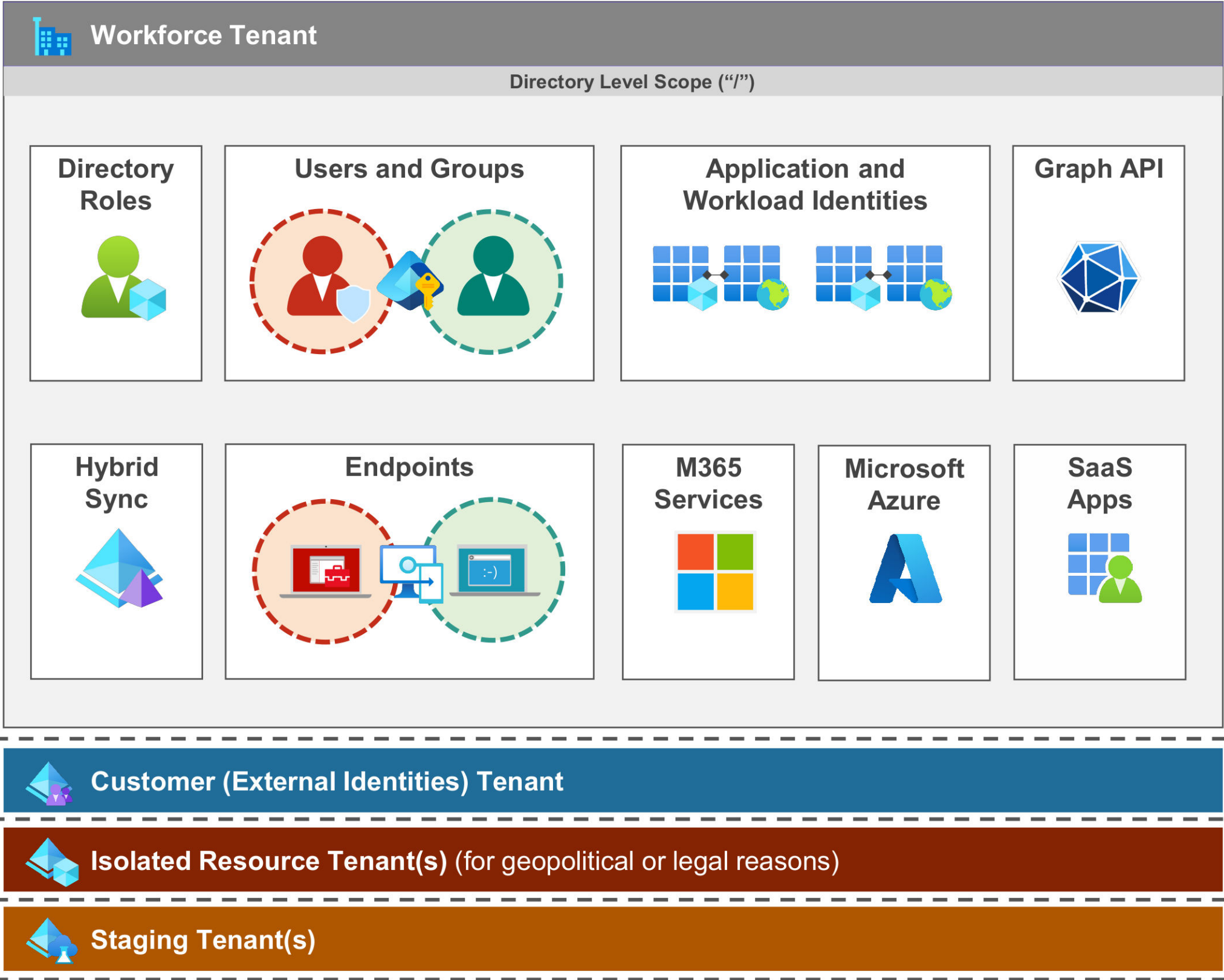
~ 80,000

Devices wiped in 3 hours
(05:00–08:00 UTC)

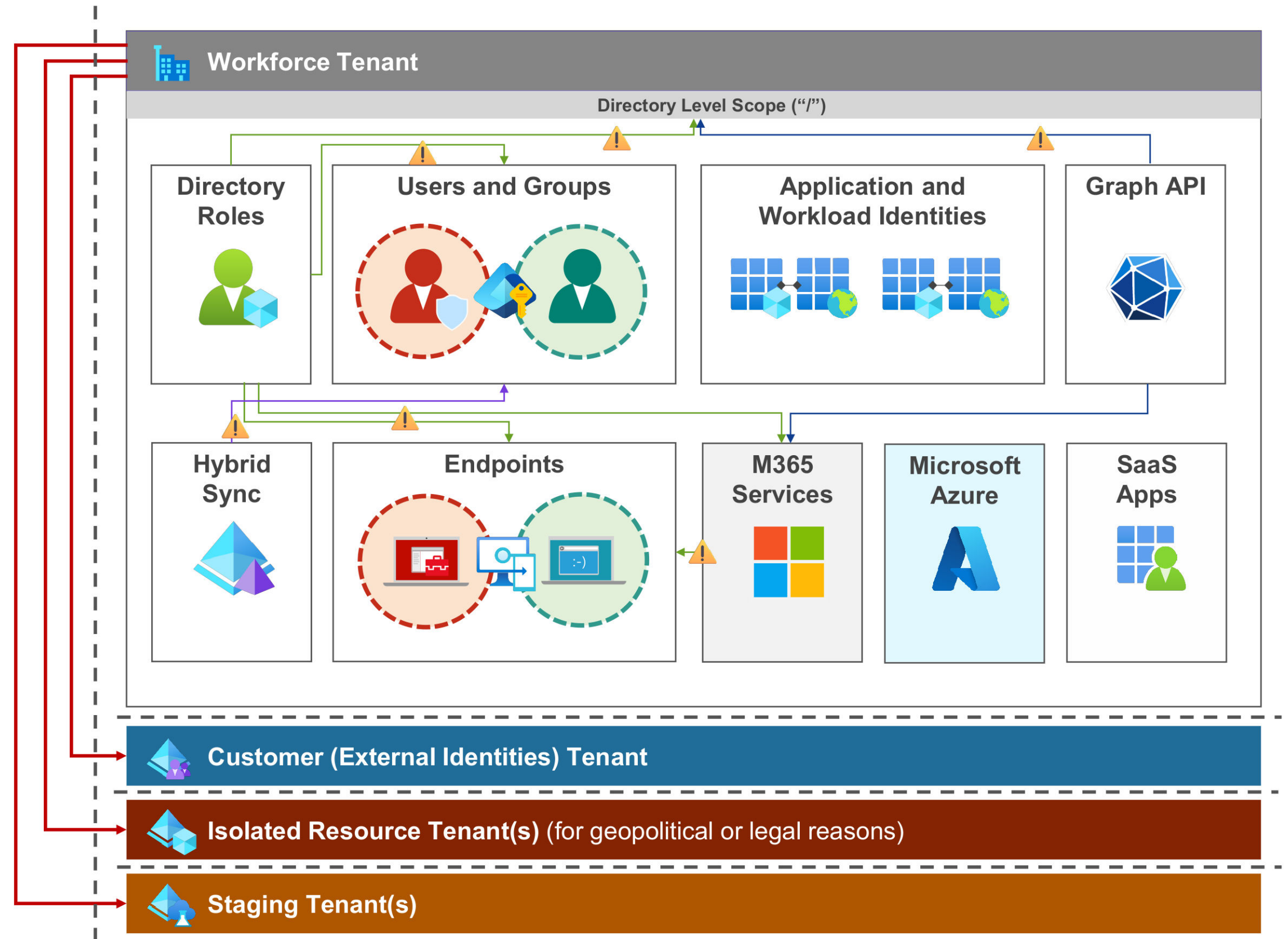
0

Malware | Exploits | Zero-Days

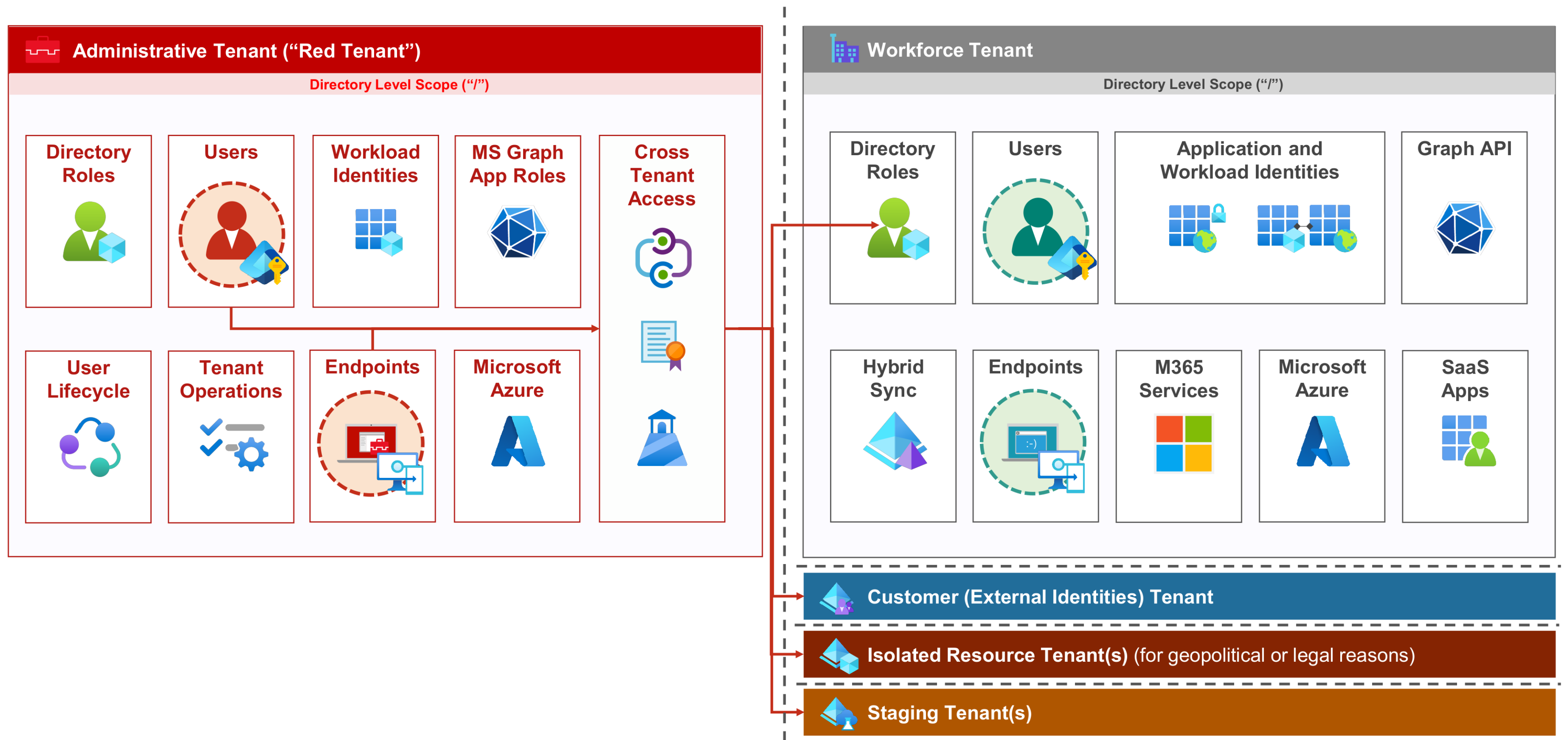
Challenges of Intra-Tenant Isolation



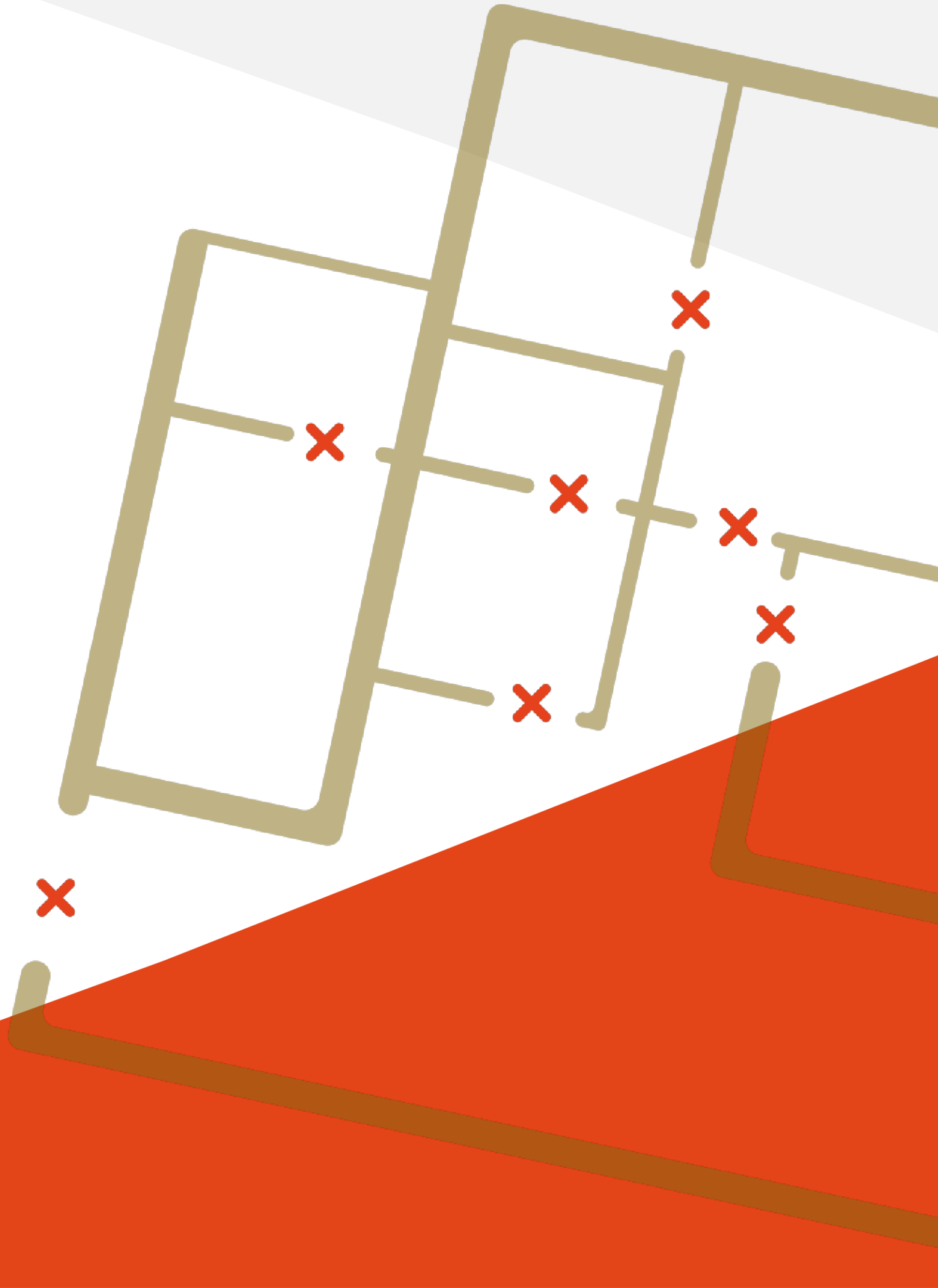
Challenges of Intra-Tenant Isolation



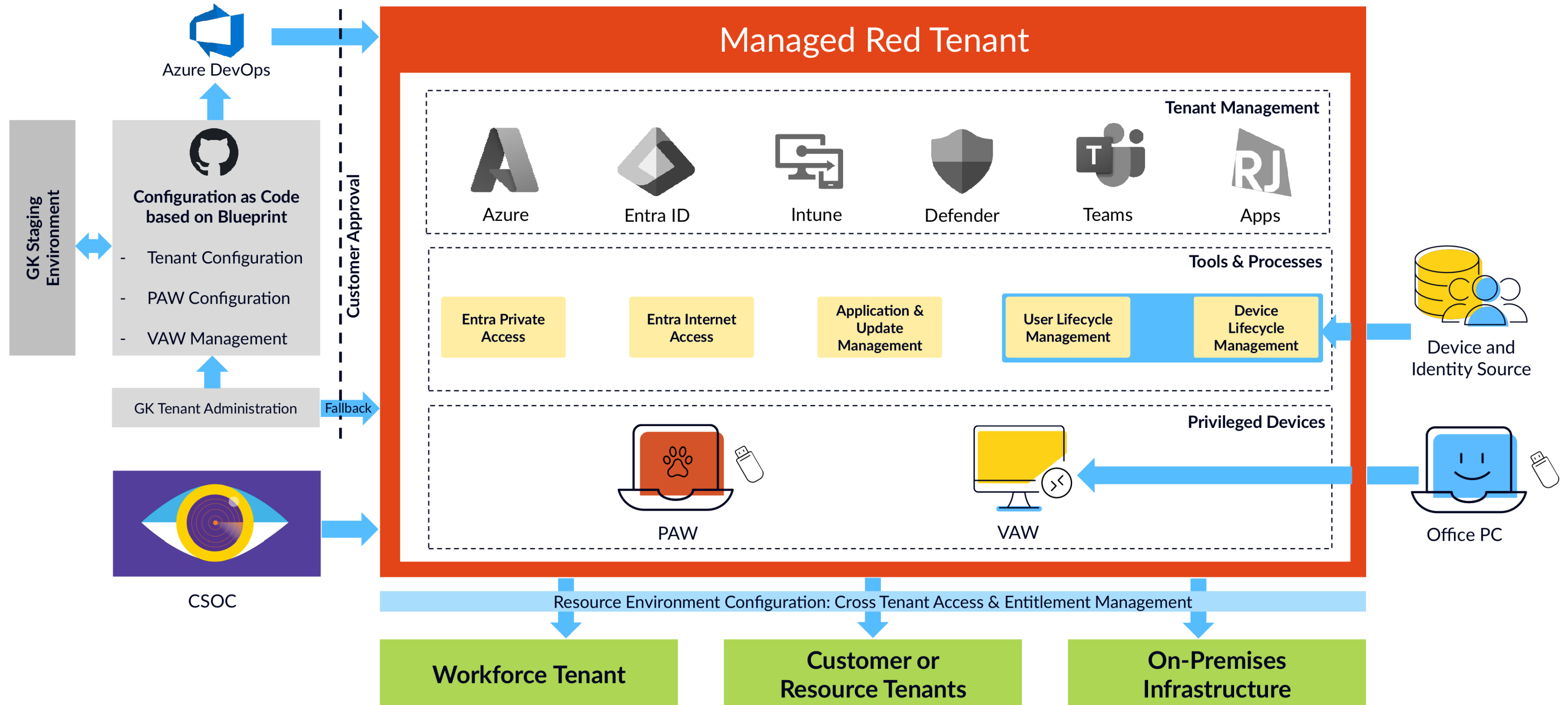
Inter-Tenant Isolation with Red Tenant



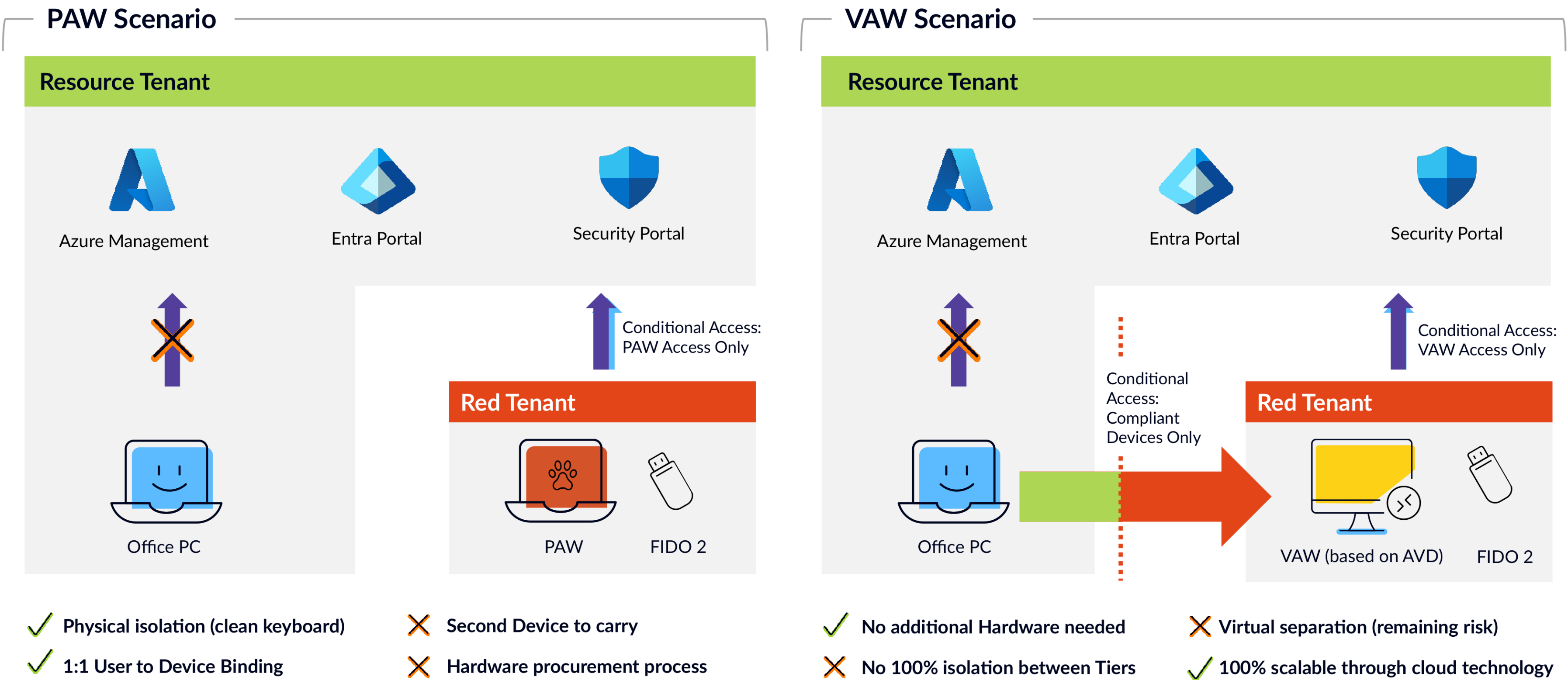
What is **Managed** Red Tenant?



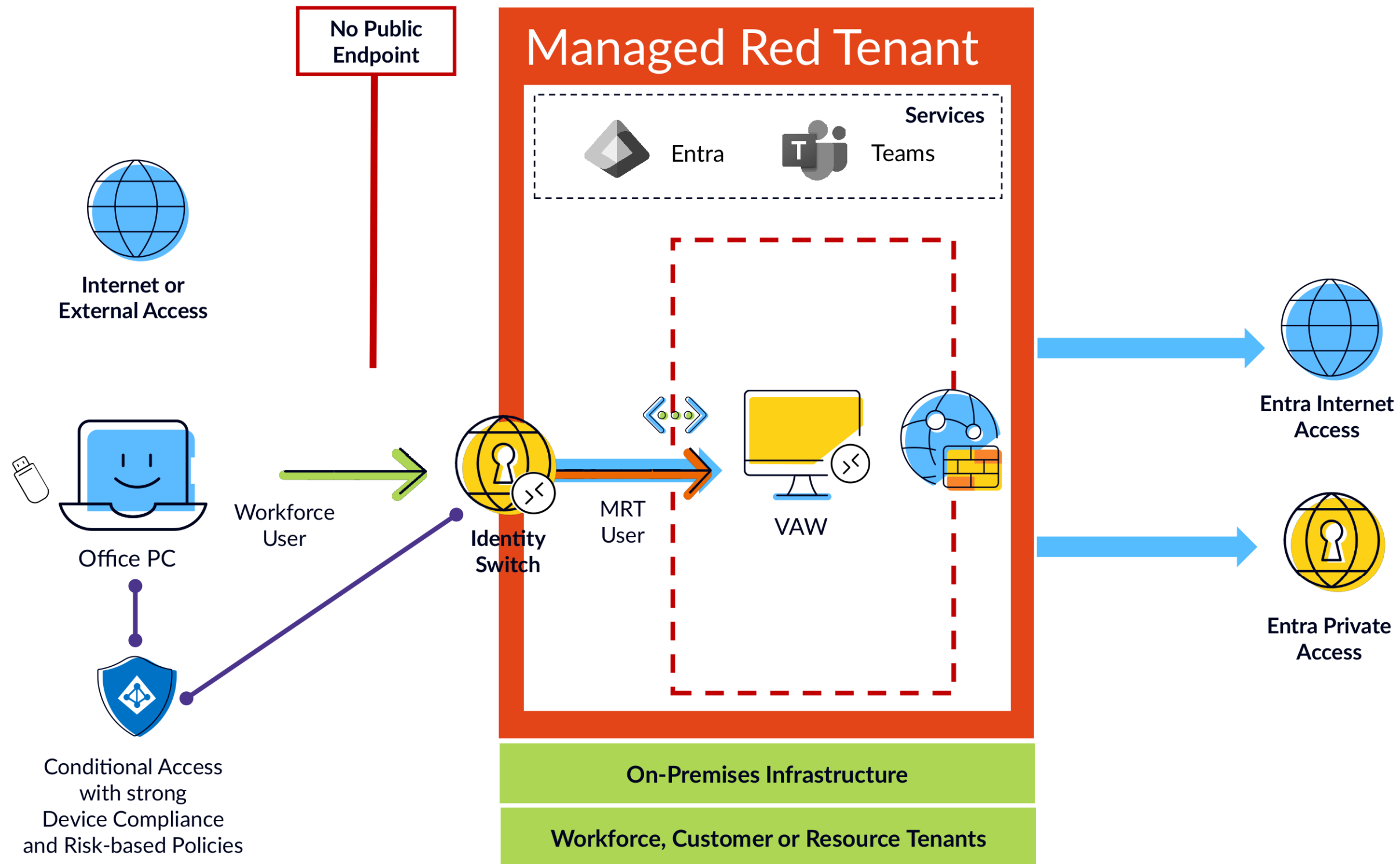
What is Managed Red Tenant?



Overview of Privileged Access Deployment options



Secure access for Management and Workload Plane Admins

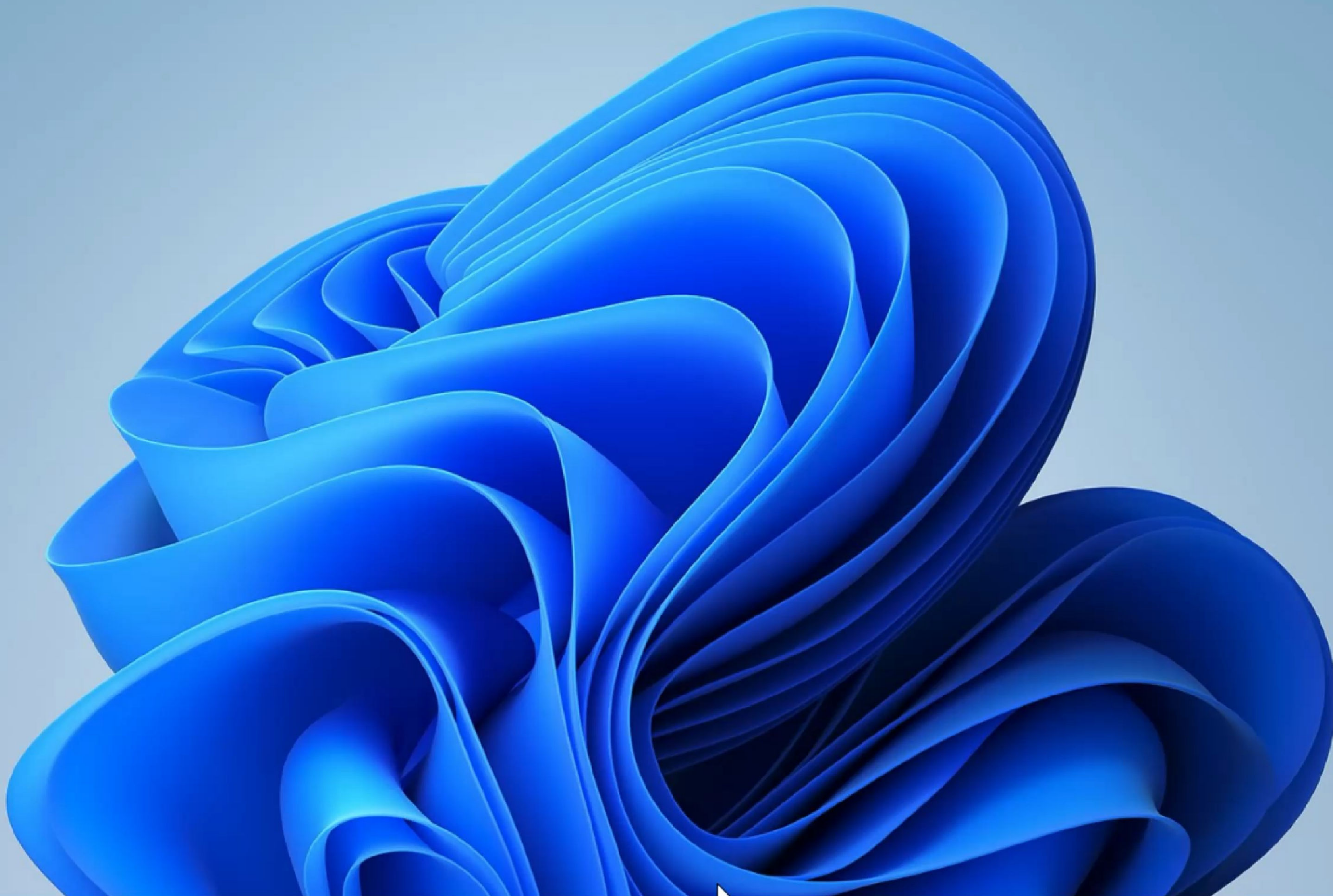
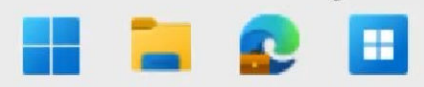




Recycle Bin



Microsoft
Edge





Recycle Bin



Microsoft Edge

Microsoft

Windows Security

Making sure it's you

Please sign in to "login.microsoft.com".

This request comes from the app "App" by "Microsoft Corporation".

Insert your security key into the USB port.

Cancel

Terms of use

Privacy & cookies

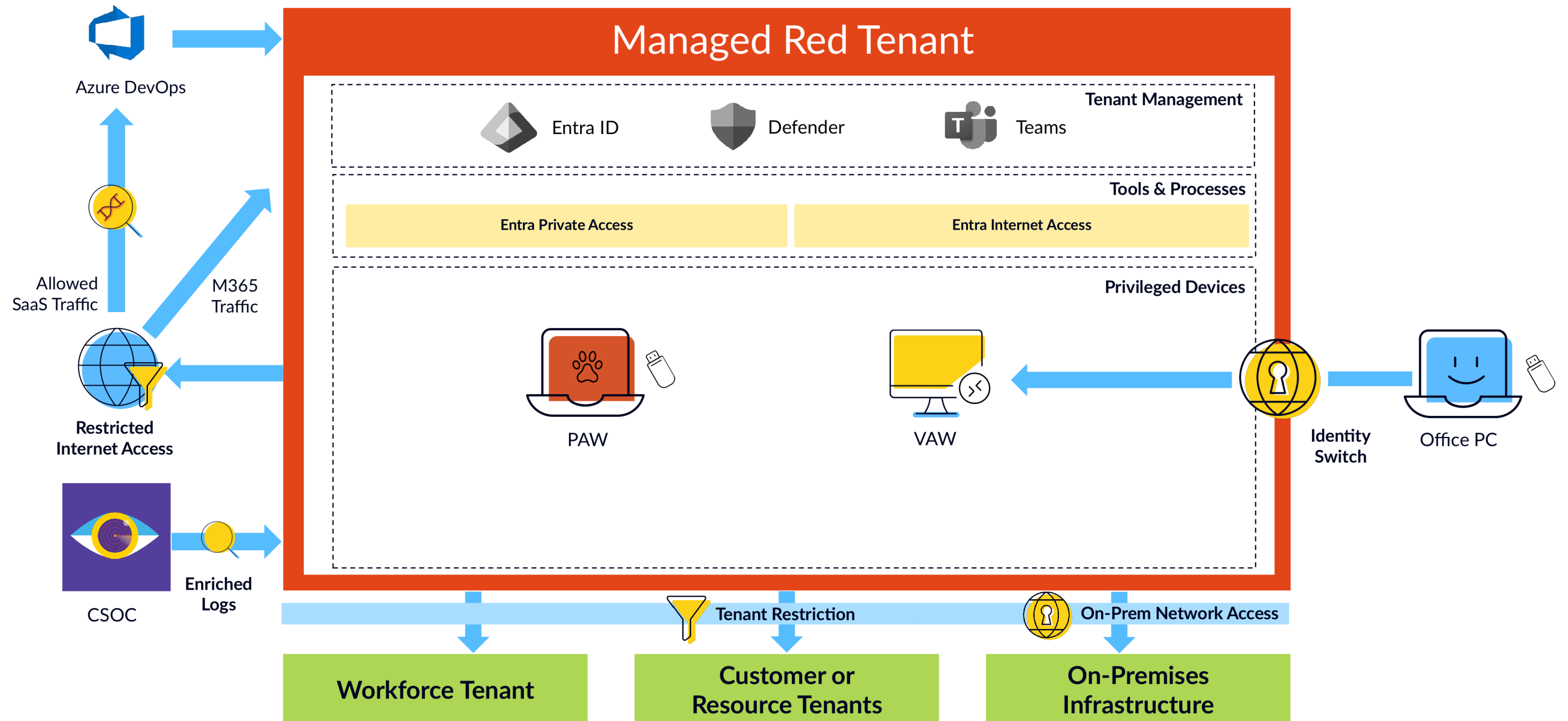
...



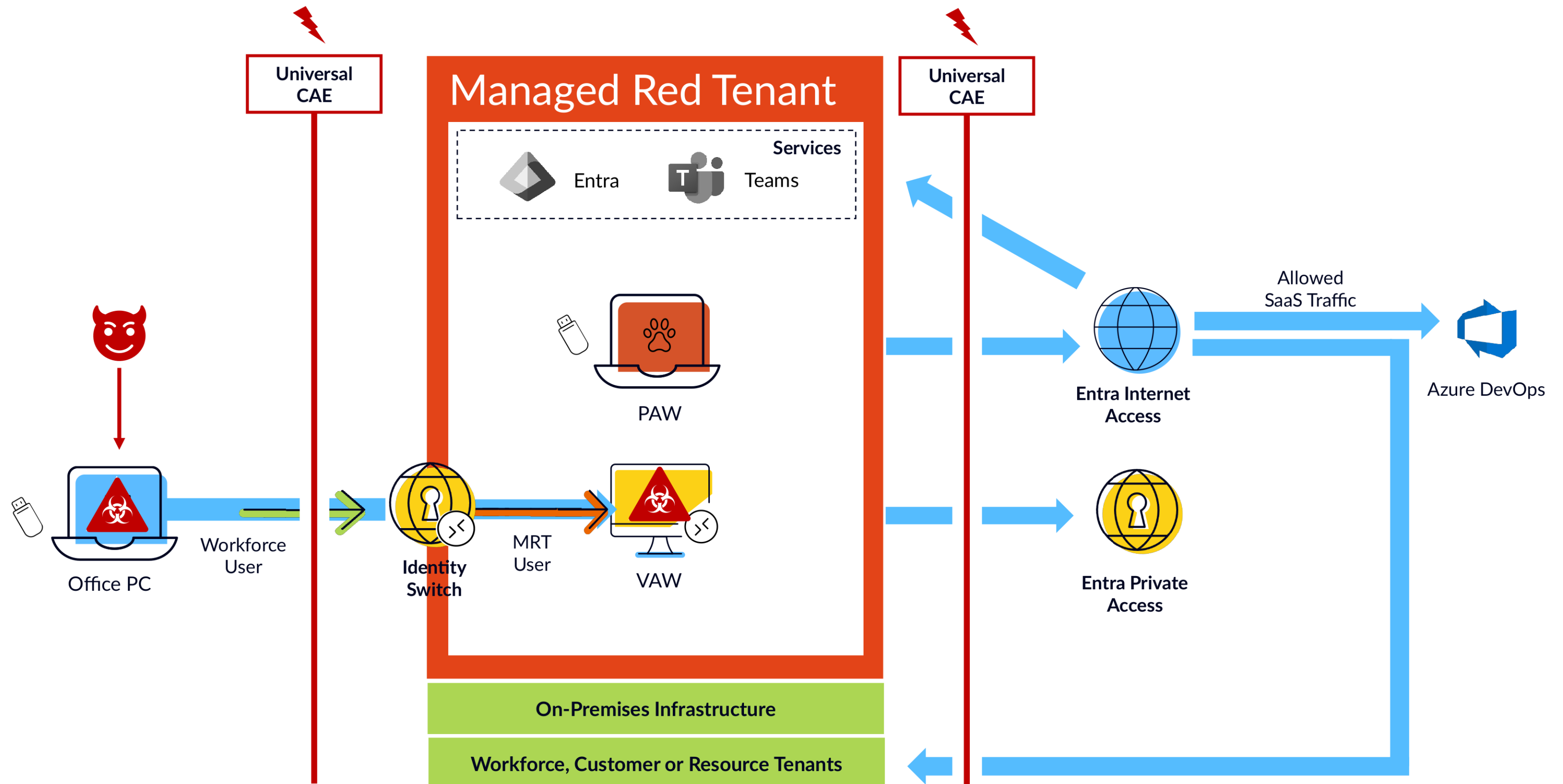
How to “**always verify**”
in the Red Tenant and
beyond?



Integration of Global Secure Access



Use Case: Revoking access in near real-time



Hunting for Global Admin Access in Workforce Tenant

```
1 let GlobalAdmins = IdentityInfo | where AssignedRoles contains "Global Administrator" | summarize by AccountObjectId;
2 union SigninLogs
3 | where UserId in~ (GlobalAdmins)
4 | where ResultType == "0"
5 | extend IsRedTenantUser = iff(HomeTenantId == true, false)
6 | project-reorder UserPrincipalName, ResourceDisplayName, IsRedTenantUser, IsThroughGlobalSecureAccess, IPAddress, GlobalSecureAccessIpAddress
7
```

Getting started

Results

Query history

Export

Show empty columns

9 items

Search

00:03.89

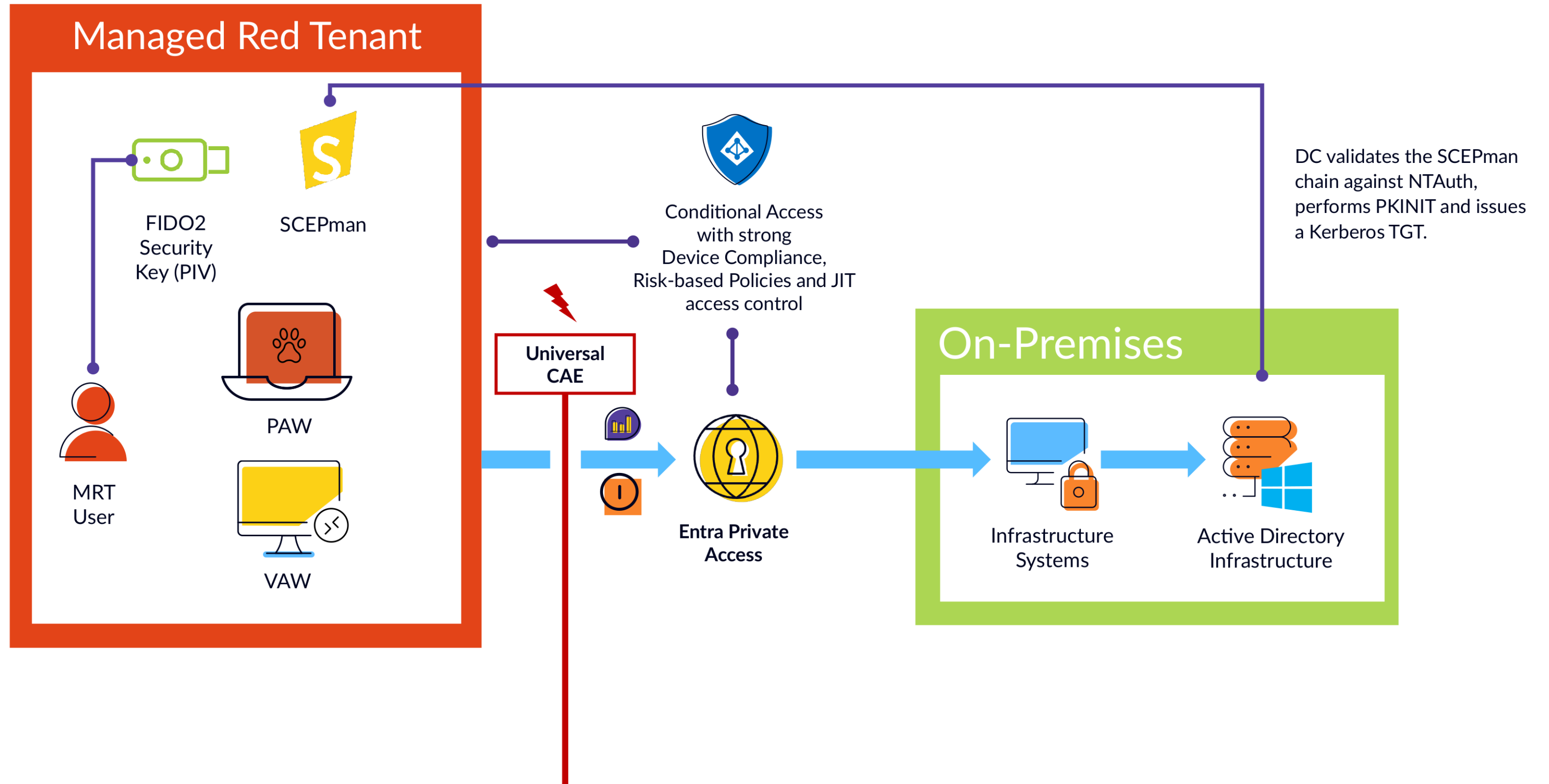
Low

filters:

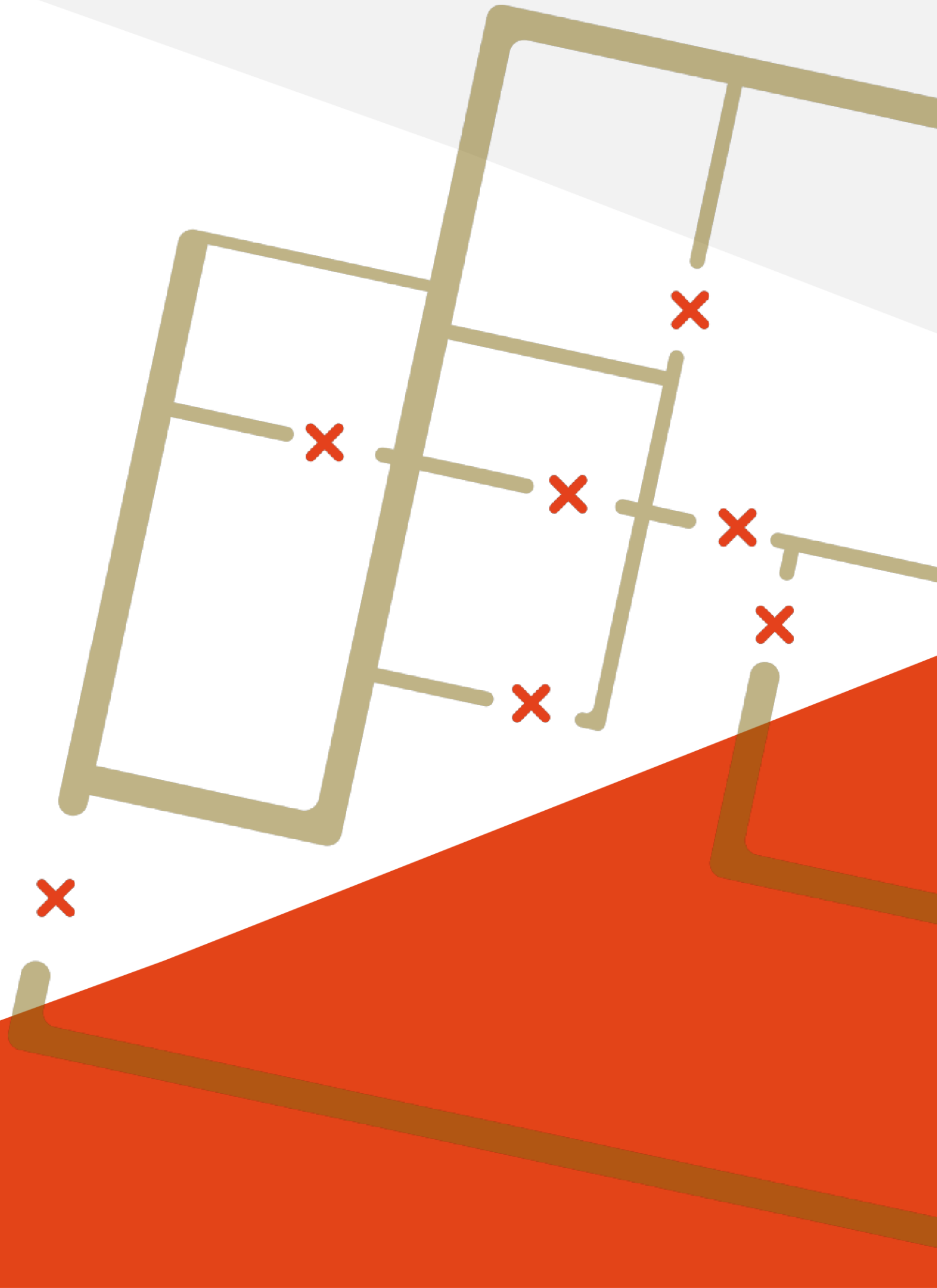
Add filter

☐	TimeGenerated	UserPrincipalName	ResourceDisplayName	IsRedTenantUser	IsThroughGlobalSecureAcce...	IPAddress	GlobalSecureAccessIpAddress
☐	> Sep 18, 2025 12:5...		Azure Resource Manager	1	1		,
☐	> Sep 18, 2025 12:3...		Microsoft Graph	1	1		,
☐	> Sep 18, 2025 12:3...		Microsoft Graph	1	1		,
☐	> Sep 18, 2025 12:3...		Azure Resource Manager	1	1		,
☐	> Sep 18, 2025 12:4...		Azure Resource Manager	1	1		,
☐	> Sep 18, 2025 12:3...		Azure Resource Manager	1	1		,
☐	> Sep 18, 2025 12:3...		My Apps	1	1		,
☐	> Sep 18, 2025 12:3...		Microsoft Graph	1	1		,
☐	> Sep 18, 2025 12:5...		Azure Resource Manager	1	1		,

Use Case: On-Premises Access



What does **adoption**
look like, and what are
the **challenges**?



Lessons learned: four questions (most) customers ask



Who is Control Plane and should get a PAW?

- Rate roles by impact and blast radius, not job title or department
- Reduce numbers of Control Plane Admins via scoped, least-privilege roles



Do Control Plane admins always need their PAW with them?

- No, read-only access can be accessible via VAW
- High-privileged changes stay on the PAW
- Separation between Global Admin (PAW) and Configuration/Security Reader (VAW)



Does a multi-tenant or multi-forest environment need several Red Tenants?

- One Red Tenant can serve all environments
- Cross tenant and environment boundaries are granted granularly



Does a Red Tenant add complexity and operating cost?

- Separate admin accounts and devices already need additional licenses today
- Isolation within tenant is more complex
- Automation and blueprints cut effort without losing control

Adopting Managed Red Tenant: plan, integrate side by side, roll out



One More Thing...

Threats & Exposure ?

! Incidents & Risks 68

Incidents on device / user in last 30 days

4 High 25 Medium 39 Low

% Non-Admin URL Traffic 37 80%

80% of browsing to non-privileged interfaces from devices with privileged access

Endpoint Attack Surface 40 687

687 VULNERABILITIES 41 EXPOSED TOKENS 569 NON-MICROSOFT APPS INSTALLED

23 critical · remote-exploitable in active attack path

Lateral Movement to Admin Device 41 63

Intune Admins 8 Device Admins 12

Local Device Admins 29 SPs · API Permission 14

MICROSOFT 365 TIER0 ASSETS · USERS



OVERALL RISK · HIGH

ADMIN DEVICES SEEN 134 devices

96 ENTRA ID-JOINED 38 REGISTERED 765 UNKNOWN · SIGN-INS

765 sign-ins from unknown (unregistered) devices

25 of 134 devices not protected in Defender

← EXPOSURE 7.8 /10 Threats · Lateral Movement ⓘ

HYGIENE 3.2 /10 20 stale users · 41 unseen devices ⓘ

BLAST RADIUS → 6.6 /10 Blast radius if compromised ⓘ

Permissions & Activities ?

Tier0 Users by Role Roles

Helpdesk Administrator 46

Global Reader 31

Security Reader 21

User Administrator 14

Authentication Administrator 13

Active users to internal/external tenants

104 TOTAL ACTIVE USERS (30D)

14 CROSS-TENANT USERS

7 EXTERNAL TENANTS

Privileged Activities 7,418

MICROSOFT GRAPH API OPERATIONS 6,750

1,260 CREATE 5,840 WRITE 318 DELETE

Thank you!