

2024

Managed Red Tenant

Cut Off Lateral Movement Paths



Jan Geisbauer

— *Security Lead*

— *jan.geisbauer@glueckkanja.com*

 .../jangeisbauer/

Thomas Naunheim

— *Cyber Security Architect*

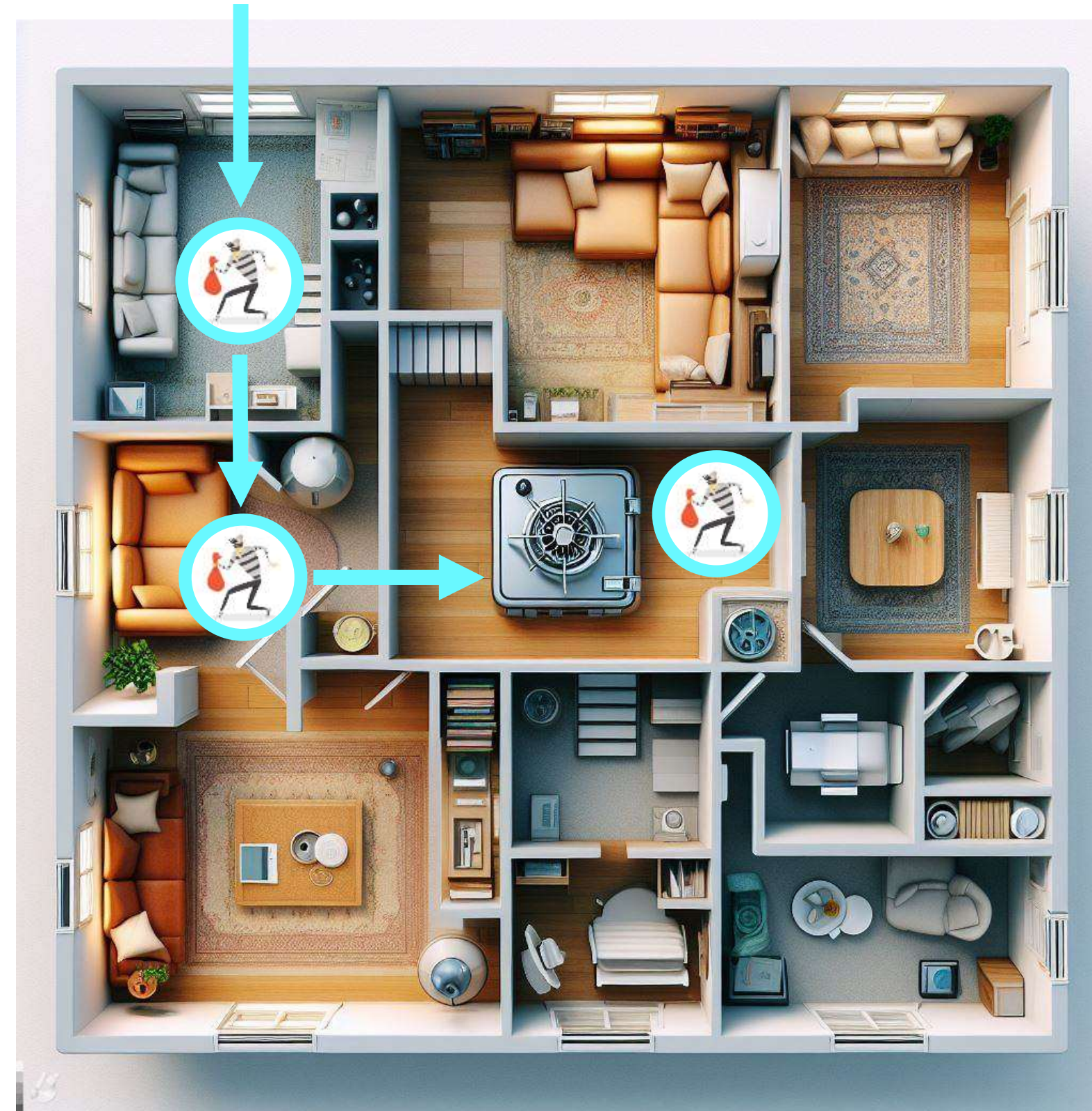
— *thomas.naunheim@glueckkanja.com*

 .../thomasnaunheim/



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 | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog | Search

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

Getting Started

Contribute

FAQ

Take a Tour

Blog

Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side

show sub-techniques

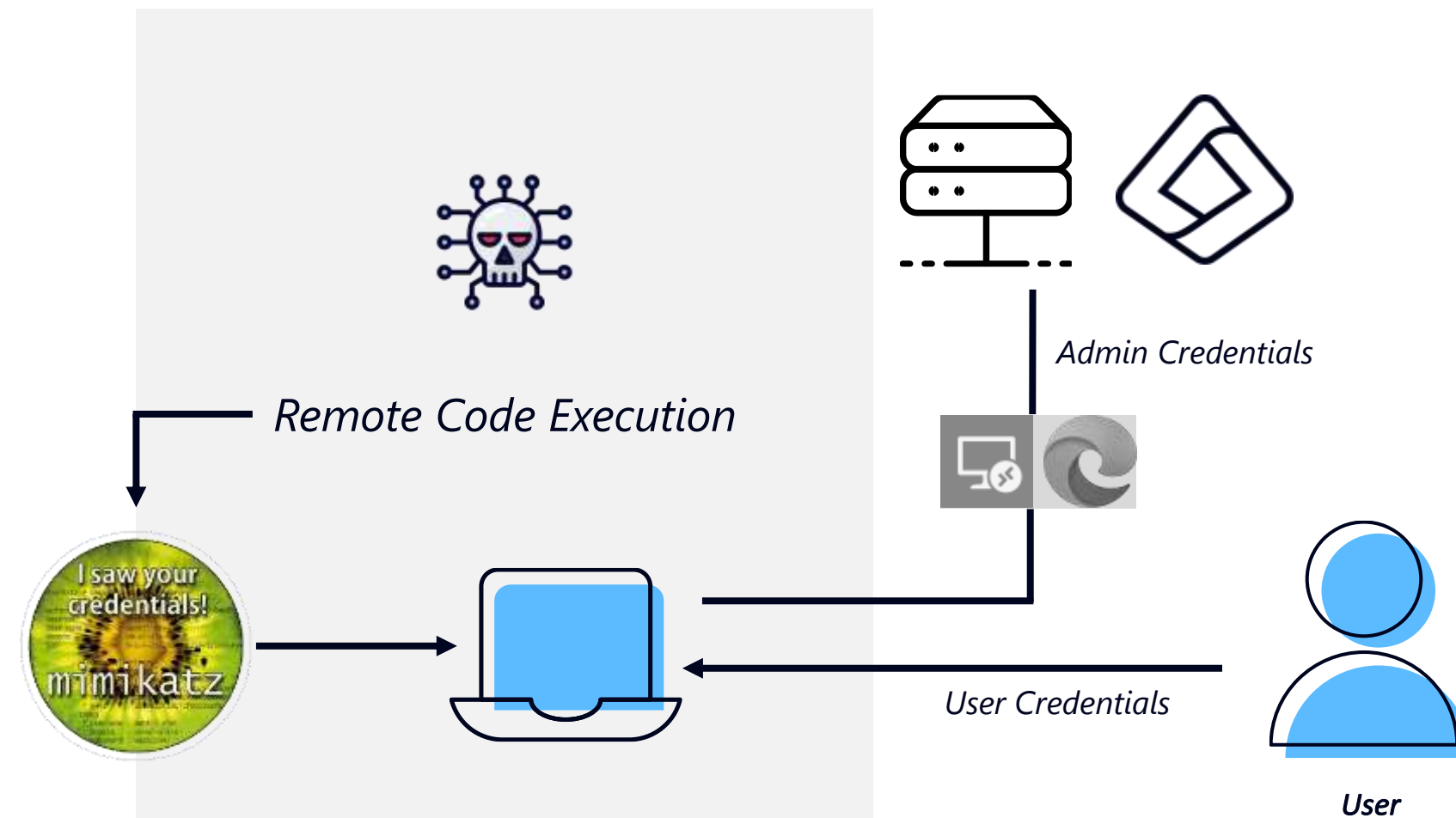
hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (1)	Create or Modify System Process (4)	Execution Guardrails (1)	Direct Volume Access	Modify Authentication Process (8)	Cloud Service Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate	Data from Information Repositories (3)	Ingress Tool Transfer		Firmware Corruption
Search Victim-Owned		Valid Accounts (4)	Shared Modules		Event Triggered	Exploitation for Defense Evasion		Domain Trust Discovery			Multi-Stage Channels		Inhibit System Recovery
													Network Denial of Service (2)

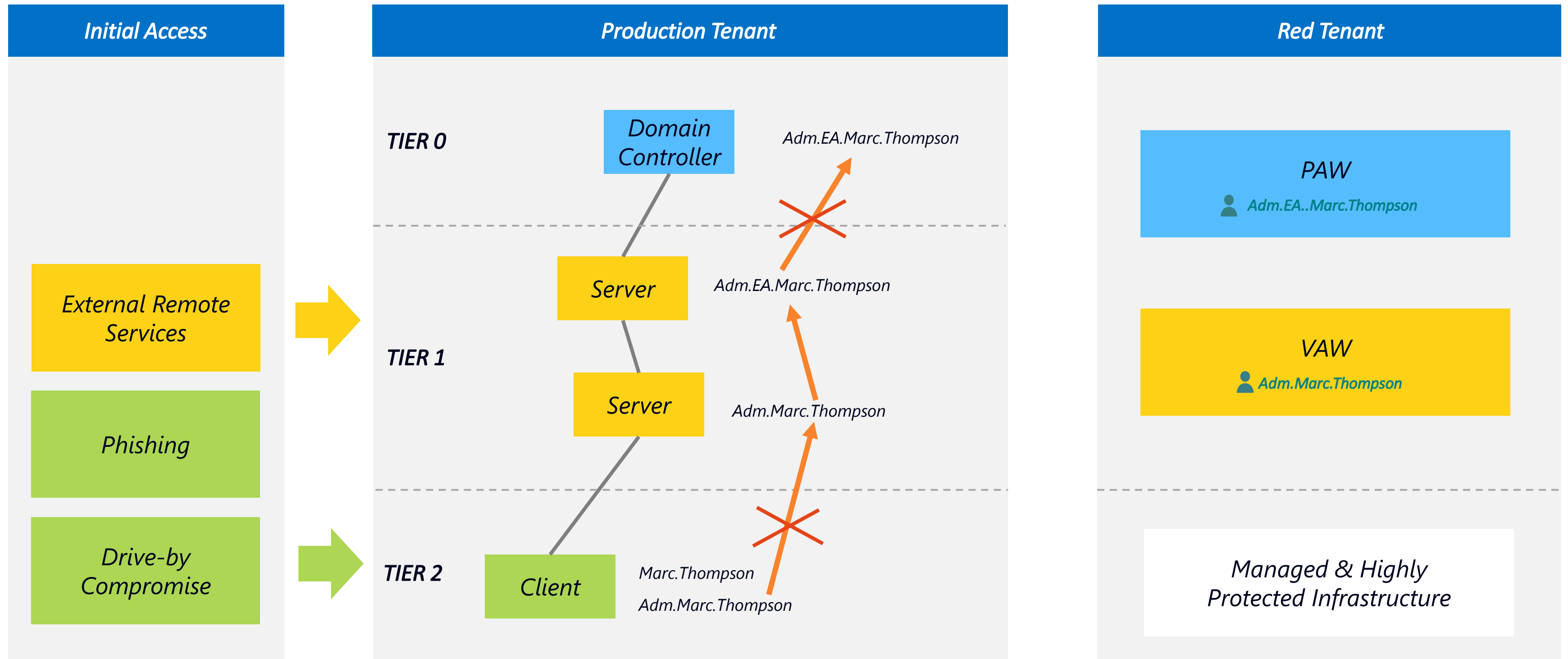
Initial Access



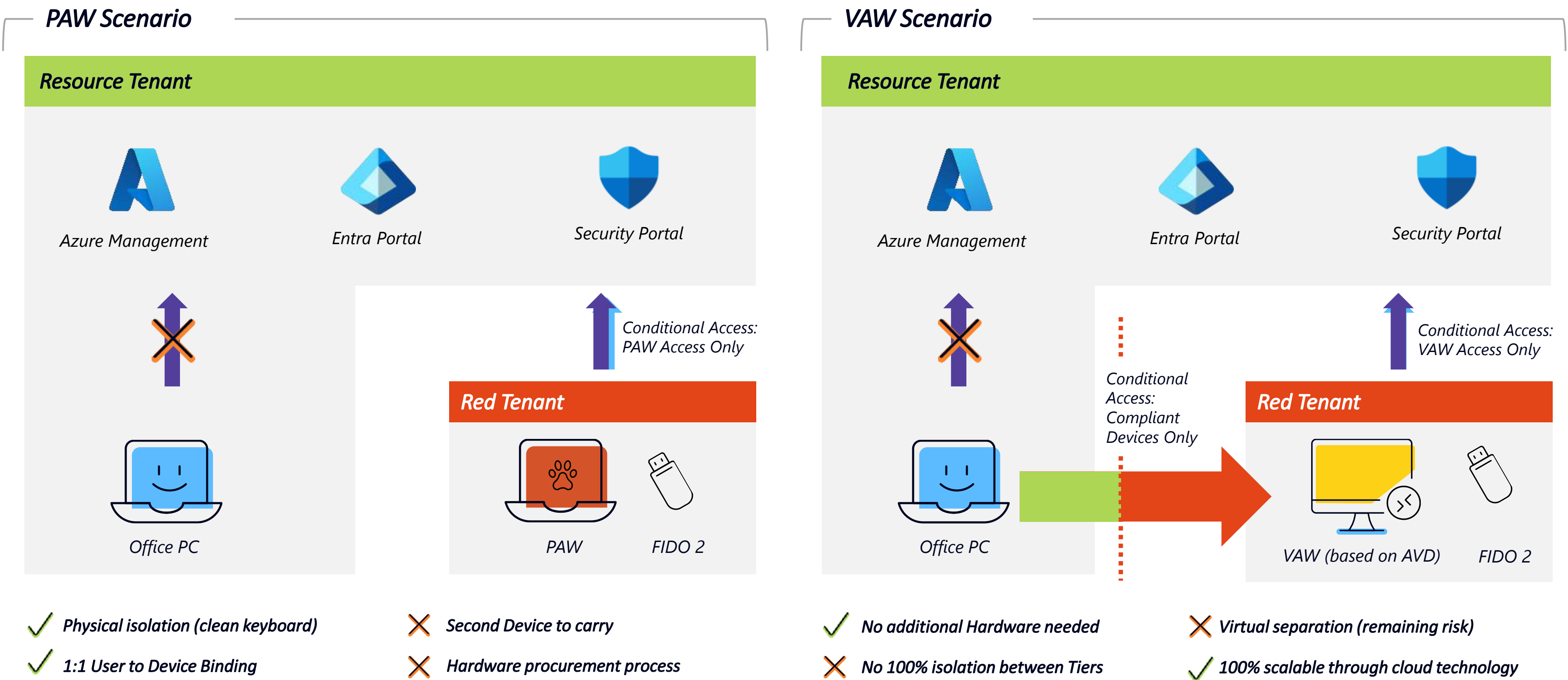
Privilege Escalation



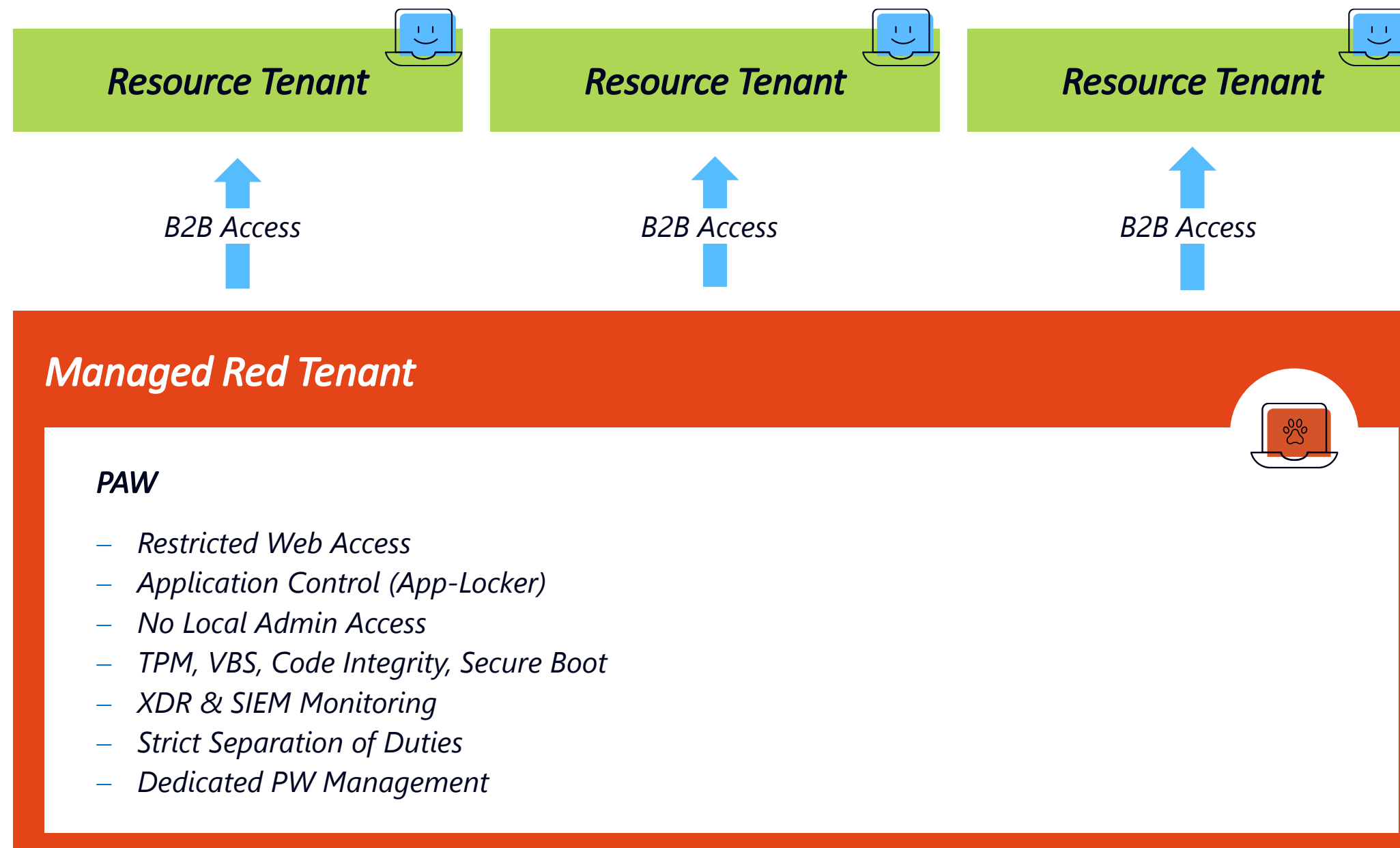
Lateral Movement through Privilege Escalation



PAW & VAW



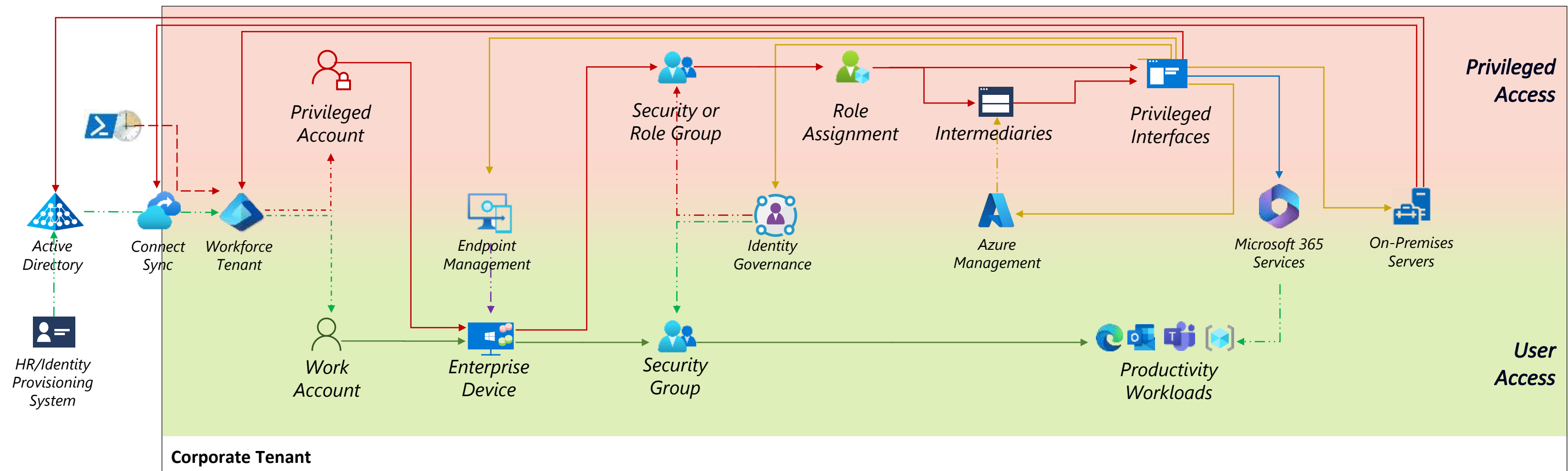
Highly Secure Working Environment PAW



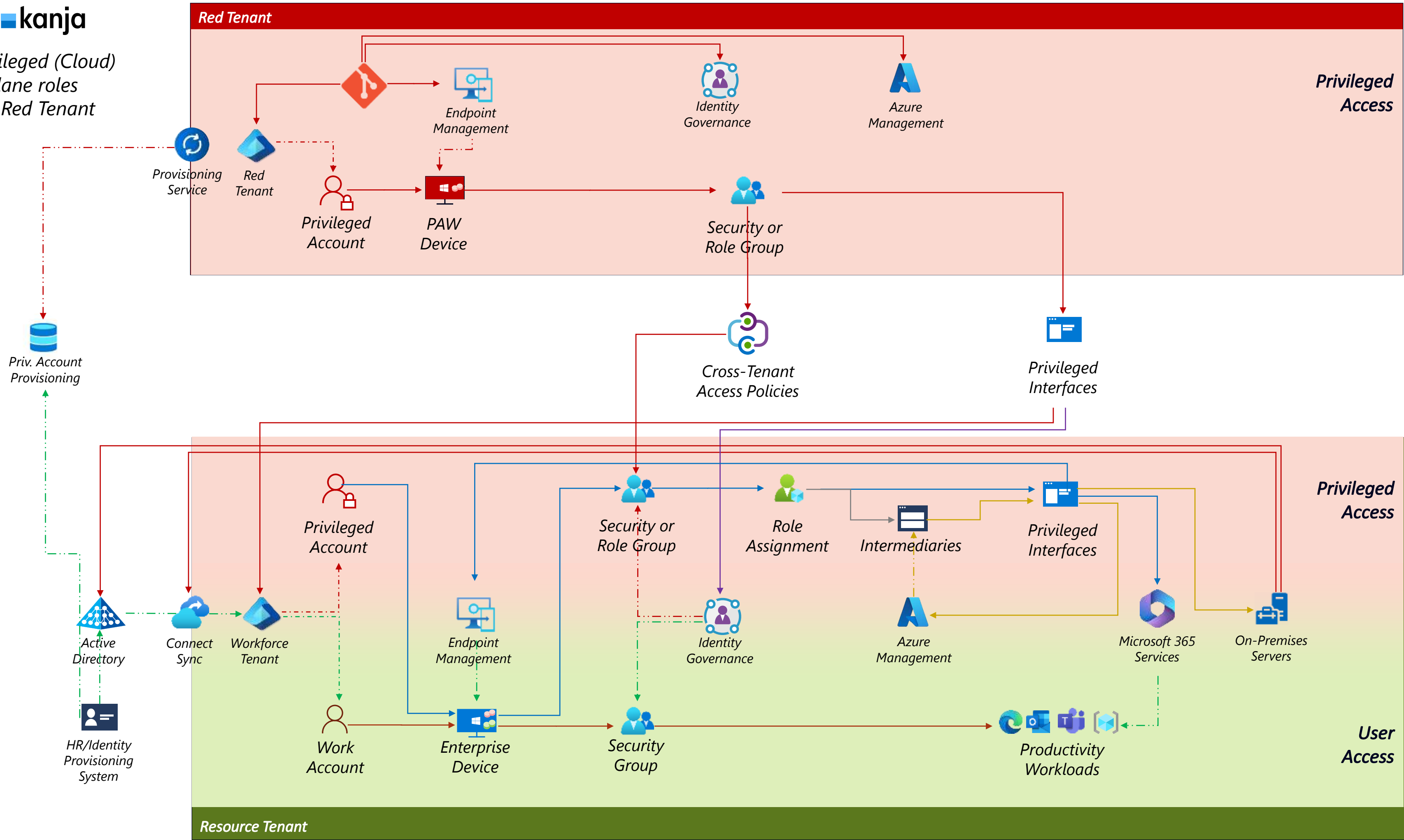
Admins login via FIDO2 only

Initial situation
Customer uses privileges
on Enterprise Device

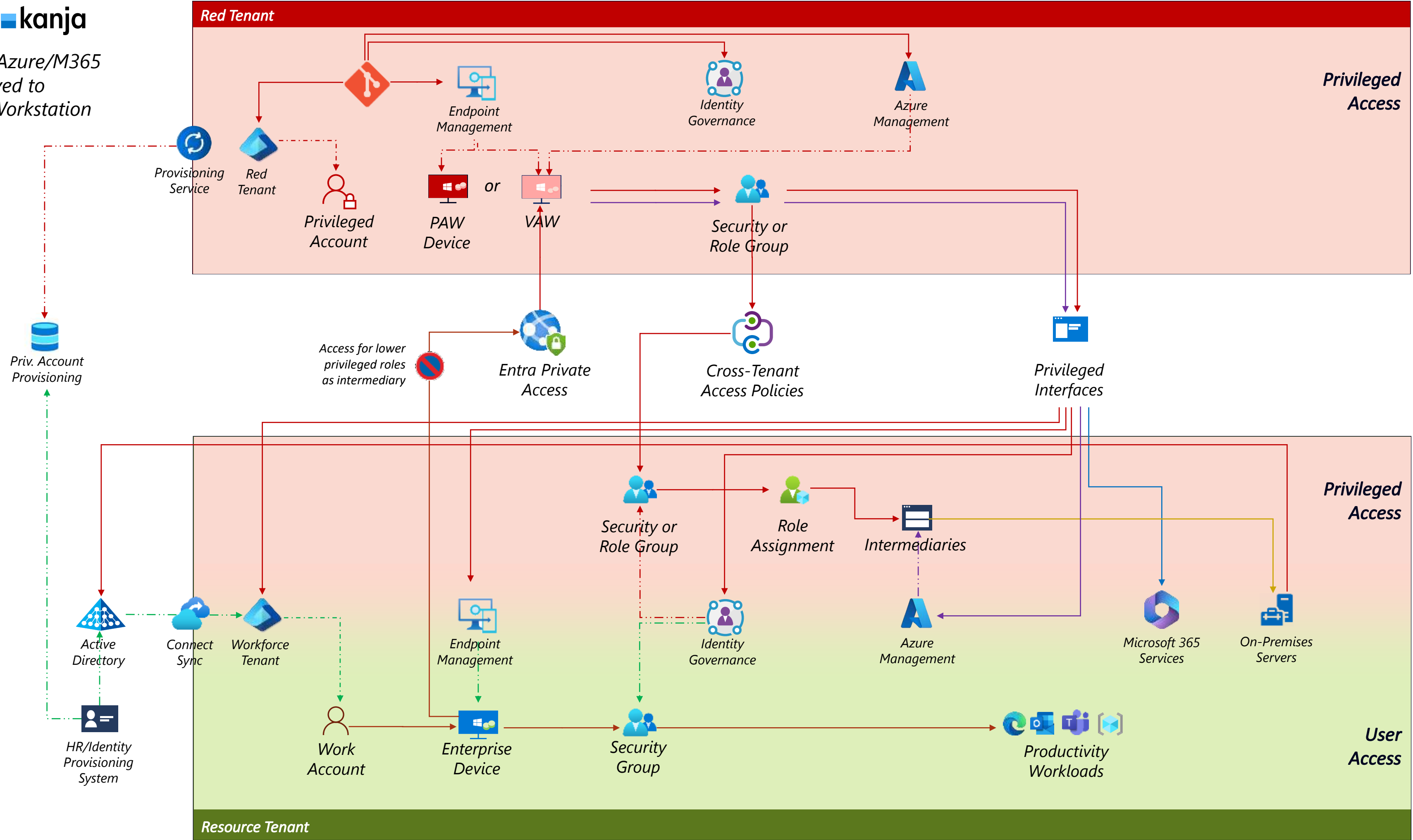
- Control Plane
- Management Plane
- Indirect Control Plane



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



Sensitive Azure/M365
Roles moved to
Support Workstation



Intra-Tenant Isolation

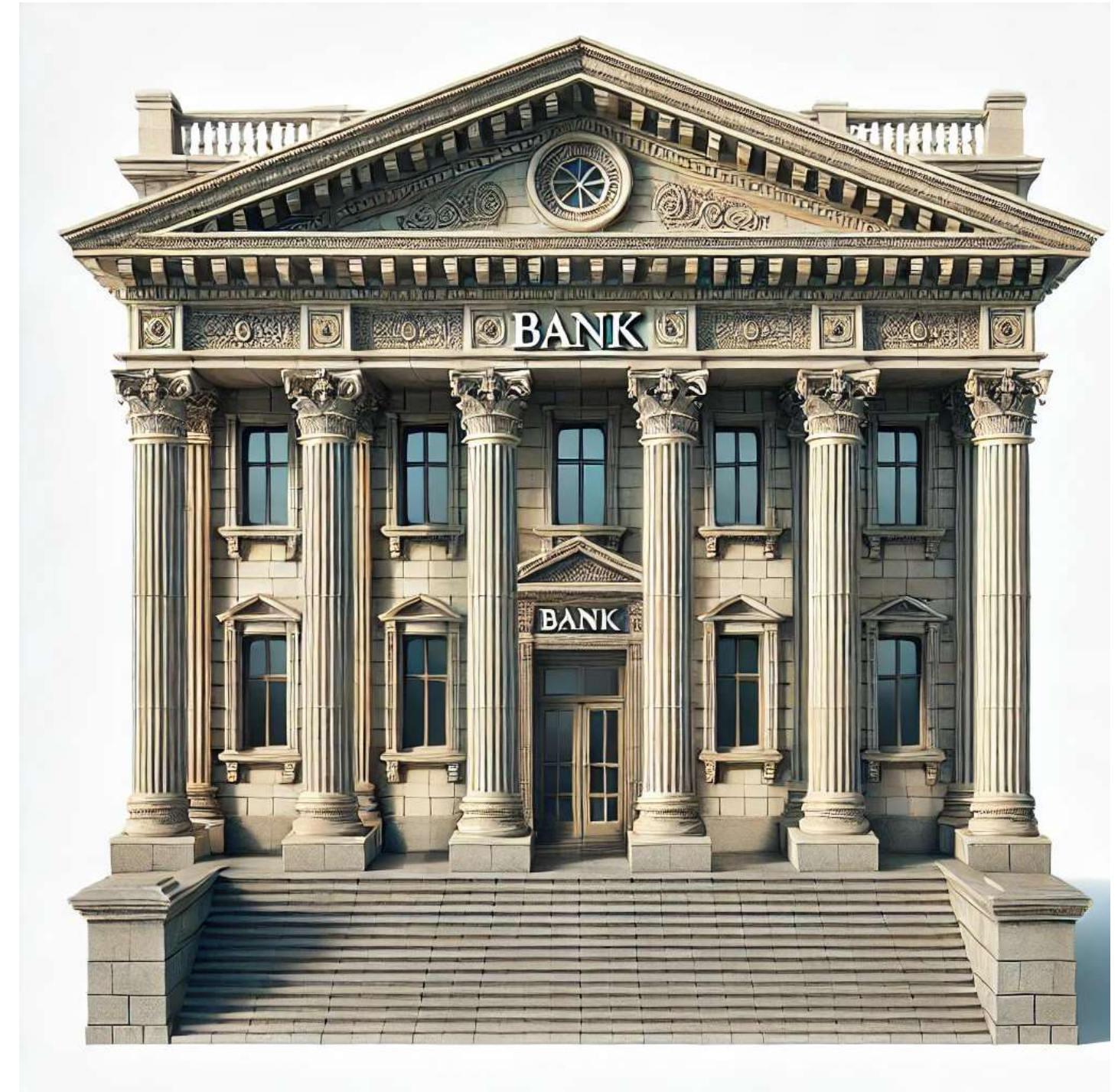


All Tiers in one Tenant

Inter-Tenant Isolation

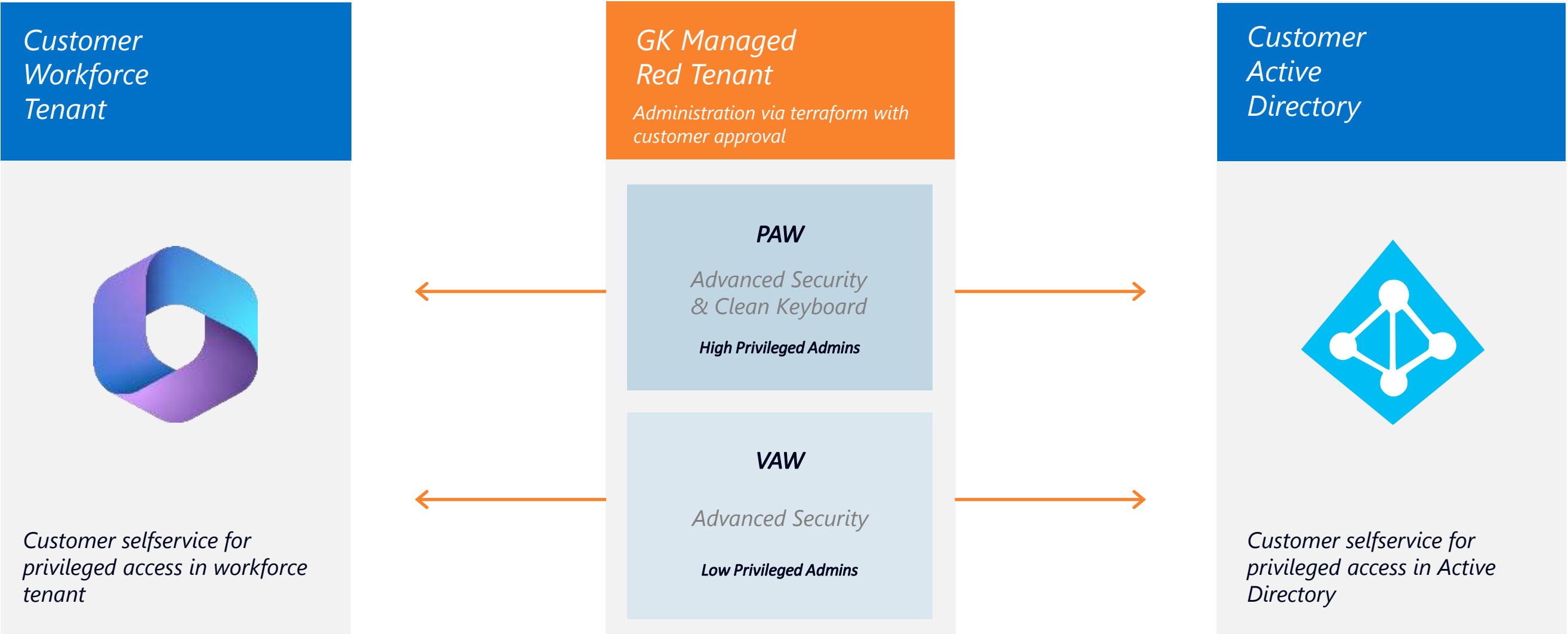


Tier 2



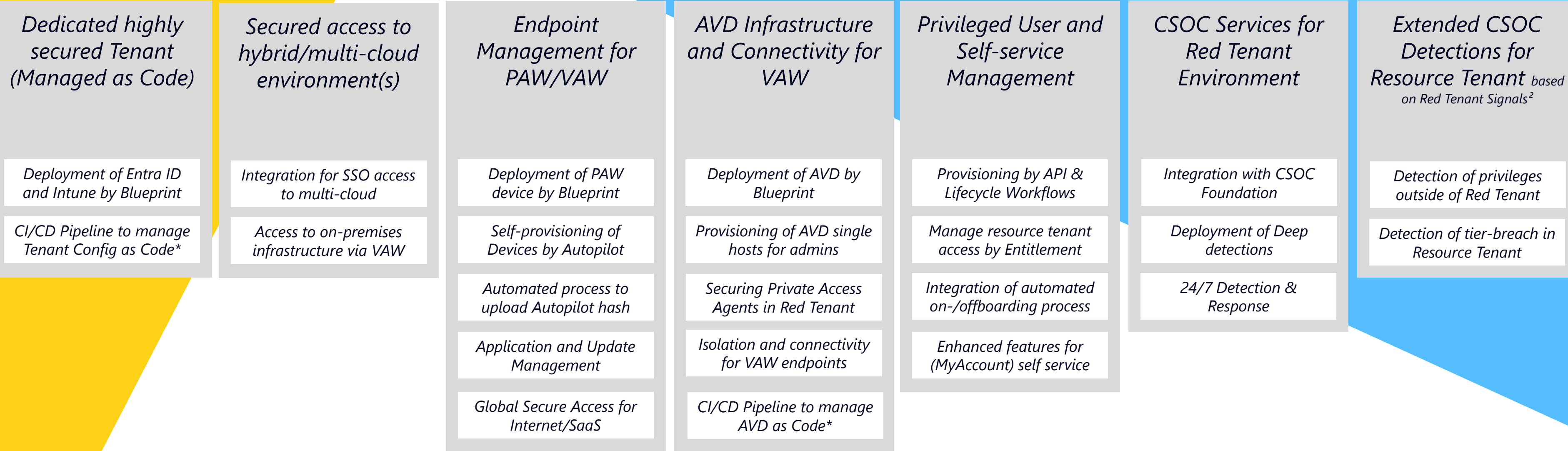
Tier 0 & Tier 1

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 <small>based on Red Tenant Signals²</small>
Managed Service for Workplace, Azure and Security						
Continuous Improvement by GK Blueprint						

Managed Red Tenant Building Blocks



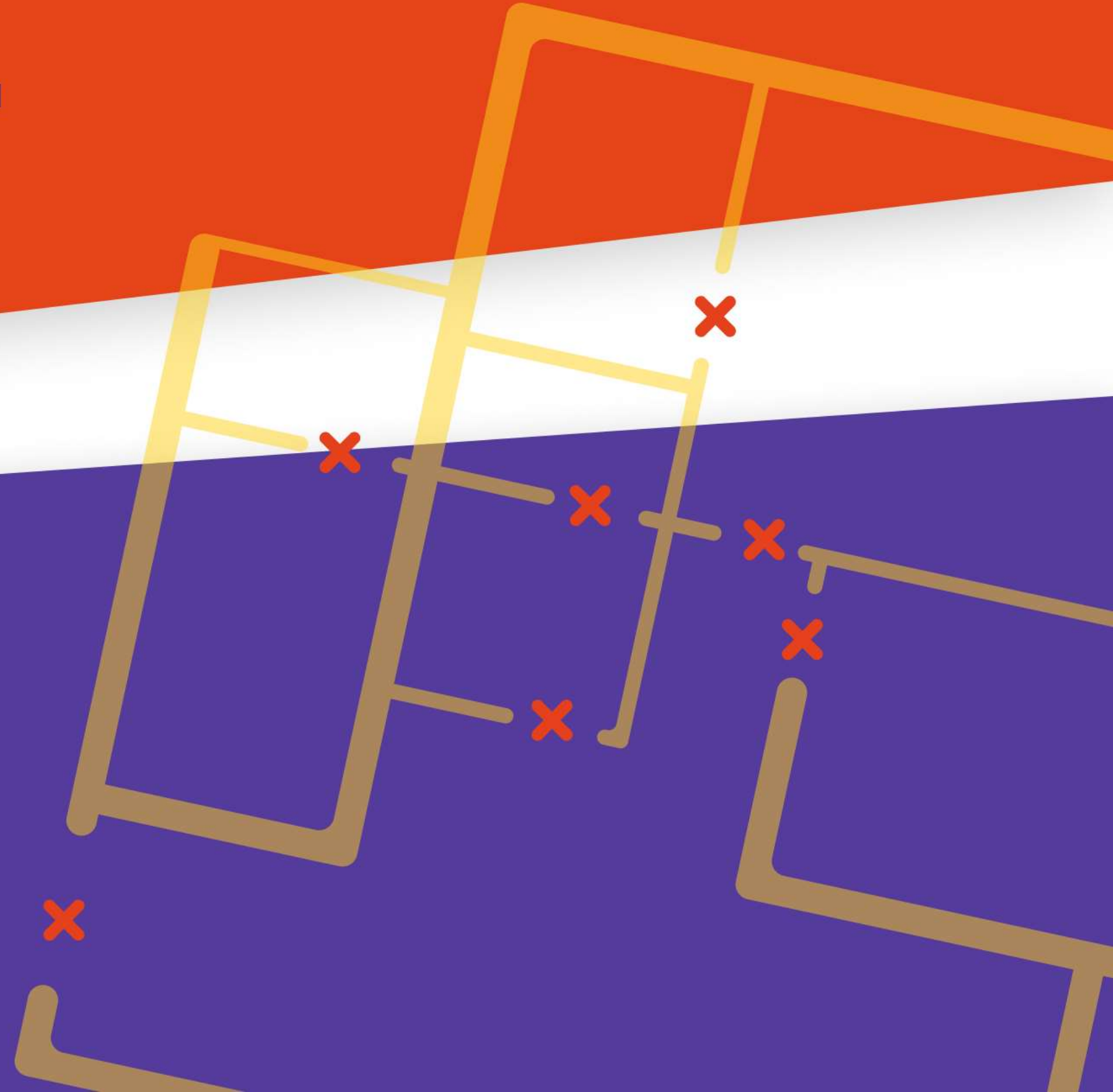
Managed Service for Workplace, Azure and Security

Continuous Improvement by GK Blueprint

NEW

Managed RED TENANT

Cut Off Lateral
Movement Paths





Thanks!

