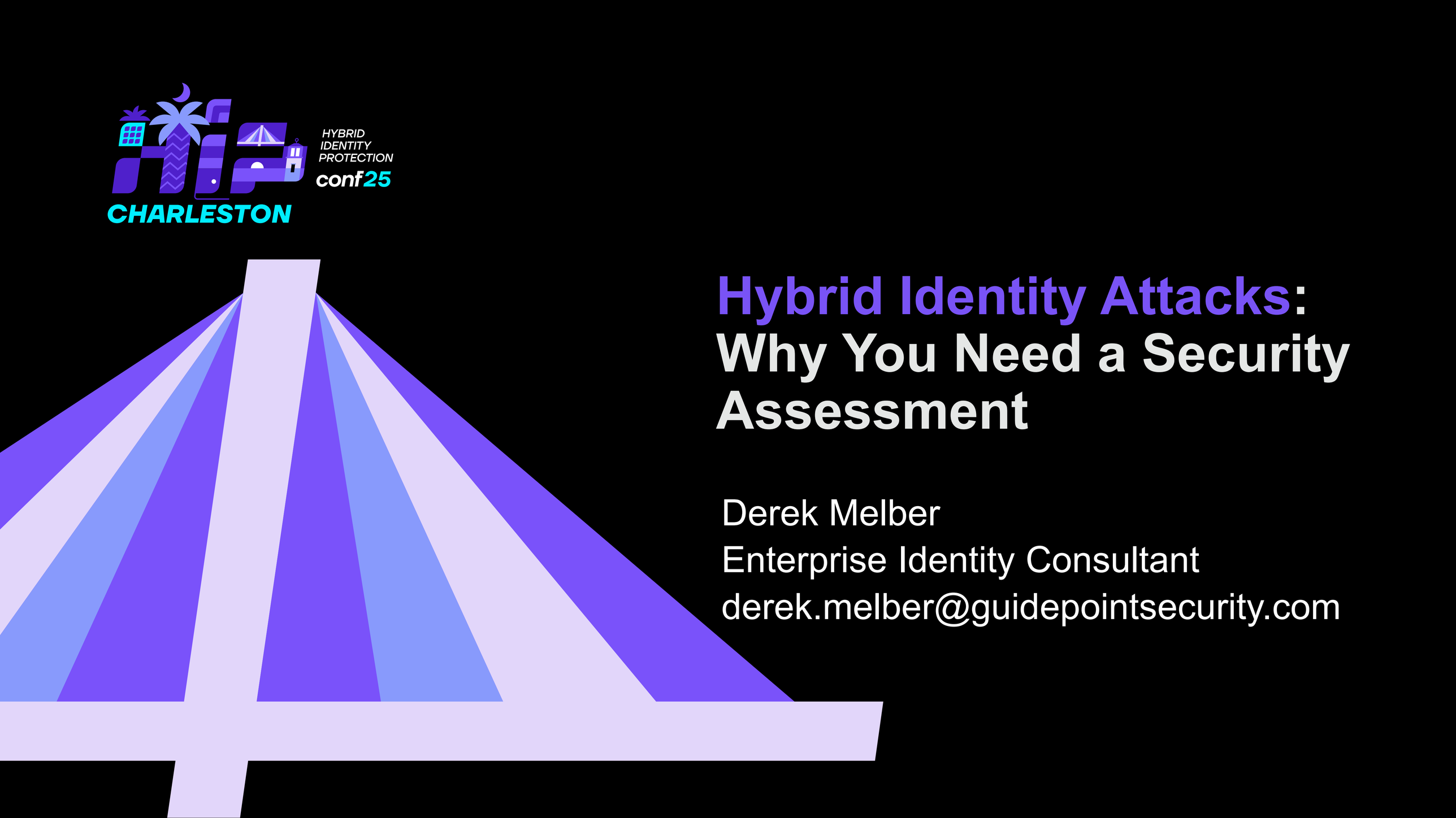


Hybrid Identity Attacks: Why You Need a Security Assessment

Derek Melber
Enterprise Identity Consultant
derek.melber@guidepointsecurity.com

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Derek Melber

Enterprise Identity Consultant,
GuidePoint Security

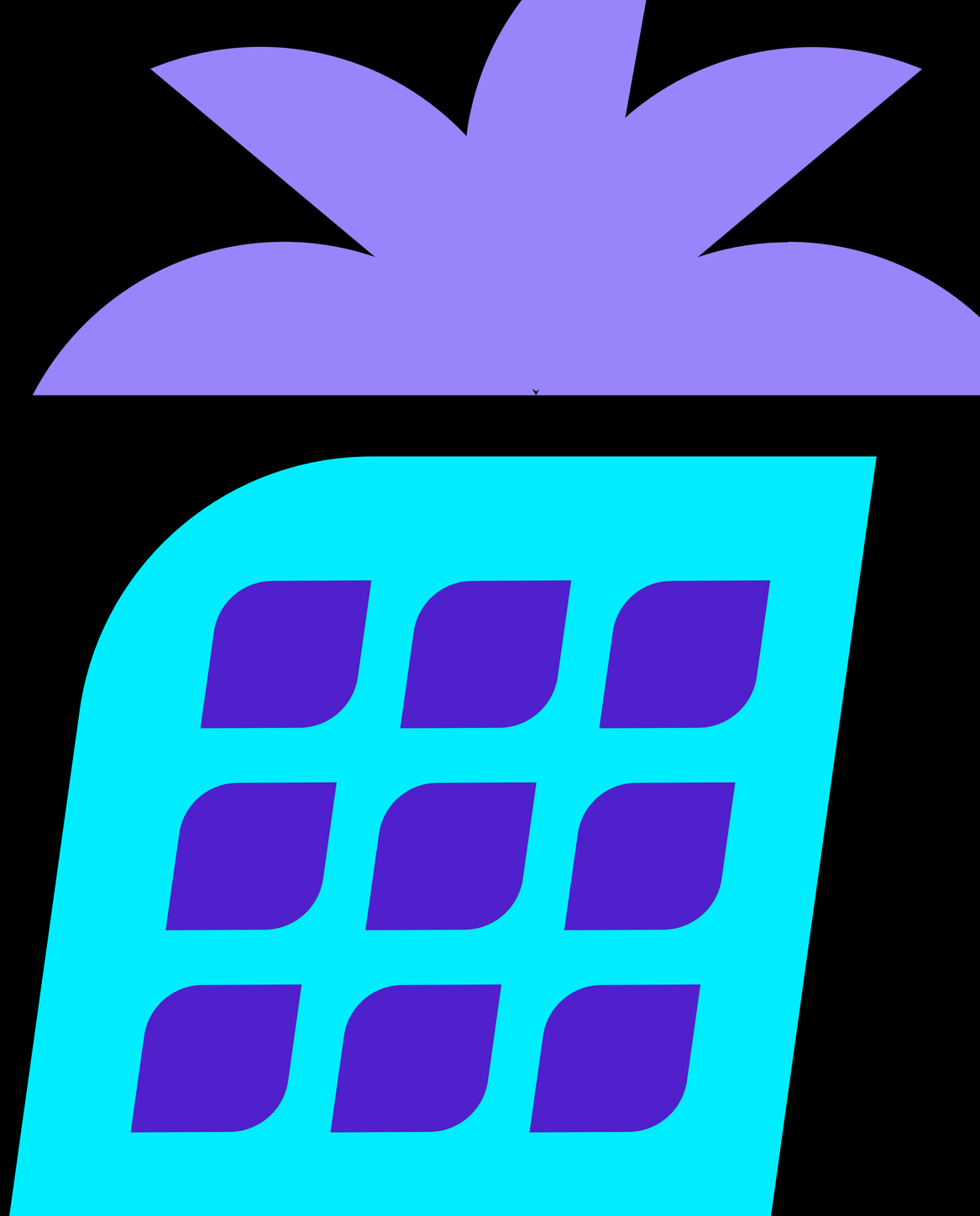
21x Microsoft MVP

16 Published Books

Keynote speaker in over 35 countries

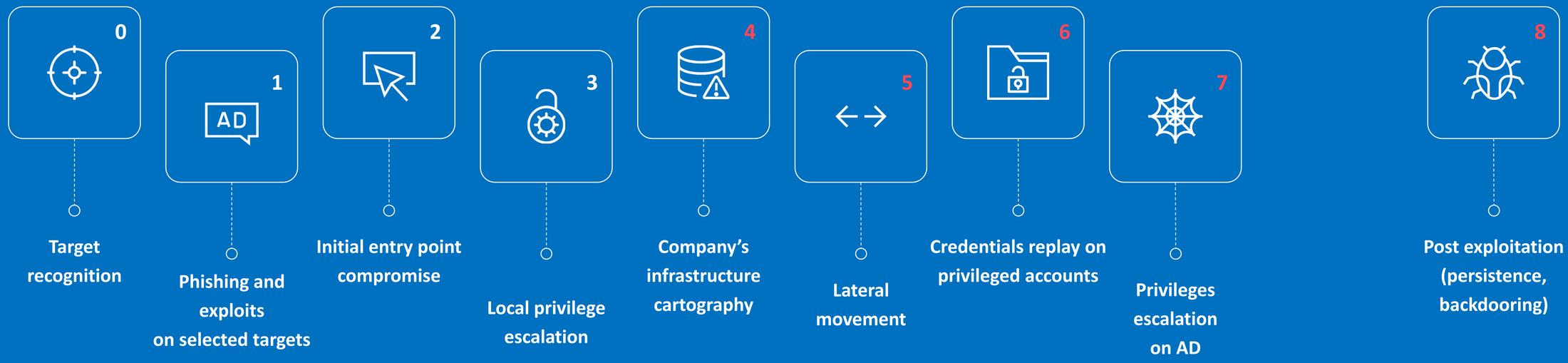
Agenda

- Typical Attack Tactics
- Securing On-Prem Active Directory
- Security Entra ID
- Hybrid AD Security Assessments



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Typical Attack Tactics



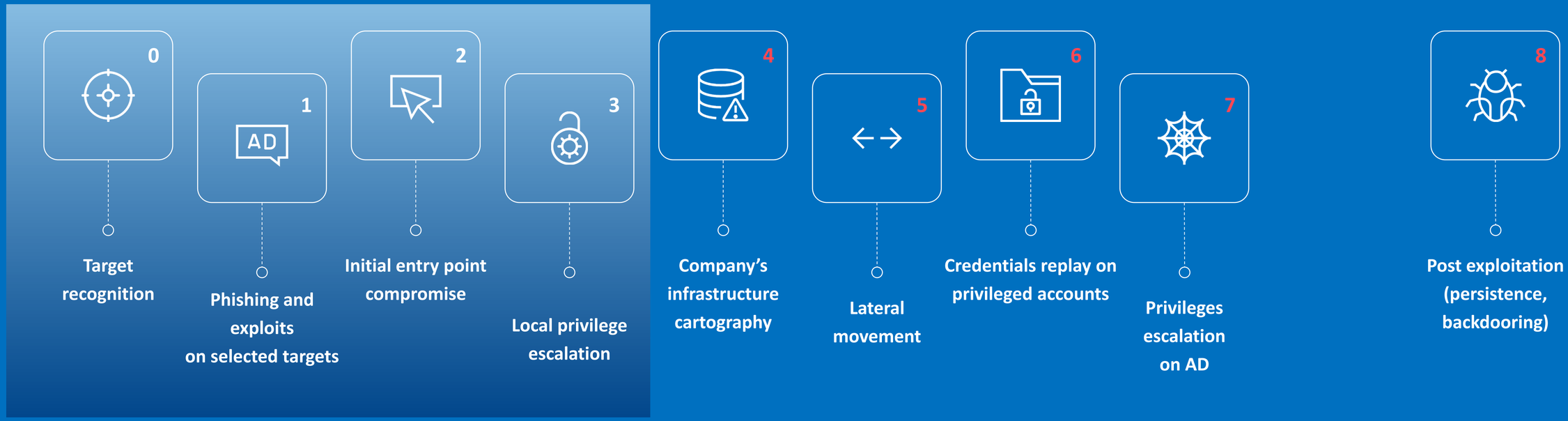
Attacker Tactics:

- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools

Current identity solutions

SECURITY TECHNOLOGIES:

PAM / MFA / IGA



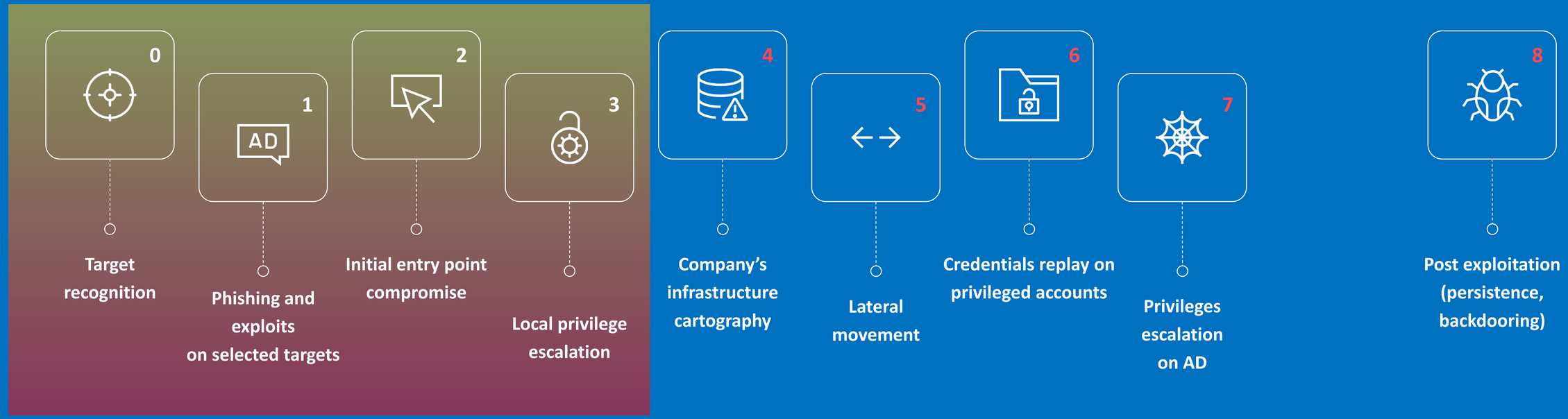
Attacker Tactics:

- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools

Current identity solutions

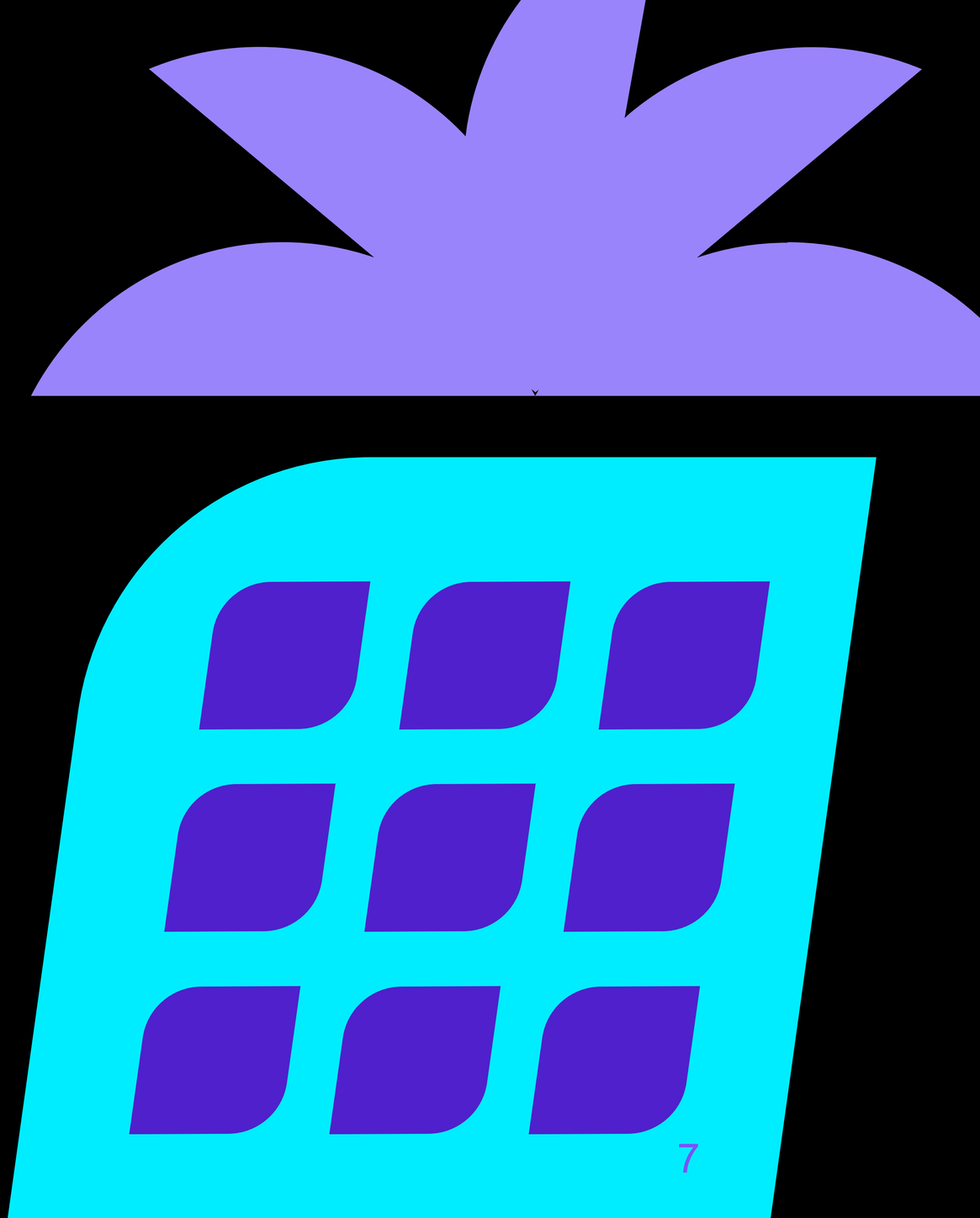
SECURITY TECHNOLOGIES:

PAM / MFA / IGA



Identities not secured

Securing On-Prem Active Directory



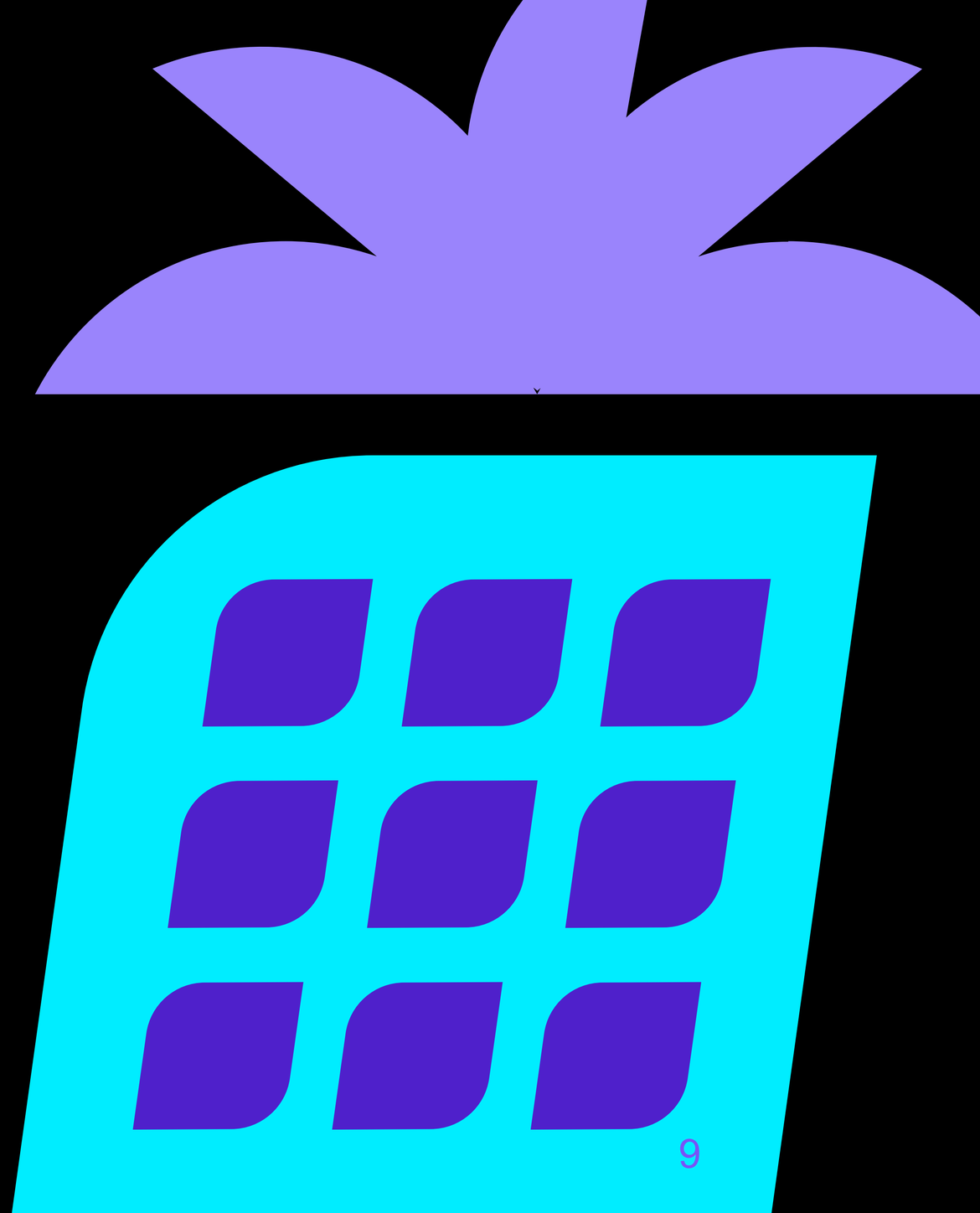
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Ensure exploitable configurations are secured

- Privileged users with SPNs
- Unconstrained Kerberos delegations
- Privileged Primary group ID
- Privileged SIDHistory
- Incorrect adminSDHolder entries
- Shadow Admins
- …

Securing Azure AD (Entra ID)



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Controlling AAD guests

- “Guest users have the same access as members”
- “Guest users have limited access to properties and memberships of directory objects”
- “Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)”

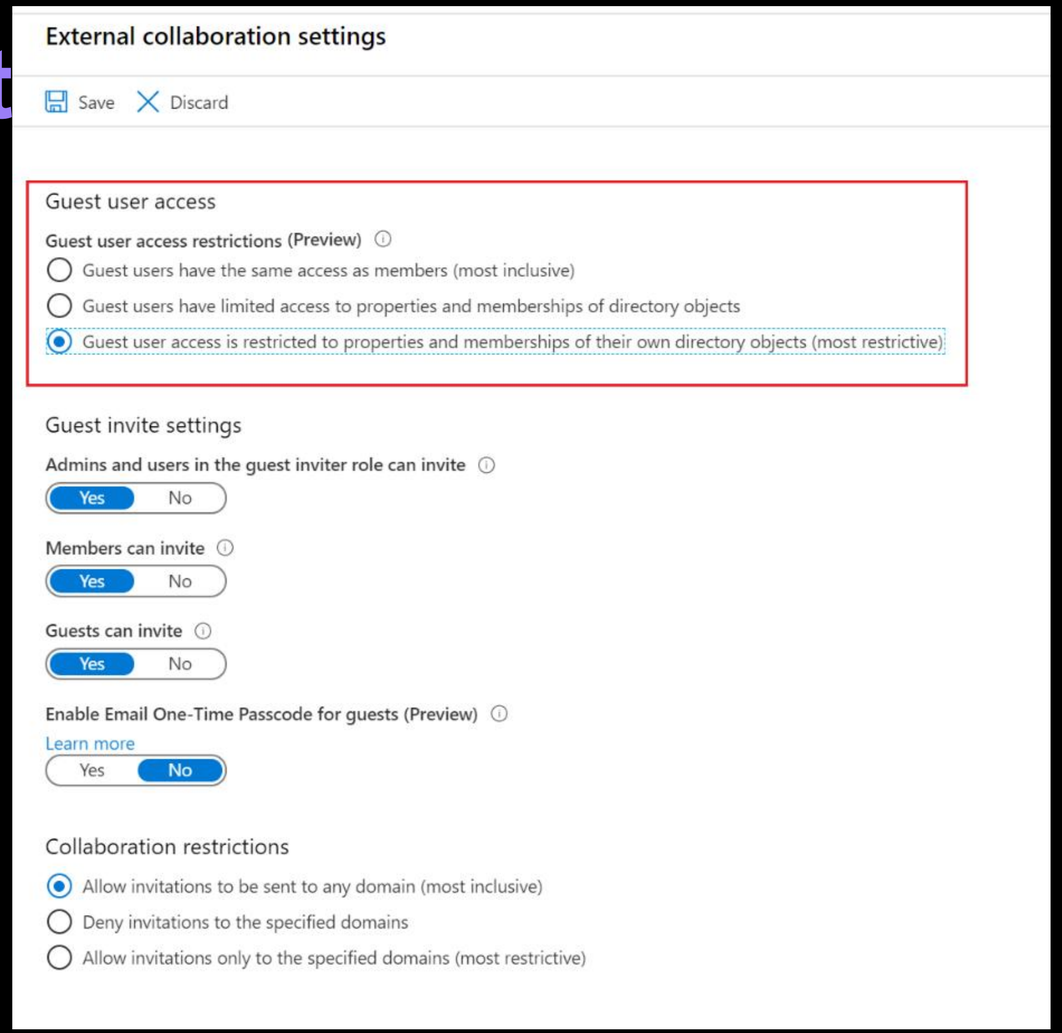
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

What can I get from AAD with guest?

- “Guest users have limited access to properties and memberships of directory objects”
  - Guest users can’t list objects
  - Guest users can read object properties
    - Users and contacts
    - Groups
    - Applications
    - Devices
    - Organization
    - Roles and scopes
    - Subscriptions
    - Policies

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AAD guest



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Azure AD Connect

- Utility installed on-premise
  - Has a high-privilege account in AD
  - Has also a high-privilege account in Azure AD
  - High value target!

```
PS C:\Users\baasbob> Get-ADUser -LDAPFilter "(samAccountName=MSOL_*)" -properties name,description | select name,descrip
tion | fl


name        : MSOL_206b1a1ede1f
description : Account created by Microsoft Azure Active Directory Connect with installation identifier
              206b1a1ede1f490e9c5caa0debc0523a running on computer o365-app-server configured to synchronize to tenant
              frozenliquids.onmicrosoft.com. This account must have directory replication permissions in the local
              Active Directory and write permission on certain attributes to enable Hybrid Deployment.
```

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

What can Sync account do?

- Dump all on-premise password hashes (if PHS is enabled)
- Log in on the Azure portal (since it’s a user)
- Bypass conditional access policies for admin accounts
- Add credentials to service principals
- Modify service principals properties
- Modify/backdoor/remove conditional access policies

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Cloud Sync

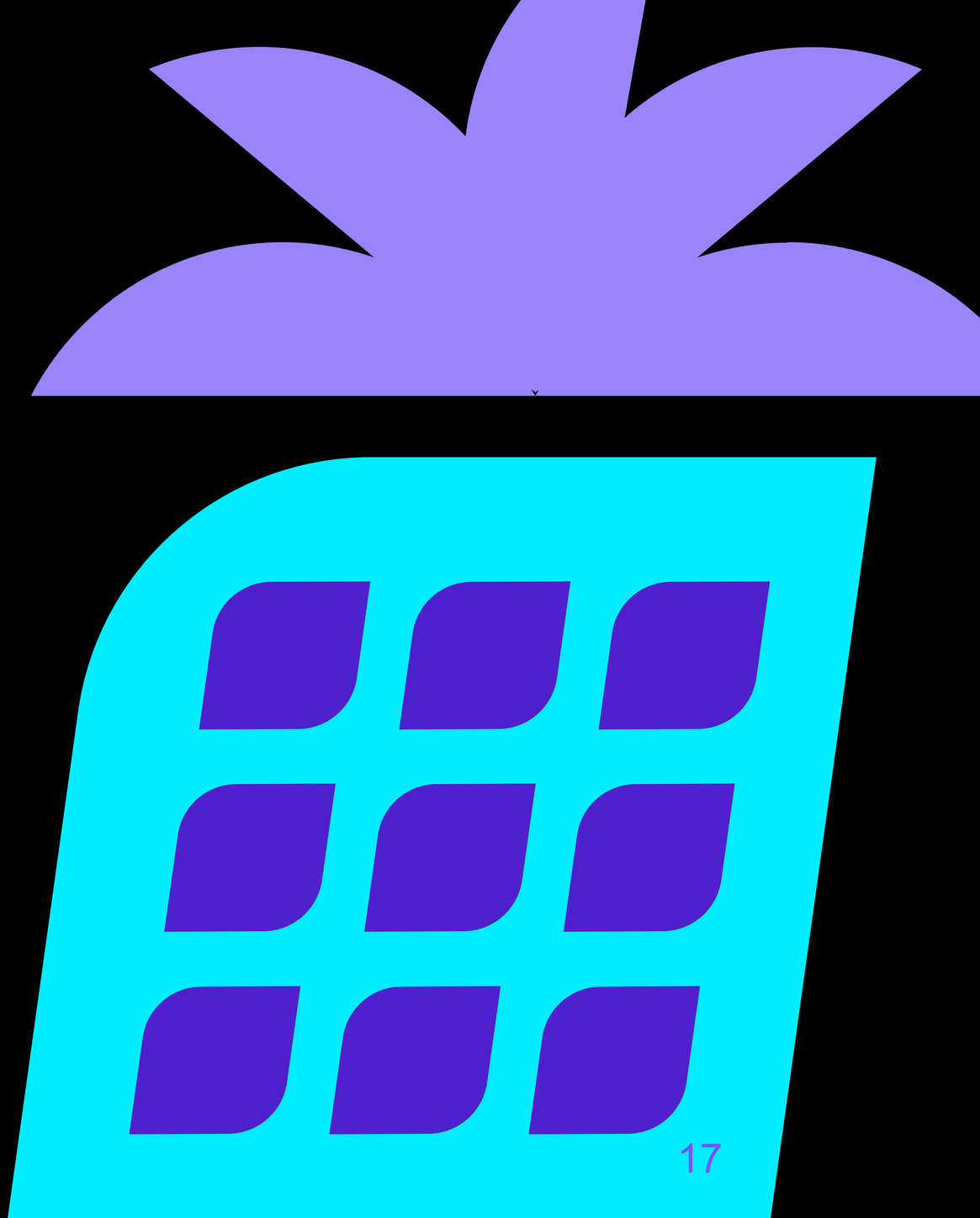
Feature	Connect sync	Cloud sync
Connect to single on-premises AD forest	•	•
Connect to multiple on-premises AD forests	•	•
Connect to multiple disconnected on-premises AD forests		•
Lightweight agent installation model		•
Multiple active agents for high availability		•

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Conditional Access Policies

- Default
- Creation of a new one
  - Default is trumped
- Difficult to know what is actually in place!
  - Who has MFA?
  - When is MFA required?
  - Can service principals use MFA?
  - Who can modify them?

Hybrid AD Security Assessments



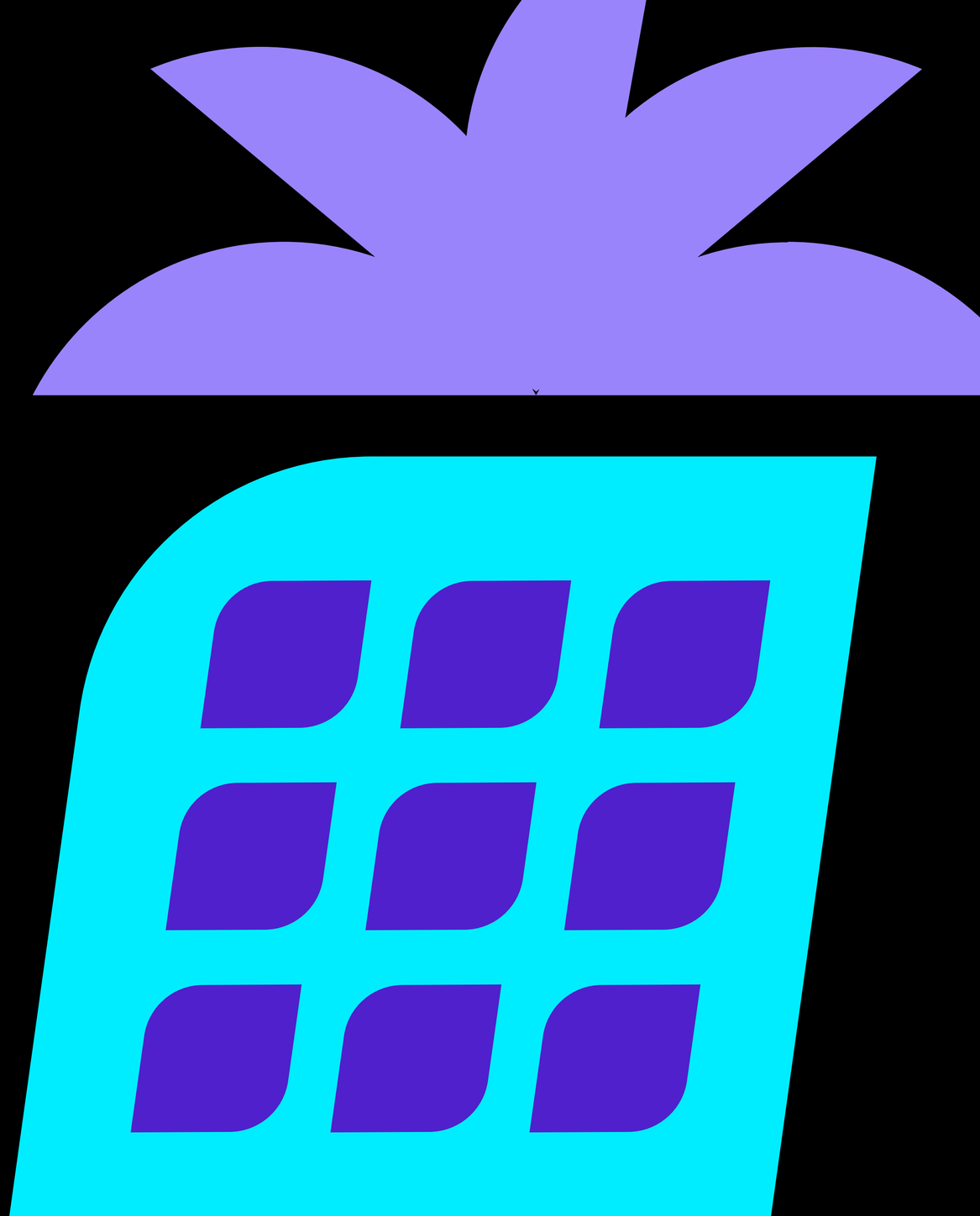
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Reasons to get an assessment

- Drift happens!
- You can’t secure what you don’t know about
- Pentests are not enough
- Your AD is not secure
- Current tools are exceptional
    - Fill gaps with PowerShell
    - Comprehensive assessment also requires GUI scrapes

Summary

- Typical Attack Tactics
- Securing On-Prem Active Directory
- Security Entra ID
- Hybrid AD Security Assessments



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Key Takeaways

- New AD CS attacks are being developed
- AD CS is **still** very easy to misconfigure 😭
- Low- and Medium-priority issues can stack quickly and go unnoticed and undefended when automated

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Derek Melber

derek.melber@guidepointsecurity.com

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON