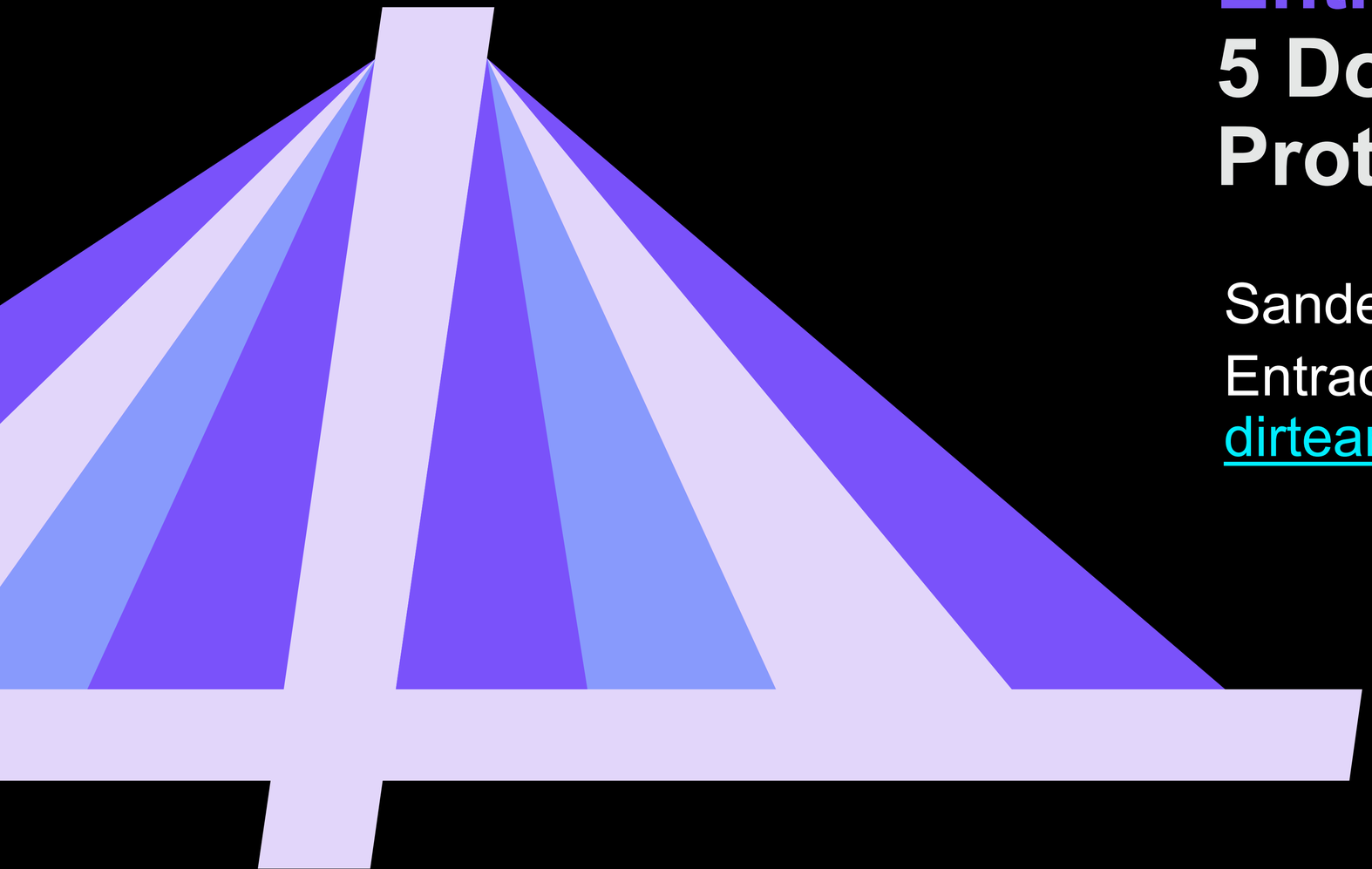
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



Entra ID Applications: 5 Dos & Don’ts to Protect Your Blind Spot

Sander Berkouwer,
Entraordinary Identity Architect
dirteam.com

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Sander Berkouwer

Entraordinary Identity Architect, dirteam.com

Sander Berkouwer is one of the most trusted voices in Active Directory and identity security. Sander is a Microsoft MVP, Veeam Vanguard, and VMware vExpert. He is also a hands-on consultant, author, and trainer with real-world insight.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Introduction

- Entra Apps are powerful but often misunderstood
- Common pitfalls can undermine security and manageability
- This presentation contains real-world examples
- This presentation provides recommended practices

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Entra App Fundamentals

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Applications in Entra ID

Applications enable secure interaction with Microsoft cloud resources

They provide identity for apps and APIs
- First-party apps (Microsoft)
- Third-party apps
- Line-of-Business apps

Key components
- App Registrations
- Enterprise Applications

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

App Registration vs Enterprise Application

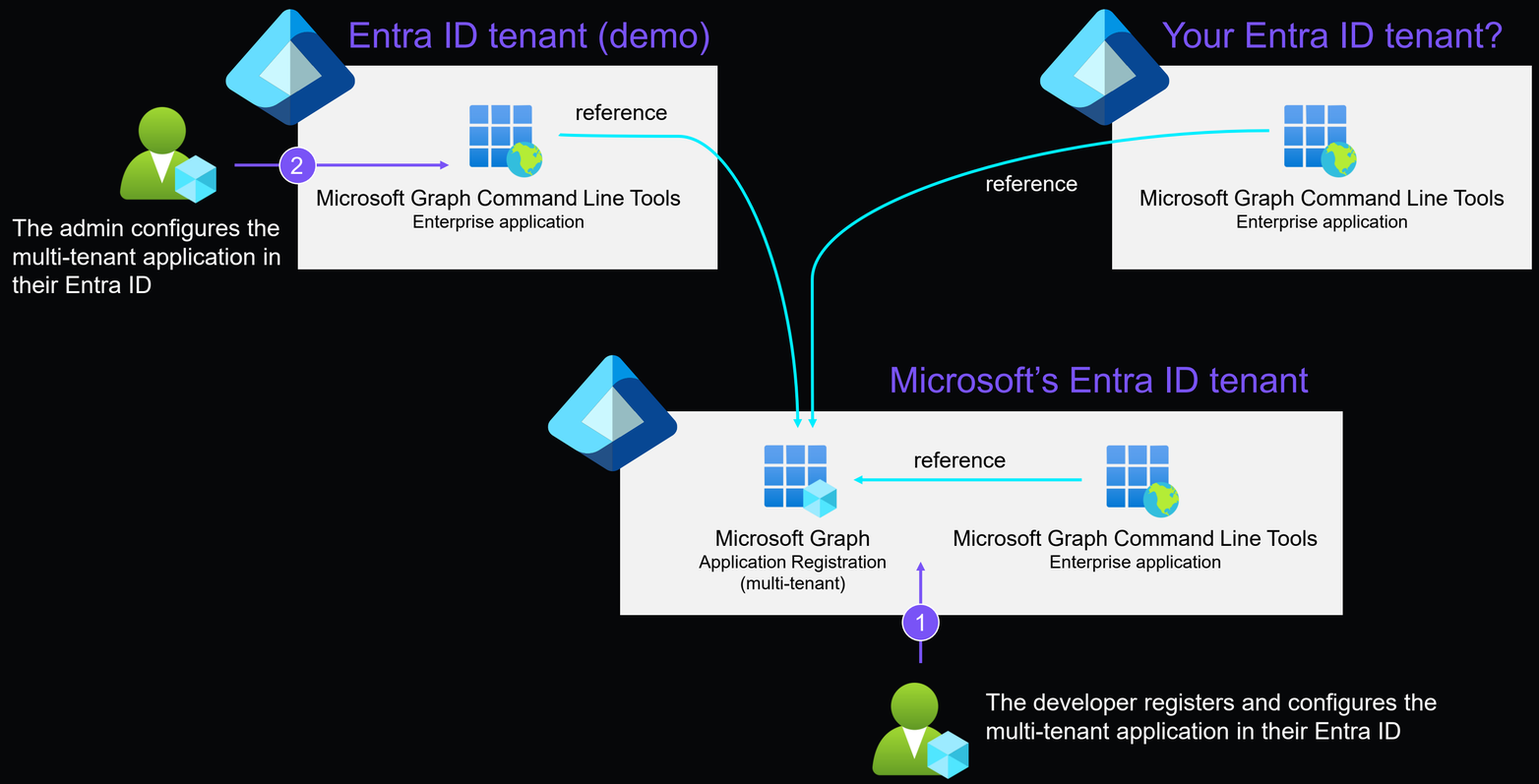
App Registration `Application`
- Blueprint (multi-tenant apps)
- Developer-side definition of the application
- Includes permissions, secrets, and branding

Enterprise Application `ServicePrincipal`
- Service principal created when the app is used in an Entra tenant
- Instance of the app in your tenant (multi-tenant apps)
- Also: user-assigned and system-assigned managed identities

Both must be reviewed for secure lifecycle management

In multi-tenant app scenarios, lifecycles of both are intertwined

Example:
Microsoft Graph Command Line Tools
Multi-tenant application



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

⛔ Don't Assume Understanding

Don’t assume anyone fully understands Entra applications.

- Your team
- Developers
- Vendors
- Microsoft…

Entra applications are not part of official Microsoft certifications or training.

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

✅ Leverage Applications for Modern Protocols

Use Entra Apps to avoid legacy protocol limitations and scenarios.

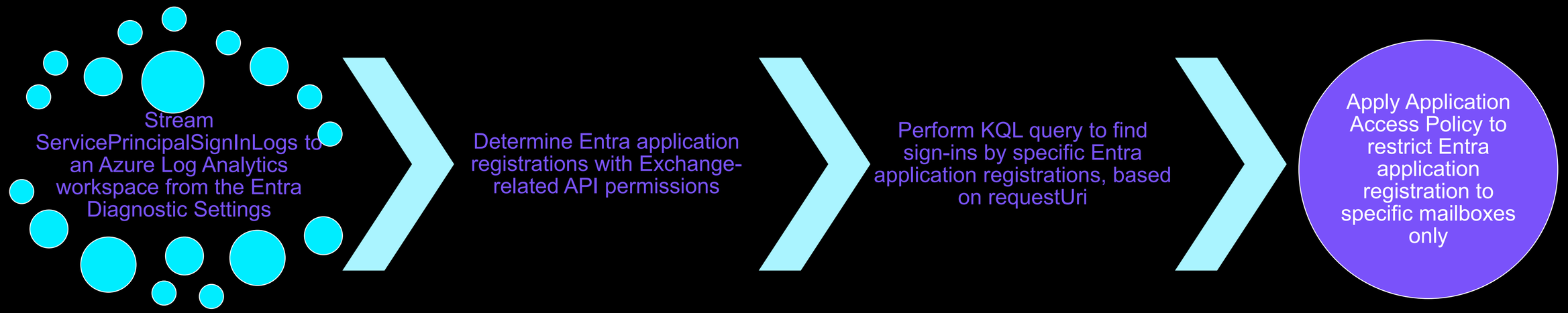
- SMTP, POP3, IMAP4 decommissioned, but apps can access mailboxes to send and/or receive mail
- Entra Connect Sync application-based authentication Default since v2.5.76.0

Scope admin-consented API permissions narrowly.

- Scope `Mail.SendAs` and `Mail.ReadWrite` down for Exchange Online
- Use `Sites.Selected` instead of `Sites.ReadWrite.All` for SharePoint Online

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Process for Scoping Down Exchange Mailbox Access



More info: appgovscore.com/blog/how-to-restrict-microsoft-graph-api-access-to-mailboxes

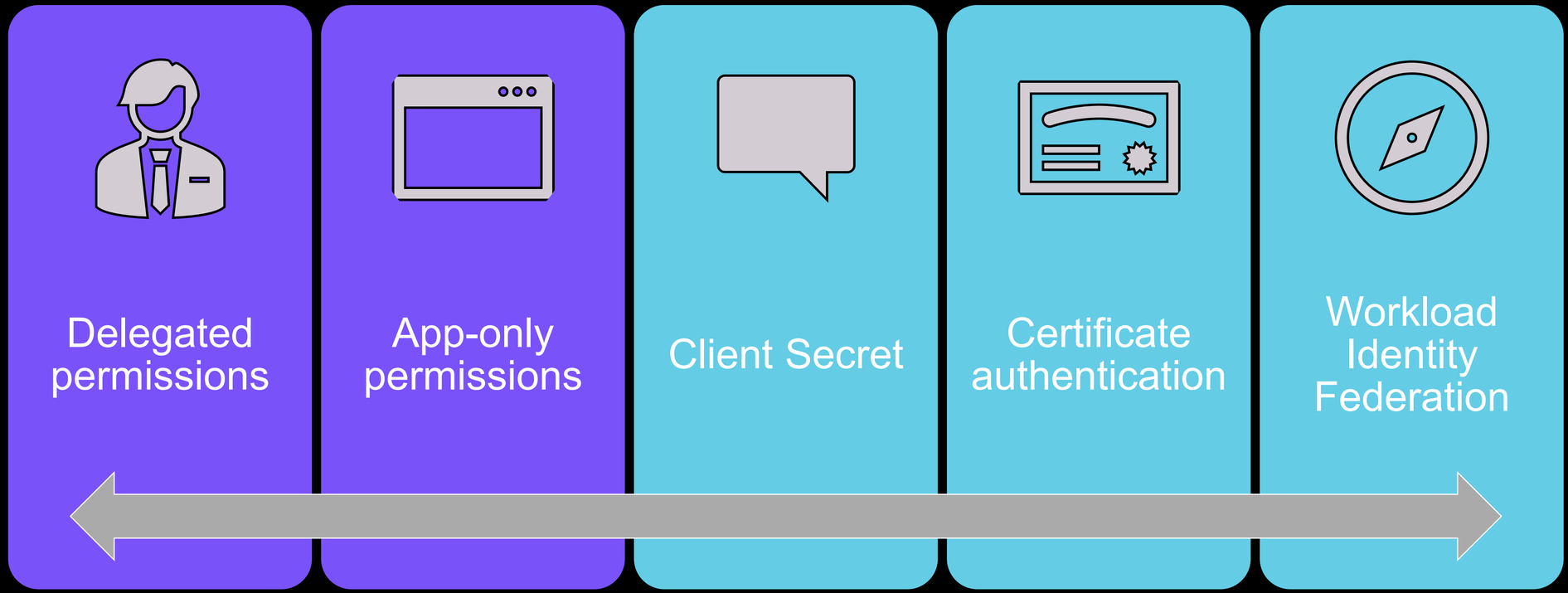
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Application Security Fundamentals

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Permissions and Authentication Options



App-only permissions

Run as the App Registration
• Client secret • Certificate-based • Federated Workload Identity
Permissions defined on the App Registration
Can only be consented by: • Privileged Role Administrator • Global Administrator

Delegated permissions

Run as the requester (user account)
Interactive Authentication
Permissions defined on the requestor’s user account
Can be consented by: • Cloud Application Administrator • Application Administrator • Privileged Role Administrator • Global Administrator

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

⛔ Don’t Use Broad Permissions

Internalize the principle of least administrative privilege.

Avoid Graph permissions like:

- Directory.ReadWrite.All
- RoleManagement.ReadWrite.All
- Application.ReadWrite.All
- User.ReadWrite.All
- GroupMember.ReadWrite.All
- Group.ReadWrite.All

Special mention for the ‘Microsoft Graph command line utilities’

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

✅ Perform Regular Access Reviews

- Audit Entra apps regularly to avoid overprivileged permissions
- Use the Application Governance feature in Microsoft Defender for Cloud Apps to gain insights in actual permissions use E5
- For own applications make changes, but for other apps work with the developer/vendor
- Monitor owners
- Monitor credentials

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Tenant-wide settings and practices

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

⛔ Don’t Accept Default Consent Settings

Microsoft has changed the default setting for all tenants from **Allow user consent** to **Do not allow user consent** as part of change MC1097272

Choose **Do not allow user consent** or **Allow user consent for apps from verified publishers for selected permissions (Recommended)**

Benign permissions that can be allowed:

- User.Read
- openid
- profile
- mail

Review and customize tenant-wide consent settings in the Entra Portal through **Enterprise Applications** > **Consent and Permissions**

Enable the Admin Consent Workflow feature

“Now that I changed the consent settings, there are all these user-consented apps still in my tenant. What do I do with these?”

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

✅ Bring Useful Apps in Scope of Your IAM Processes

- Review the necessity to keep the app
- Use the **Assignment required** option on the **Properties** page of the app
- Assign a new per-app group to the app on the **Users and groups** page
- Assign app **Owners**
- Use the **Notes** field or tags for organizational information
- Have users request access, for instance, through:
  - Entra Access Packages
  - ServiceNow
  - Your SMA tooling

Note:

The Entra group ‘All Users’ includes both people in your organization and all guests…

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

⛔ Don’t leave stale apps

Remove Enterprise Apps tied to defunct systems.

The Application Activity report in the Entra Portal through Enterprise Applications > Usage and insights

Typical indicators:

- Start with the application registration
- No user sign-ins and no service principal sign-ins (unless it’s used for SCIM provisioning)
- No interactive sign-ins
- No non-interactive sign-ins
- All passwords and certificates have expired

Checklist: appgovscore.com/blog/entra-id-app-registration-enterprise-app-cleanup

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

✅ Clean Up During Upgrades

For on-premises apps and apps that your admins install

Before major upgrades:

- Revoke admin consent to associated App Registrations and Enterprise Apps
- Delete associated App Registrations and Enterprise Apps

In the upgrade experience, opt to recreate these artifacts to align with the latest vendor insights

- Least privilege permissions
- Branding and other changes

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Recommended Admin Practices

Global Administrator rights are not human rights.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

⛔ Don’t Underestimate the Power of Admin Roles

Application Administrator and **Cloud Application Administrator** are powerful roles.

Who are **owners** of your privileged apps?

Misuse and misconfiguration can lead to accidental Global Admin access.

✅ Implement App Credential Hygiene

Avoid credential expiration issues.

No more secrets or certificate worries.

Entra App Proxy and Entra Connect Sync use their own certificate life cycle process. Don’t worry about that.

Monitor federated endpoints in use (GitHub, Azure DevOps, etc.) to detect abuse through malicious endpoints.

(i.e., github.com/azurekid/blackcat)

Use Application Management Policies to manage credential configuration.

Available through **Enterprise Applications** > **Application Policies** New!

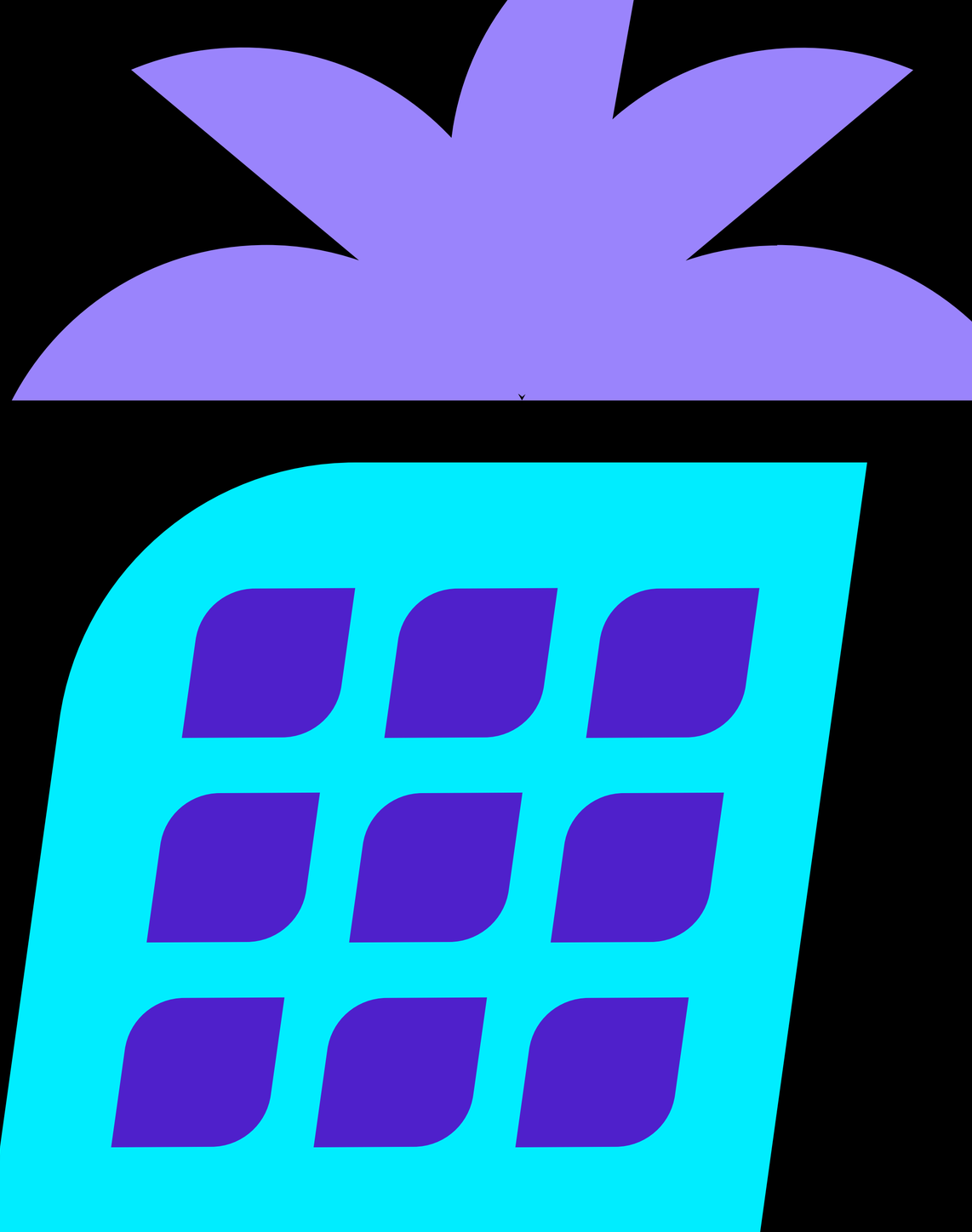
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Conclusion

Your To-Do List

- ❑ Review your user consent settings
- ❑ Enable the Admin Consent Workflow
- ❑ Review your apps and permissions
- ❑ Bring apps into your IAM processes … or get rid of them
- ❑ Review the administrator roles assigned to people in your organization
- ❑ Monitor owners and credentials



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON