TRUESEC

How To Use Speed Bumps to Prevent Breach

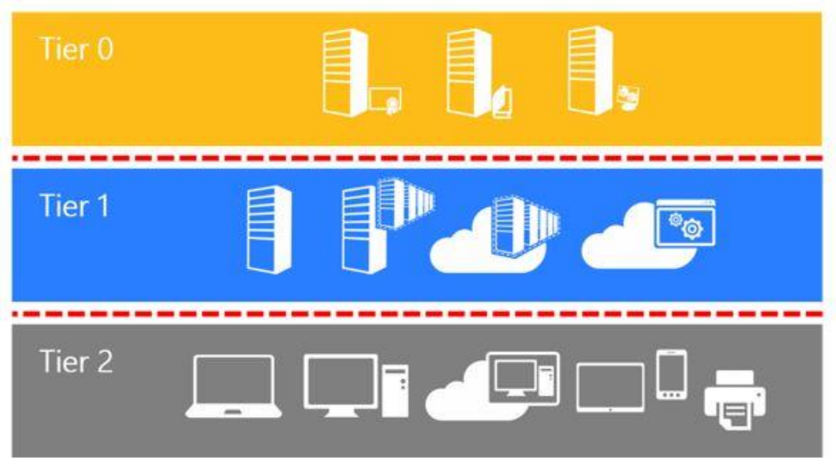
Mikael.Nystrom @truesec.se
Peter.Lofgren @truesec.se

Processes

- Cleanup
  - Old user accounts
  - High-privileged access
  - Inactive systems
- Patch Management
  - Reversed patching
- Lifecycle
  - Everything has a beginning and an end

Tiering / Enterprise access model

- What is Tiering / Enterprise access model?
- Who is affected?
- How much does it cost?

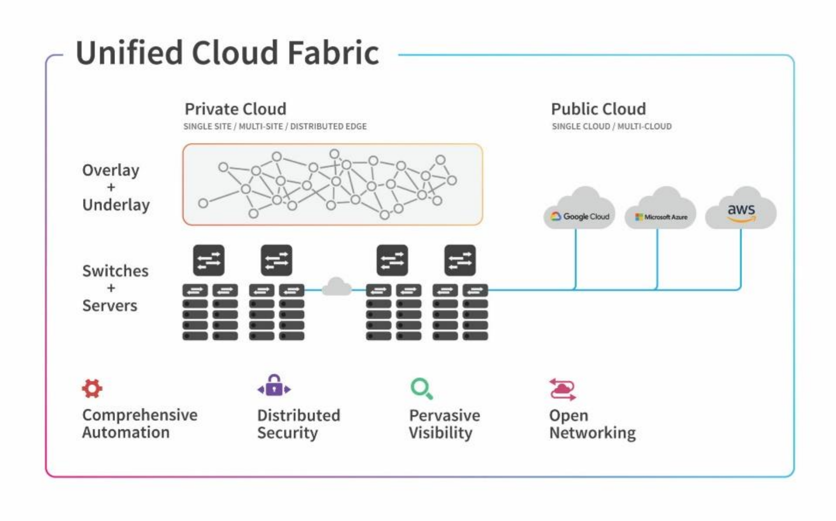


Local Access Password

- Prevent Lateral Movement
- Unique Passwords on
    - Servers
    - Network devices
    - Cloud services
    - Workstations

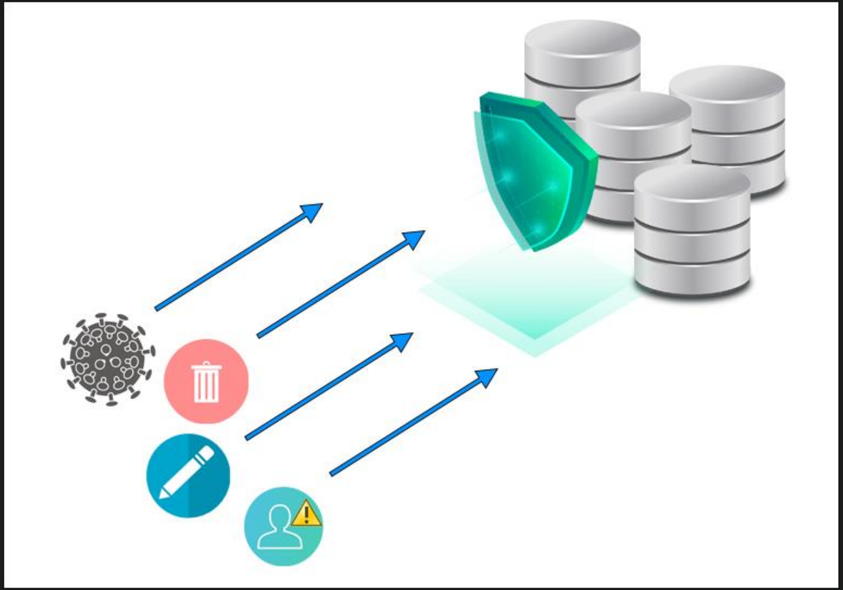
Fabric / Hypervisor Isolation

- Modern Isolation
- Hypervisor agnostic
- Restricted access
- With fewer applications comes less responsibility
- Guarded fabric and shielded VMs (Hyper-V only)



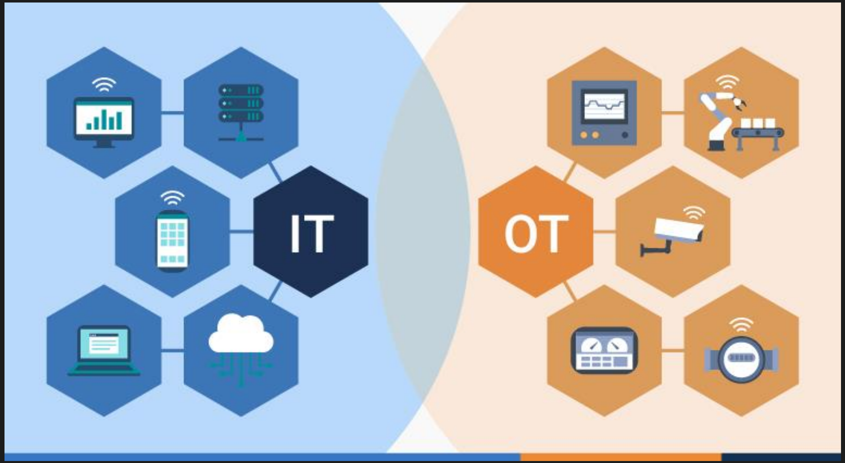
Backup

- Isolated
- One-Way
- Off-Line
- Off-Site
- Immutable
- Separate Authentication
- Separate Storage



IT and OT

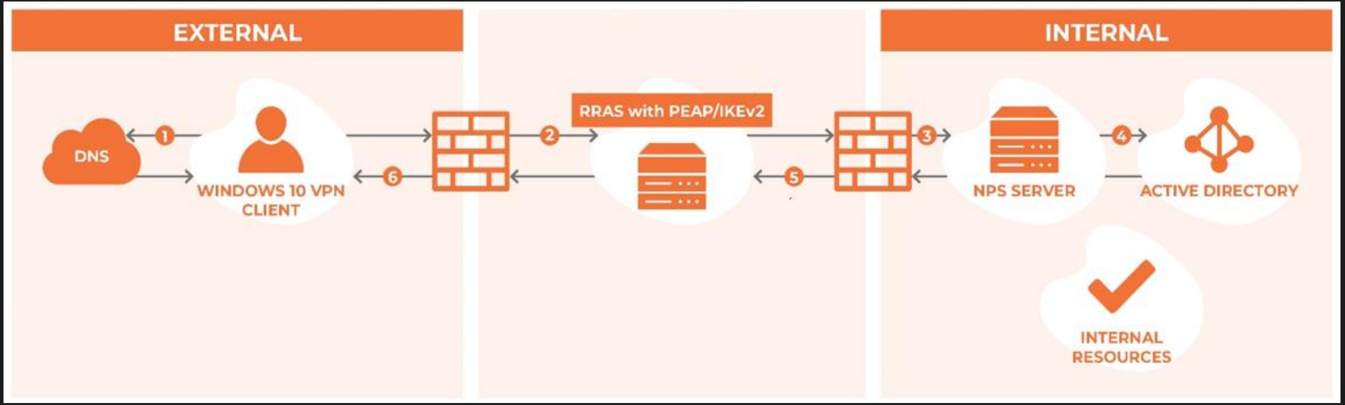
- Do your IP-cameras really need to reach the HR system?
- Who needs access?
- From where should access be possible?



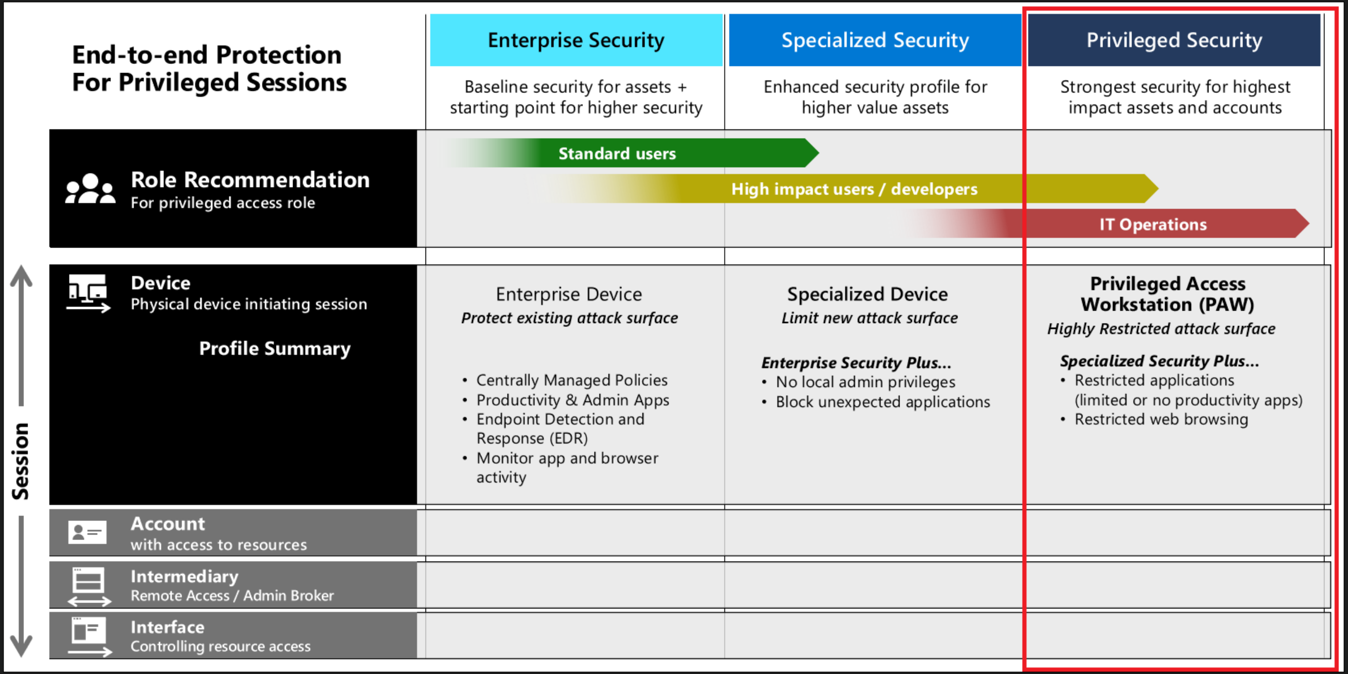
TRUESEC

VPN / Remote Access

- Protect yourself from password spray
- Certificate Based
- Multifactor Authentication
- Managed Devices
- Administrative Access



Privileged Access Workstations



End-to-end Protection For Privileged Sessions	Enterprise Security Baseline security for assets + starting point for higher security	Specialized Security Enhanced security profile for higher value assets	Privileged Security Strongest security for highest impact assets and accounts
Role Recommendation For privileged access role	Standard users	High impact users / developers	IT Operations
Device Physical device initiating session **Profile Summary**	Enterprise Device *Protect existing attack surface* • Centrally Managed Policies • Productivity & Admin Apps • Endpoint Detection and Response (EDR) • Monitor app and browser activity	Specialized Device *Limit new attack surface* ***Enterprise Security Plus…*** • No local admin privileges • Block unexpected applications	**Privileged Access Workstation (PAW)** ***Highly Restricted attack surface*** ***Specialized Security Plus…*** • Restricted applications (limited or no productivity apps) • Restricted web browsing
Account with access to resources			
Intermediary Remote Access / Admin Broker			
Interface Controlling resource access			

Windows Admin Center

- Remote PowerShell
- Non-interactive logon
- Password in memory on source device
- Multitasking

Computer and Operating System

- UEFI
- Secure Boot
- TPM
- Bitlocker
- AppLocker
- Security Baselines
- Shielding VMs

TRUESEC

Thank you

www.truesec.com

x.com/truesec

linkedin.com/company/truesec