SECURING PRIVILEGED ACCESS ON-PREMISES AND IN THE CLOUD

Brian Desmond
www.ravenswoodtechnology.com
bdesmond@ravenswoodtechnology.com
Ravenswood Technology Group, LLC

Thomas Kurth
blog.basevision.ch
thomas.kurth@basevision.ch
CEO & Modern Workplace Consultant
baseVISION

2Pint Software adaptiva vmware 1E DELL Microsoft

ABOUT ME – THOMAS KURTH

Microsoft 365 CERTIFIED
ENTERPRISE ADMINISTRATOR
EXPERT

Microsoft 365 CERTIFIED
SECURITY ADMINISTRATOR
ASSOCIATE

baseVISION
SECURE & MODERN WORKPLACE

@ThomasKurthCH
@baseVISION

www.linkedin.com/in/thomas-kurth-a86b7851

https://blog.baseVISION.ch
https://www.baseVISION.ch

MEMBER OF EVENT
CONFIGMGR.CH

ABOUT ME – BRIAN DESMOND

RAVENSWOOD
TECHNOLOGY GROUP

@brdesmond

https://www.linkedin.com/in/briandesmond/

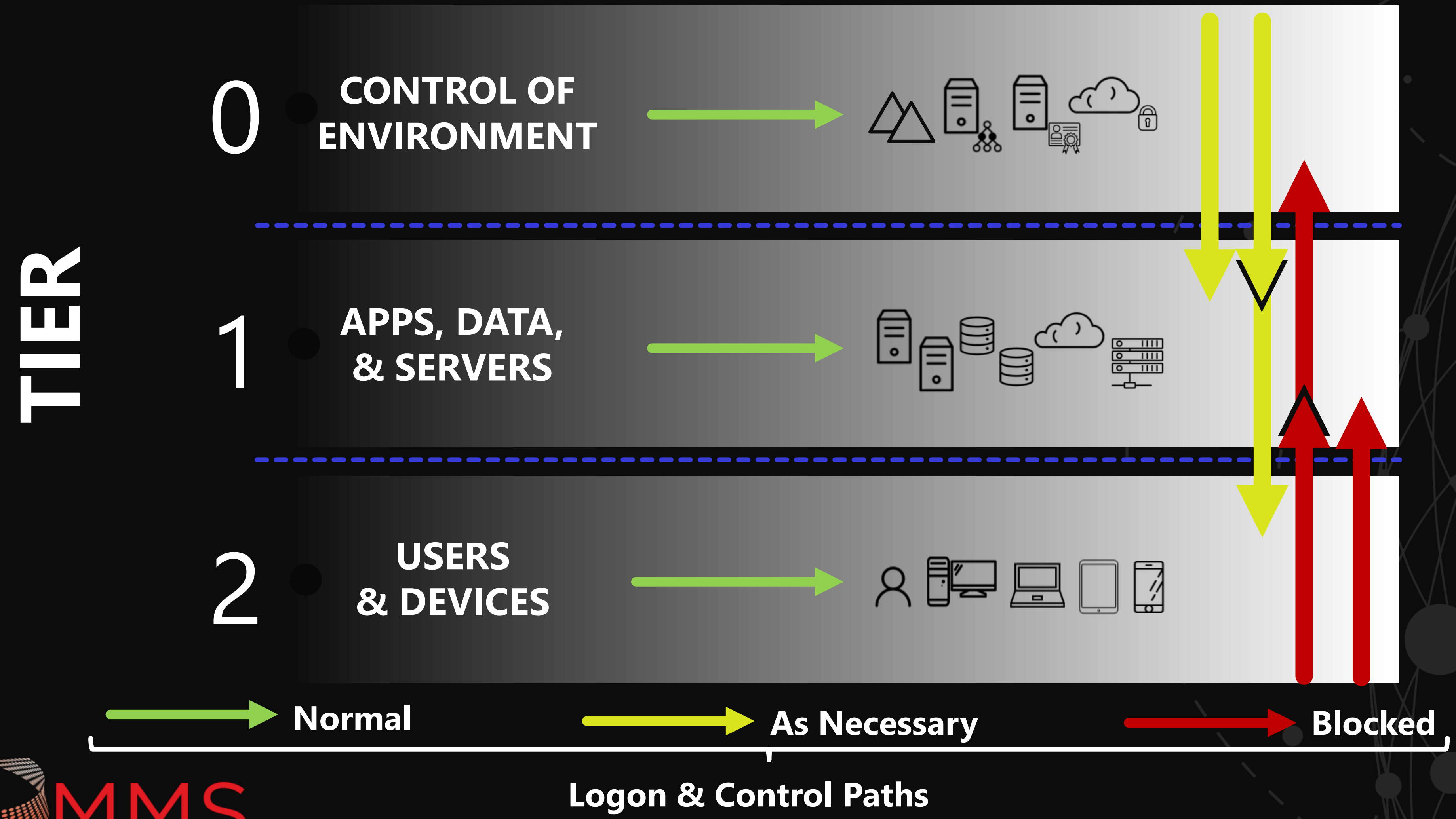
https://www.ravenswoodtechnology.com

SECURING ON-PREMISES PRIVILEGED ACCESS

WHY HAVE THIS CONVERSATION?

- Active Directory (AD) is the gate to most IT assets in most large enterprises
- Privilege escalation in AD is the path to persistence and control in the enterprise
- Taking steps to make the adversary's job much harder are critical in today's world
- Organizations must manage AD as a security asset, not just as infrastructure

TIERED ACCESS MODEL: RISK CONTAINMENT



- Tiering of privileged credentials isolates privilege and risk
- Technical controls prevent a credential from being exposed to a lower assurance system
- The ability for an adversary to move laterally and escalate is dramatically reduced

MMS

AD PRIVILEGED ACCESS ESSENTIALS

- ✓ Minimize Tier 0 identities (Domain Admins, etc.)
- ✓ Separate privileged user accounts
- ✓ Prevent Tier 0 exposure to lower tiers
- ✓ Address Tier 0 equivalencies
- ✓ Prevent lateral movement

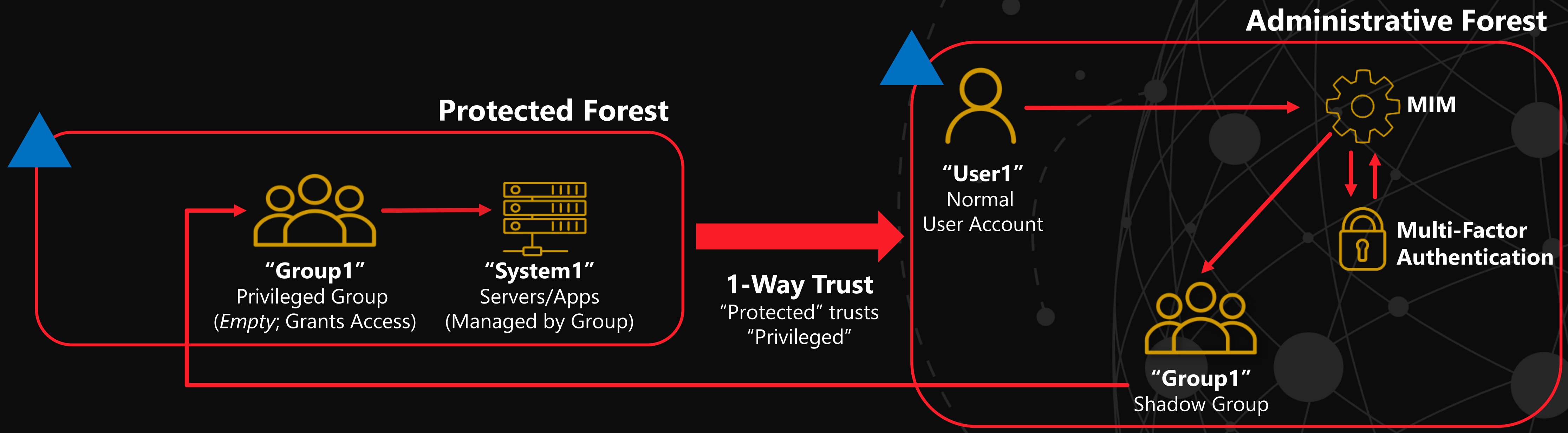
SEGMENTING TIER 1 AND TIER 2

- Tier 1 may be a complex undertaking
- Place new / lifecycled apps into Tier 1
- Remediate high risk apps

- Tier 2 should be relatively easy to tackle
- Interactions between systems should be limited
- Separation of agents may be complicated

JUST-IN-TIME ACCESS

- Privileged credentials are isolated in a hardened, isolated administrative forest
- Access is granted to privileged credentials on a time-bound basis after two-factor authentication



ACTIVE DIRECTORY AND JIT

- Windows Server 2016 introduces a new optional feature called “Privileged Identity Management” (PIM)

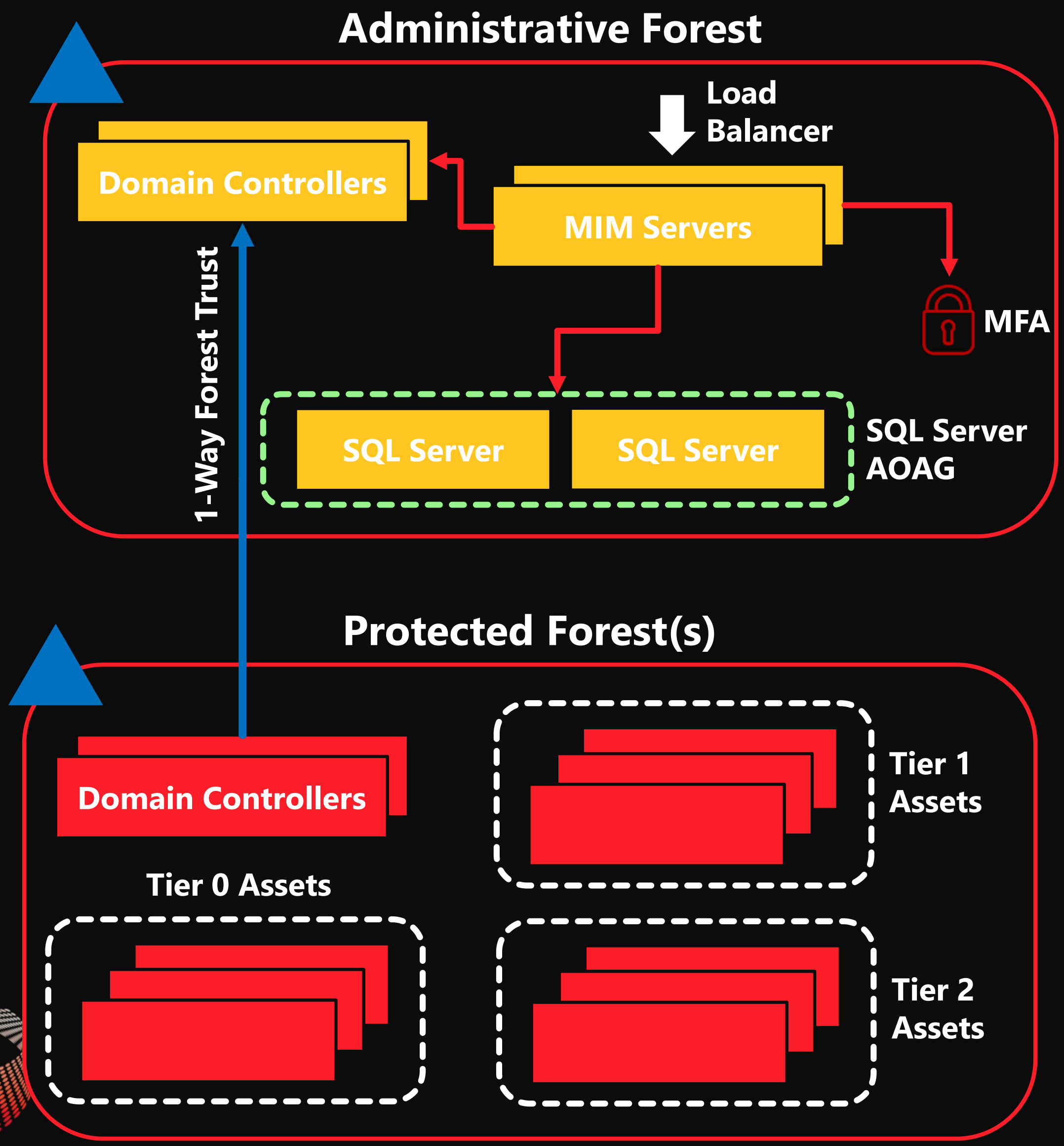
Time Bound Linked Attributes

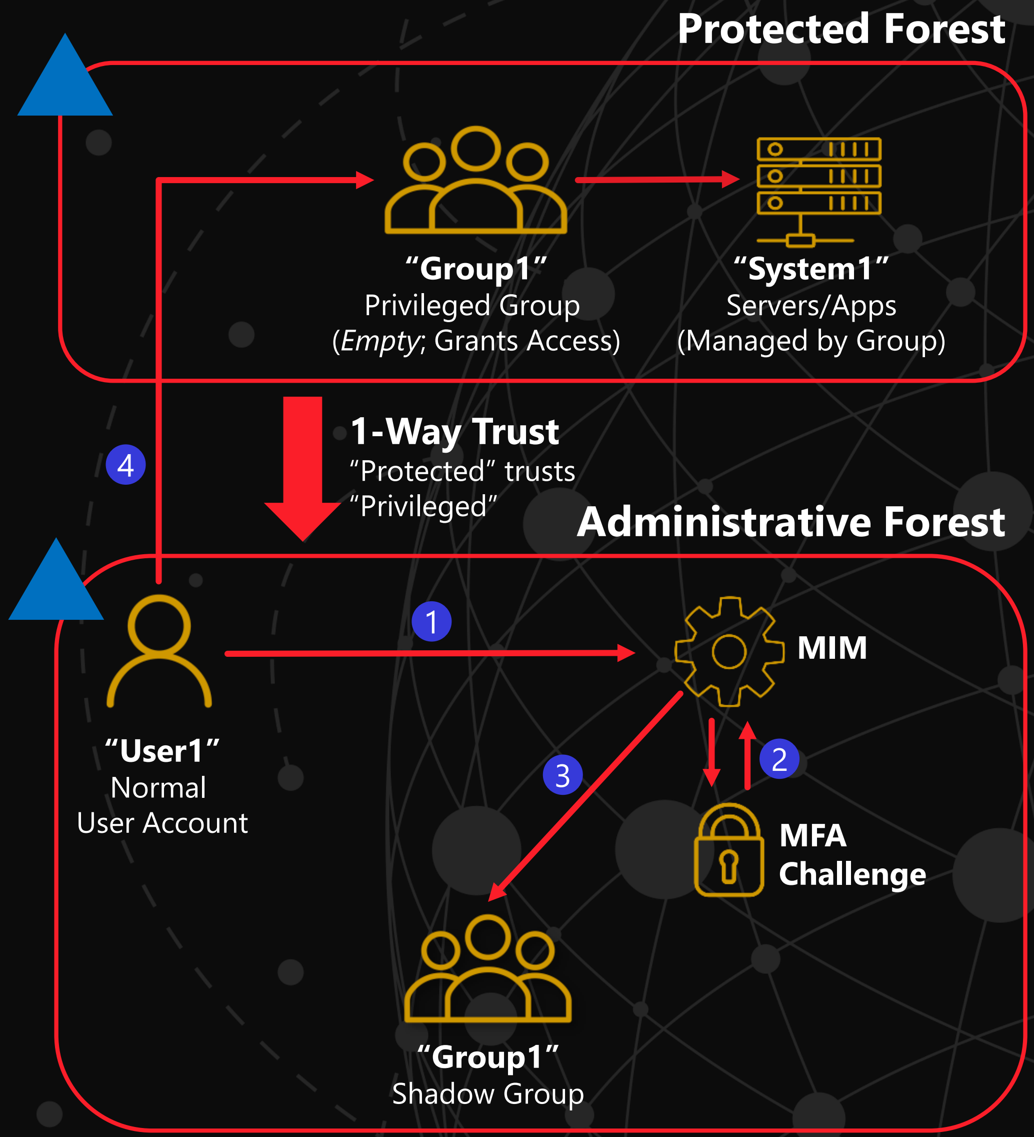
- Linked attributes can now have an optional time-to-live
- Domain controllers automatically remove linked attribute values at expiry
- Kerberos TGTs expire based on the shortest group membership lifetime

PIM Trusts

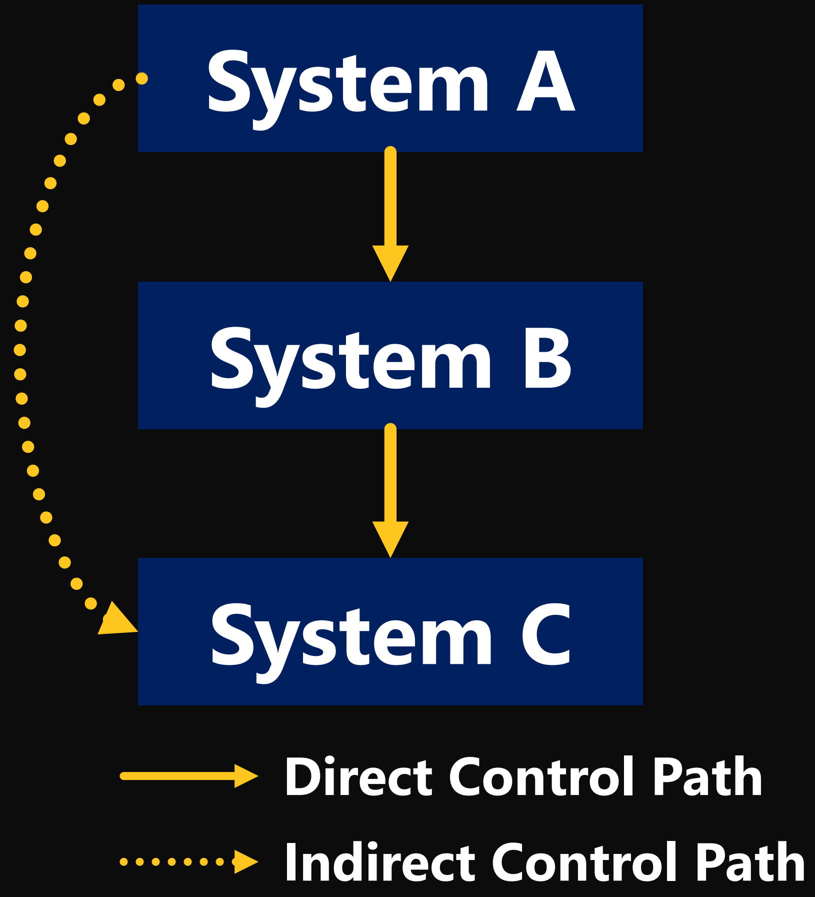
- New trust flag for external trusts
- Modifies the behavior of SID Filtering
- Allows SIDs from the trusting domain to be included in tokens issued by the trusted domain
- Backported to Windows Server 2012 R2 in a update rollup

MIM JUST-IN-TIME ACCESS ARCHITECTURE





CLEAN SOURCE PRINCIPLE



- If “System C” is AD, then all upstream control paths must operate at the same level of assurance
- This extends to agents and management tools
- Clean Source also creates the need for privileged access workstations (PAWs)

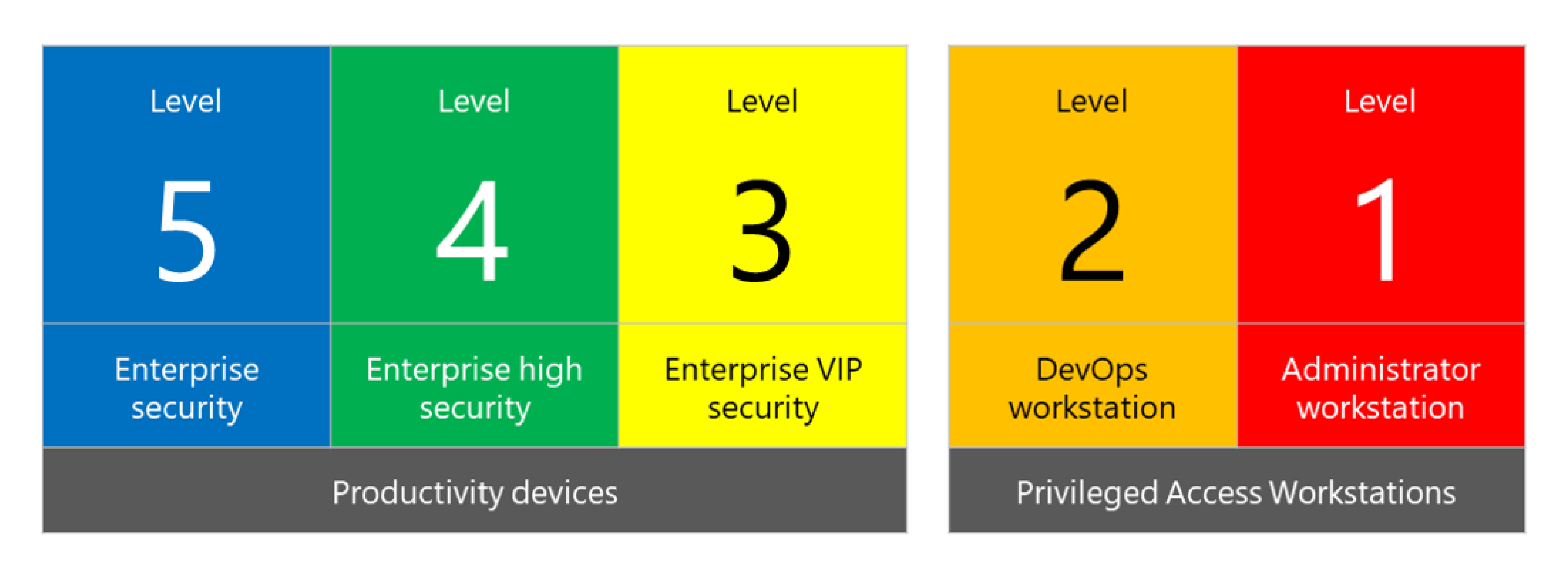
PRIVILEGED ACCESS WORKSTATIONS: A CLEAN SOURCE FOR IT TASKS

- Privileged Access Workstations (PAWs) provide a known-good, clean keyboard for performing privileged or sensitive tasks.
- PAWs isolate sensitive accounts and processes from the risk of a potentially compromised workstation
- Isolation is achieved by ensuring that the PAW is built from clean media and prevented from accessing threat vectors such as the Internet
  - Internet filtering typically excludes trusted sites (e.g. cloud management portals)

MMS

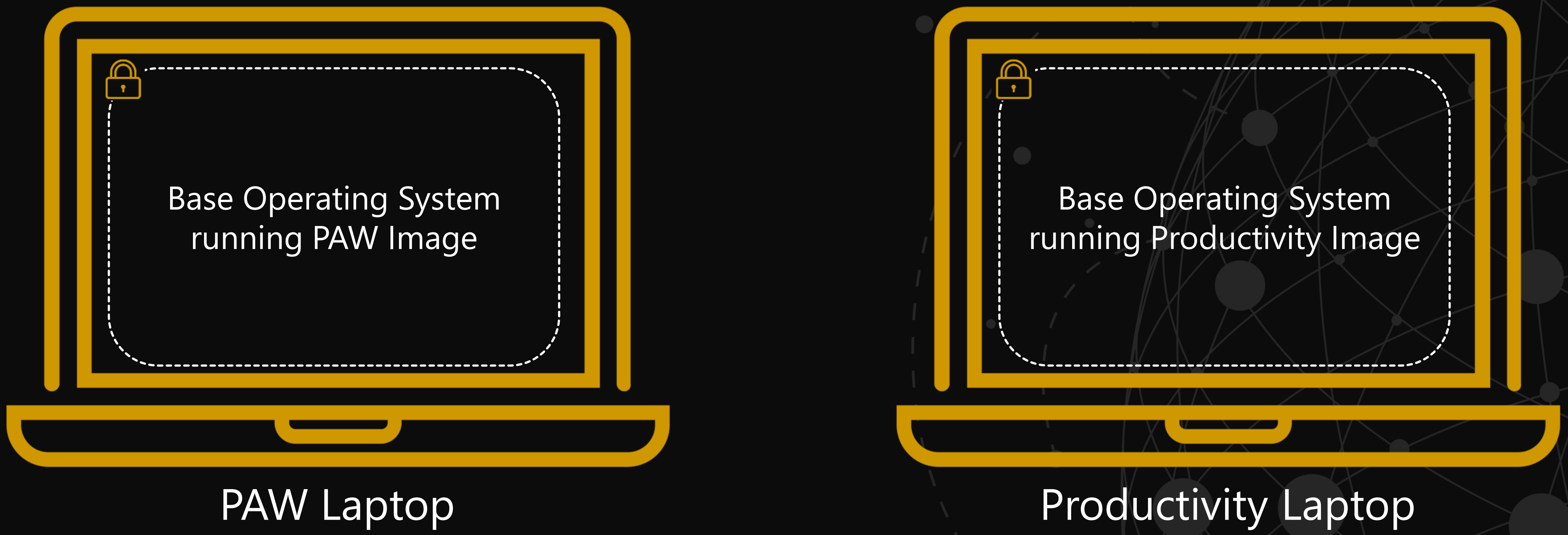
MICROSOFT SECURITY CONFIGURATION FRAMEWORK

- https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/



Level 5	Level 4	Level 3	Level 2	Level 1
Enterprise security	Enterprise high security	Enterprise VIP security	DevOps workstation	Administrator workstation
Productivity devices			Privileged Access Workstations	

STANDALONE PAW



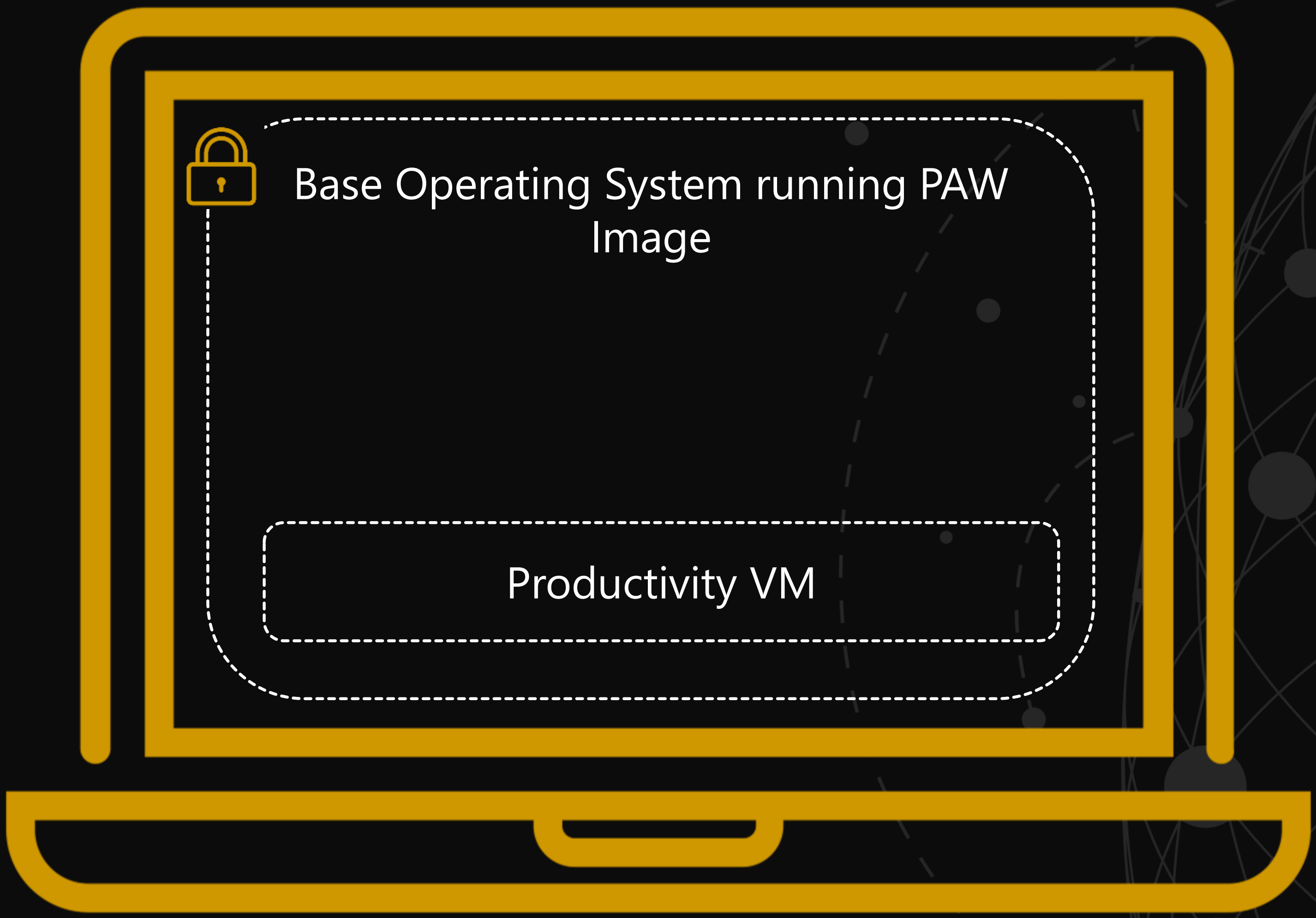
Base Operating System running PAW Image

PAW Laptop

Base Operating System running Productivity Image

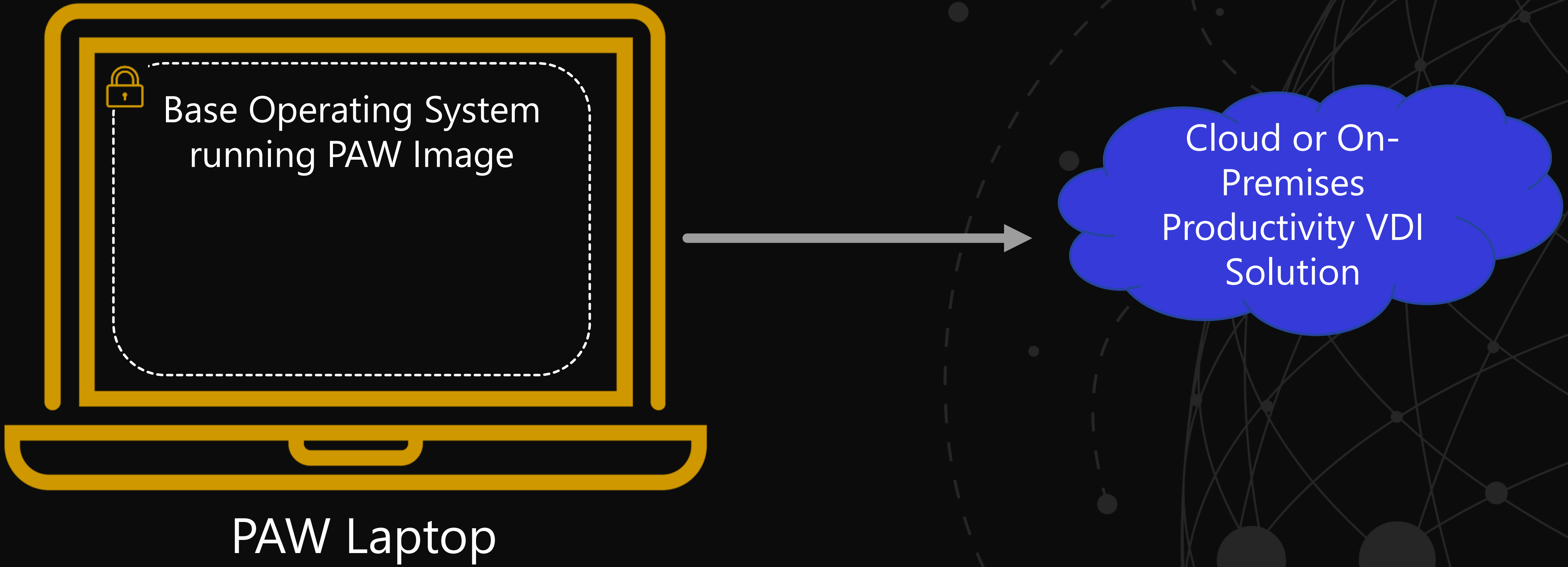
Productivity Laptop

CONSOLIDATED PAW + PRODUCTIVITY VM



PAW Host Laptop

HARDENED VDI CLIENT



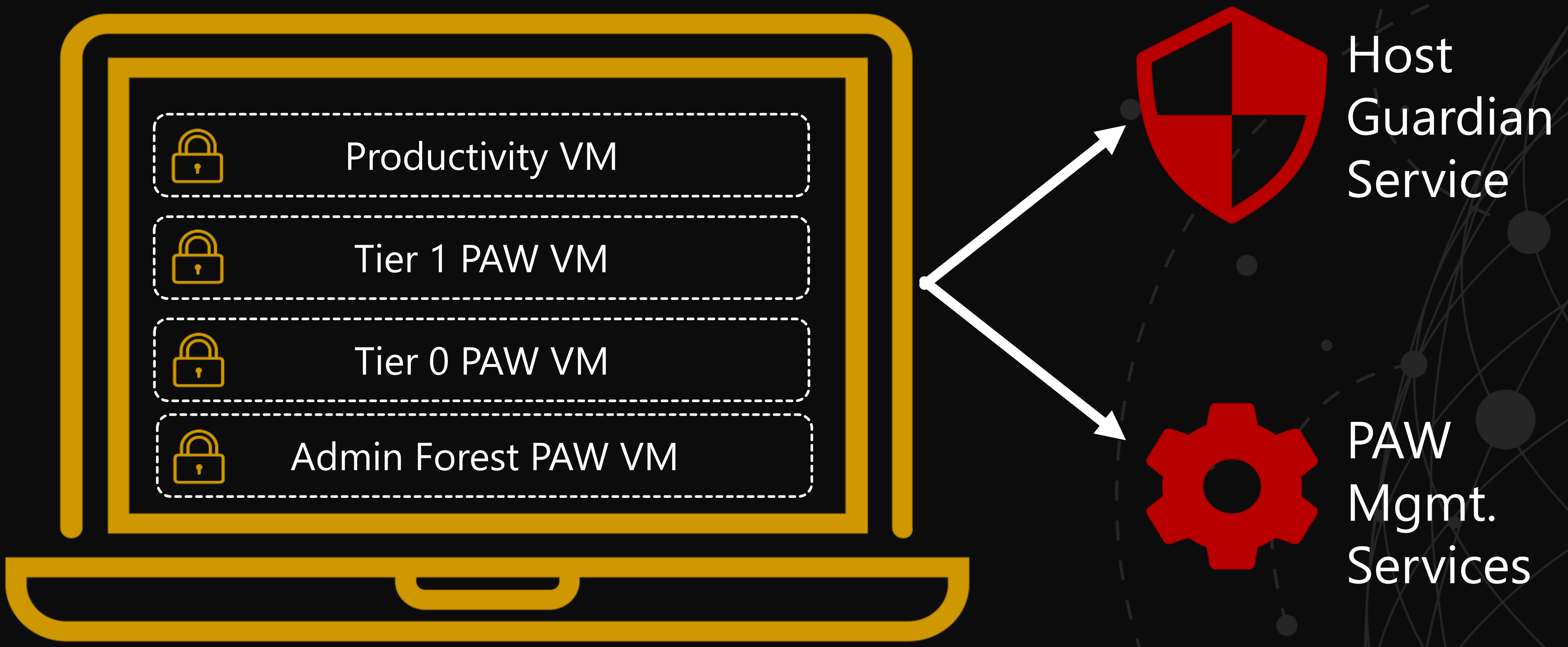
Base Operating System running PAW Image

PAW Laptop

Cloud or On-Premises Productivity VDI Solution

MMS

SHIELDED VM PAW HOST



PAW Host Laptop

https://blogs.technet.microsoft.com/datacentersecurity/2018/04/30/paw-deployment-guide

MMS

PAW PROJECT COMPLEXITIES: NOT JUST THE IMAGE

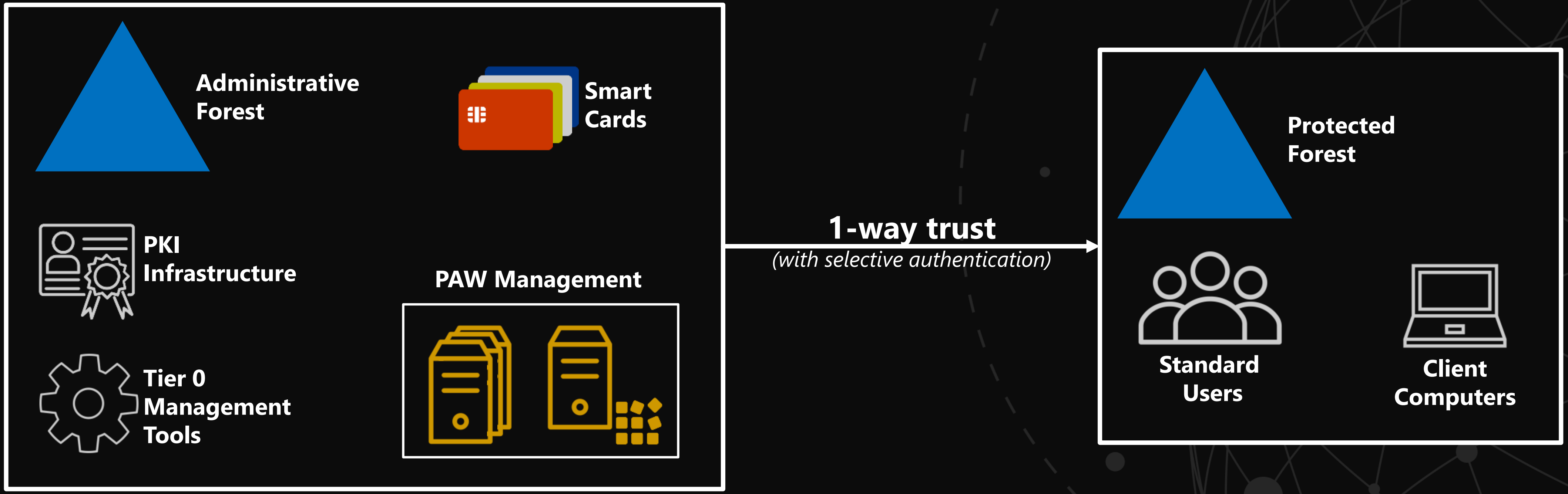
The clean source principle must be pervasive in your design

- **Supply Chain** – new-in-box hardware that is only touched by trusted individuals
- **Provisioning** – PAWs built in “clean rooms” with limited access
- **Networking** – dedicated VPN tunnels for PAWs that should be “always-on”
- **Management Tools** – trusted tooling for endpoint management, vulnerability management, etc.
- **End User Support** – managing hardware issues, rebuilds, etc.

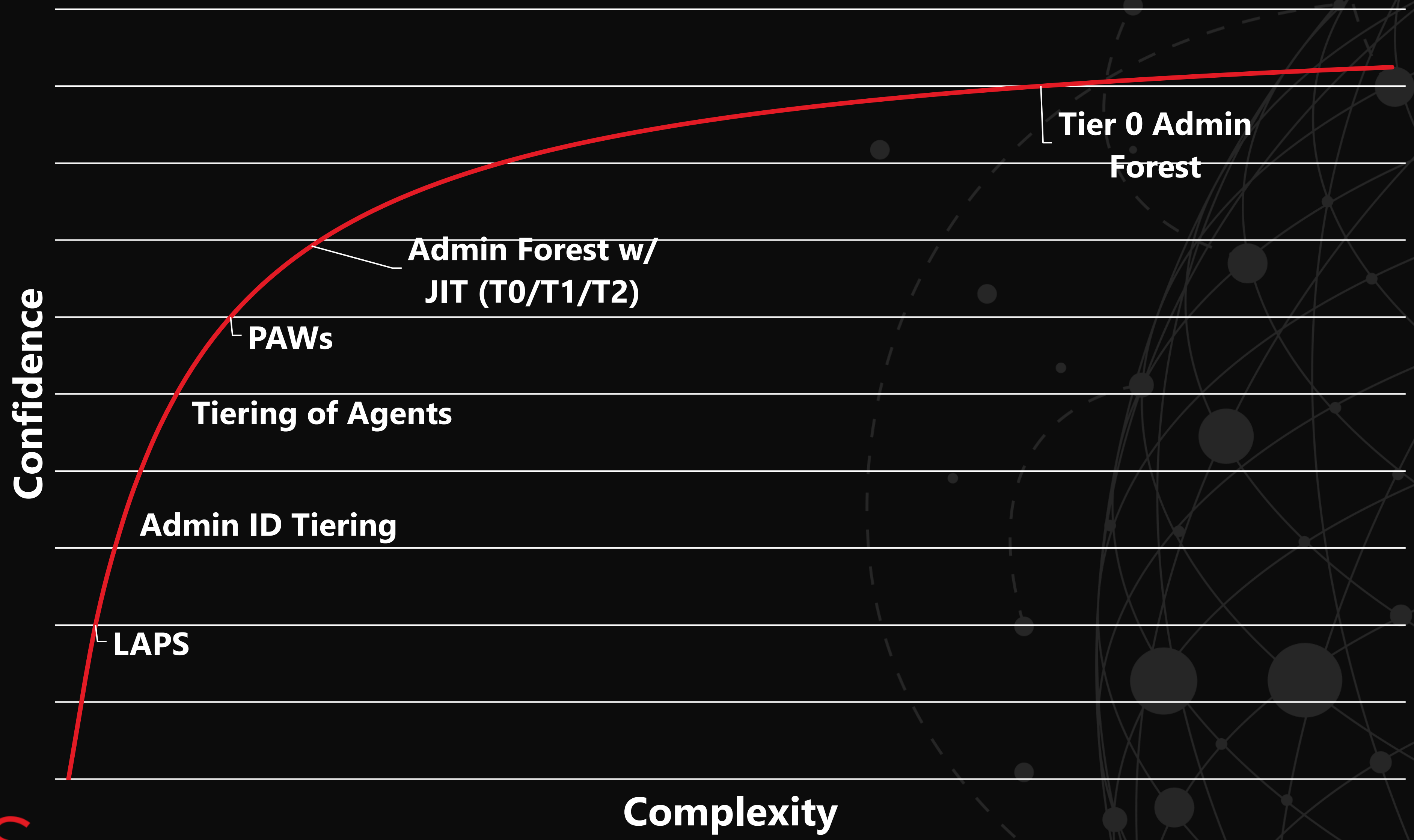
MMS

TIER 0 FOREST: STRONG CREDENTIAL PROTECTION

- Admin forests separate highly privileged credentials into a secure, isolated AD forest
- Privileged credentials are removed from protected forests, dramatically reducing the ability for an adversary to gain control of a protected AD forest
- Administration should be performed exclusively from a clean source, PAWs



PRIVILEGED ACCESS PROTECTION: COMPLEXITY VS REWARD



PRIVILEGED ACCESS IN THE CLOUD

PERMISSION TYPES IN THE CLOUD

SaaS

- Role based in Azure AD
  - No assignment by group possible
  - Azure AD PIM support
- SaaS Applications
  - Sometimes by Azure AD Roles
  - Own implementations

IaaS / PaaS

- Access Control IAM
- Azure AD PIM support

The Domain Admin disaster happens again with Global Admin permissions!

The different permission types

AZURE AD ROLES WITH AAD GROUPS

- Azure Automation to simplify role assignment
- Existing IAM solutions can be leveraged
- Keep in mind permission changes require new token (Logoff/logon)

- Step by Step
  https://blog.basevision.ch/2019/05/assign-azuread-o365-roles-based-on-groups/
- Script
  https://github.com/ThomasKur/ModernAndSecureWorkplace/tree/master/AzureADGroupBasedRoles

MMS

Automating role management in the cloud

MMS

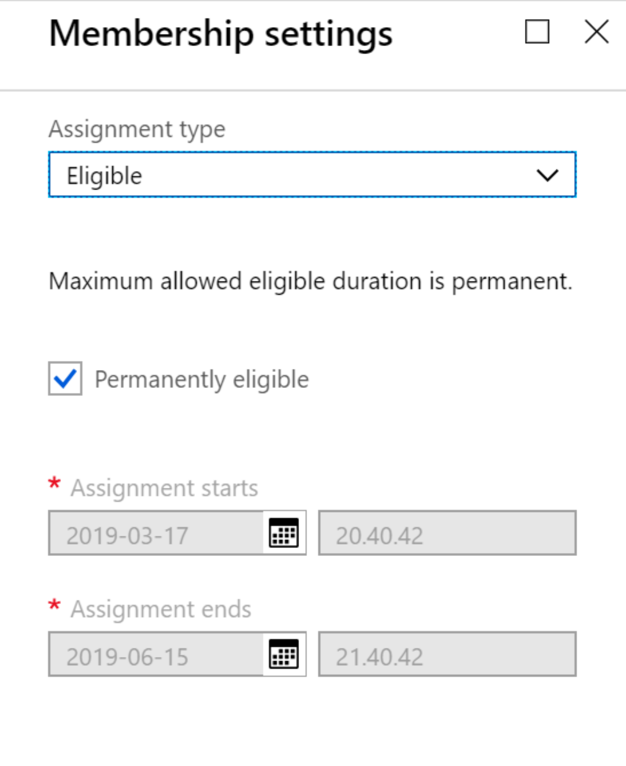
AZURE AD PRIVILEGED ACCESS MANAGEMENT

- O365
  - Request Options
    - MFA
    - Ticket Number
    - Approval
  - Activation Times O365
    - Logoff and Logon required
    - Since 1901 super fast also for Exchange Online
  - Effect on Conditional Access rules
    - When Role is Active it will detect it

Configure Azure AD PIM O365

AZURE AD PRIVILEGE ACCESS MANAGEMENT

- Azure IaaS
  - Effective permissions based on scope and role and identity
  - PIM types
    - Active (like Permanent in O365 roles)
    - Eligible
  - "Permanent" is used for the assignment
  - Eligible duration per default not permanent possible



Membership settings

Assignment type

Eligible

Maximum allowed eligible duration is permanent.

☑ Permanently eligible

* Assignment starts

2019-03-17 20.40.42

* Assignment ends

2019-06-15 21.40.42

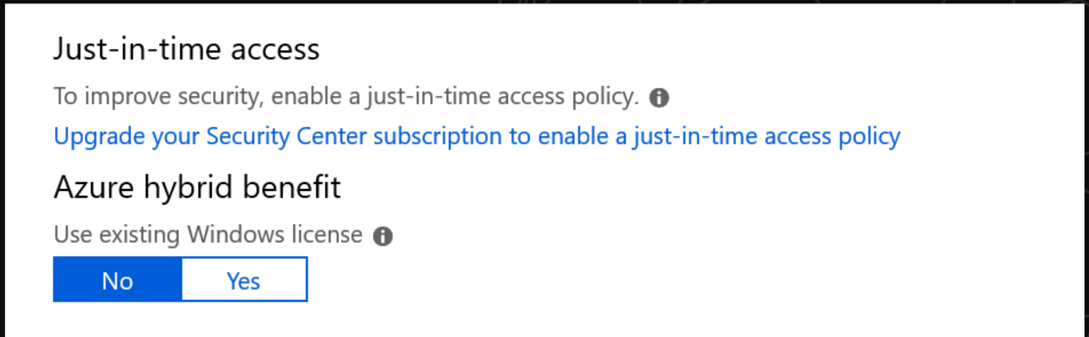
Configure Azure AD PIM
Azure IaaS

VM JUST-IN-TIME ACCESS

- Reduce attack surface of Virtual Machines

- Based on
  - Network Access Rules
  - RDP, SSH, Remote PowerShell and more

- Configuration possibilities
  - Azure Security Center
  - VM Configuration



Just-in-time access

To improve security, enable a just-in-time access policy.

Upgrade your Security Center subscription to enable a just-in-time access policy

Azure hybrid benefit

Use existing Windows license

[✓ No] Yes

How to enable VM JIT

MMS

Extended Q&A

2Pint Software

adaptiva

vmware®

1E

DELL

Microsoft

Kollective

Parallels®

Patch My PC
PATCH MANAGEMENT MADE EASY

Recast Software

LogicDS
SWimage

Lenovo

ivanti

MMS

Radisson Blu · Mall of America