

Identity Workshop

Workshop overview

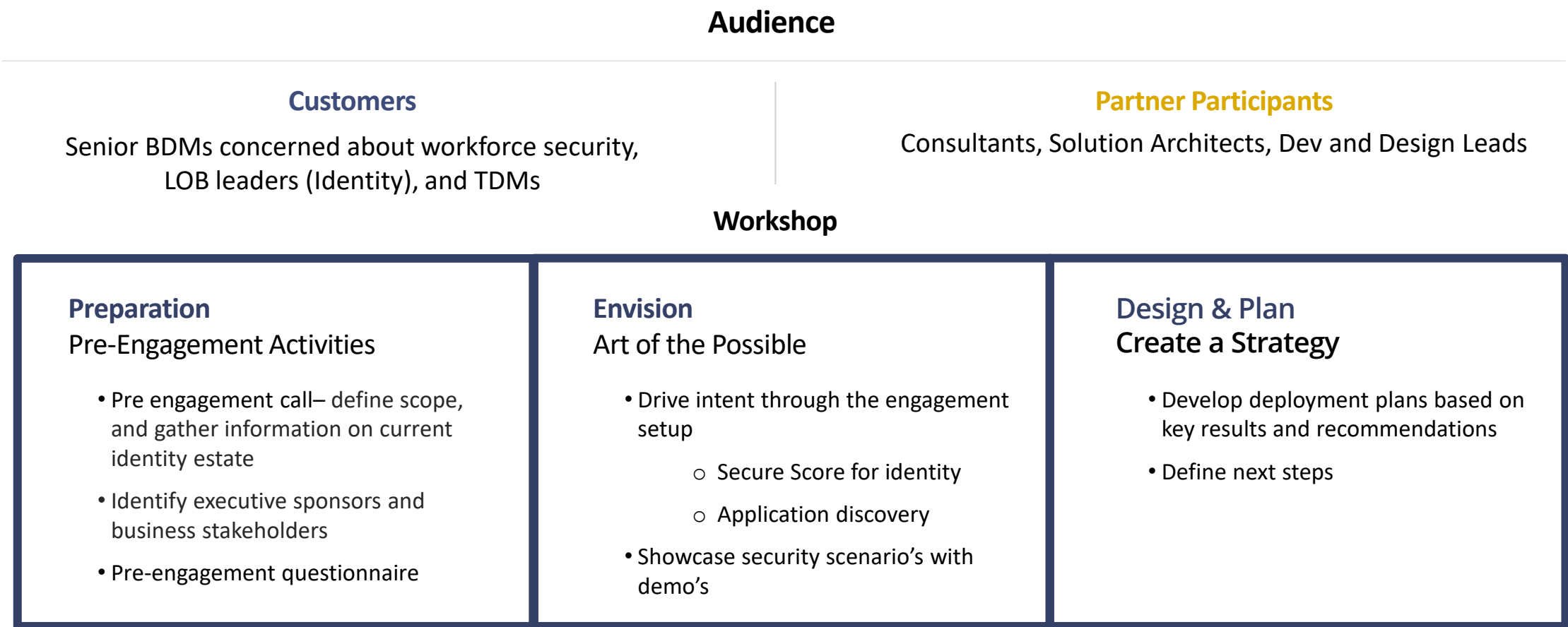
Kyle Perkins
Sr. Security Architect
Enterprise IT Security



An executive deep dive into foundational identity strategy, tailored to a customer's organization

Identity Workshop overview

Designed as a 20 day engagement, the Identity Workshop enables partners to assess the maturity of a customer’s identity estate. By making use of **Secure Score** and **application discovery tools**, this workshop gives customers visibility into their present state and will help define clear next steps and the best ways to mitigate risks.



Identity Workshop phases and activities

PRE-ENGAGEMENT CALL

ENGAGEMENT SETUP

REPORTING

DESIGN & PLANNING

OUTCOME & RESULTS

Pre-engagement call

- Introductions
- Engagement walk-through
- Expectations
- What's next

Kick-Off Meeting

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Week 1

Identity Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Week 1

Secure Score Overview and Identity Security Posture Assessment

- Present Secure Score
- Gather Identity Security Posture

Week 1

Application Discovery presentation and setup

- Application Discovery presentation
- Configure engagement tools

Application Discovery Reporting and discussion

- Report discovered applications and get ready for prioritization
- Application discussion

Week 2

Identity Fundamentals

- Integration scenarios
- Cloud and Hybrid Identities

Week 3

Azure AD Application Management

- Secure Hybrid Access
- Single Sign-on
- Application Proxy
- My Apps

Week 3

Conditional Access

- CA options

Week 2

Self-Service Password Reset (SSPR)

- SSPR options

Multifactor Authentication (MFA)

- MFA options

Customer Value Conversation

- Value of the Microsoft Identity platform

Week 3

Week 4

Discovery Session

- Discuss security strategy

Week 4

Demos

- MS identity experience

Week 4

Key results, recommendations and next steps

- Present design decisions
- Present prioritization
- Discuss next steps



Customer benefits of the Identity Workshop

With identity attacks on the rise, this workshop provides you with the tools and resources you need to evolve your infrastructure by securing identities. You will receive a strategic plan based on recommendations from Microsoft identity experts and customized specifically for your organizational needs.

The workshop will help you design and plan out your optimal identity model to ensure you have a roadmap for enhanced security.

Optimize identity

Identify potential risks related to identity and see opportunities for improvement.

Assess security posture

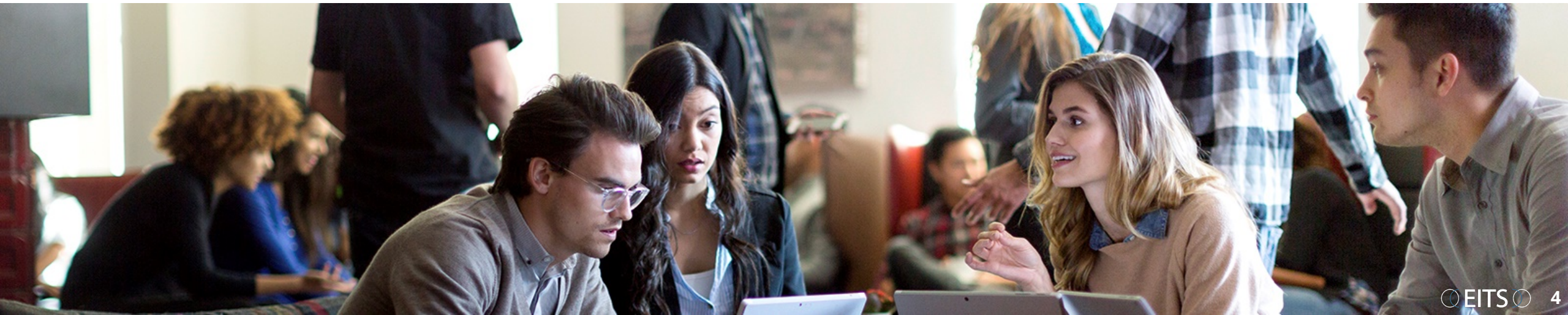
Receive a numerical rating of your identity security posture and see how it compares to similar organizations

Reduce costs

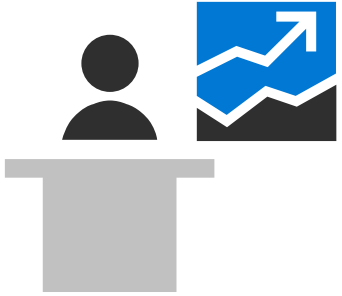
Minimize expenses associated with password reset and helpdesk resources.

Increase visibility

Get a sample survey of apps your employees are using and if IT supports them or not.

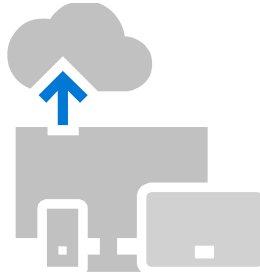


Who should attend



Security decision makers

- C-Suite
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Identity and or Application owners/decision makers



Other roles

- IT Security
- IT Operations
- Security Architect
- Security Engineers
- Application business owners

Top concerns

- Remote workers won't have the same secure, productive experiences from home as they do from the office.
- Lack of visibility to potential threats that could compromise users' identity.
- Uncertainty about unsanctioned apps usage and their impact on the organization's security.
- Workers are geographically scattered, making it difficult to keep up with all the people who need remote access to apps and information.
- Mixed apps (on-premises and cloud) make it hard to provide consistent access.



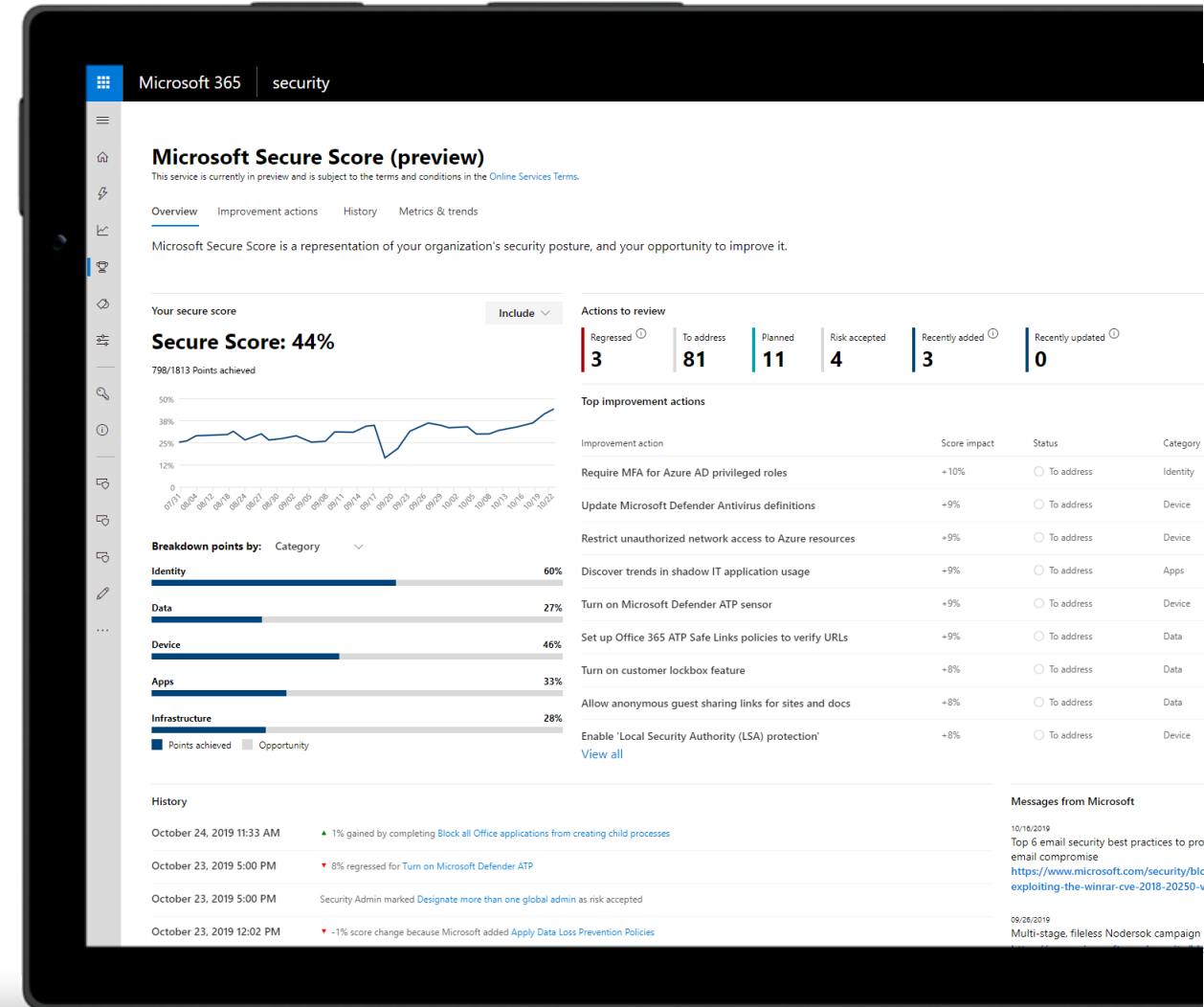
Engagement Setup
Secure Score & application discovery

Microsoft Secure Score Vision

Empower every organization to achieve their most secure, most productive security posture.

One number for org-wide posture;
Higher number indicating lower risk

- Absolute true posture
- Built-in and integrated
- Heterogenous environment



How does it work?

Secure Score 75 %

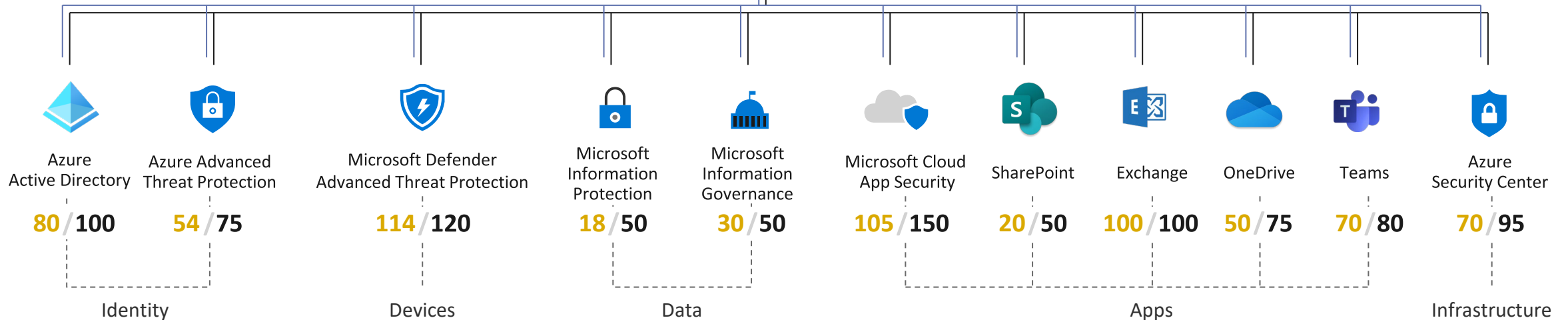
711 / 945

Points achieved

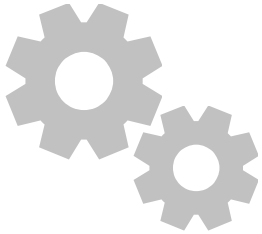
Applicable controls only

Licenses don't matter

Security controls
& Assessment signals



Collect your facts...



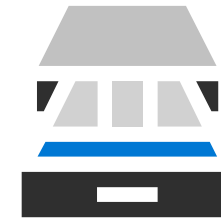
New App Policy

All new applications must support modern authentication protocols and are authenticated via Azure Active Directory



Discovery

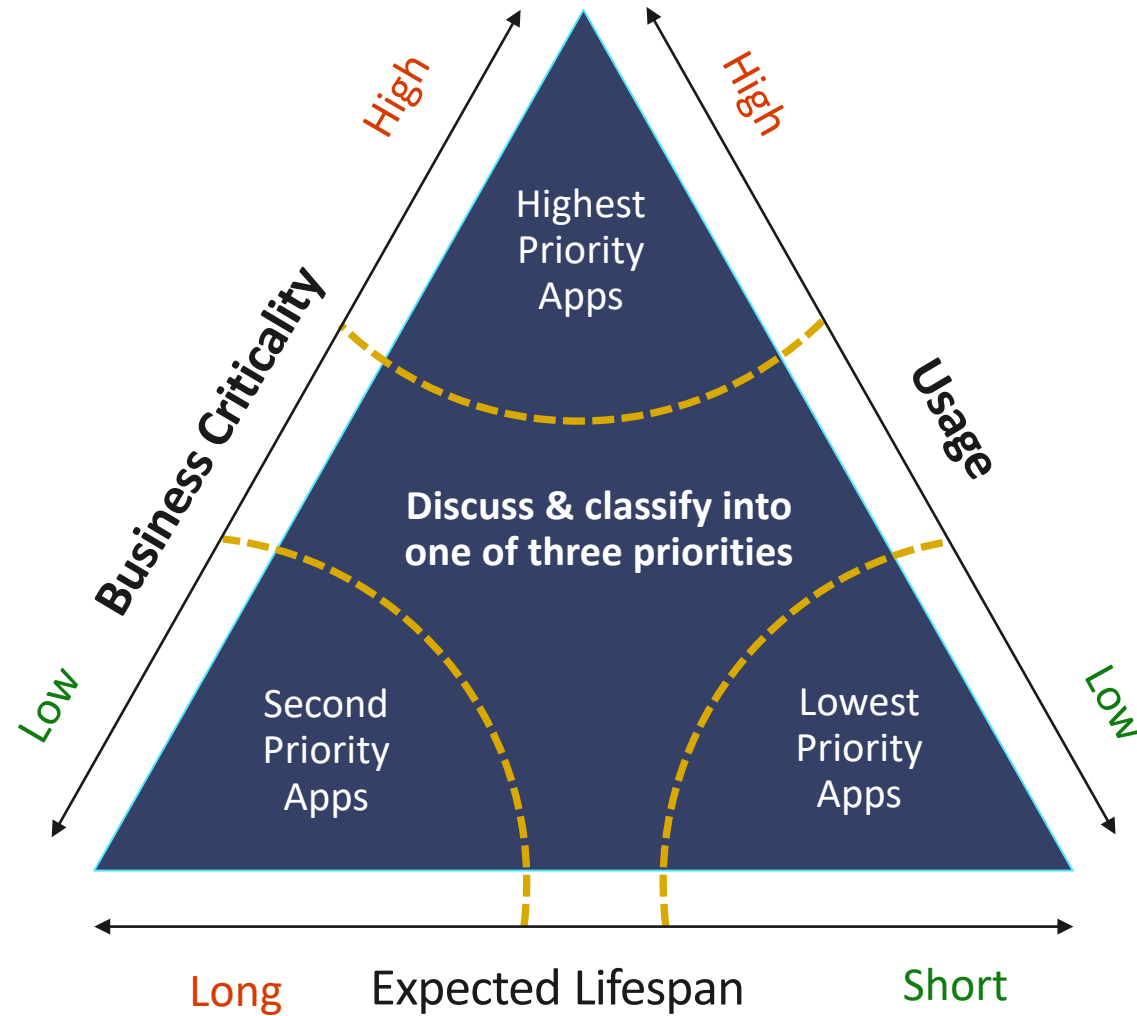
App inventory
Cloud App Security Broker
ADFS Readiness tool
Identity Transporter Tool
Start sniffing traffic
Log analysis



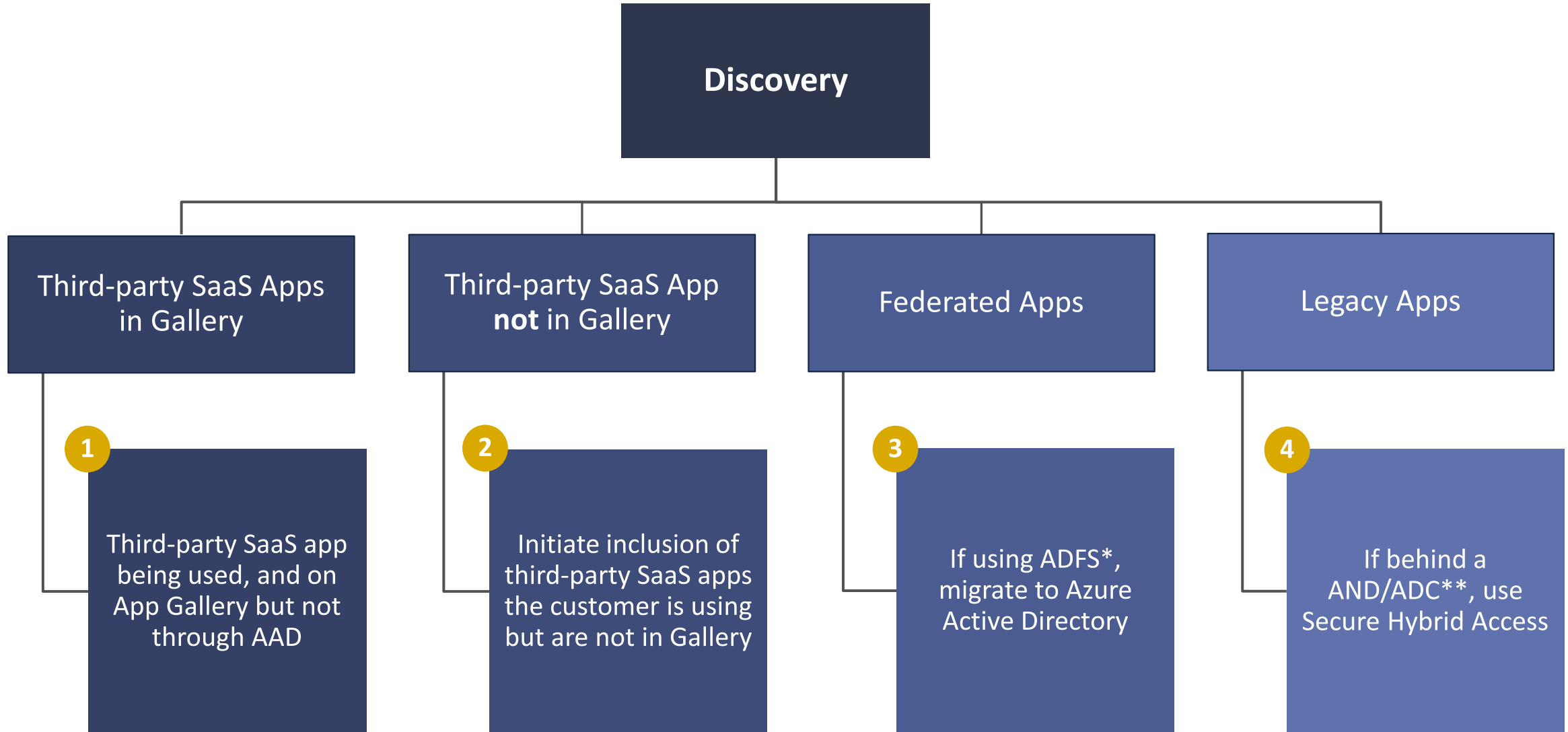
Classify

Categorize applications
Scope applications to be Migrated, Not migrated and Deprecated

App Categorization



Application Prioritization



*Active Directory Federation Service

**Application Network Delivery/Application Delivery Controller



Design and Planning

Design and Planning



Identity Fundamentals

- Review Azure AD integration scenarios (ADFS, AAD Connect with PHS or PTA, Cloud Identities)
- ADFS to Managed Identity migration discussion



Self-Service Password Reset (SSPR)

- Review SSPR options and opportunity to lower password reset helpdesk costs



Multifactor Authentication (MFA)

- Review Azure AD MFA enablement and different options available



Conditional Access (CA)

- Review CA concepts
- Deep dive into CA assignments, conditions and controls



Azure AD Application management

- Discuss why you should care and what 'modernizing' actually means
- How to build your migration strategy (My Apps, Azure AD App proxy, third-party application delivery controllers)

Discovery session

Clarify your current state, priorities, objectives and key influences on your identity strategy.

- Learn about people & processes, current technology as well as network/core infrastructure.
- Define foundational security objectives and priorities for Identity and access management
- Discover the factors that will help or hinder your identity objectives.
- Define the top five initiatives to focus on in the next months



Demos

Practical guidance and recommendations designed to facilitate a clear understanding of the role played by Identity in the following key areas

- Enabling remote access to all cloud applications
- Managing applications
- Protecting corporate resources



Key results, recommendations and next steps

- Technical-level next steps
- Strategic-level next steps
- Agree on follow-up engagements



Key results, recommendations and next steps

Technical-level next steps



Identity security posture improvement through Secure Score deployment plan



Identity Fundamentals – Azure AD integration and authentication scenario design decision



SSPR, MFA and CA design decisions and high-level deployment plans



Application Classification and Prioritization Plan



EITS
Thank you.