glueck kanja

2024

Managed Red Tenant

Cut Off Lateral Movement Paths

glueckkanja

Jan Geisbauer

— *Security Lead*

— *jan.geisbauer@glueckkanja.com*

.../jangeisbauer/

Thomas Naunheim

— *Cyber Security Architect*

— *thomas.naunheim@glueckkanja.com*

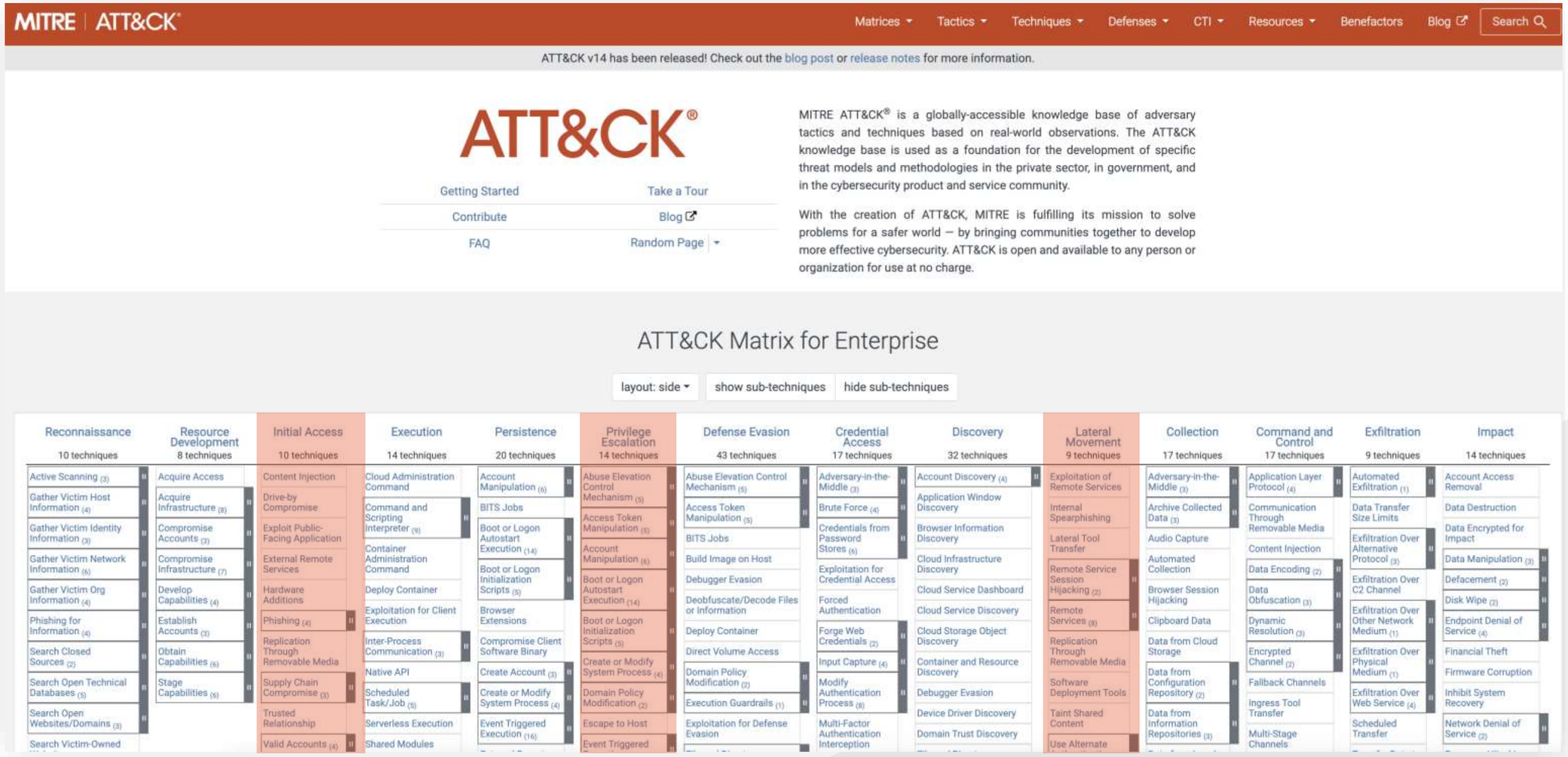
.../thomasnaunheim/

glueck kanja

Lateral Movement

- *There is no attack without lateral movement*
- *In most cases the crown jewels are not exposed directly*
- *Crown jewels are not put on a table in a room with an open window to the street*
- *They are kept at a safe place*
- *That's why a burglar must move laterally through the rooms of a building*

MITRE ATTACK

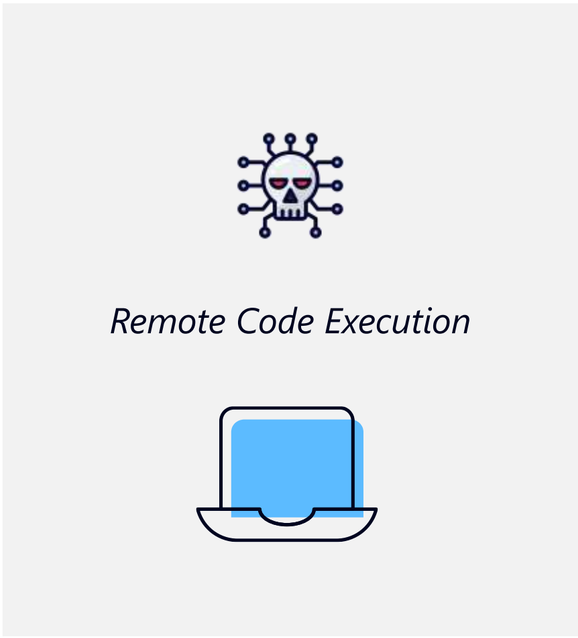


Initial Access

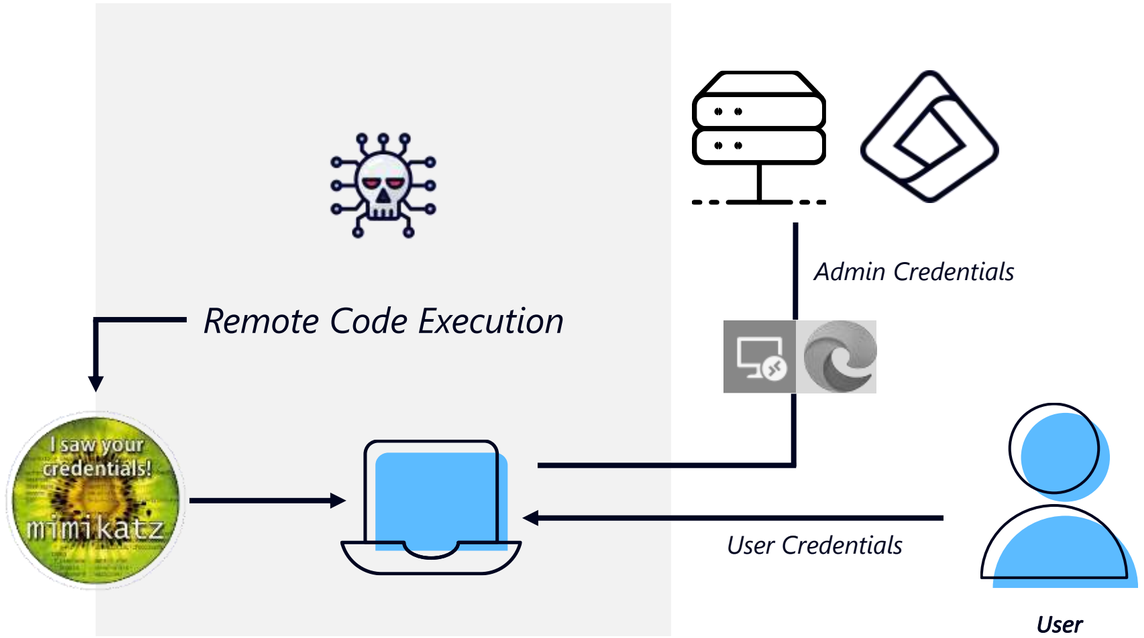
External Remote Services

Phishing

Drive-by Compromise

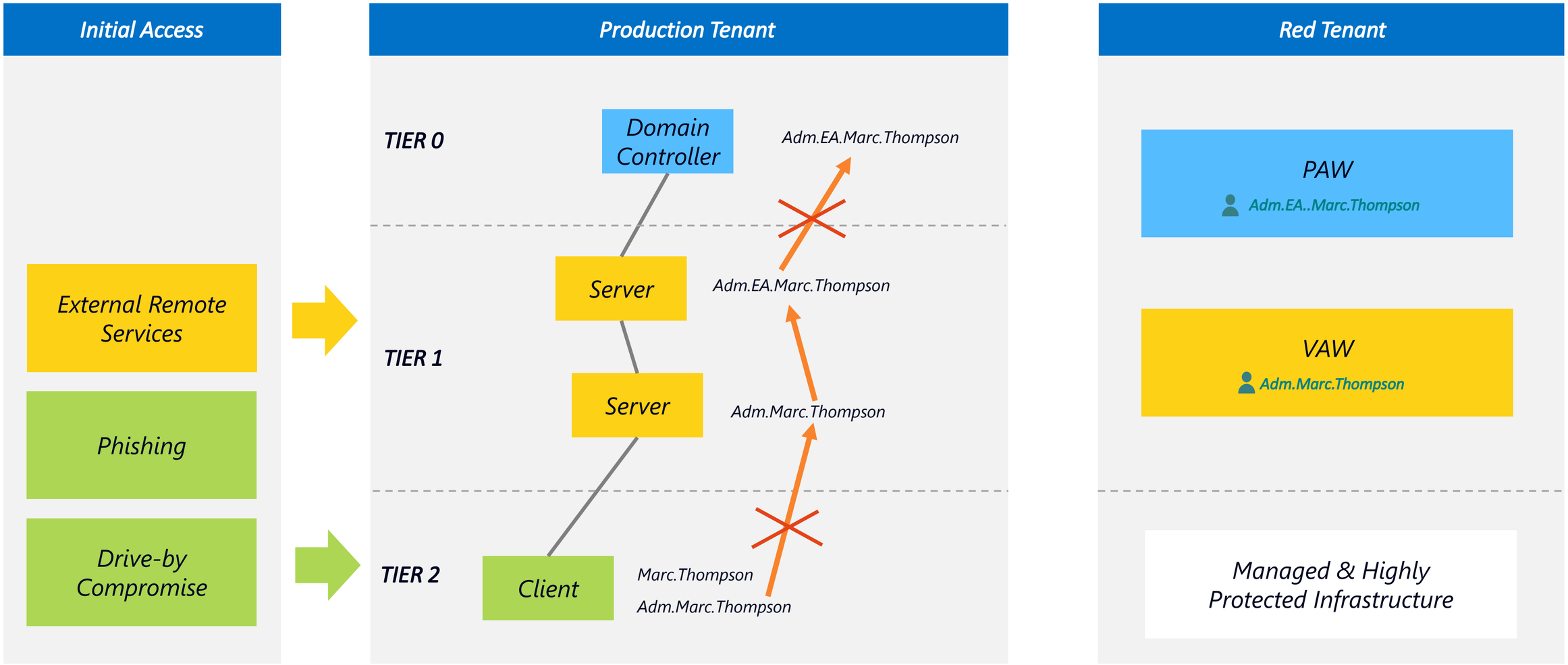


Privilege Escalation



glueck kanja

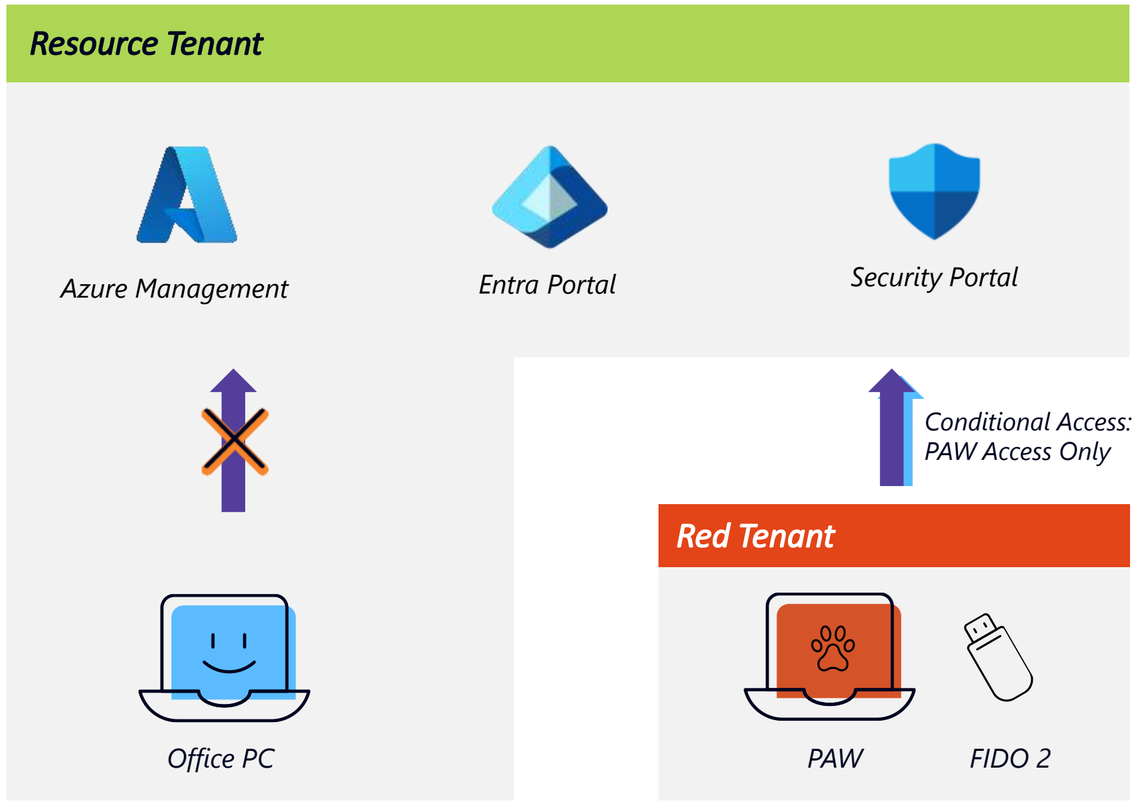
Lateral Movement through Privilege Escalation



glueck kanja

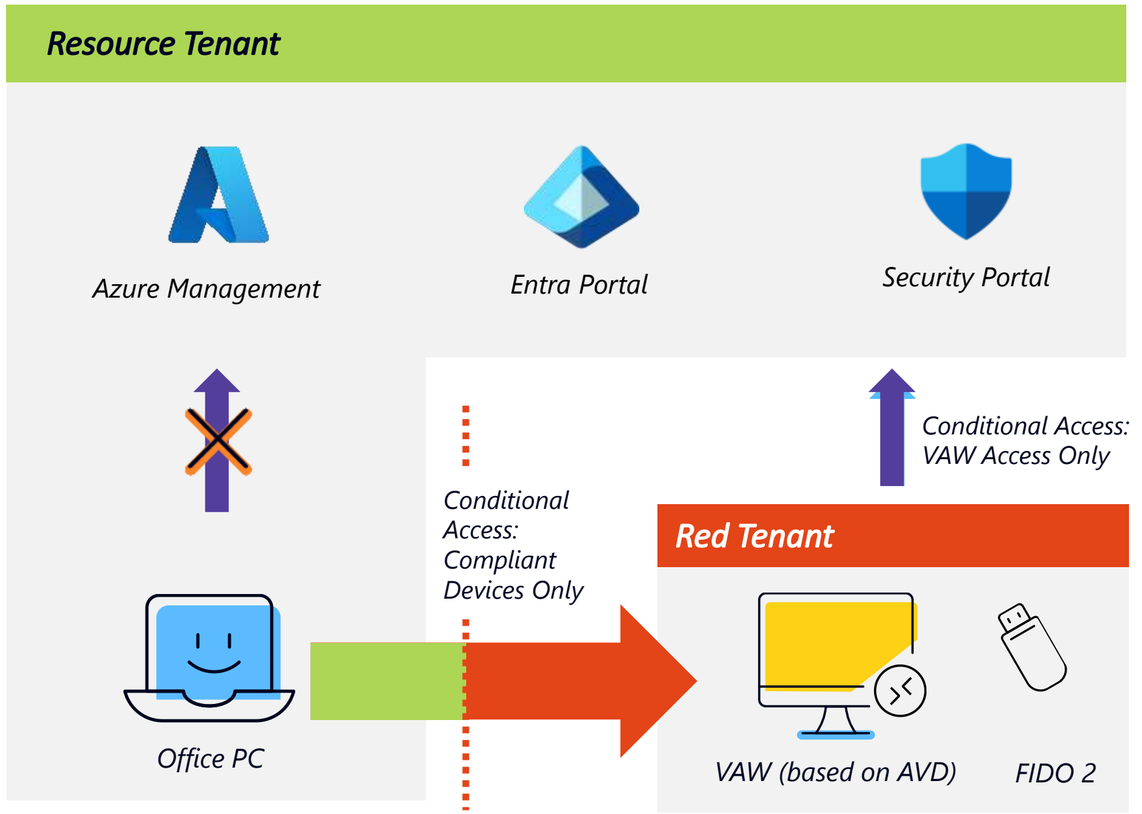
PAW & VAW

PAW Scenario



- ✓ Physical isolation (clean keyboard)
- ✓ 1:1 User to Device Binding
- ✗ Second Device to carry
- ✗ Hardware procurement process

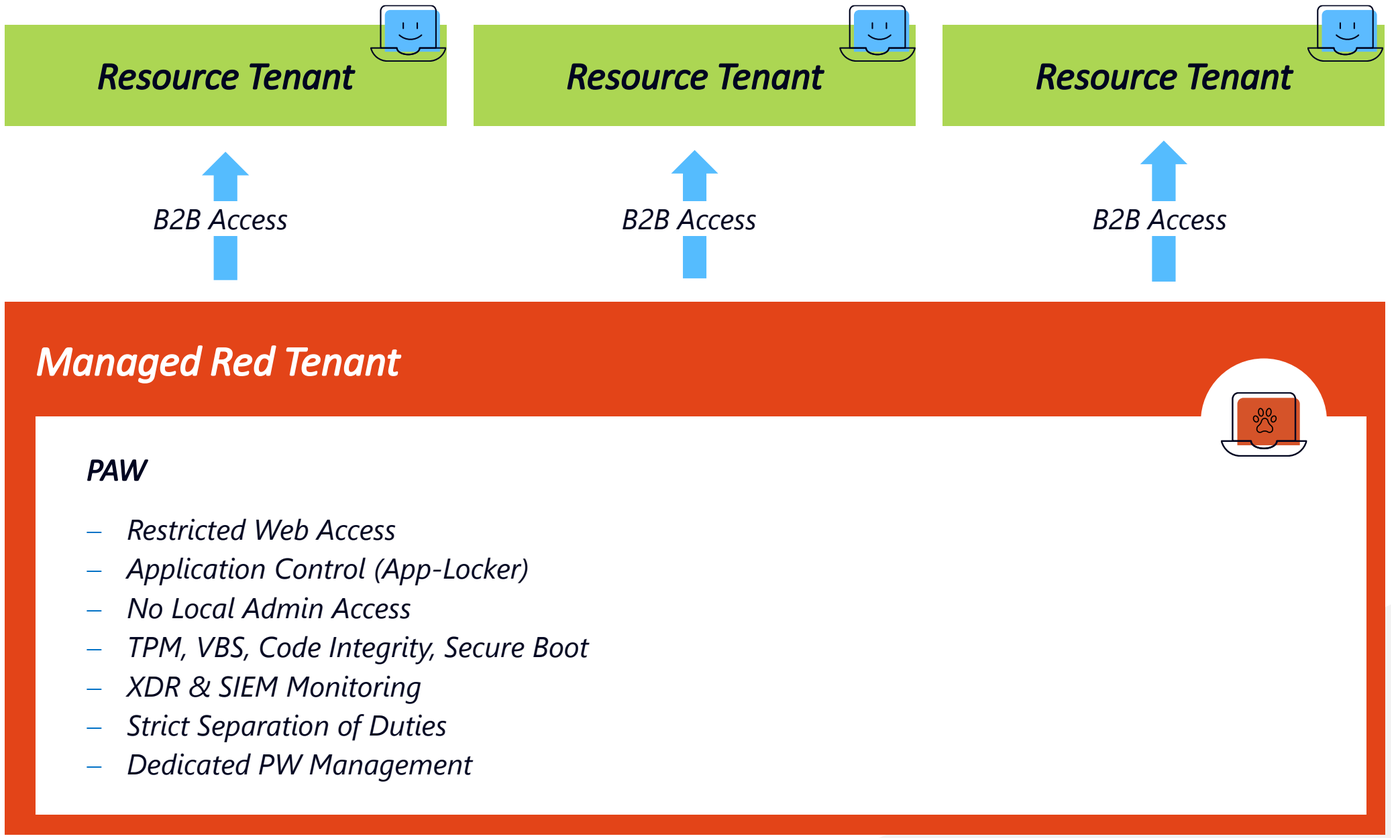
VAW Scenario



- ✓ No additional Hardware needed
- ✗ No 100% isolation between Tiers
- ✗ Virtual separation (remaining risk)
- ✓ 100% scalable through cloud technology

glueck kanja

Highly Secure Working Environment PAW

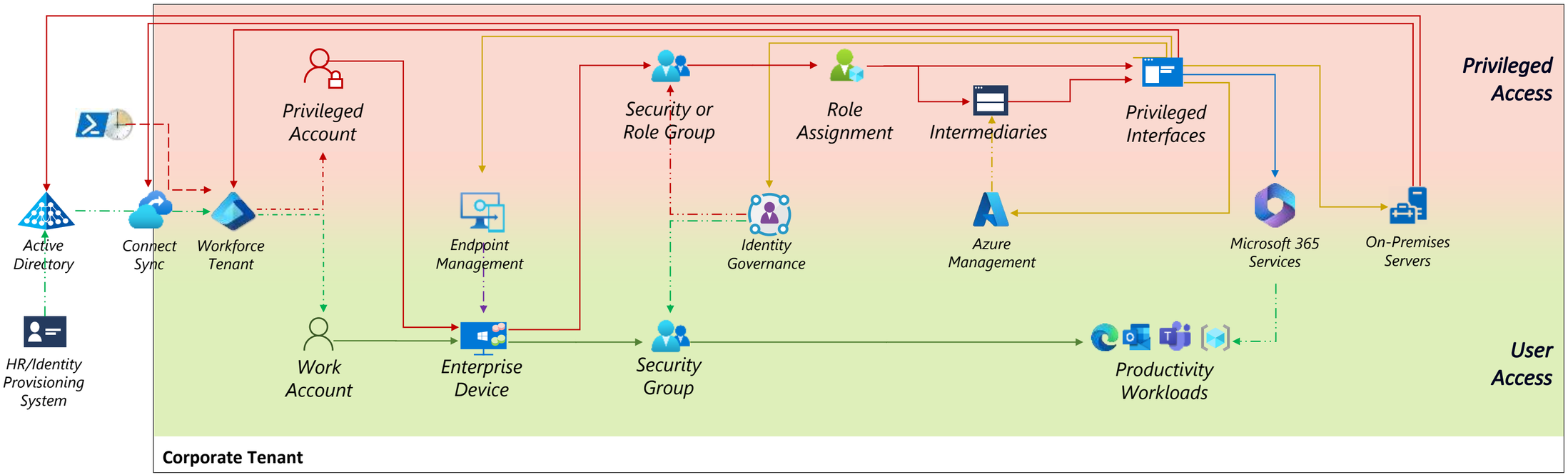


Admins login via FIDO2 only

glueck kanja

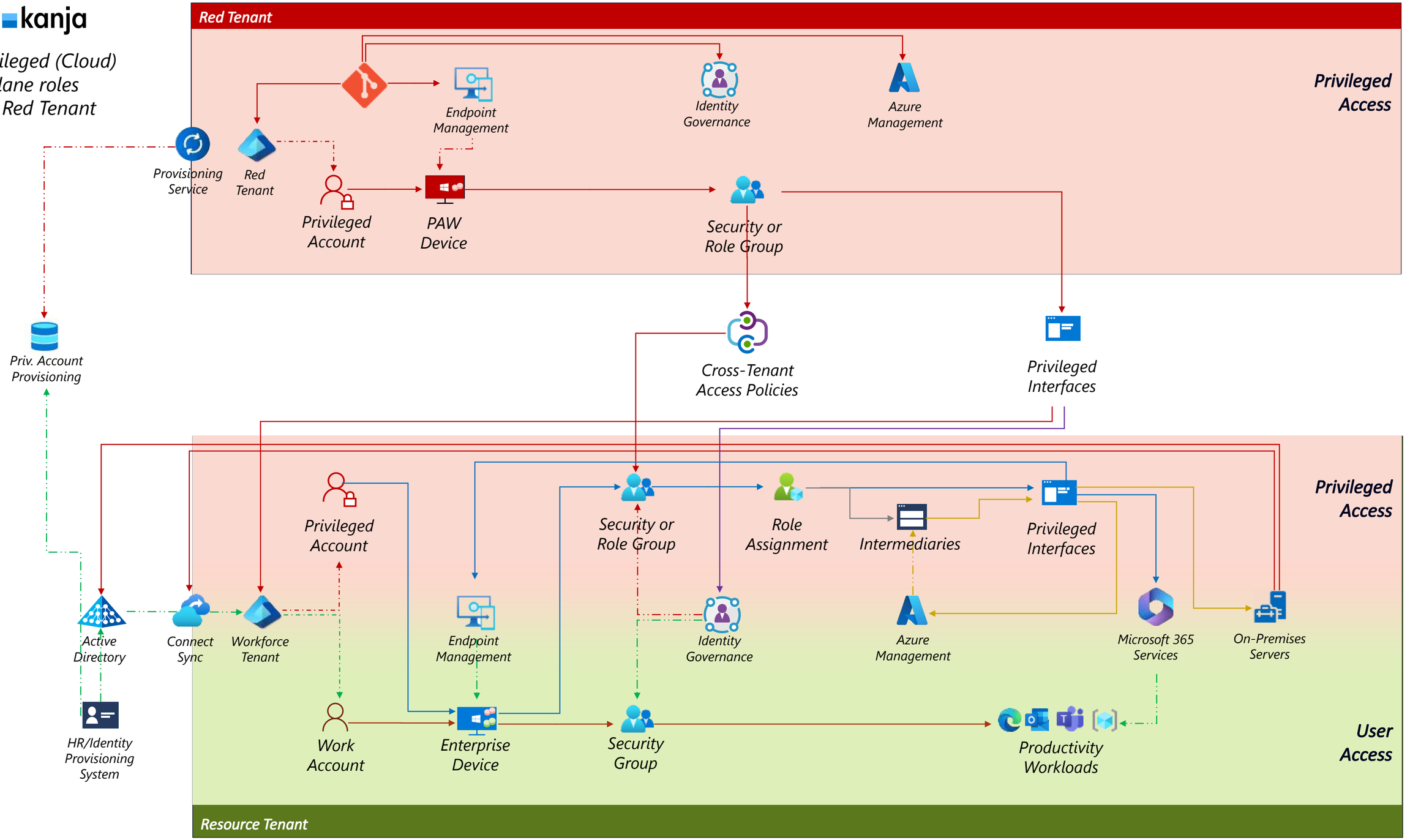
Initial situation
Customer uses privileges on Enterprise Device

- Control Plane
- Management Plane
- Indirect Control Plane



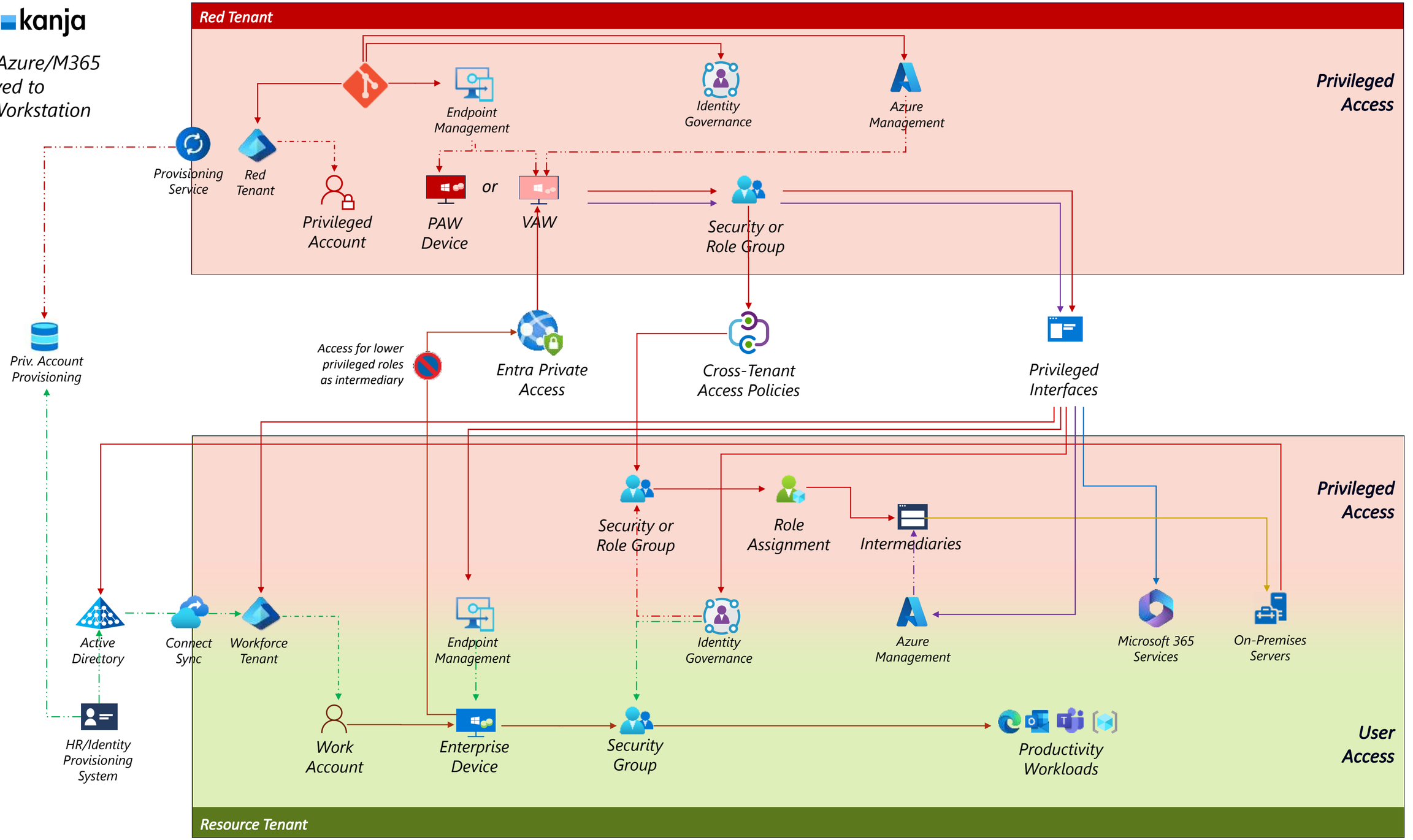
glueck kanja

High-Privileged (Cloud) Control Plane roles moved to Red Tenant



glueck kanja

Sensitive Azure/M365 Roles moved to Support Workstation



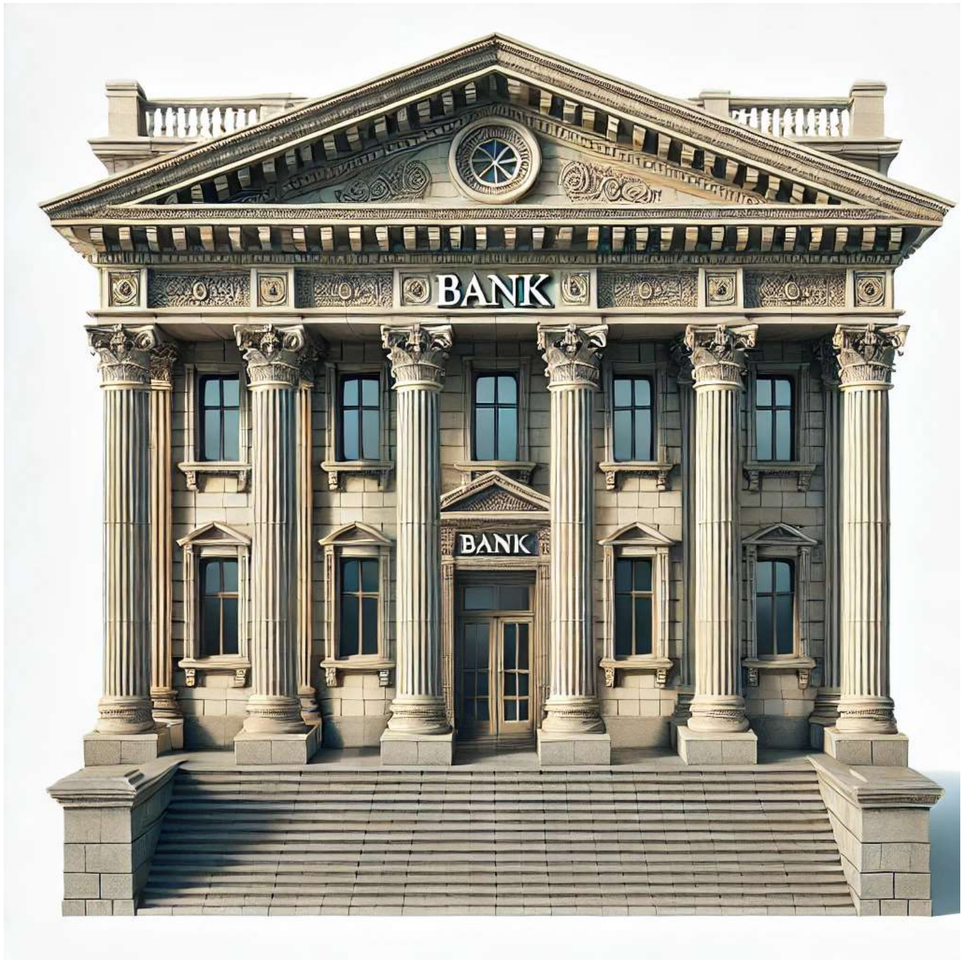
glueck kanja

Intra-Tenant Isolation

All Tiers in one Tenant

glueck kanja

Inter-Tenant Isolation

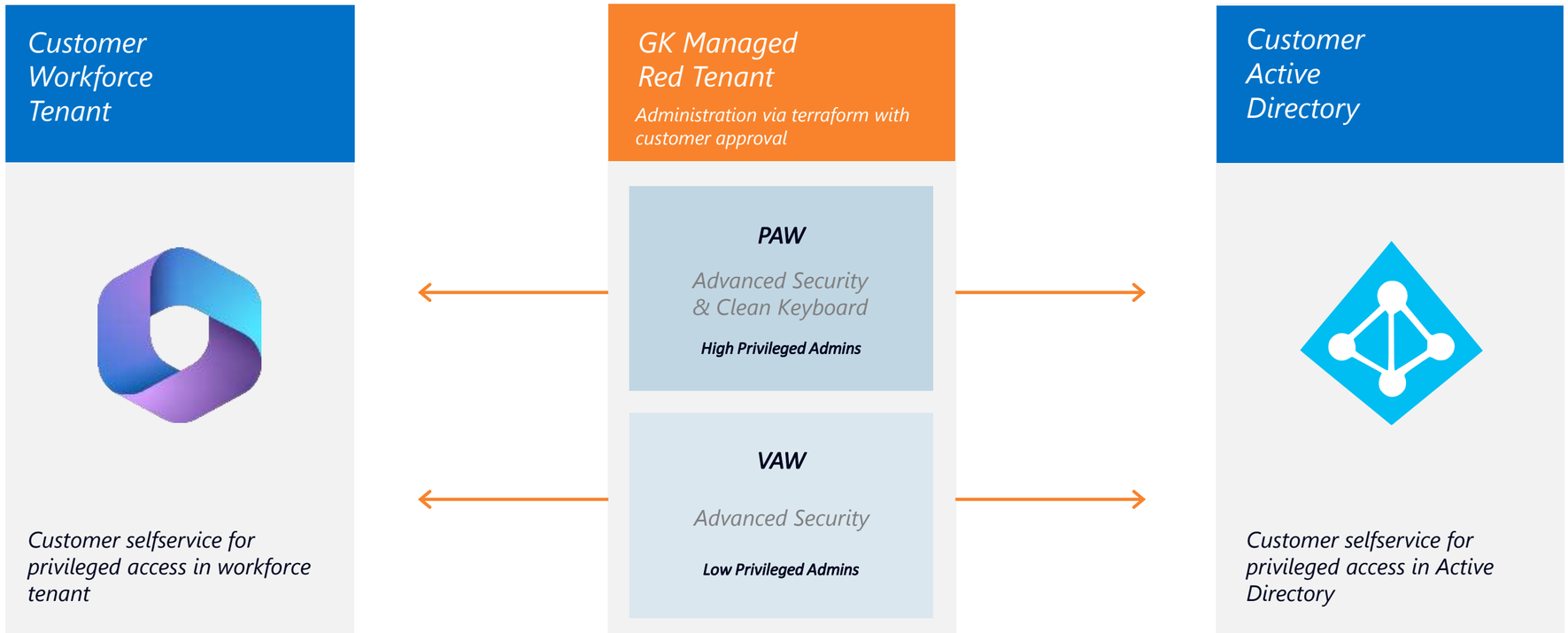


Tier 2

Tier 0 & Tier 1

glueck kanja

Managed Red Tenant



Dedicated highly secured Tenant (Managed as Code)	Secured access to hybrid/multi-cloud environment(s)	Endpoint Management for PAW/VAW	AVD Infrastructure and Connectivity for VAW	Privileged User and Self-service Management	CSOC Services for Red Tenant Environment	Extended CSOC Detections for Resource Tenant based on Red Tenant Signals[2]

Managed Service for Workplace, Azure and Security

Continuous Improvement by GK Blueprint

glueck kanja

Managed Red Tenant Building Blocks

Dedicated highly secured Tenant (Managed as Code)

- Deployment of Entra ID and Intune by Blueprint
- CI/CD Pipeline to manage Tenant Config as Code*

Secured access to hybrid/multi-cloud environment(s)

- Integration for SSO access to multi-cloud
- Access to on-premises infrastructure via VAW

Endpoint Management for PAW/VAW

- Deployment of PAW device by Blueprint
- Self-provisioning of Devices by Autopilot
- Automated process to upload Autopilot hash
- Application and Update Management
- Global Secure Access for Internet/SaaS

AVD Infrastructure and Connectivity for VAW

- Deployment of AVD by Blueprint
- Provisioning of AVD single hosts for admins
- Securing Private Access Agents in Red Tenant
- Isolation and connectivity for VAW endpoints
- CI/CD Pipeline to manage AVD as Code*

Privileged User and Self-service Management

- Provisioning by API & Lifecycle Workflows
- Manage resource tenant access by Entitlement
- Integration of automated on-/offboarding process
- Enhanced features for (MyAccount) self service

CSOC Services for Red Tenant Environment

- Integration with CSOC Foundation
- Deployment of Deep detections
- 24/7 Detection & Response

Extended CSOC Detections for Resource Tenant based on Red Tenant Signals[2]

- Detection of privileges outside of Red Tenant
- Detection of tier-breach in Resource Tenant

Managed Service for Workplace, Azure and Security

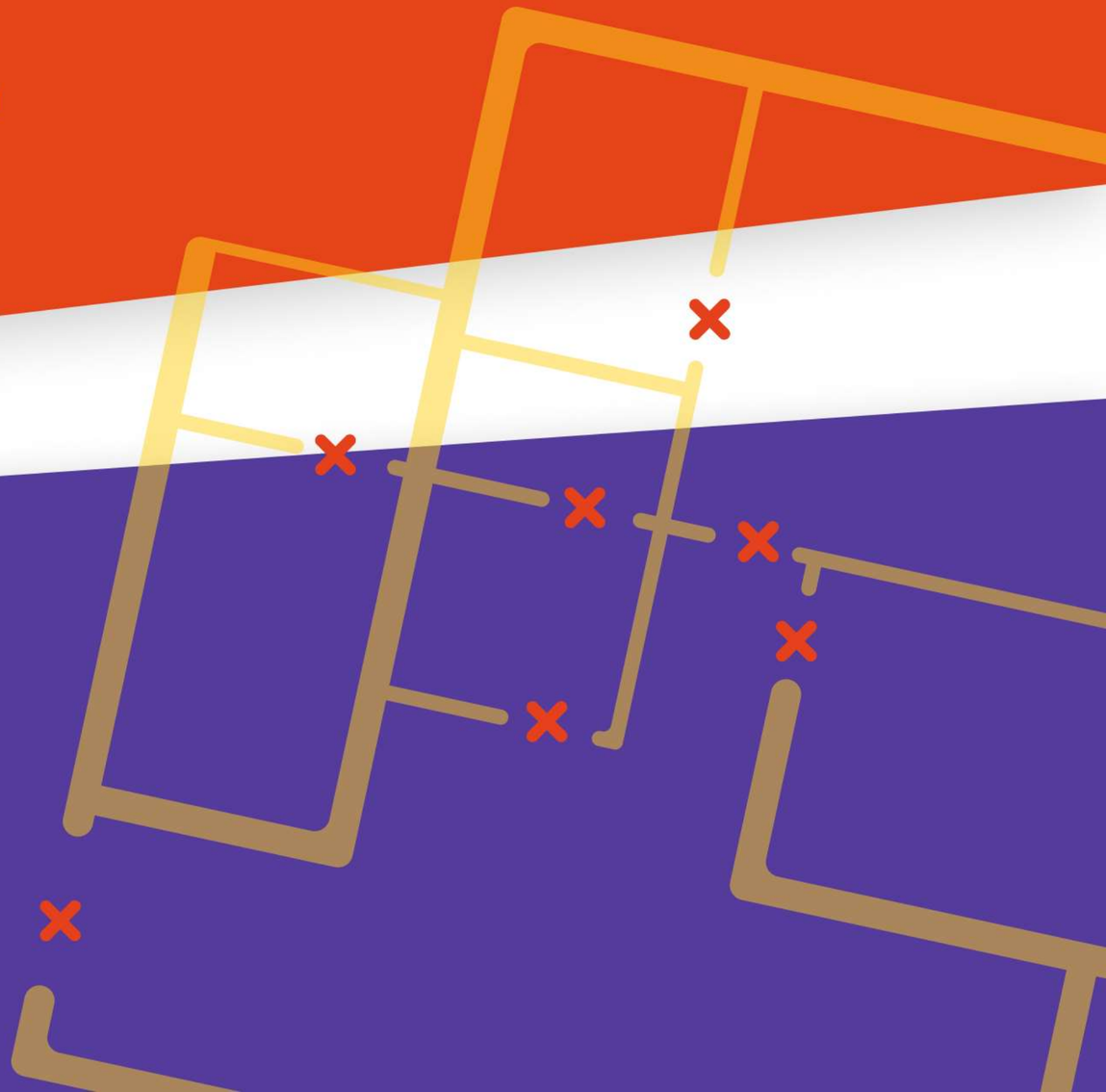
Continuous Improvement by GK Blueprint

[2] Configurations without programmatically or API access be applied interactively, [3] Only available for CSOC customers

*for CSOC Customers

NEW

Managed
RED TENANT



Cut Off Lateral Movement Paths

glueck kanja

Thanks!