Microsoft Security

Securing Privileged Access

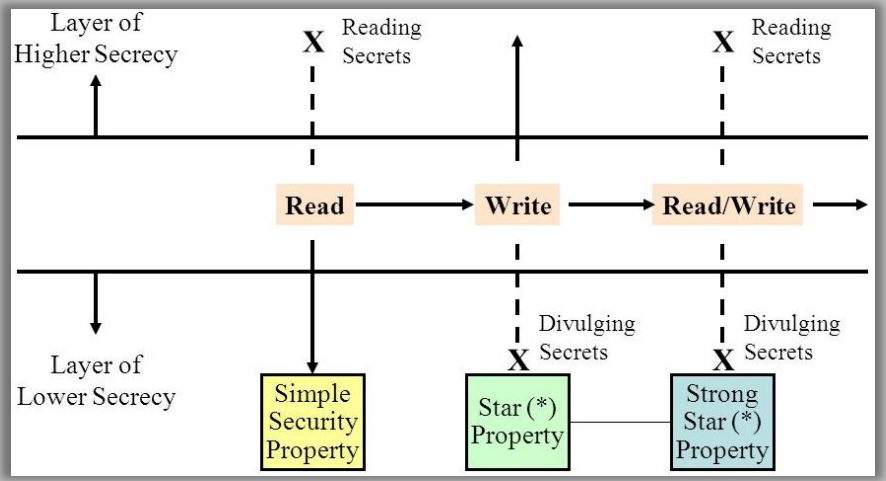
Privileged Access Workstations

Privileged Access strategy

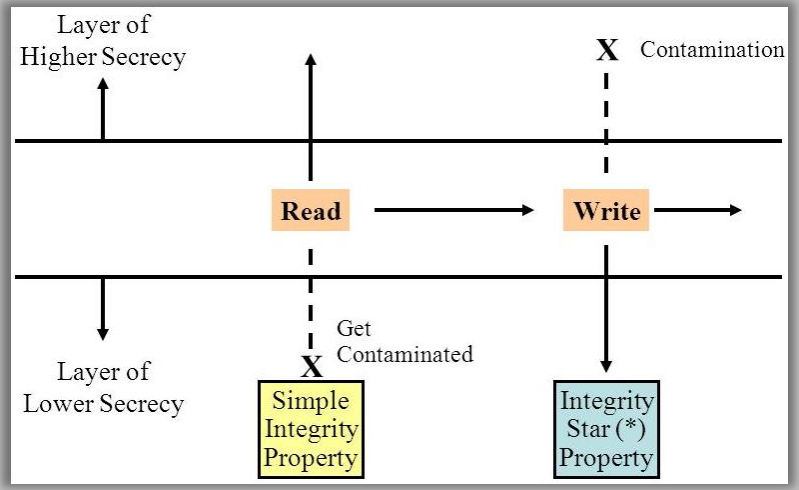
- Securing Privileged Access has two simple goals
  1. Strictly limit the ability to perform privileged actions to a few authorized pathways
  2. Protect and closely monitor those pathways

- Strategy is to:
  - Build a ‘closed loop’ system for privileged access
  - Ensure only trustworthy ‘clean’ devices and intermediaries are used
  - Control which accounts are allowed to perform privileged tasks

BELL-LA PADULA MODEL



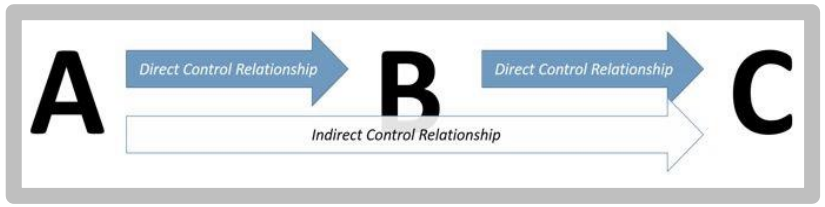
BIBA MODEL



Microsoft's privileged access guidance is based on the long-standing security principles represented in these (and other) security models, such as:

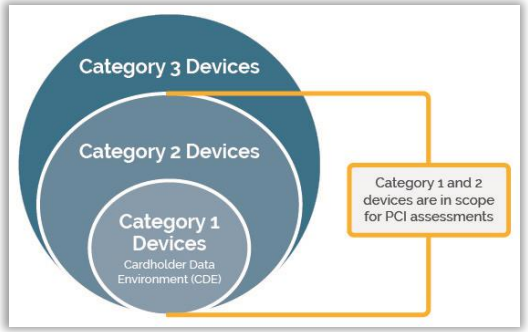
- Trust is transitive ("infectious" in PCI-DSS language).
- Any subject in control of an object is a security dependency of that object.

"Attackers think in graphs": Trust transitivity and security relationships between objects

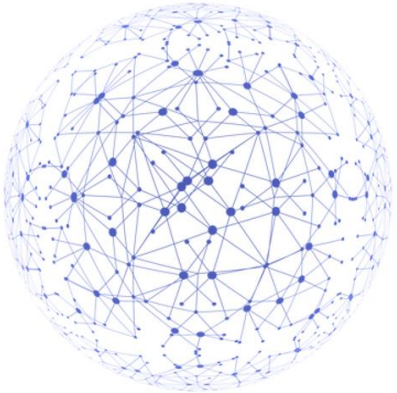


- These principles are represented in many other models as well, not just in Microsoft's guidance:

PCI-DSS



NCSC Security Architecture Anti-Patterns



Zero Trust Frameworks

NIST National Institute of Standards and Technology

Microsoft

FORRESTER®

UK NCSC stance on secure privileged access

Maintain level of assurance in systems used to manage cloud services

UK National Cyber Security Centre (NCSC) Antipatterns - Anti-pattern 1: Browse-up' for administration

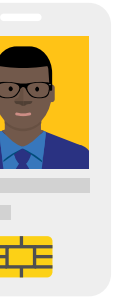
When administration of a system is performed from a device which is less trusted than the system being administered.

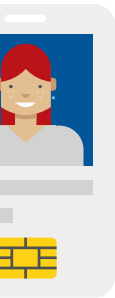
"if you don't have confidence in devices that have been used to administer or operate a system, you can't have confidence in the integrity of that system."

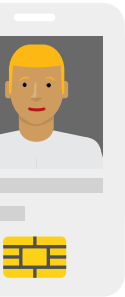
https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_3

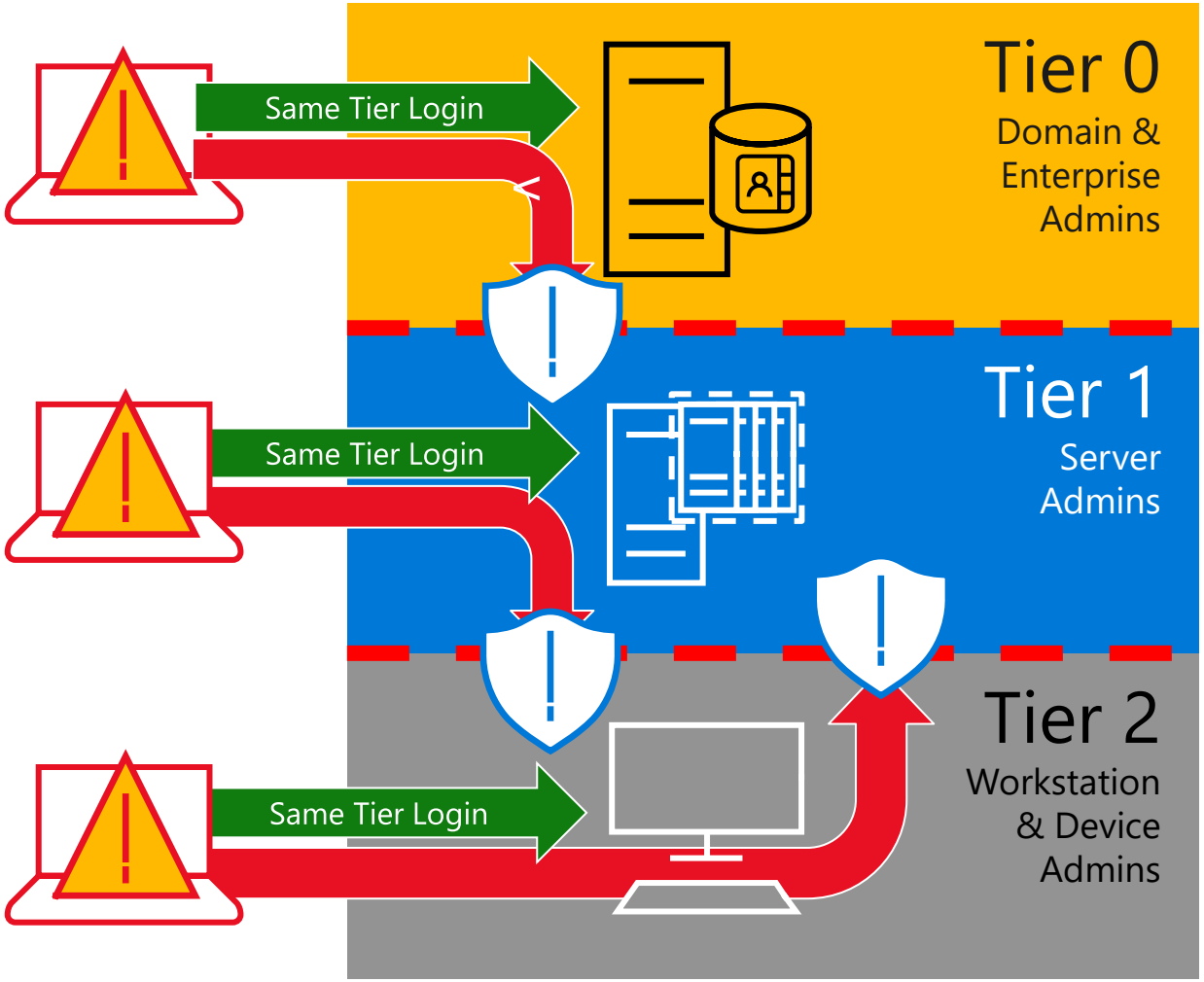
Privileged administration journey

First there was AD DS and the Tiered Admin Model

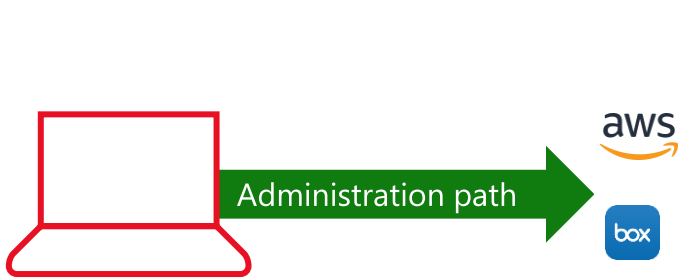


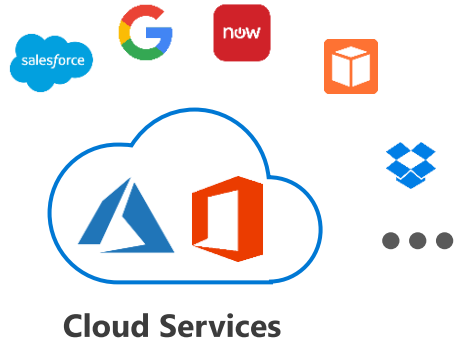






Access blocked between Tiers.



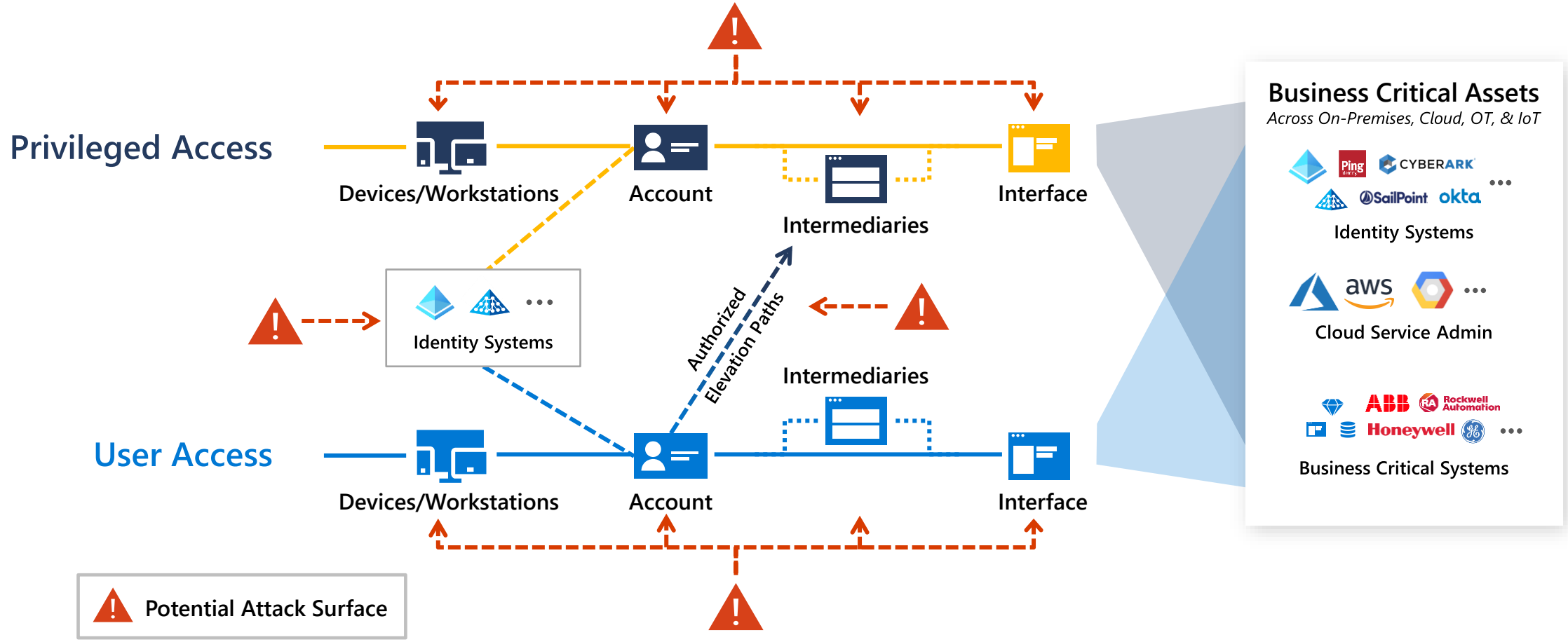


Then there was the cloud

There has always been productivity

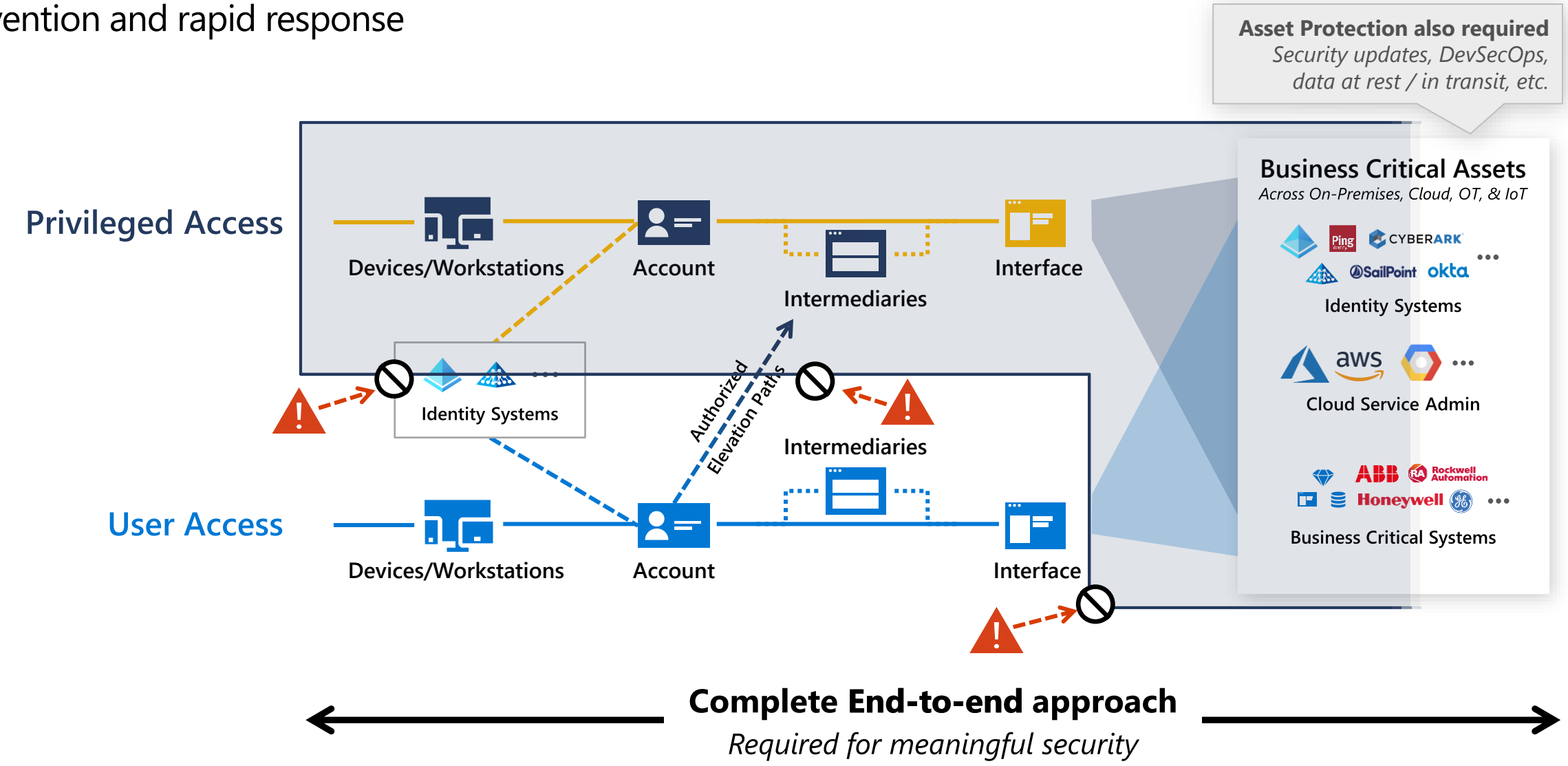
Attackers have options

to compromise privileged access



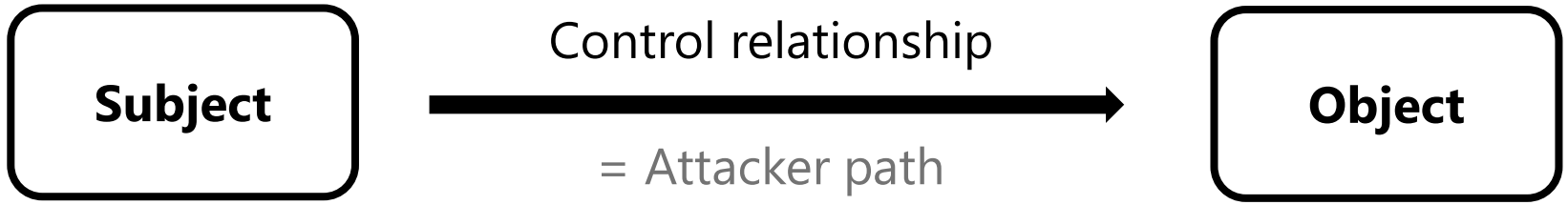
Limit and protect pathways to privileged access

Prevention and rapid response



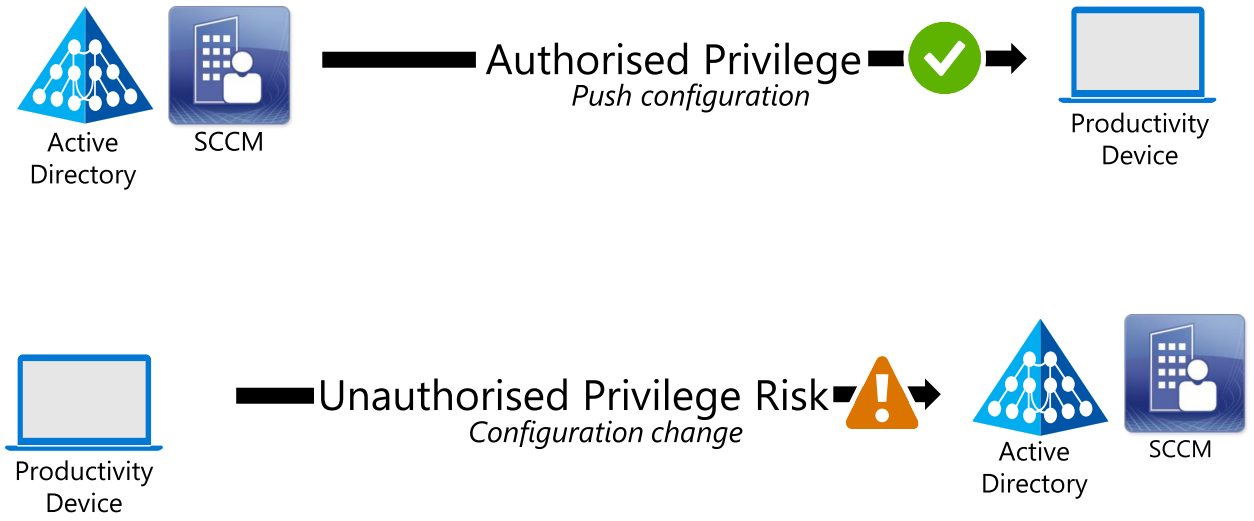
Clean Source and Clean Keyboard Principle

- Clean Source principle requires all security dependencies to be as trustworthy as the object being secured



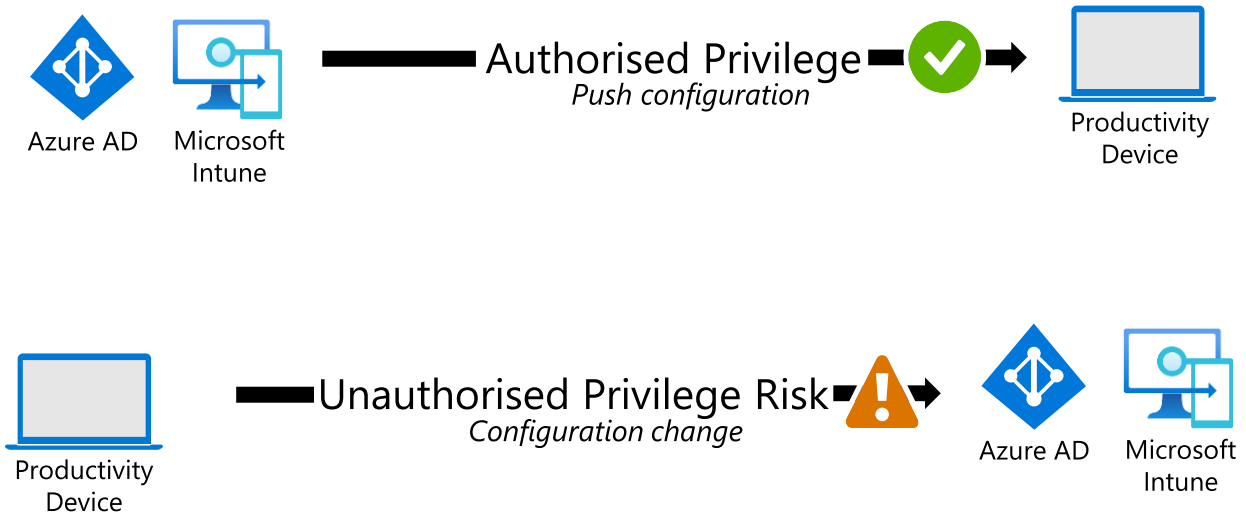
Clean Source and Clean Keyboard – Architecture and Design

- System is not dependent on lower trust systems



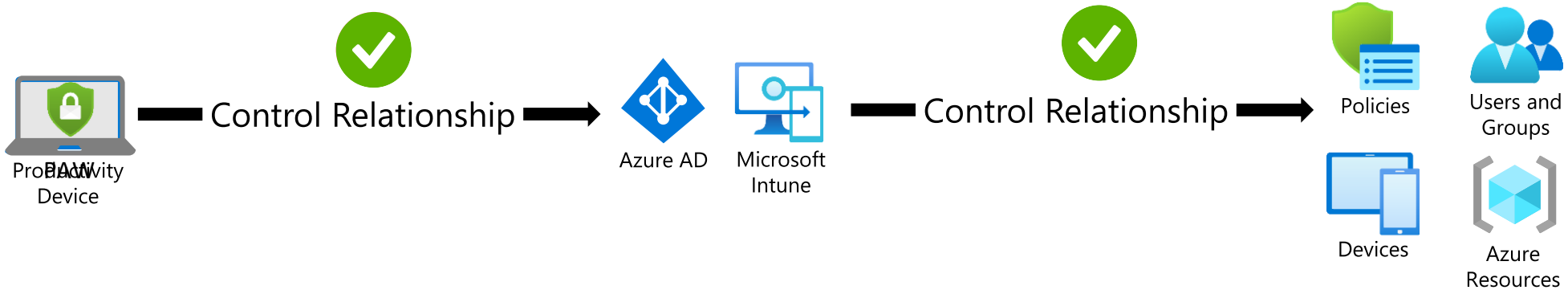
Clean Source and Clean Keyboard – Architecture and Design

- System is not dependent on lower trust systems



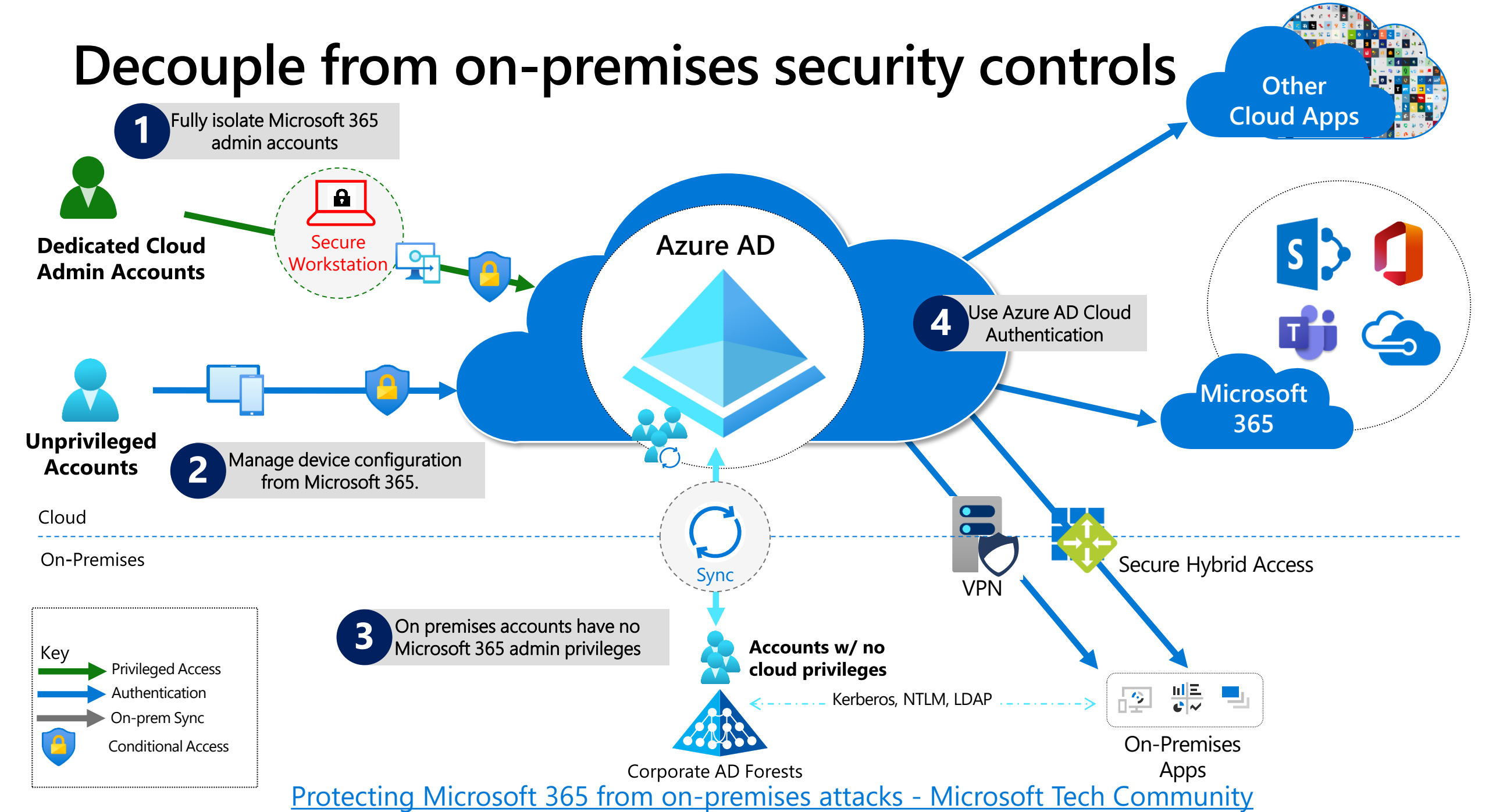
Clean Source and Clean Keyboard – Azure AD Control Relationship

- Extending this to Azure AD and Azure resources
- But system is not dependent on lower trust systems
- System controlling Azure AD needs to be trusted



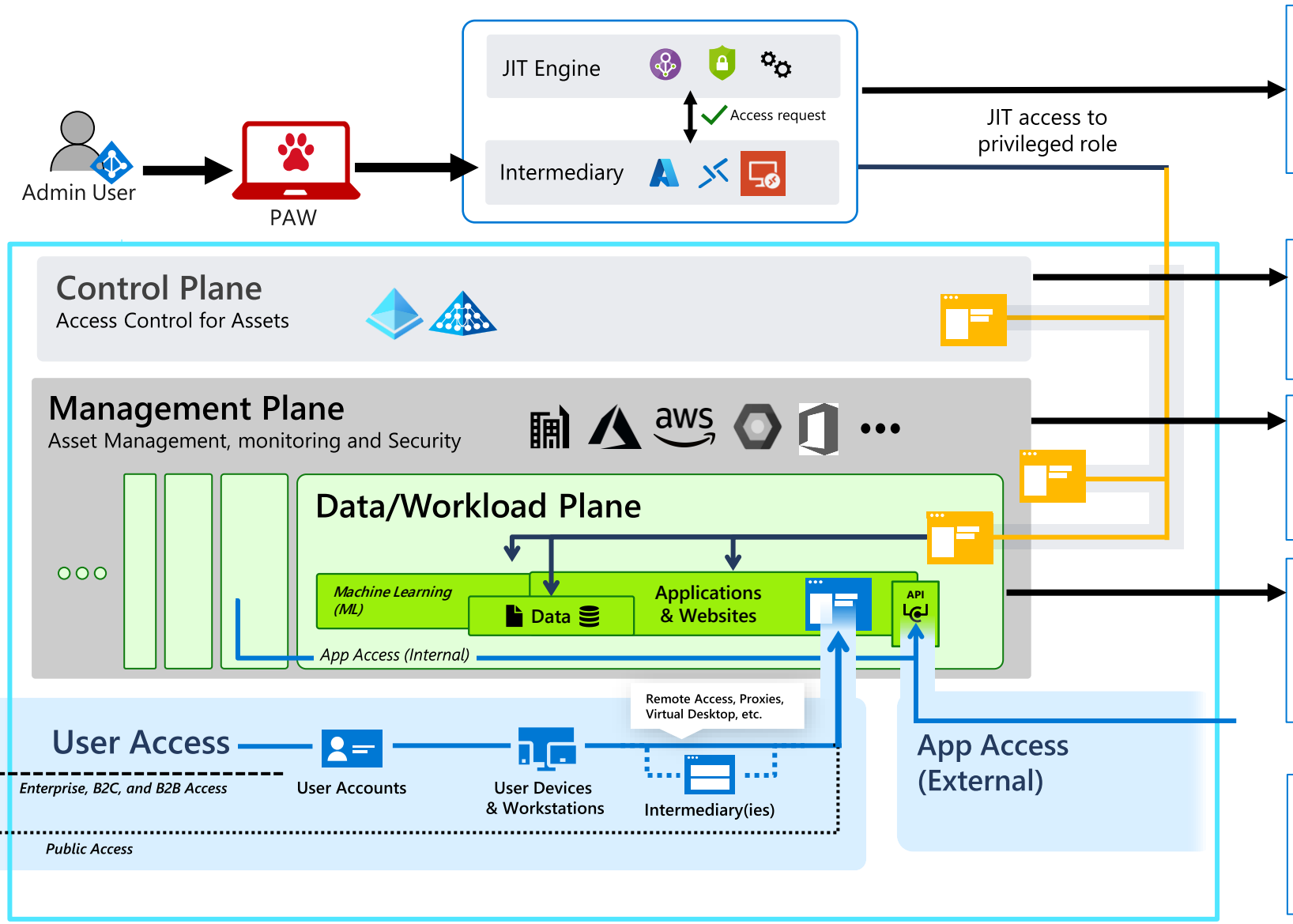
- PAW for Cloud Services Management device is required
- Anchored in Azure AD with no external trust dependencies

Decouple from on-premises security controls



[Protecting Microsoft 365 from on-premises attacks - Microsoft Tech Community]

Enterprise Access Model



Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control Plane

- Identity system admin (e.g., Azure AD, Active Directory Domain Services admin)

Management Plane

- Infra admin (e.g., AWS, Azure resource admin)
- Application service administration (e.g., Office 365, Service Now

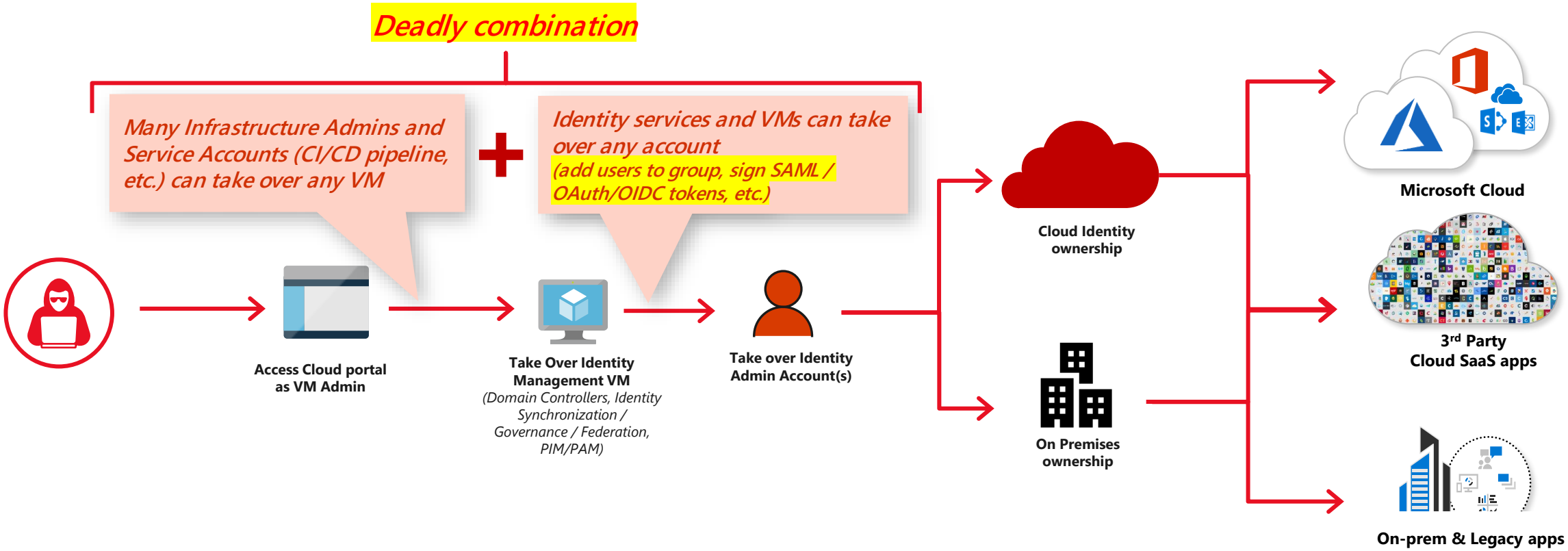
Data/Workload Plane

- Application admin
- Per-workload management focused on protecting business critical systems/data

User access

All Standard User, B2B, B2C, and public access scenarios

Management plane attack paths



"But we use MFA….."

There are (at least) 12 common ways we see MFA bypassed/defeated:

- Session Hijack/Man-in-the-Middle: Including web interfaces like in <your PIM/PAM tool>
- Steal cryptographic keys: Smartcards, rogue CSPs, TPM
- Duplicate Code Generator: Learn shared secret/algorithm (various APTs, RSA, and Lockheed-Martin hacks)
- Not Required/Downgrade attacks: You have disabled Legacy Authentication in your Conditional Access policy, right?
- Recovery Attacks: SMS/phone spoofing
- Social Engineer Tech Support: "My laptop died, I need a code sent to my temporary email"
- Subject Hijack: If you can create a certificate for a privileged account, you can authenticate as them
- Reuse Stolen Biometrics
- Hijacking Shared Auth: oAuth session tokens and SSO to other sites
- Brute Force (on MFA auth screen)
- Buggy MFA
- Physical Attacks: Fake fingerprints and faces, electron microscopes (!)

What does this have to do with dedicated admin workstations?

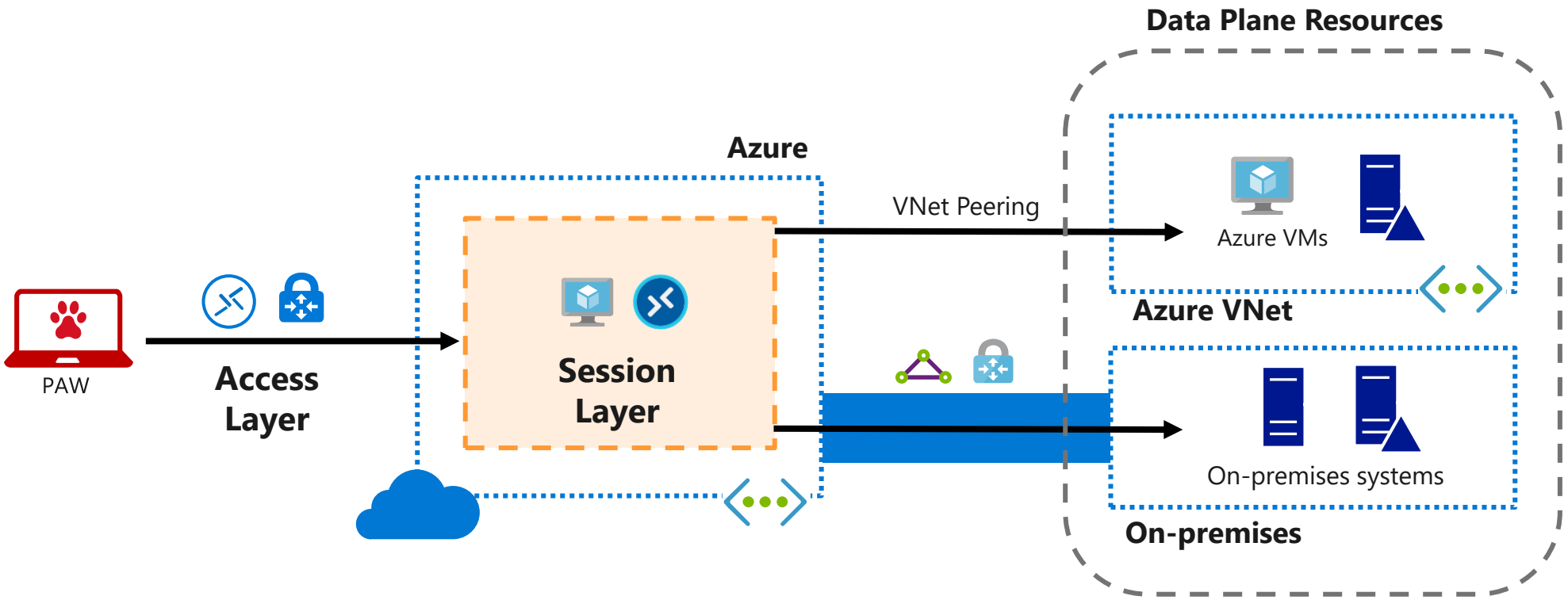
1.) EVERYTHING…all of these attacks are trivial, if not fully automatable, if you own the endpoint

2.) Dedicated Administrative Workstations (we call them PAWs/SAWs in Microsoft) are built to break the attack chain, not mitigate it (e.g. the most common vectors of attack). MFA + PAW device required

3.) Your PIM/PAM solution has nothing to do with any of this

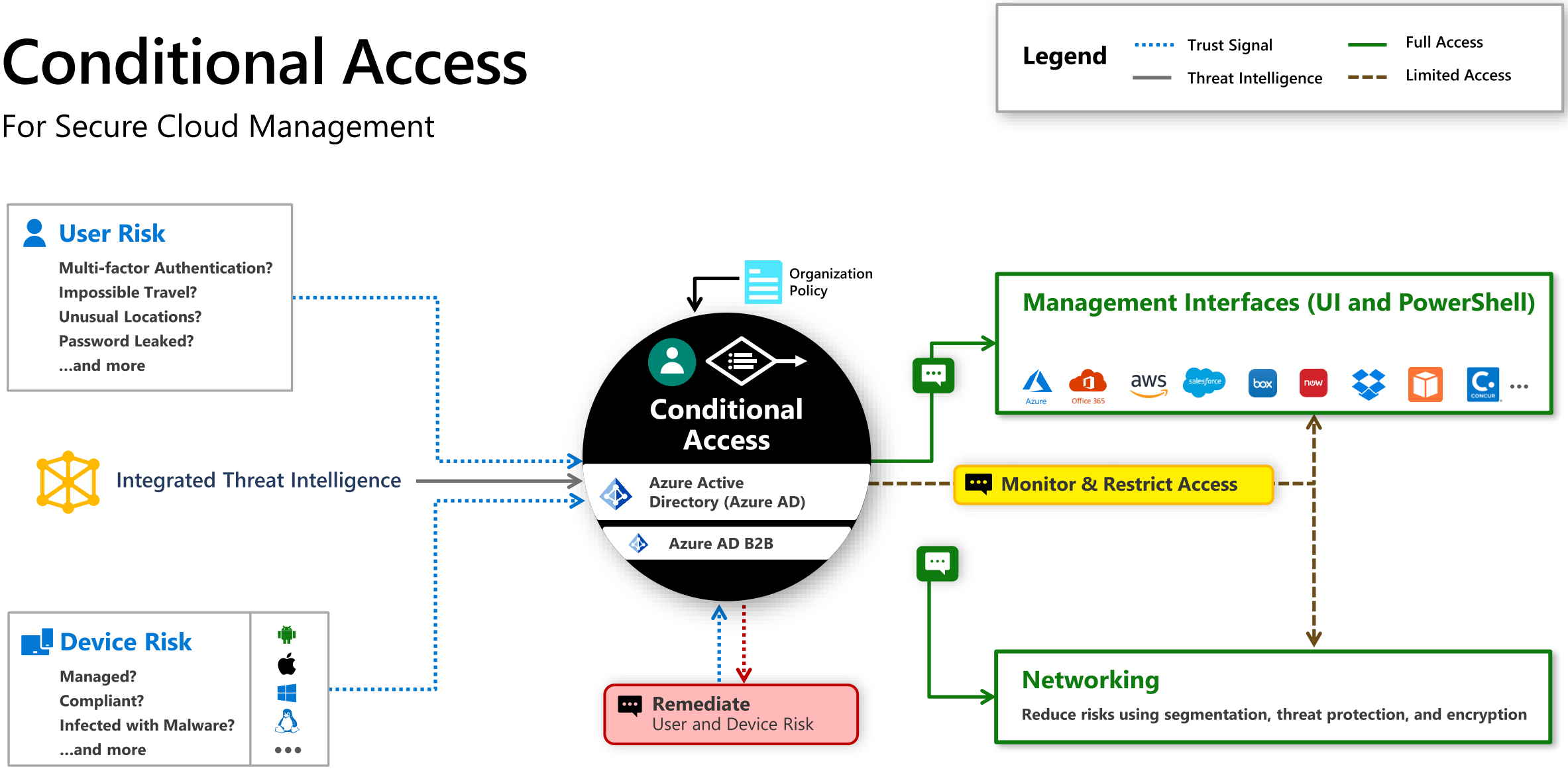
Remote Administration

Privileged Resource Management



Conditional Access

For Secure Cloud Management



Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Emergency Access Accounts

Emergency access accounts

- It is possible to lock out access when applying a policy to all cloud apps or to Azure Resource Management API (i.e. Azure portal).
- We recommend excluding specific break-glass account(s) from the policy.
- Ensure password for any break-glass account is stored securely.
  - Recommend that passwords a 16 characters long and use complexity rules.
  - Complexity rules are appropriate as these accounts are not used regularly

Emergency Access / Break Glass Accounts

Overview	Emergency access accounts will allow you to mitigate the impact of inadvertent lack of administrative access due to misconfiguration, loss of MFA device, personnel turnover, or service outages. These accounts are permanently-privileged, and not assigned to specific individuals.
Account Details	▪ Emergency access accounts should be cloud-only accounts that use the *.onmicrosoft.com domain. ▪ These accounts should not be synchronized or federated with an on-premises environment. ▪ The Global Administrator Azure AD role should be permanently assigned. ▪ These accounts should be excluded from MFA and Conditional Access policies. ▪ Account passwords should be 16+ characters long, never expire, separated into two or three parts, written on separate pieces of paper, and stored in secure, fireproof safes in secure, separate locations.
Usage	▪ Accounts should not be normally signing in or making changes ▪ Security-monitoring staff should be aware of these accounts and regularly check for activity ▪ Accounts should be validated following Microsoft public guidance at least every 90 days
Recommendation	Create at least two (2) emergency access accounts. Learn more by reading Manage emergency access accounts in Azure AD