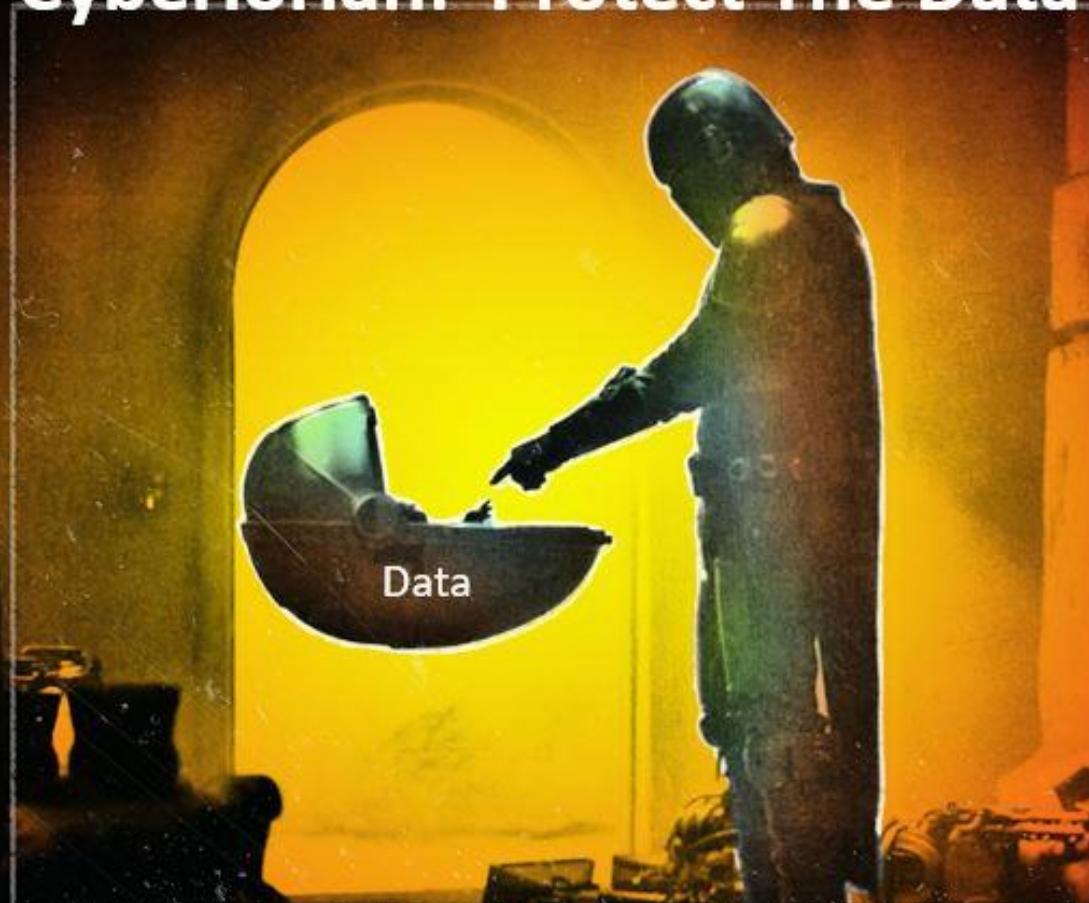


Cyberlorian: Protect The Data



9th Annual Hacking Conference

October 24-25, 2022

2



The Institute of
Internal Auditors
Chicago



ISACA
Chicago Chapter

Welcome To The 9th Annual Hacking Conference

Remember to check-in to this session on the app!

SECURITY THREATS AND EXPLOITS

The Needle in the Needlestack: Discovering Identity Risks

Bar Maor

Security Researcher, Illusive



EVOLUTION

Whoami



Bar Maor

- Lives in Tel-Aviv, Israel
- Security Researcher
- Ex-Penetration tester

illusive

Whoarewe

illusive

- “Built by attackers to stop attackers”
- Discover & remediate privileged identity vulnerabilities



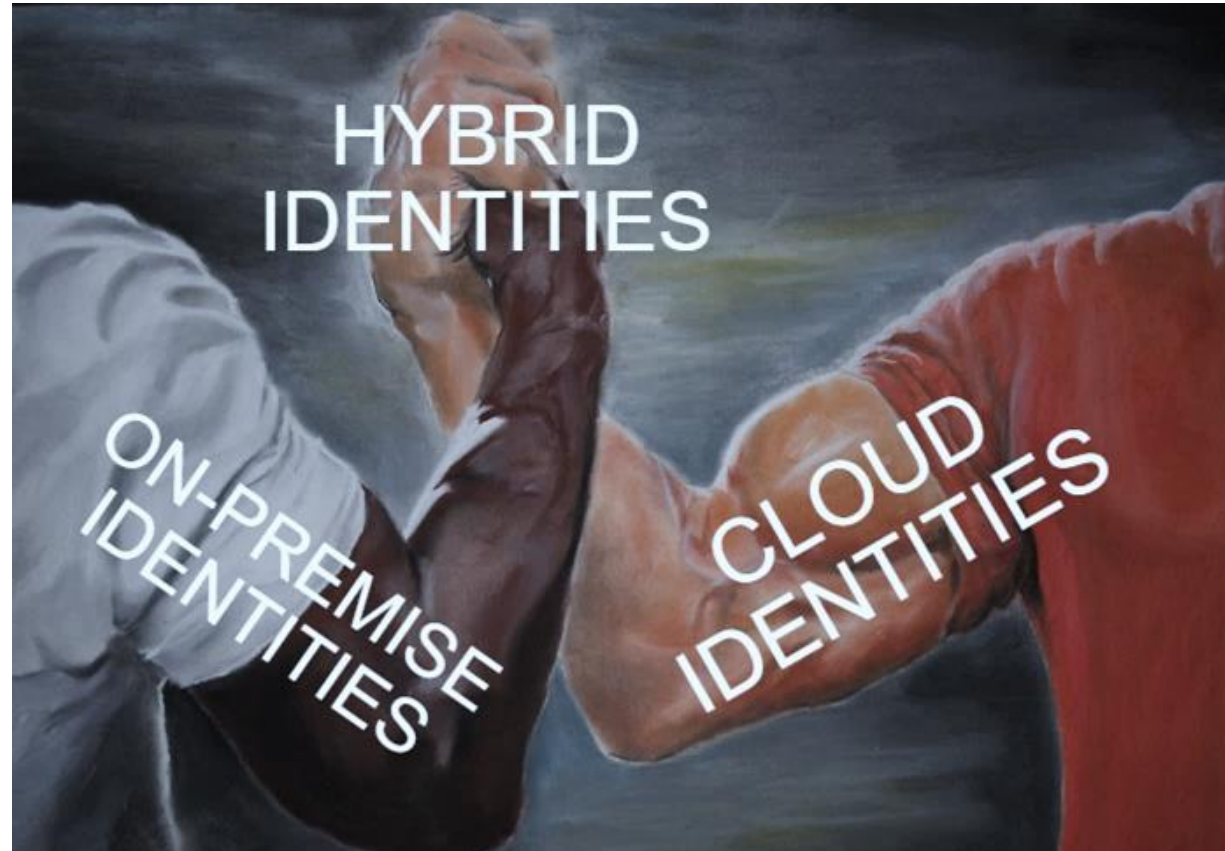


vulnerability

Identity is the new ~~perimeter~~

ITDR












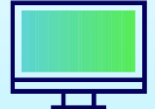





“... collection of tools and best practices to **defend identity systems.**”



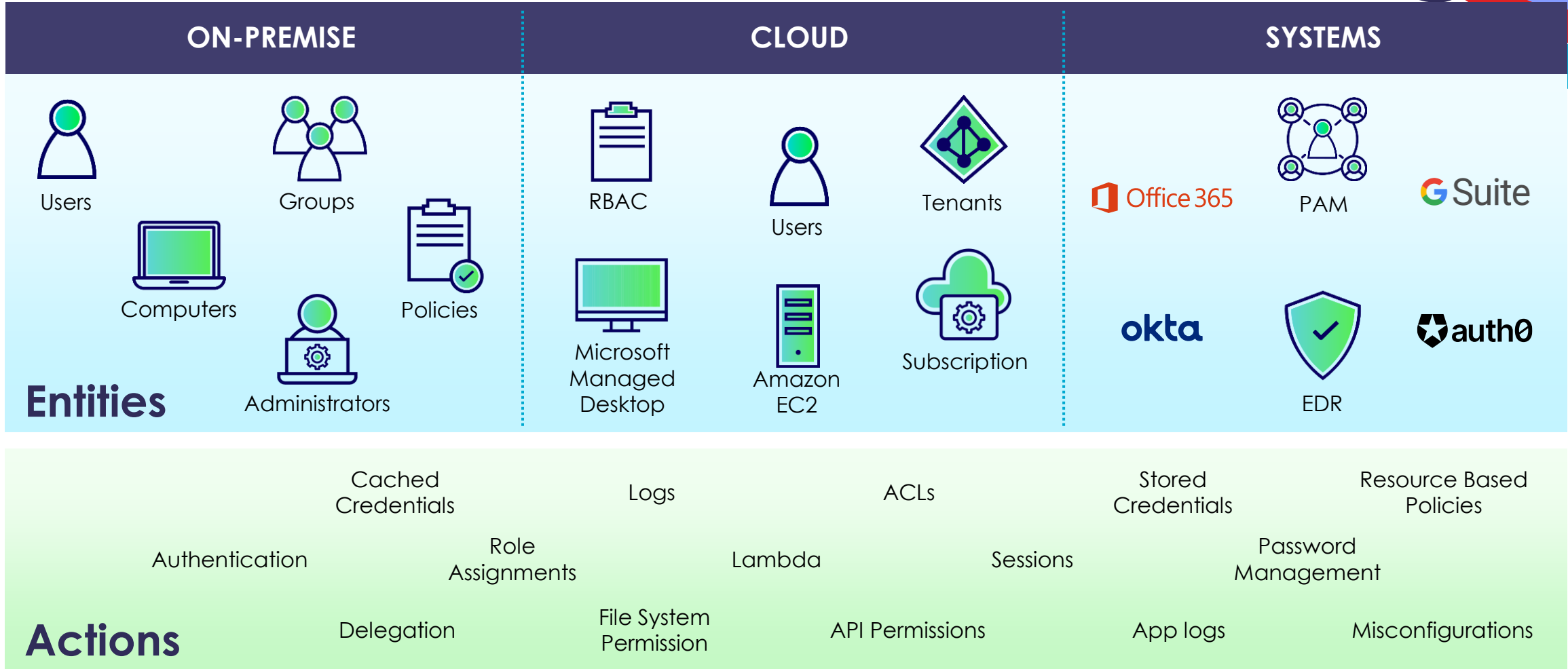
A Whole New World



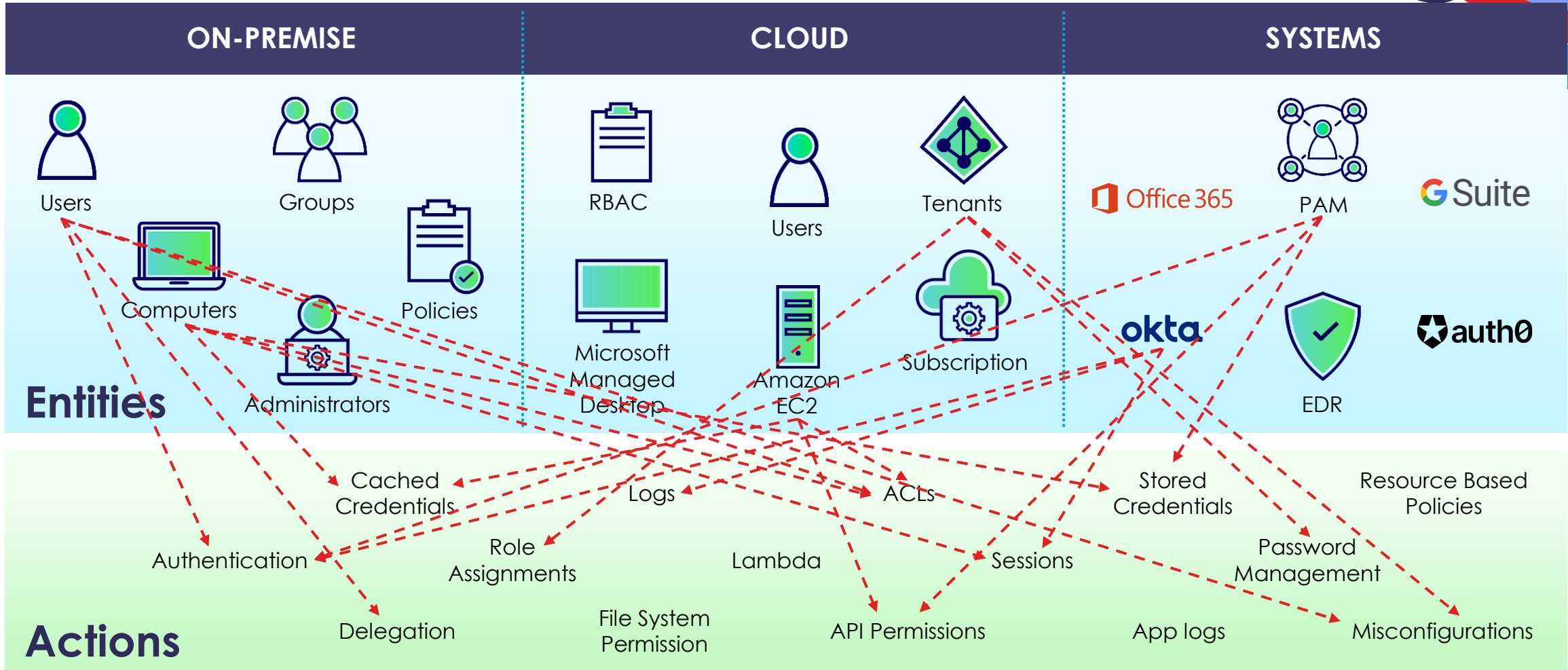
Entities

| | | | | | | | | |
|--|---|---|---|---|---|--|--|---|
|  Users |  Groups |  RBAC |  Users |  Tenants |  |  PAM |  | |
|  Computers |  Administrators |  Policies |  Microsoft Managed Desktop |  Amazon EC2 |  Subscription |  |  EDR |  |

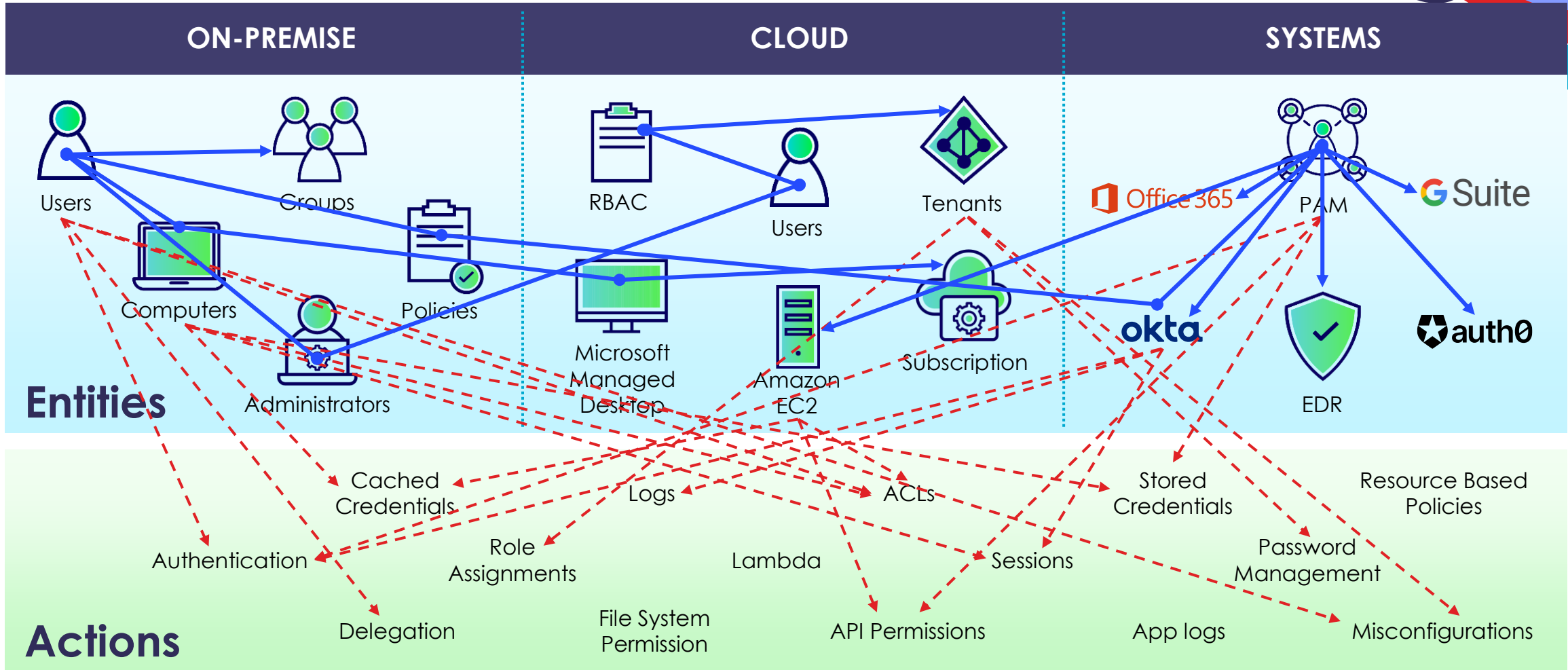
A Whole New World



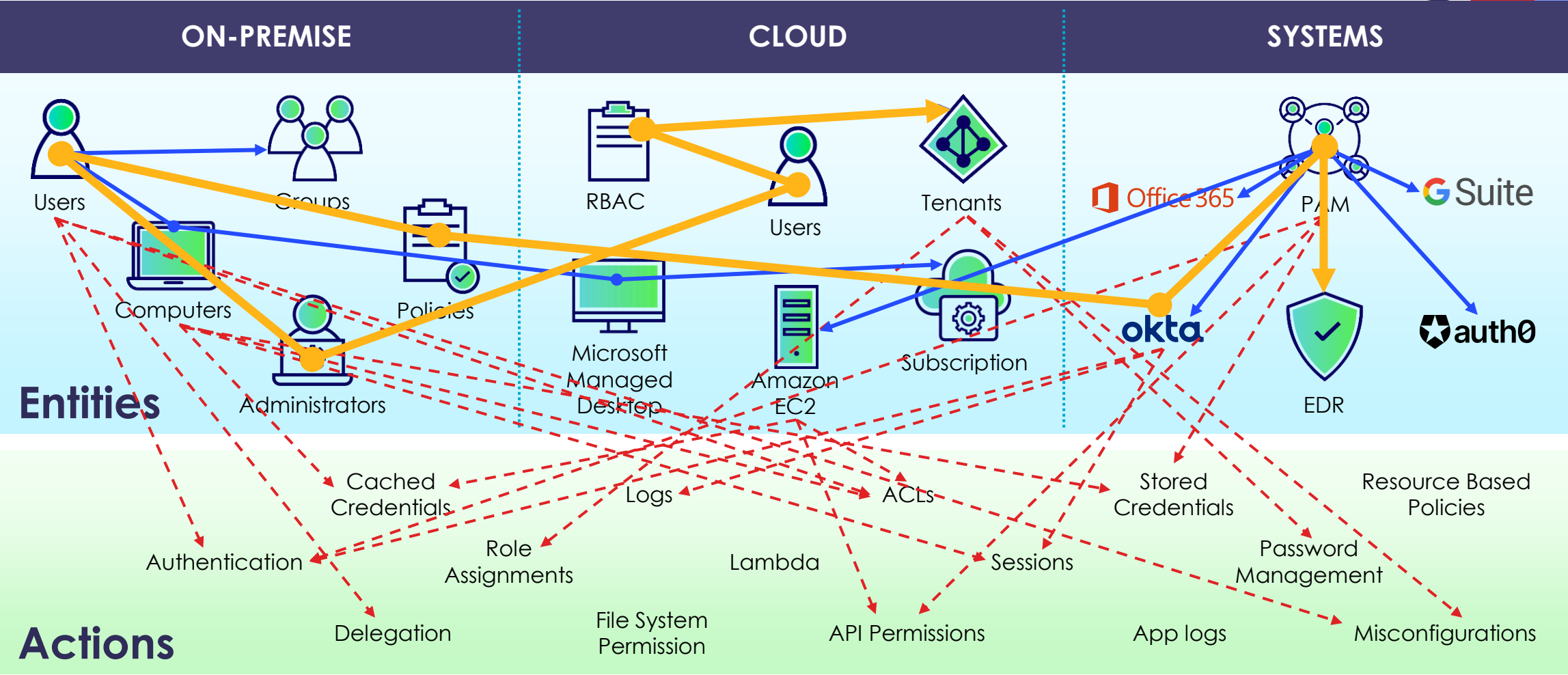
A Whole New World



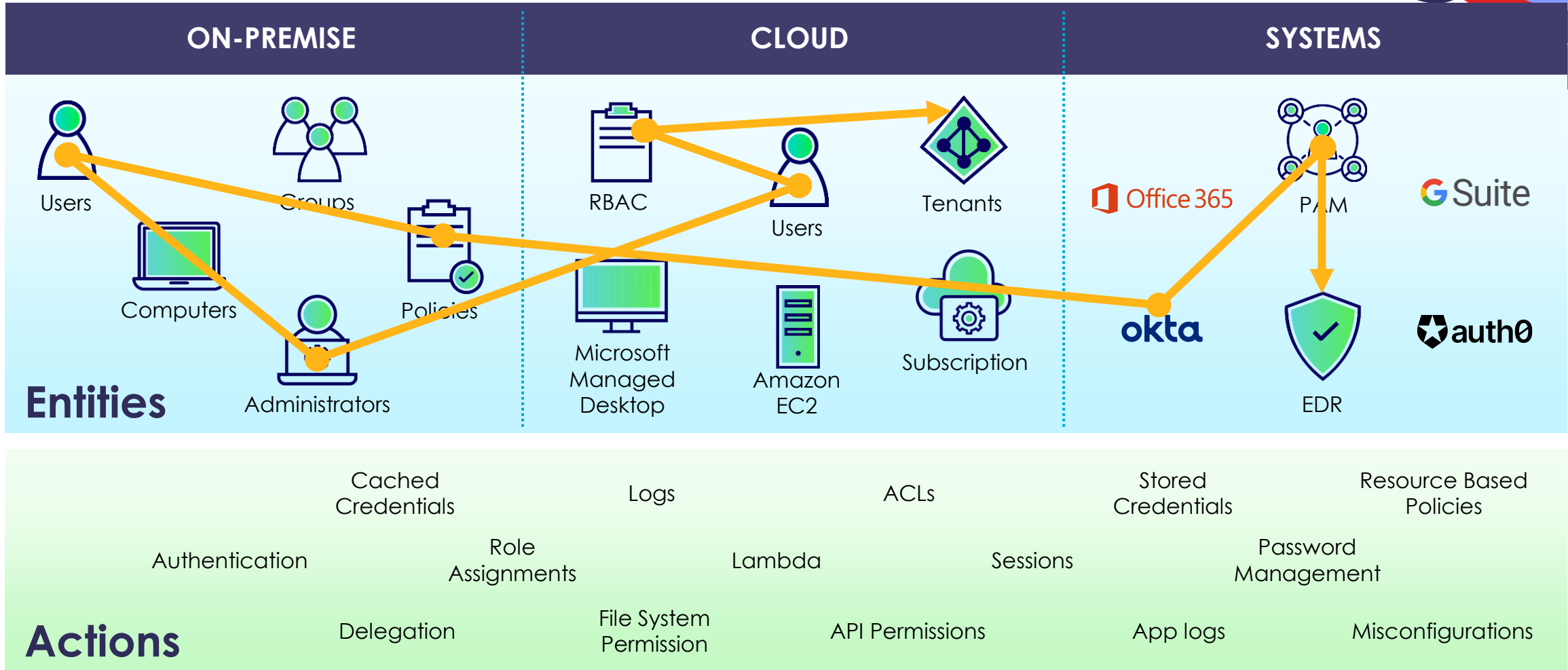
A Whole New World



A Whole New World



A Whole New World



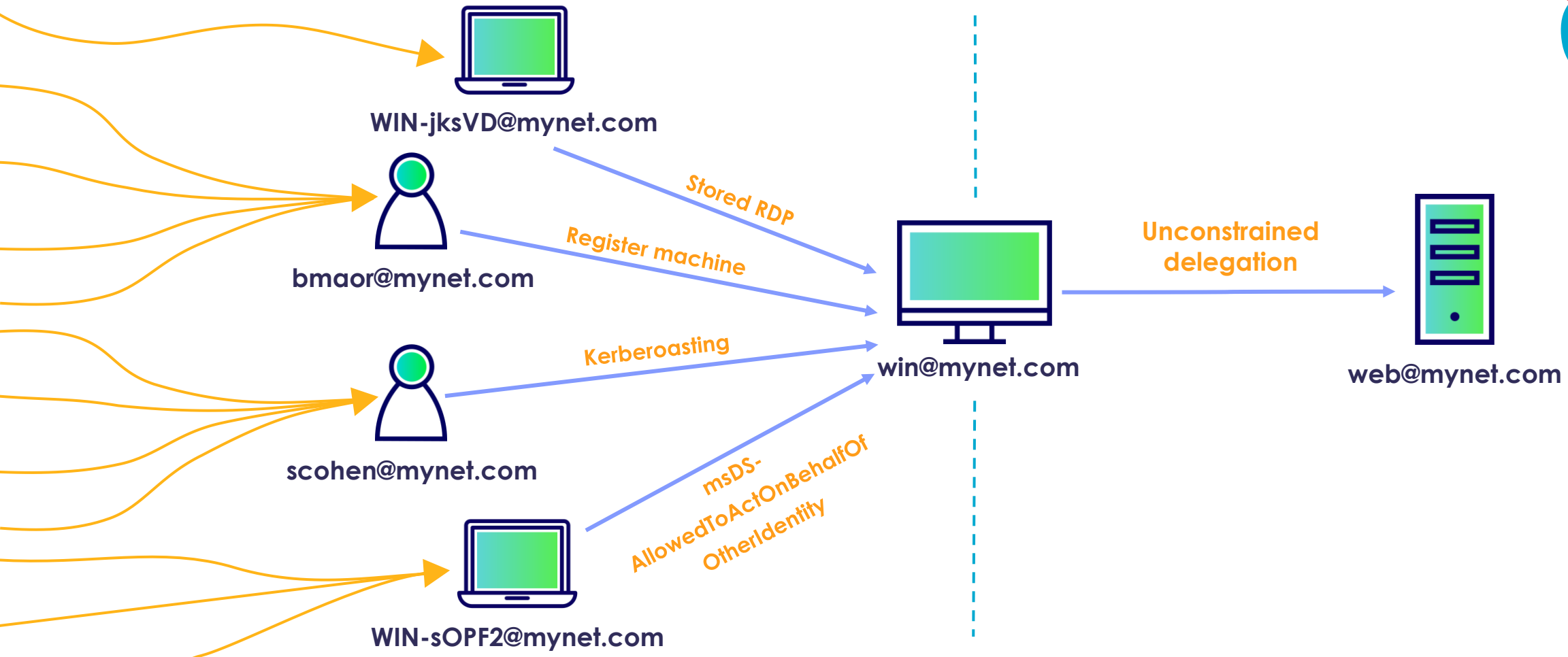
Shadow Administration

Identities that are privileged **outside of best practices**, and aren't easily **visible** to IT or security teams.

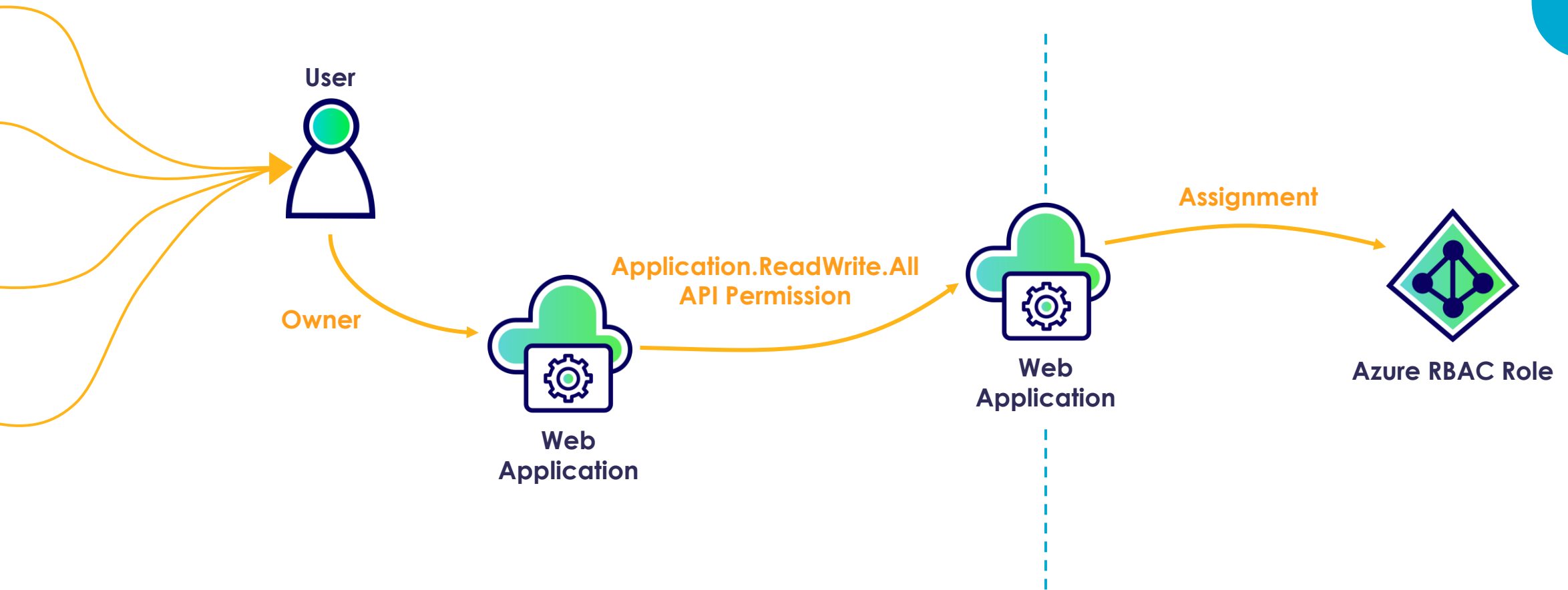
100% of organizations have **shadow admin** risks



Shadow Administration



Shadow Administration



Identities Classification



Unmanaged



87% of local admins are not enrolled in a LAPS or PAM

Misconfigured



100% of organizations have shadow admin risk

Exposed



Privileged account passwords are left exposed on **13%** of endpoints

Identities Classification



Unmanaged



87% of local admins are not enrolled in a LAPS or PAM

Misconfigured



100% of organizations have shadow admin risk

Exposed



Privileged account passwords are left exposed on **13%** of endpoints

Identities Classification



Unmanaged



87% of local admins are not enrolled in a LAPS or PAM

Misconfigured



100% of organizations have shadow admin risk

Exposed



Privileged account passwords are left exposed on 13% of endpoints

Identities Classification



Unmanaged



87% of local admins are not enrolled in a LAPS or PAM

Misconfigured



100% of organizations have shadow admin risk

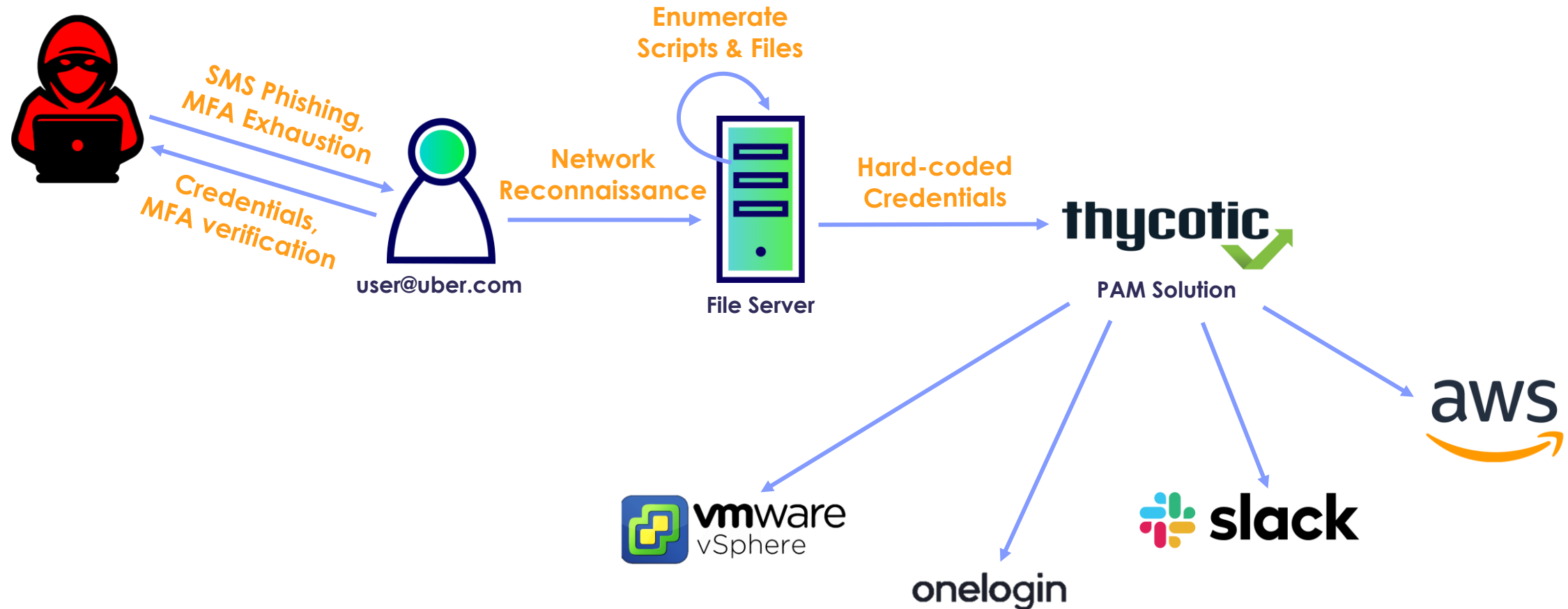
Exposed



Privileged account passwords are left exposed on **13%** of endpoints

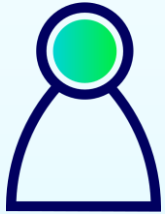
UBER Attack

Attack Scenario



UBER Attack

Identity Perspective



user@uber.com

UNMANAGED

- Stale object
- Can register machines to the domain



File Server

MISCONFIGURED

- Permissive access to sensitive data
- Hard-coded credentials in scripts



PAM Solution

EXPOSED

- Password-based authentication
- No approvals for privileged session



Identity & Access Provider

MISCONFIGURED

- Max number of failed login attempts
- Phishing-resistant is disabled

Making it Actionable



1. Protect **Identity Systems** as much as the **Identities** themselves
2. Find and remediate **Shadow Admins** threats
3. Search attack **Paths**, not points

Questions?



Welcome To The 9th Annual Hacking Conference

**How would you protect Grogu
(Baby Yoda), if Grogu was sensitive
data?**

Welcome To The 9th Annual Hacking Conference

**Thank you for attending, remember
to check-in to this session on the
app!**