

Protect Your Privilege: The Key Security Measures Administrators in M365 and Azure Should Take

NYMJCSC

October 19th, 2023



**Eric on
Identity**

Protect Your Privilege: The things to **please** do



Eric Woodruff



Product Technical Specialist

Microsoft Security MVP

IDPro Certified ID Professional (CIDPRO)



[@ericonidentity.com](mailto:ericonidentity.com)



[@msft_hiker](https://twitter.com/msft_hiker)



[/in/msfthiker](https://www.linkedin.com/in/msfthiker)



[@ericonidentity@infosec.exchange](mailto:ericonidentity@infosec.exchange)

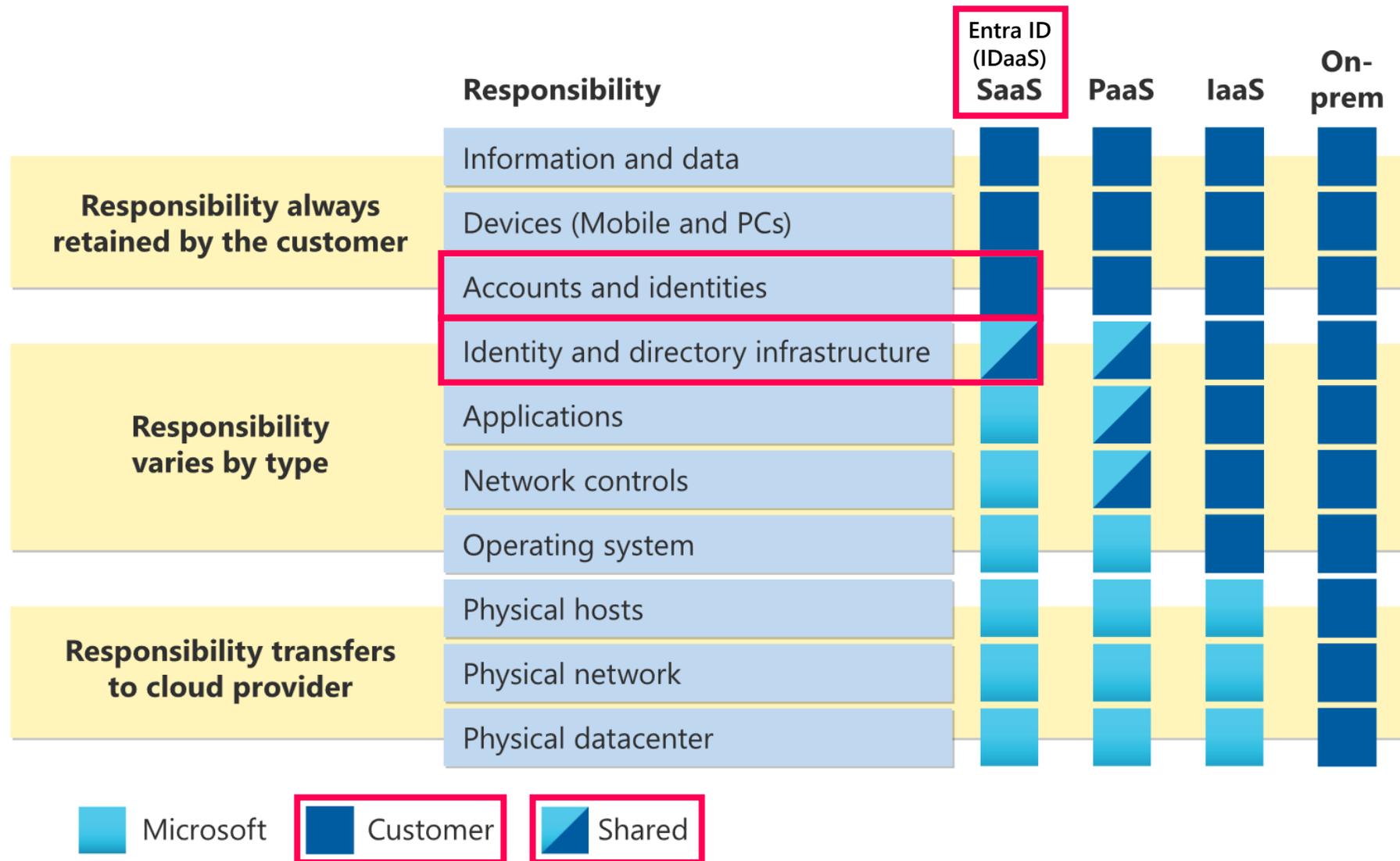
The Security vs Usability Struggle



The Security vs Usability Struggle

Why is this our problem...

The Shared Responsibility Model



Microsoft Digital Defense Report 2022

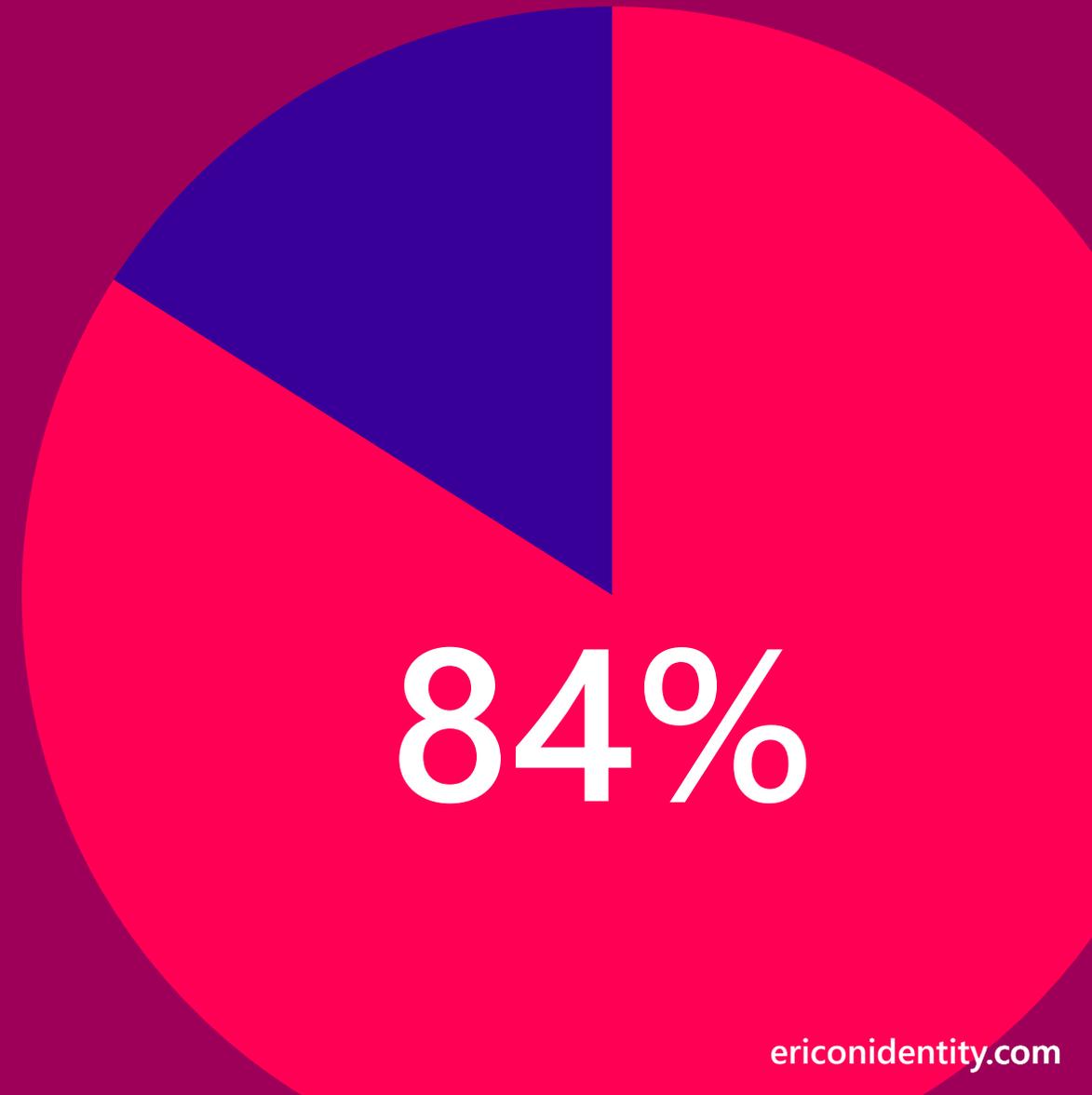
The number one contributing factor in onsite response engagements:

Weak identity controls¹

¹Microsoft Digital Defense Report 2022, page 15

Microsoft Digital Defense Report 2022

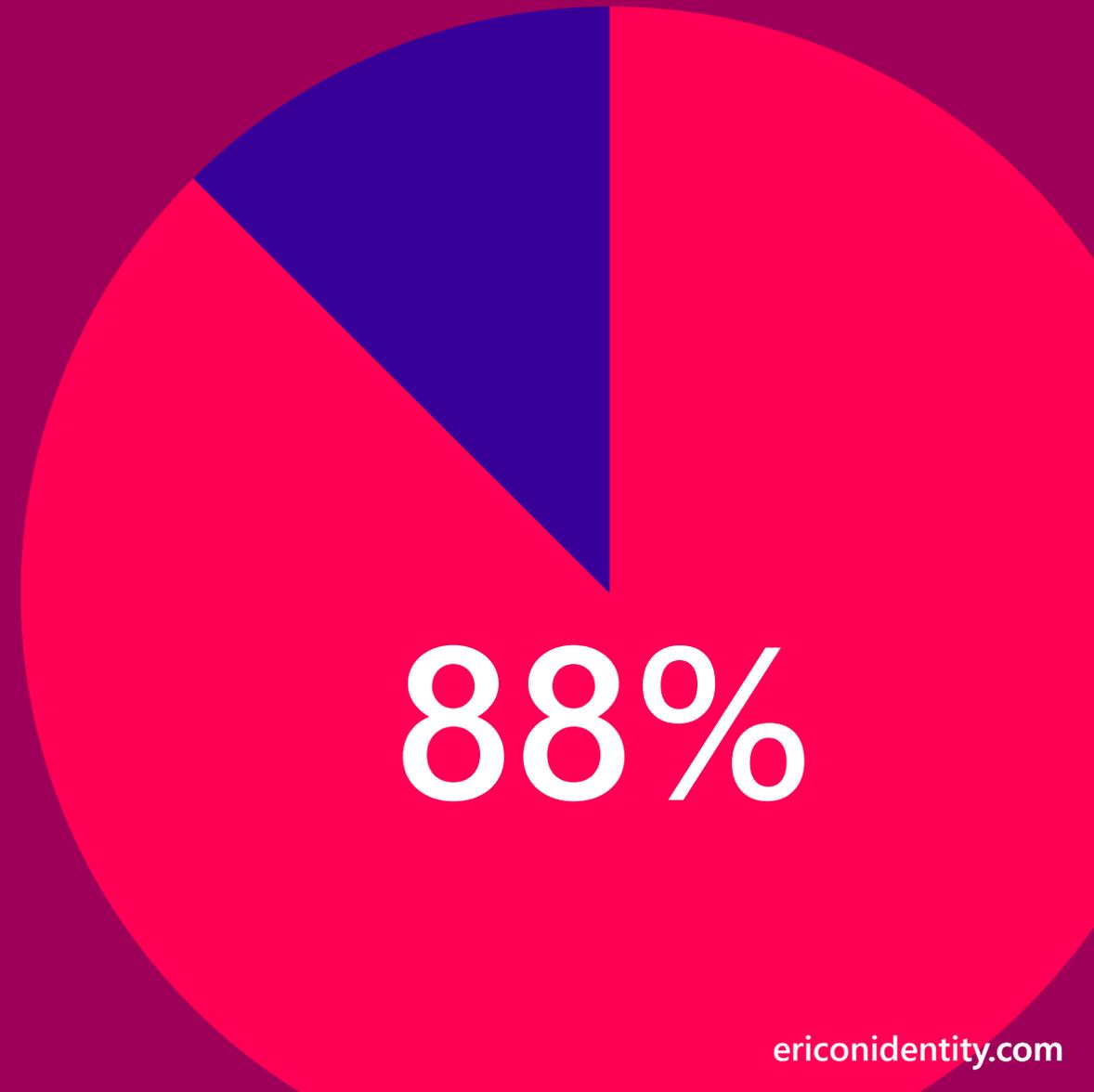
Administrators across organizations did **not** use **privileged identity controls**¹



¹Microsoft Digital Defense Report 2022, page 15

Microsoft Digital Defense Report 2022

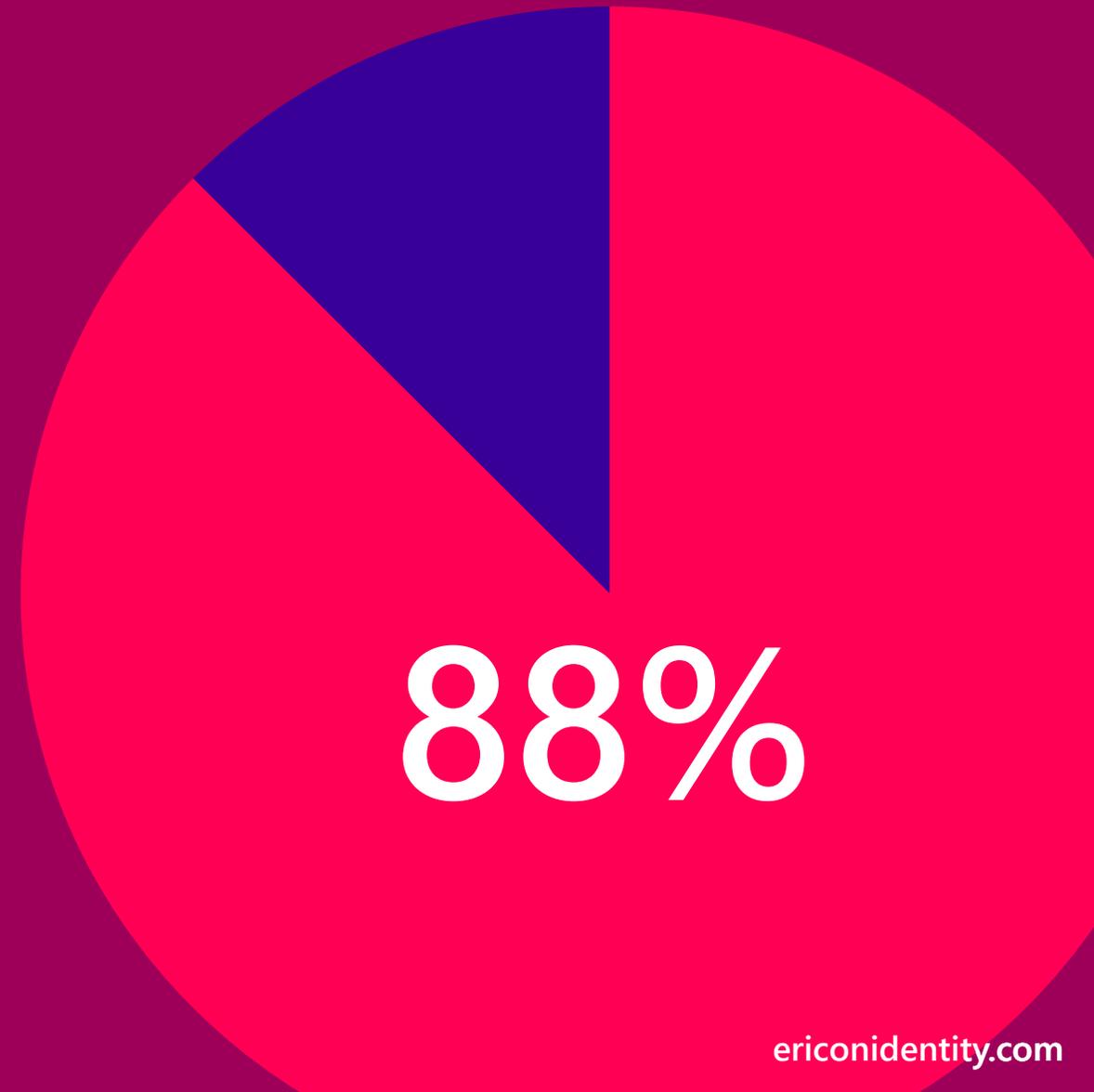
Did **not** employ AD
and Azure AD **security**
best practices¹



¹Microsoft Digital Defense Report 2022, page 15

Microsoft Digital Defense Report 2022

MFA was not implemented for sensitive and high privileged accounts¹



¹Microsoft Digital Defense Report 2022, page 15

Microsoft Digital Defense Report 2022

Did **not** implement
proper **least privilege**
principals via
dedicated
workstations¹

100%

¹Microsoft Digital Defense Report 2022, page 15

Securing Privileged Access

What is a privileged role?

Microsoft Defined Roles (21 roles)

- Global Administrator
- Application Developer
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Synchronization Accounts
- Directory Writers
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

Securing Privileged Access

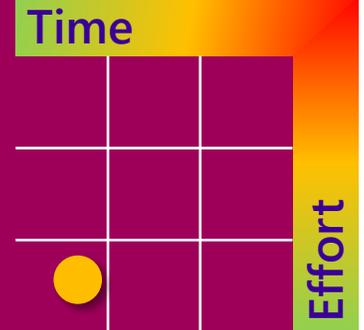
Privileged User

  Strong Credentials

 Entra ID

Securing Privileged Access

Strong Credentials



- Dedicated Privileged Credentials
- Configured for mail-forwarding or not mail-enabled
- Cloud-native credentials sourced in Entra ID
- Phishing-resistant authentication
- Use P2 for privileged users

<https://sl.entra.ms/spa1>

MCSB PA-1

ericonidentity.com



Securing Privileged Access

Privileged User

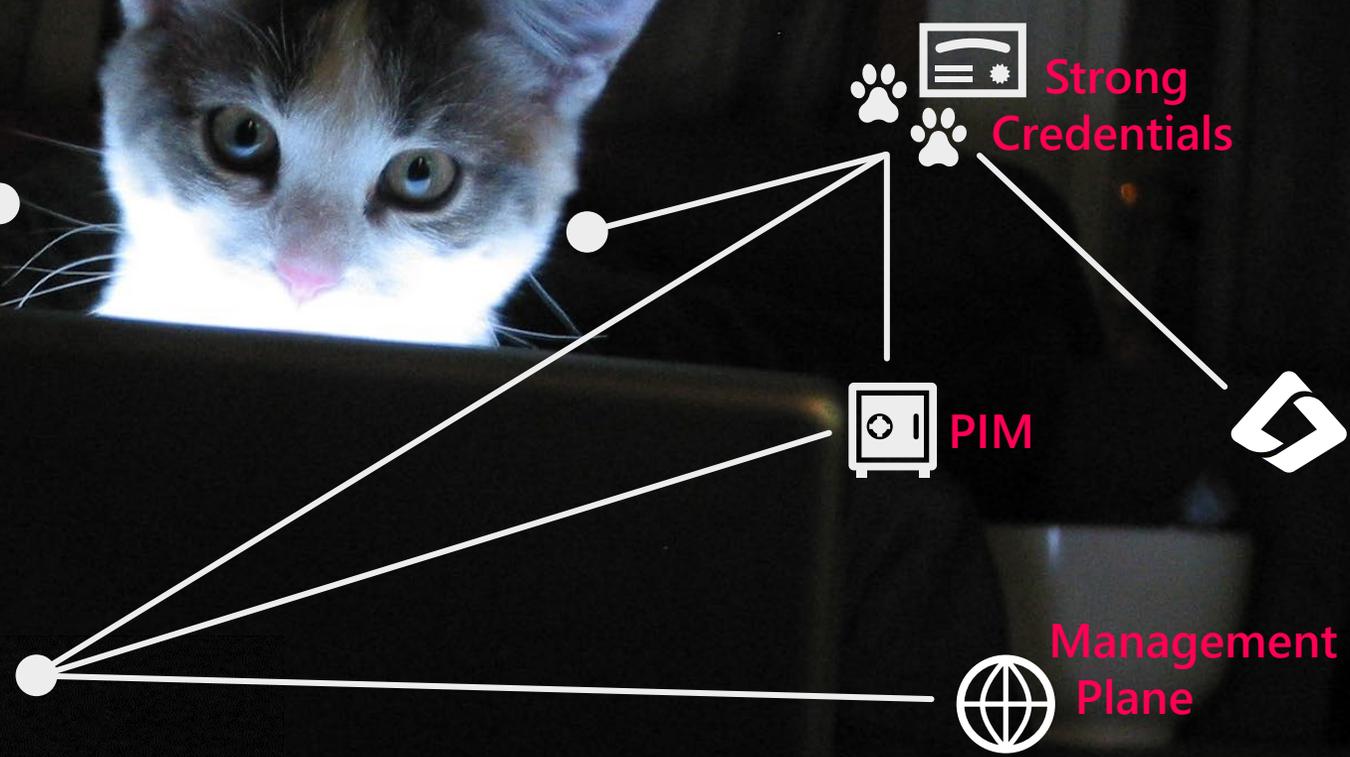


Strong Credentials

PIM

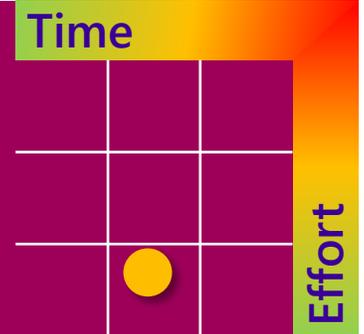
Entra ID

Management Plane



Securing Privileged Access

Privileged Roles



- Require PIM for privileged roles
- Limit activation duration to 1-2 hours
- Use PIM-enabled groups for privileged role flexibility
- Require authentication context over MFA for role activation
- Use service principals over users for applications that require privilege
- Audit and enforce least privileged roles
- Build governance processes around role assignment

MCSB PA-7

MCSB PA-2

ericonidentity.com

<https://sl.entra.ms/spa2>



Securing Privileged Access

Privileged User



Strong Credentials

Clean Keyboard Design

PIM

Entra ID

Management Plane

Hardened Dedicated Workstation

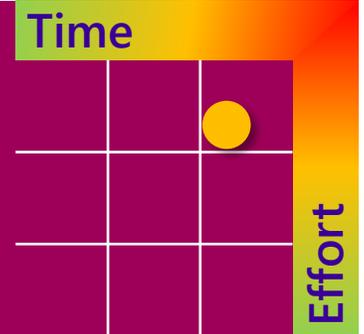
Endpoint Protection

MDM & XDR



Securing Privileged Access

Privileged Access Workstations



- Ensure that clean keyboard design is leveraged
- Follow hardening recommendations from Microsoft
- Devices follow a hardware root of trust
- User is not local administrator
- Device management team joins the privileged tier

<https://sl.entra.ms/spa3>

MCSB PA-6

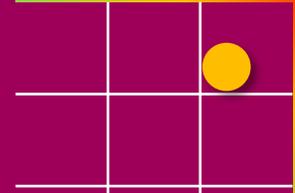
ericonidentity.com



Securing Privileged Access

Privileged Access Workstations

Time



Effort

End-to-end Protection For Privileged Sessions		Enterprise Security	Specialized Security	Privileged Security
		Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
Role Recommendation For privileged access role		Standard users High impact users / developers IT Operations		
Session 	Device Physical device initiating session Profile Summary	Enterprise Device <i>Protect existing attack surface</i> <ul style="list-style-type: none"> Centrally Managed Policies Productivity & Admin Apps Endpoint Detection and Response (EDR) Monitor app and browser activity 	Specialized Device <i>Limit new attack surface</i> Enterprise Security Plus... <ul style="list-style-type: none"> No local admin privileges Block unexpected applications 	Privileged Access Workstation (PAW) <i>Highly Restricted attack surface</i> Specialized Security Plus... <ul style="list-style-type: none"> Restricted applications (limited or no productivity apps) Restricted web browsing
	Account with access to resources			
	Intermediary Remote Access / Admin Broker			
	Interface Controlling resource access			

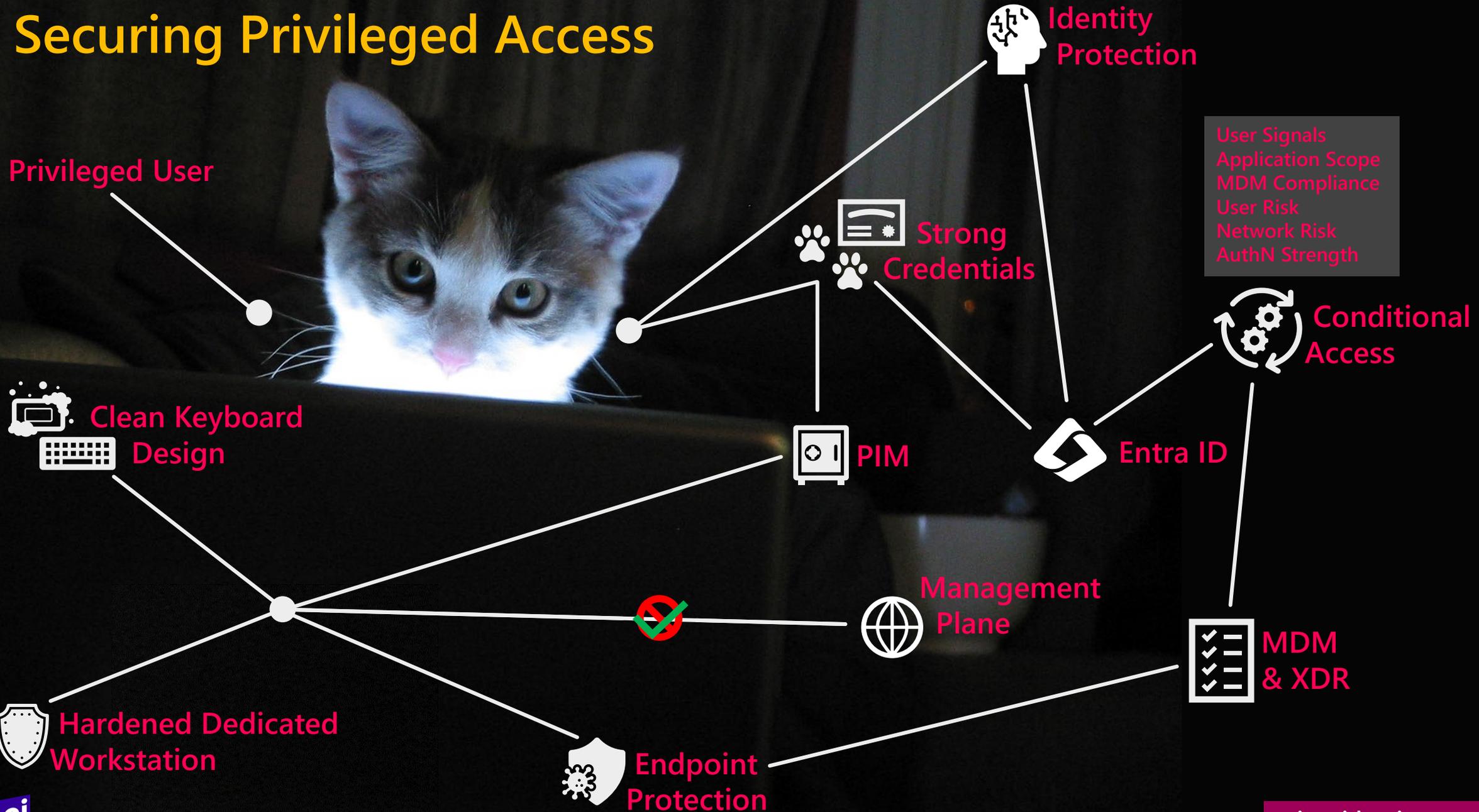
<https://sl.entra.ms/spa3>

MCSB PA-1

ericonidentity.com

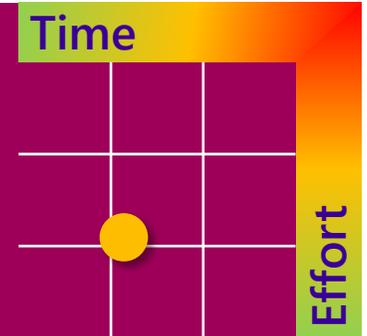


Securing Privileged Access



Securing Privileged Access

Conditional Access Enforcement



- Building robust CA policies leveraging:
 - Device compliance
 - Device filtering
 - Identity Protection
 - Strong authentication requirements
 - Network requirements
 - Sign-in frequency

<https://sl.entra.ms/spa4>

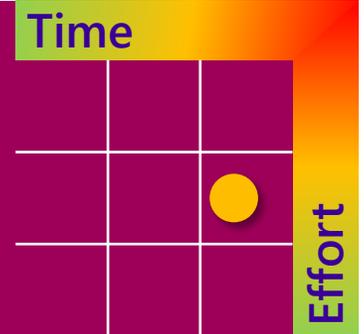
MCSB PA-1

ericonidentity.com



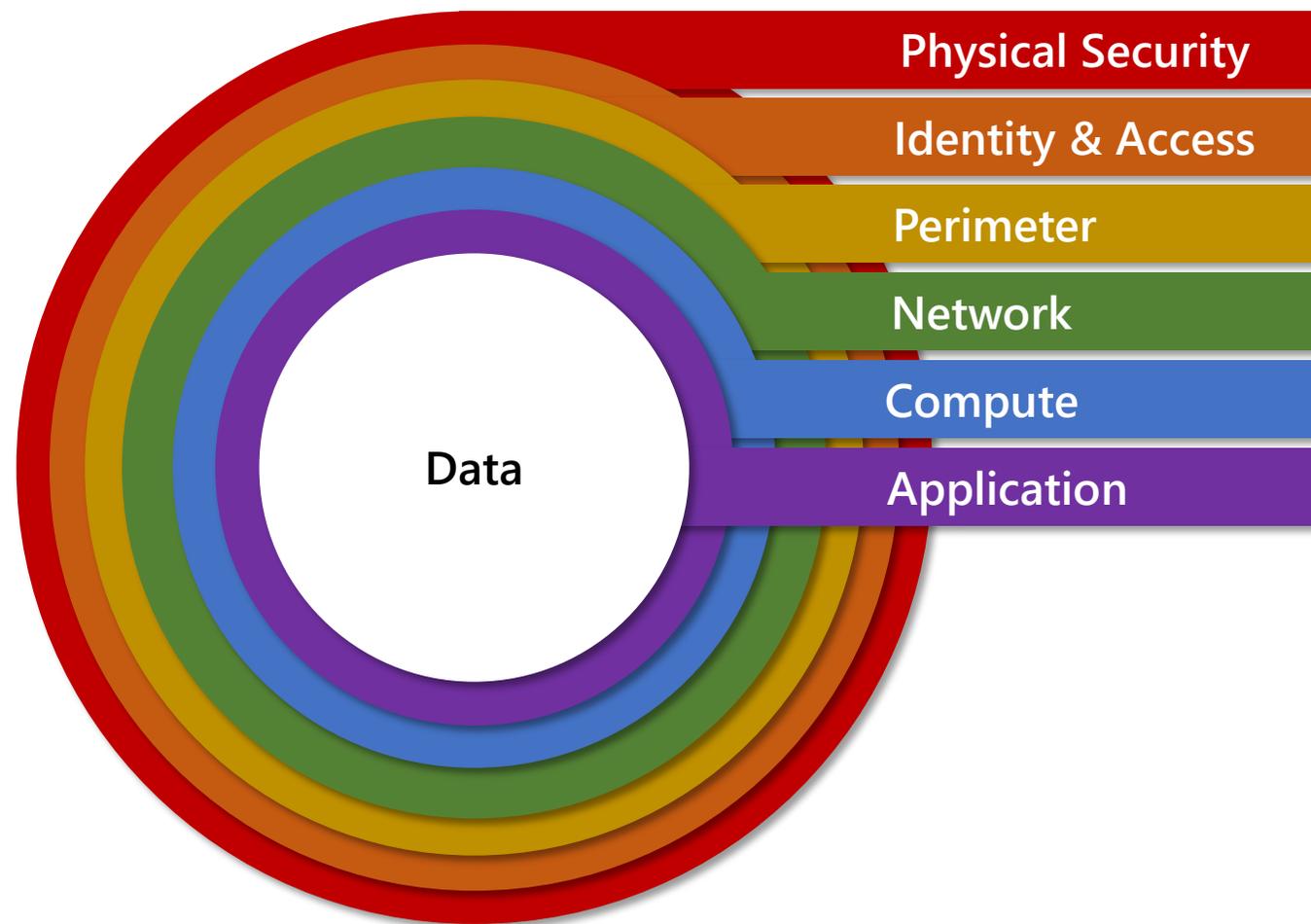
Securing Privileged Access

Conditional Access Enforcement

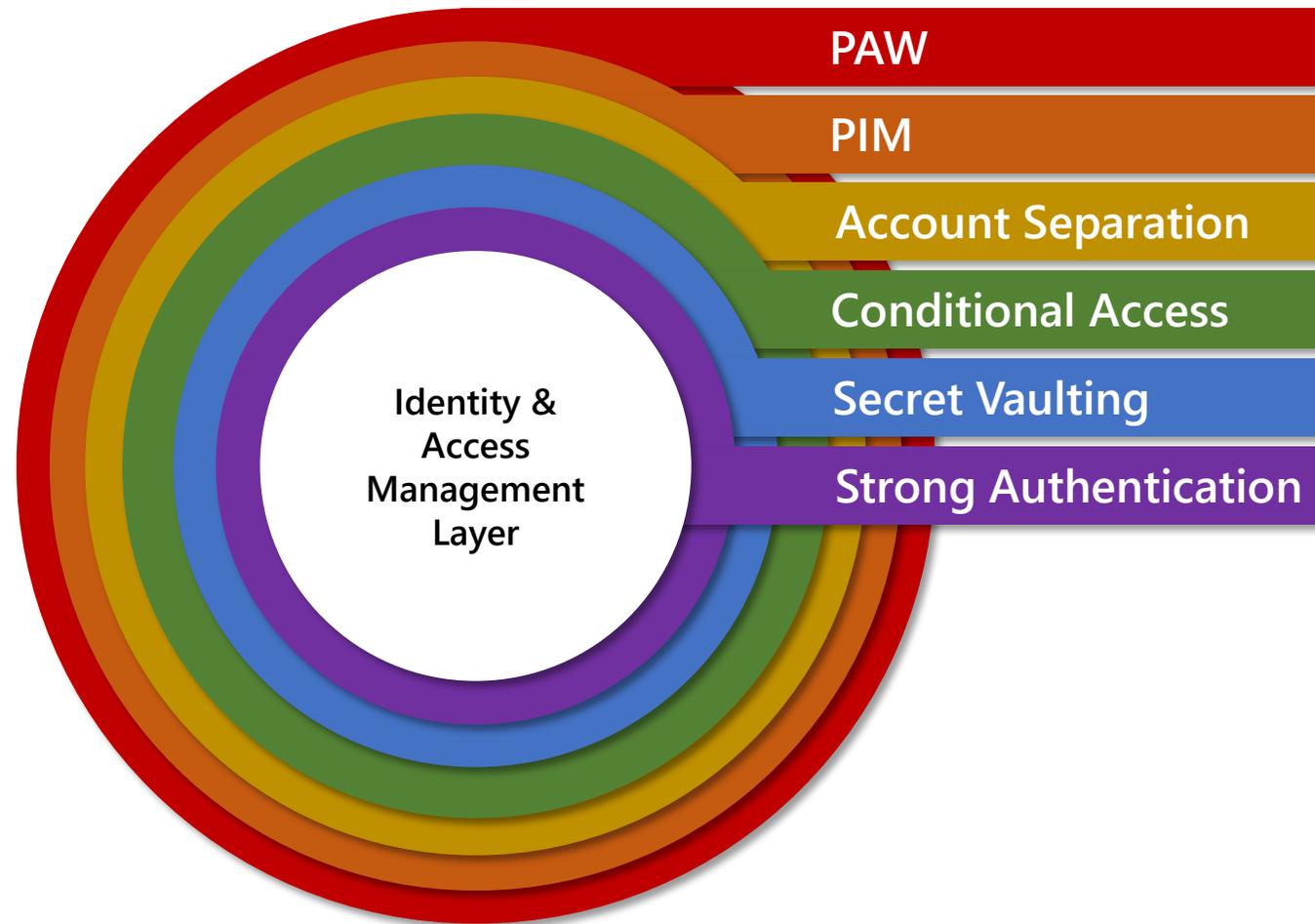


- For workloads and service accounts
 - Use Workload Identity Protection
 - Restrict access to trusted IP ranges

Defense in Depth

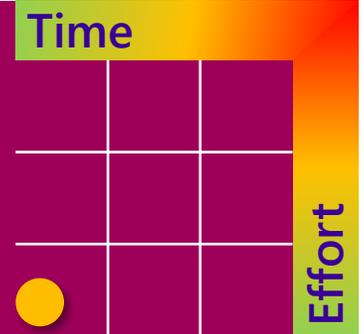


Defense in Depth



Securing Privileged Access

Break-glass Accounts



- Two break-glass accounts
 - One excluded in Conditional Access
 - One PIM permanent assignment
- Accounts should be highly monitored
- Passwords should be securely managed
- Device-bound passkey (FIDO2) may be an alternative

Questions?

