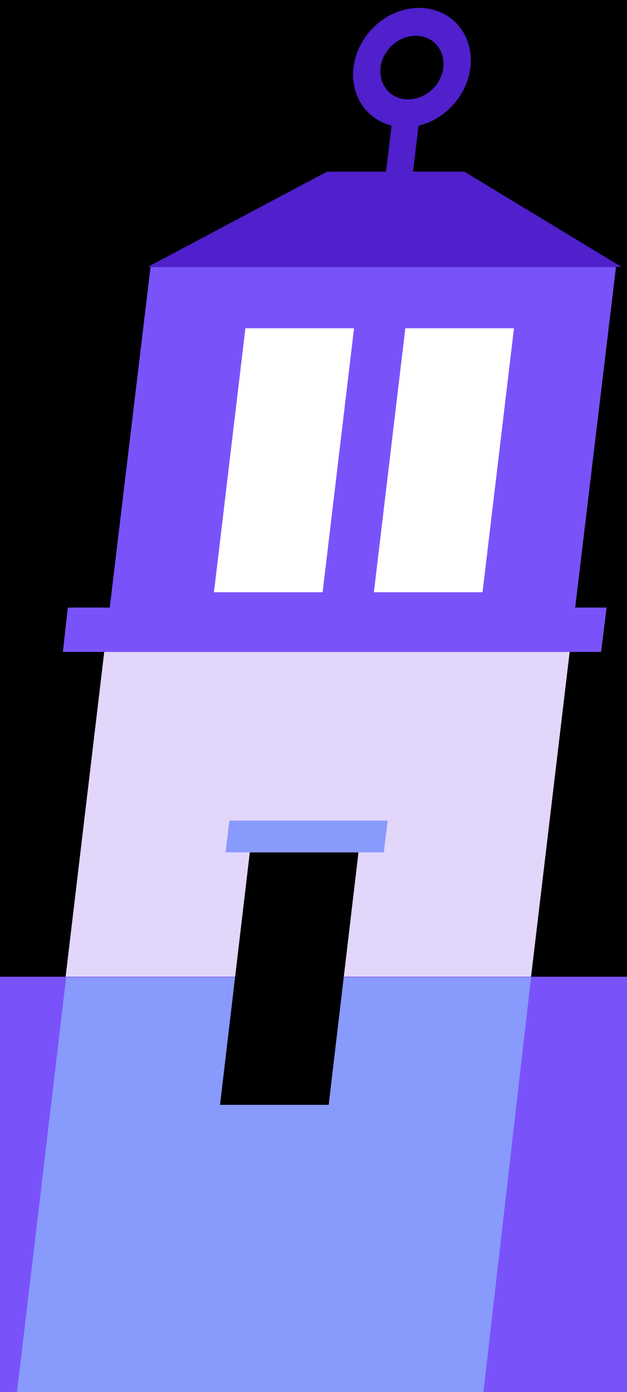
HYBRID
IDENTITY
PROTECTION

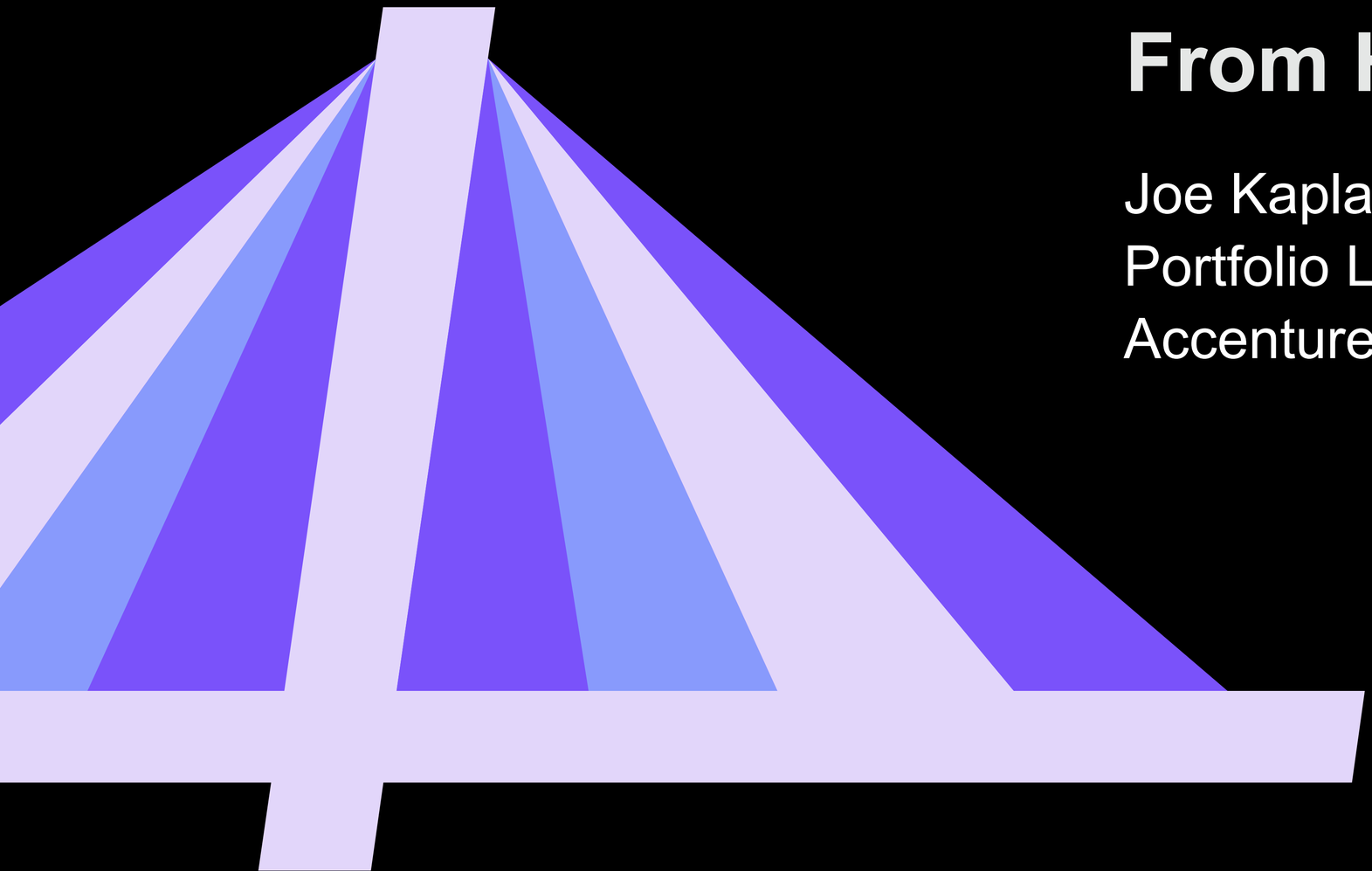
conf25

CHARLESTON



HYBRID IDENTITY PROTECTION conf25

CHARLESTON



From Hybrid to Cloud

Joe Kaplan
Portfolio Lead for Identity,
Accenture Global IT

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Joe Kaplan

Global IT Identity Lead, Accenture

Joe Kaplan is the Identity Lead in Accenture's Global IT organization. He focuses on solving real world problems for a large, complex business of over 750K employees globally. He has over 30 years of professional experience in IT, with 20+ focused on directories, identity, and cybersecurity.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Getting a Bit Old, Are We?

DC=dir,DC=svc

```
***Searching...
ldap_search_s(ld, "DC=dir,DC=svc,DC=accenture,DC=com", 0, "(ob
Getting 1 entries:
Dn: DC=dir,DC=svc,DC=accenture,DC=com
        whenCreated: 11/9/2000 4:31:01 PM Central Daylight Time;
```

It was a Thursday…

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

The Hybrid Dilemma…

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

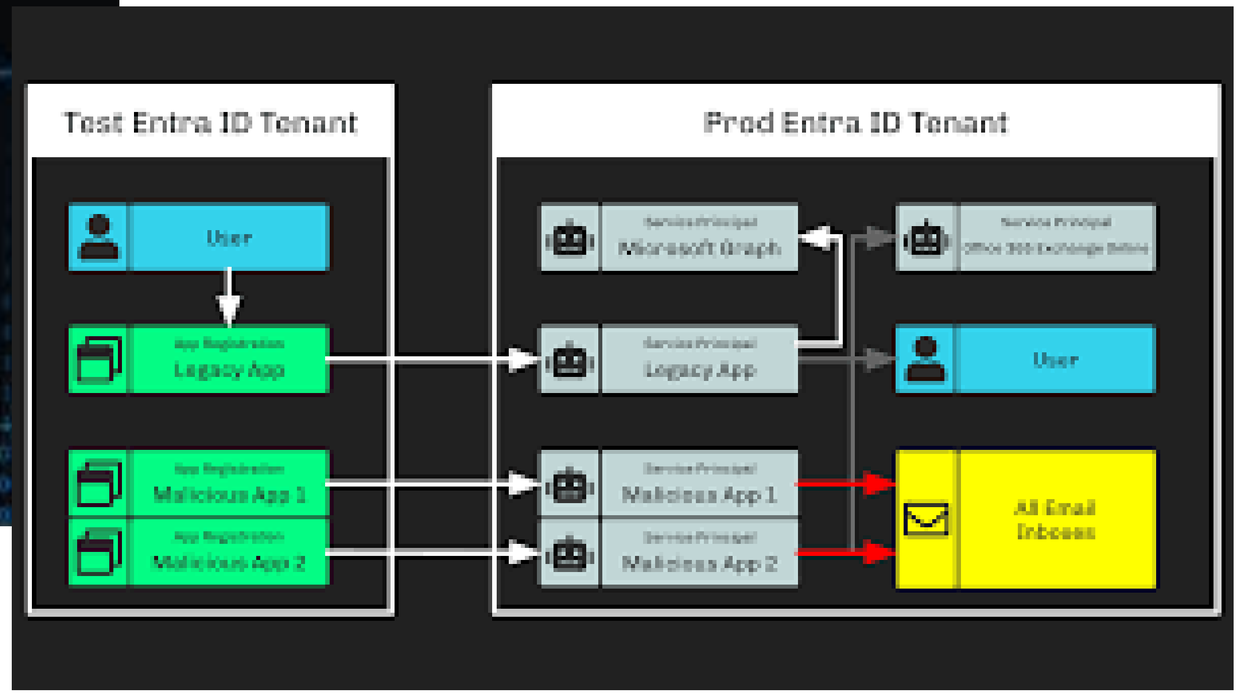
You Could Defend This…

accenture

Image credits to Bank Info Security and Joe Kaplan

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Or You Could Defend This…



accenture

Image credits to BeyondTrust and SpecterOps

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

But with hybrid, you must defend both!

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Why Entra-Only?

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Why Go Entra-Only?

RUNNING AND DEFENDING BOTH ACTIVE DIRECTORY AND ENTRA WASTES MONEY AND INCREASES RISK

RUNNING AND DEFENDING JUST ONE WOULD BE MUCH SIMPLER TO MAINTAIN, LESS EXPENSIVE TO DEFEND, AND LESS RISKY TO OPERATE

THE ONLY SANE ONE TO GET RID OF IS ACTIVE DIRECTORY BECAUSE MODERN SERVICES LIKE O365 DEPEND ON ENTRA

ACTIVE DIRECTORY ISN’T GOING TO UNINSTALL ITSELF, SO YOU WILL NEED TO COMMIT RESOURCES TO MAKE THIS HAPPEN

accenture

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

But…

- This is a big, complex problem to solve
- It will struggle for attention and resources
- It will need to be done incrementally
- The cost-based payoff may be long

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

How to Entra-Only?

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

This Is Not Impossible!

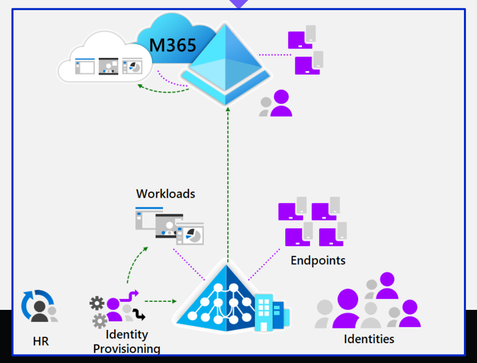
accenture

AD-to-Entra Key Milestones

Hybrid

Characteristics

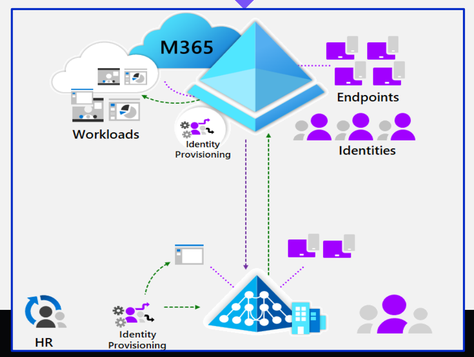
- Majority of object creation occurs in AD and is synced to Entra
- Directory identities, endpoints, and applications are available in both AD and Entra
- Authentication and authorization occur in both AD and Entra
- Both Entra and AD capabilities are used depending on scenario



Entra First

Characteristics

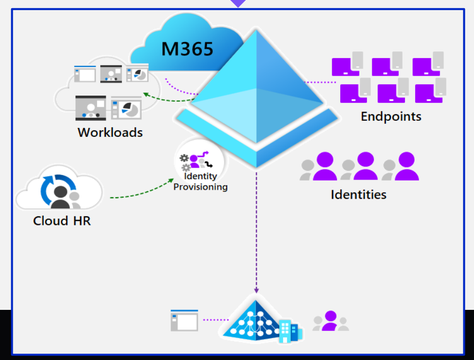
- Identities are created and managed in Entra and synced to AD when needed
- All new endpoints are created and managed in Entra; not synced to AD
- All solutions required to consume Entra; directory resources exist for applications



AD Minimized

Characteristics

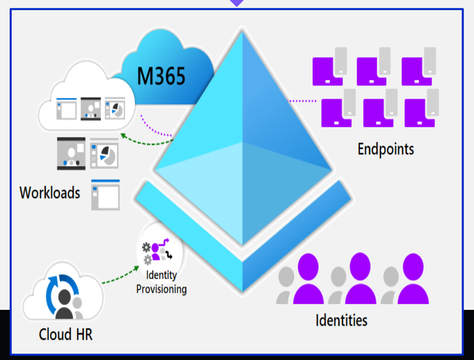
- All end user identities are removed from AD
- Only identities for administration and integration remain in AD
- No endpoint objects exist in AD
- Applications no longer use AD for end user authentication or identity data (authorization)



AD Retired

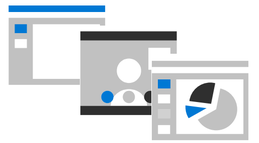
Characteristics

- AD is gone
- Only Entra remains



https://learn.microsoft.com/en-us/entra/architecture/road-to-the-cloud-posture

Areas of Work

	Identities	Endpoints	Applications
			
Objective	• Provisioning all identities in Entra. Writeback sync required objects until no longer needed in AD.	• Provisioning all workstations to be created and managed from Entra/Intune technologies. Entra Join instead of Hybrid Join. Intune instead of GPO. No endpoint Kerberos dependencies.	• Eliminate on-prem AD identity dependencies to run workloads (applications) • Eliminate servers or stop using AD to manage them
Components	• End Users (employees, contractors) • Administrators • Service Accounts • Groups	• Workstations	• Application identity integration • End user legacy authentication • End user identity data • Domain Joined Servers • Server management
Key Technologies	• Cloudsync with Writeback • Entra inbound provisioning API • Your identity provisioning tool stack	• Autopilot • Intune	• Azure Arc • Microsoft Graph • “The Cloud Itself”

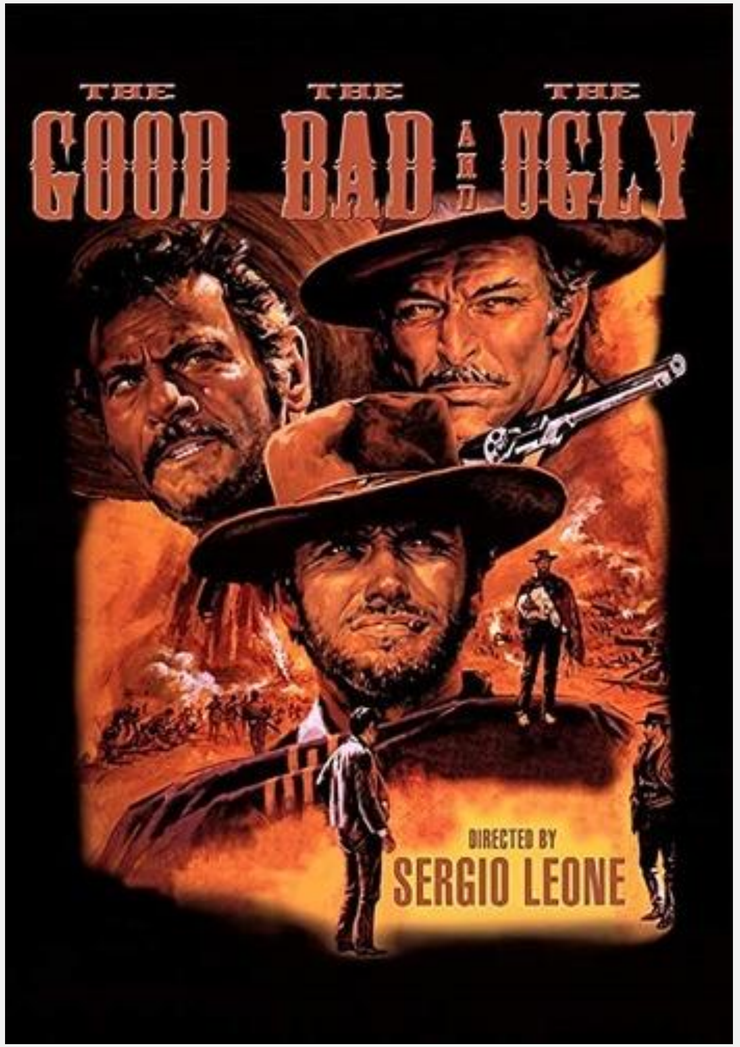
Milestone Completion Definitions

	Hybrid	Entra First	AD Minimized	AD Retired
Identities	Users and groups created in AD, synced to Entra. They may be consumed on-prem or in the cloud.	Users and groups are created in Entra and synced back to AD using cloud sync writeback if applications.	“Normal” users and groups are removed from AD (disable sync). Remaining users are admins and service accounts. Groups support app/server management.	Only Entra remains.
Endpoints	Workstations are hybrid joined and synced from AD to Entra.	All new workstations are Entra Join/Modern Management.	All workstations are Entra Joined. Hybrid workstations are gone. No workstation objects exist in AD.	Only Entra remains.
Applications	Applications may depend on either AD or Entra for directory data. Servers are hybrid joined.	No new applications are introduced with AD dependencies for identity data or management. No new hybrid join servers are introduced.	AD only exists run legacy applications, typically on legacy servers. Administrator accounts for AD are either unsynced or created in Entra and written back to AD via Cloud sync.	Only Entra remains.

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

What Is Accenture's Progress?


THE GOOD
THE BAD
AND
THE UGLY
DIRECTED BY
SERGIO LEONE

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

The Good: Workstations

Current status	What was easy	What was hard
• Entra Join is default build in some geographies • ~5 years until all hybrid workstations replaced	• No Kerberos apps • Normal work doesn't require VPN	• Rationalizing thousands of GPOs used for client-specific requirements • Scaling auto-pilot globally

accenture

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

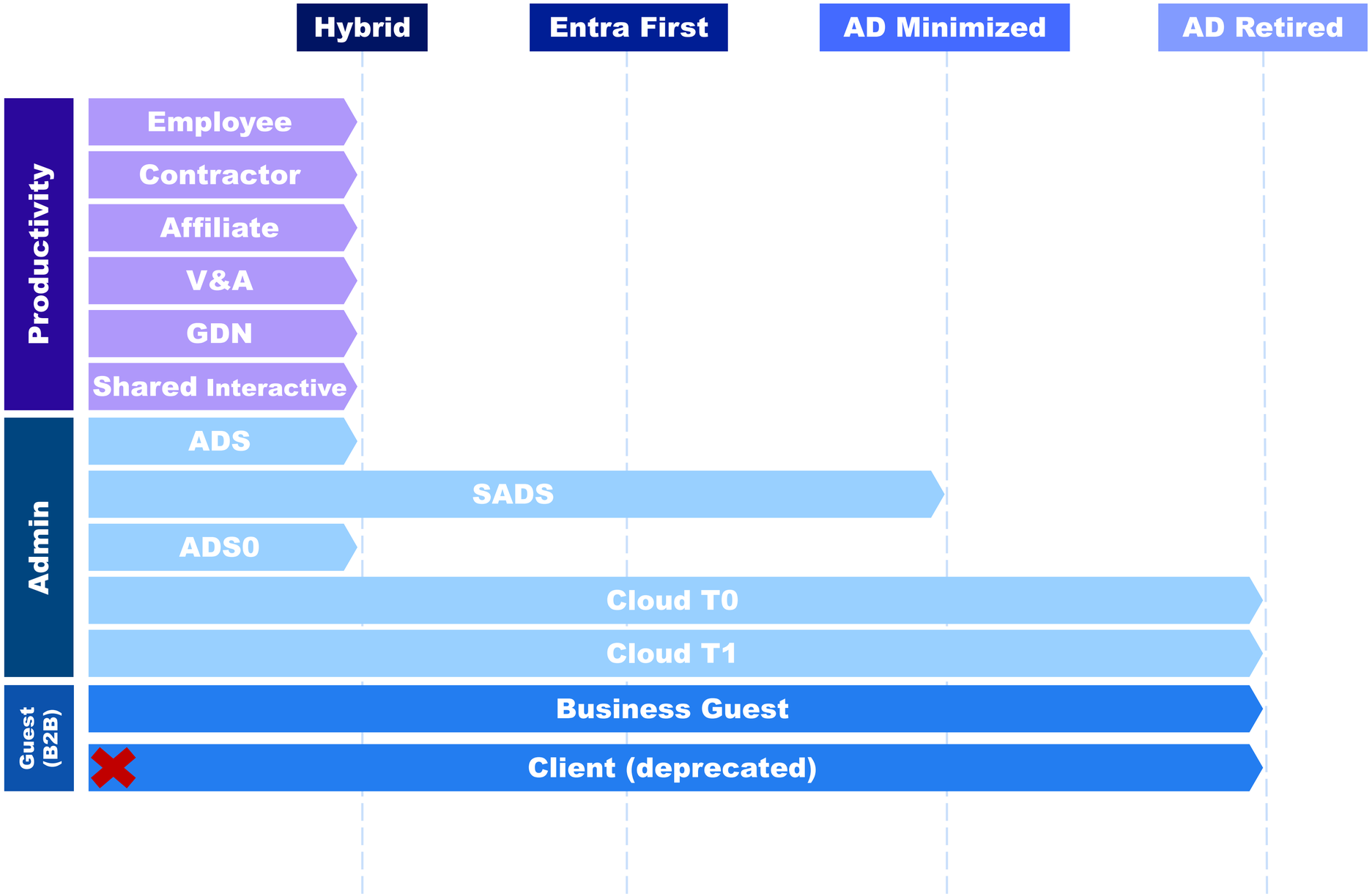
The Bad: Identities

Current status	What was easy	What was hard
• Some cloud-only accounts • Waiting for writeback	• Creating cloud-only accounts	• Cloud sync writeback scalability • Rationalizing our group management model

Important note: Our scale blocker for writeback likely does not impact you!

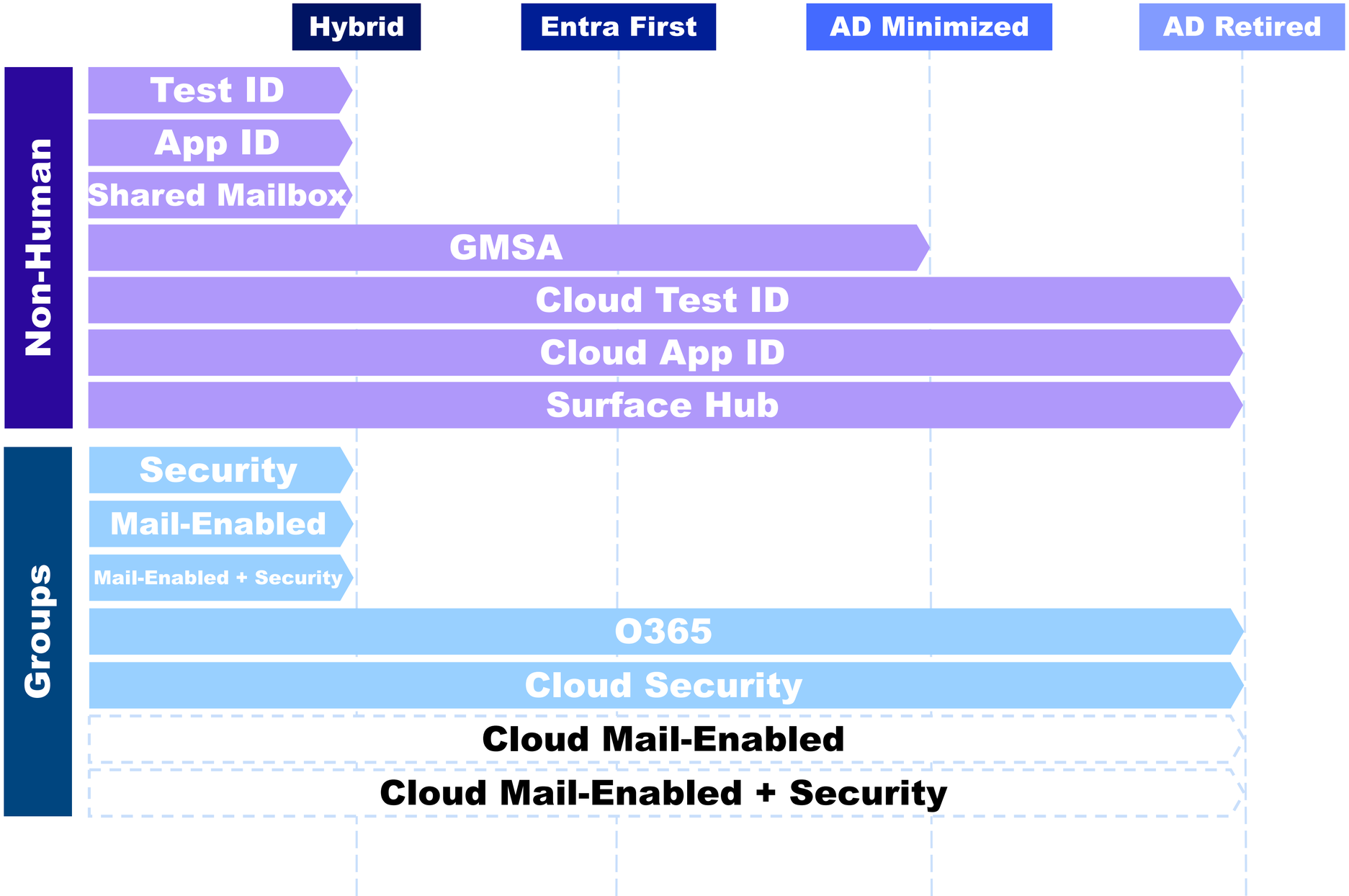
accenture

Human Identity Types Status by Milestone



accenture

Non-Human User and Groups Types Status by Milestone



accenture

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

The Ugly: Applications

Current status	What was easy	What was hard
• Possibility of using Azure Arc for server management • Limited remediation of some authentication and identity data dependencies	• Nothing	• Understanding behavior patterns and grouping services • Scaling remediation efforts • Committing to eliminating all servers

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Is It Worth It?

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Absolutely! But it can be a tough sell…

The timelines are likely in years. Patience and commitment needed.

New business functionality often gets prioritized over fixing tech debt.

Progress results in improved security posture.

Is it cheaper just to run and defend the legacy platform forever?

If I wait, does this get easier and cheaper in a few years?

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Call to Action!

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Call to Action!

Plan	Learn	Progress	Measure	Patience
Plan for a long campaign.	Learn the model and use the language. Learn the key technologies.	Look for opportunities to make progress with every program.	Measure all other investments and programs against these objectives.	Be patient and don’t give up!

And migrate those endpoints!

accenture

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?