Microsoft Security | Quadra

Entra Permissions Management Risk Assessment Overview

Entra Permissions Management Risk Assessment overview

Designed as a three-week engagement, the Entra Permissions Management Risk Assessment enables partners to help customers assess their identity security posture across Multi-Cloud environments. By addressing the permissions gap risk, this assessment helps customers define clear next steps and the best ways to address remediation.

Audience

Customers

Senior BDMs concerned about workforce security, LOB leaders (Identity), and TDMs

Partner Participants

Consultants, Solution Architects, Dev and Design Leads

Assessment

Preparation

Pre-Engagement Activities

- Pre engagement call – define scope, and gather information on current identity estate and identify target cloud environments
- Identify executive sponsors and business stakeholders
- Permissions Management needs **read role** to collect identities, permission, activity logs and resource metadata.

Envision

Art of the Possible

- Drive intent through the engagement setup
  - Setup Permission Management
  - Discovery of cloud over-privilege identities, permissions and their impact over resources

Design & Plan

Create a Strategy

- Develop remediation plans based on key results and recommendations
- Define next steps
  - Best Practices for Remediation
  - Best Practices for Permissions On-demand
  - Monitor & alert
  - Key Reports

Customer benefits of the Entra Permissions Management Risk Assessment

This assessment is designed to help you evaluate where you are today and where you need to be to meet your risk mitigation goals, identify the areas of greatest risk, so you know where to focus your efforts and improve your risk posture with actionable insights and prescriptive recommendations.

The assessment will help you design and plan out your risk mitigation strategy to reduce the permissions gap that affect your infrastructure.

Discover

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

Improve

Understand how Entra Permissions Management can help you address the mitigation of the permissions gap.

Reduce

Reduce the complexity for IAM security teams to manage permissions across multicloud environments.

Plan

Get recommendations and next steps to move forward with Entra Permissions Management.

Stakeholders

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

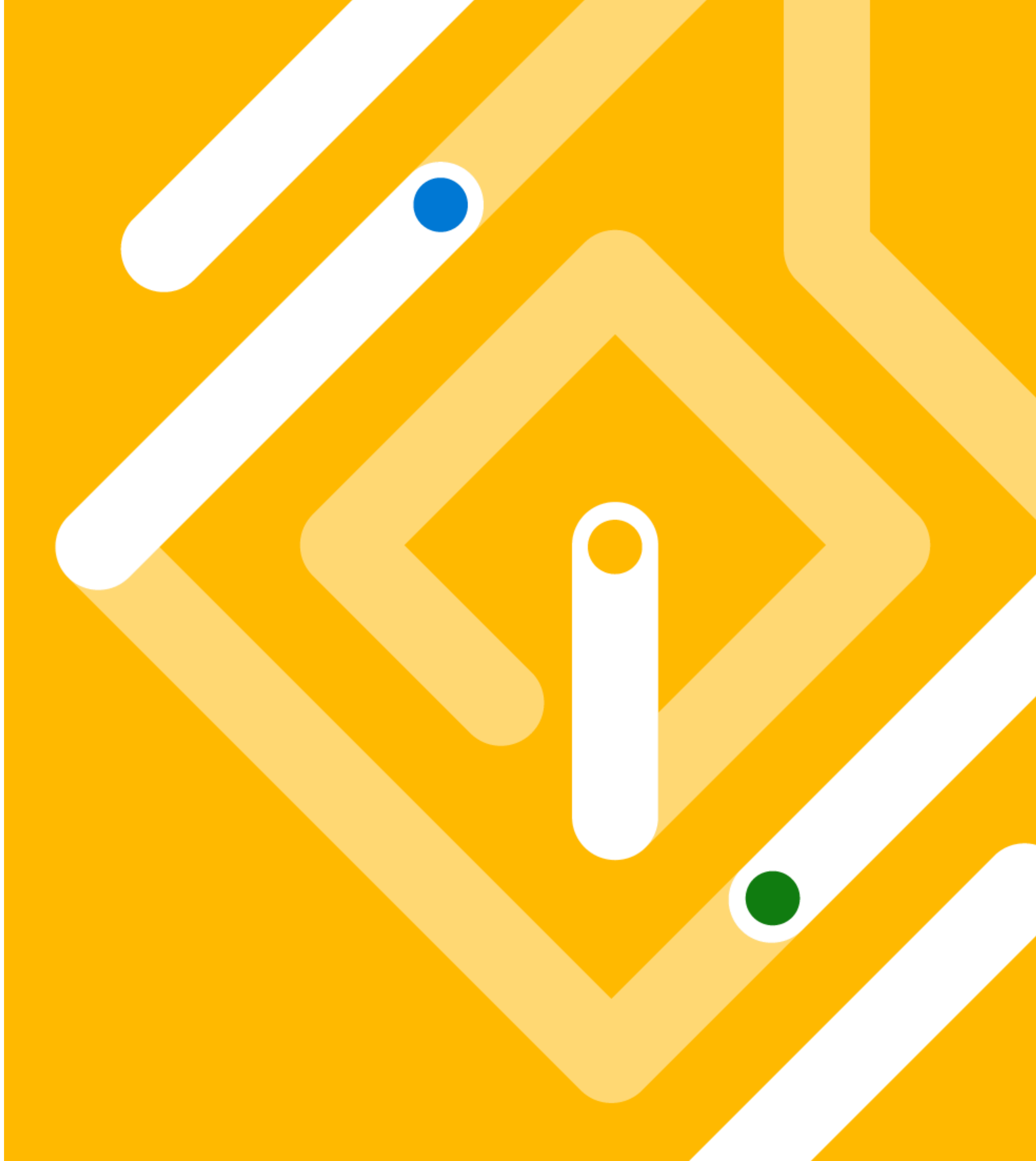
Other roles

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

Top concerns

- Lack of comprehensive visibility into identities, permissions and resources
- Increased complexity for IAM and security teams to manage permissions across multicloud environments
- Increased risk of breach from accidental or malicious permission mis-use

Risk Assessment modules and flow



Entra Permissions Management Risk Assessment brings modular flexibility

Engagement Setup

Entra Permissions Management

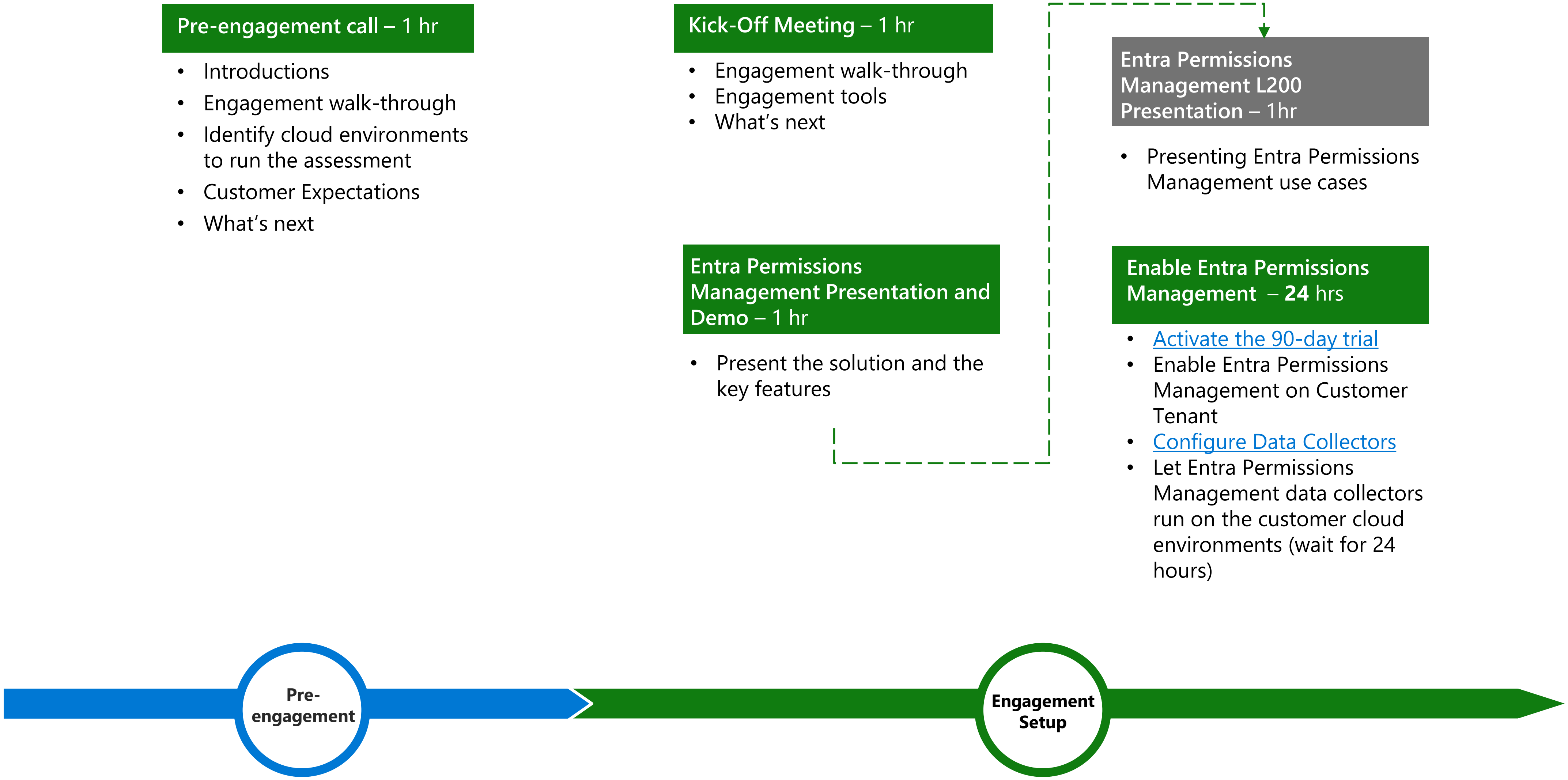
Design and Planning

Customer value conversations

Key results, recommendations and next steps

Demos

Entra Permissions Management Risk Assessment phases and activities



Pre-engagement call – 1 hr

- Introductions
- Engagement walk-through
- Identify cloud environments to run the assessment
- Customer Expectations
- What's next

Kick-Off Meeting – 1 hr

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

Entra Permissions Management Presentation and Demo – 1 hr

- Present the solution and the key features

Entra Permissions Management L200 Presentation – 1hr

- Presenting Entra Permissions Management use cases

Enable Entra Permissions Management – **24** hrs

- Activate the 90-day trial
- Enable Entra Permissions Management on Customer Tenant
- Configure Data Collectors
- Let Entra Permissions Management data collectors run on the customer cloud environments (wait for 24 hours)

🟩 MANDATORY ▨ OPTIONAL

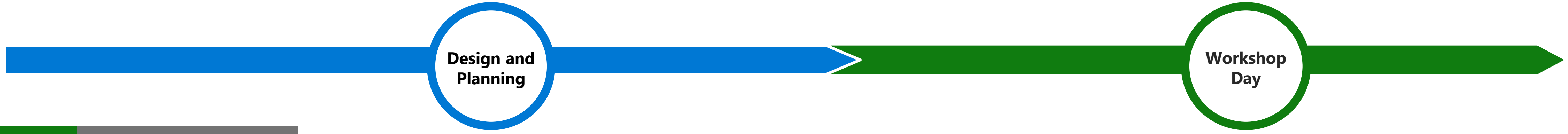
Entra Permissions Management Risk Assessment phases and activities

Discover & Assess – 1 Week

- Key Findings:
    - Over Permission Identities
    - Inactive Identities
    - Super Identities
    - Identities that can access secret information
    - Identities that can administer security tools
    - PCI Distribution
    - Resources findings
- Use queries to view information about user access
- Create and view reports
- Understand Implications:
    - Excessively permissioned active identities are exposed to credential theft risks
    - Cross-account access enables identities to access all resources in target accounts, leading to data leakage or malicious service disruption
    - Leveraging the same roles/policies and permissions in development and production environments exposes your infrastructure to insider threats and malicious external threats
    - Inactive identities leave organizations open to credential misuse or exploitation for malicious activities

Key results, recommendations and next steps – **2** hr

- Key Results:
    - >90% of identities using <5% of permissions granted
    - Cross-account access is frequently granted to external identities
    - Lack of separation of duties: Users with excessive roles/policies in both development and production subscriptions/accounts
    - Workload identities are over-provisioned and >40% inactive
- Recommendations for:
    - Removing inactive roles/ policies and identities to avoid unauthorized access to resources
    - Right-size permissions based on the past activities of these identities and grant additional permissions on an on-demand basis
    - Right-size permissions in development environments and clone permissions into production only as a starting point, then rightsize permissions to tighten controls
    - Right-size scope of roles/ policies to access limited resources and limit access to specific identities in other accounts

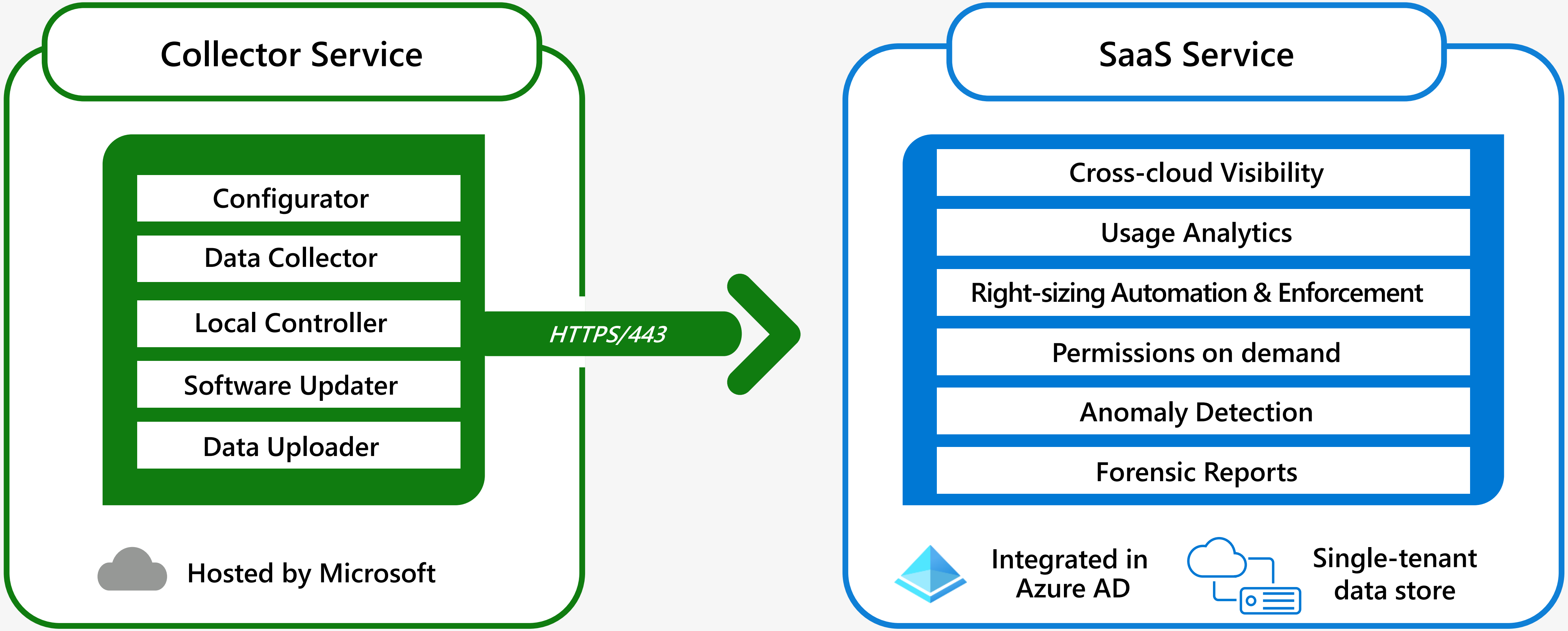


MANDATORY

OPTIONAL

Appendix

Deployment architecture



Collector Service

Configurator

Data Collector

Local Controller

Software Updater

Data Uploader

Hosted by Microsoft

HTTPS/443

SaaS Service

Cross-cloud Visibility

Usage Analytics

Right-sizing Automation & Enforcement

Permissions on demand

Anomaly Detection

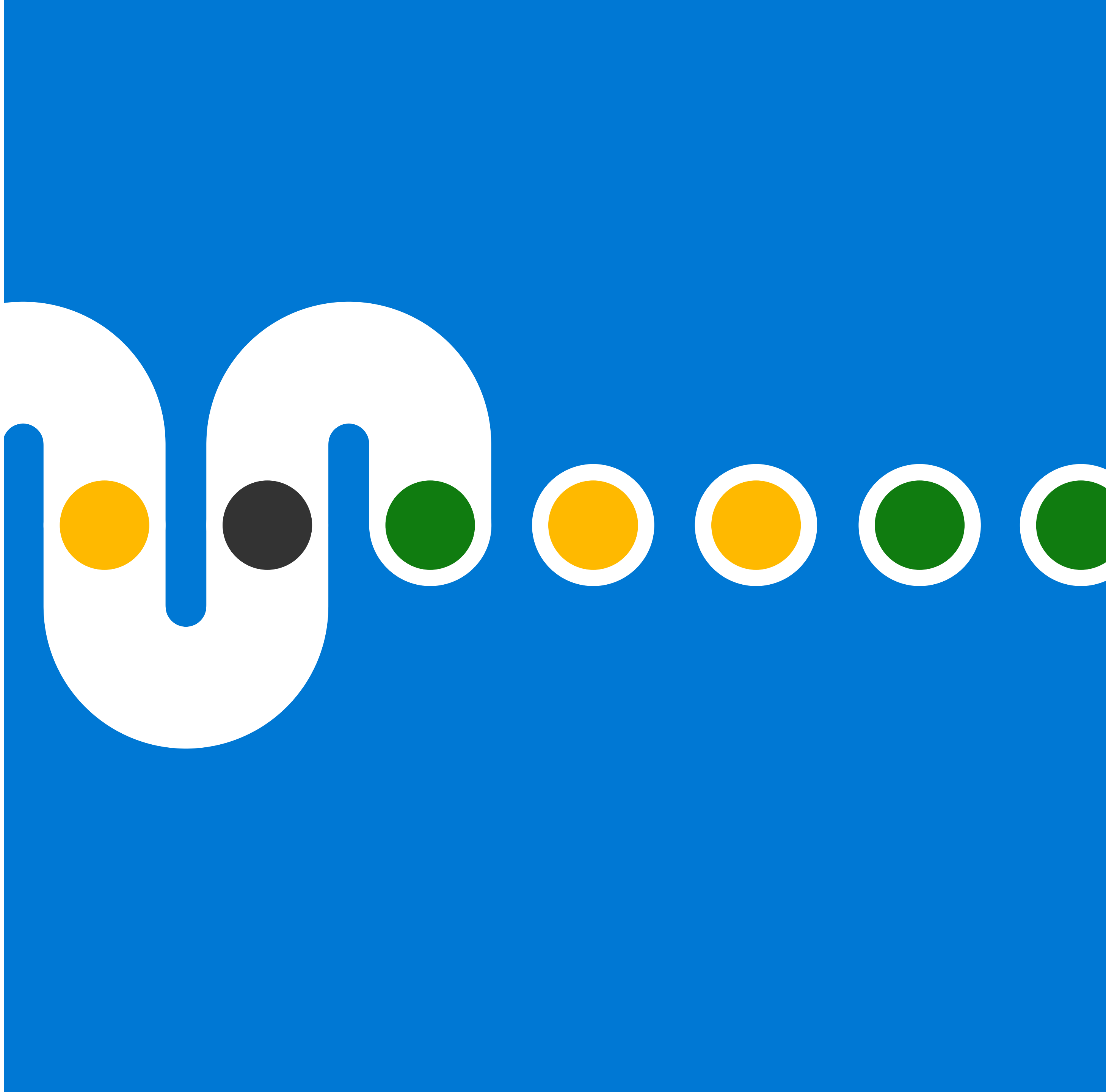
Forensic Reports

Integrated in
Azure AD

Single-tenant
data store

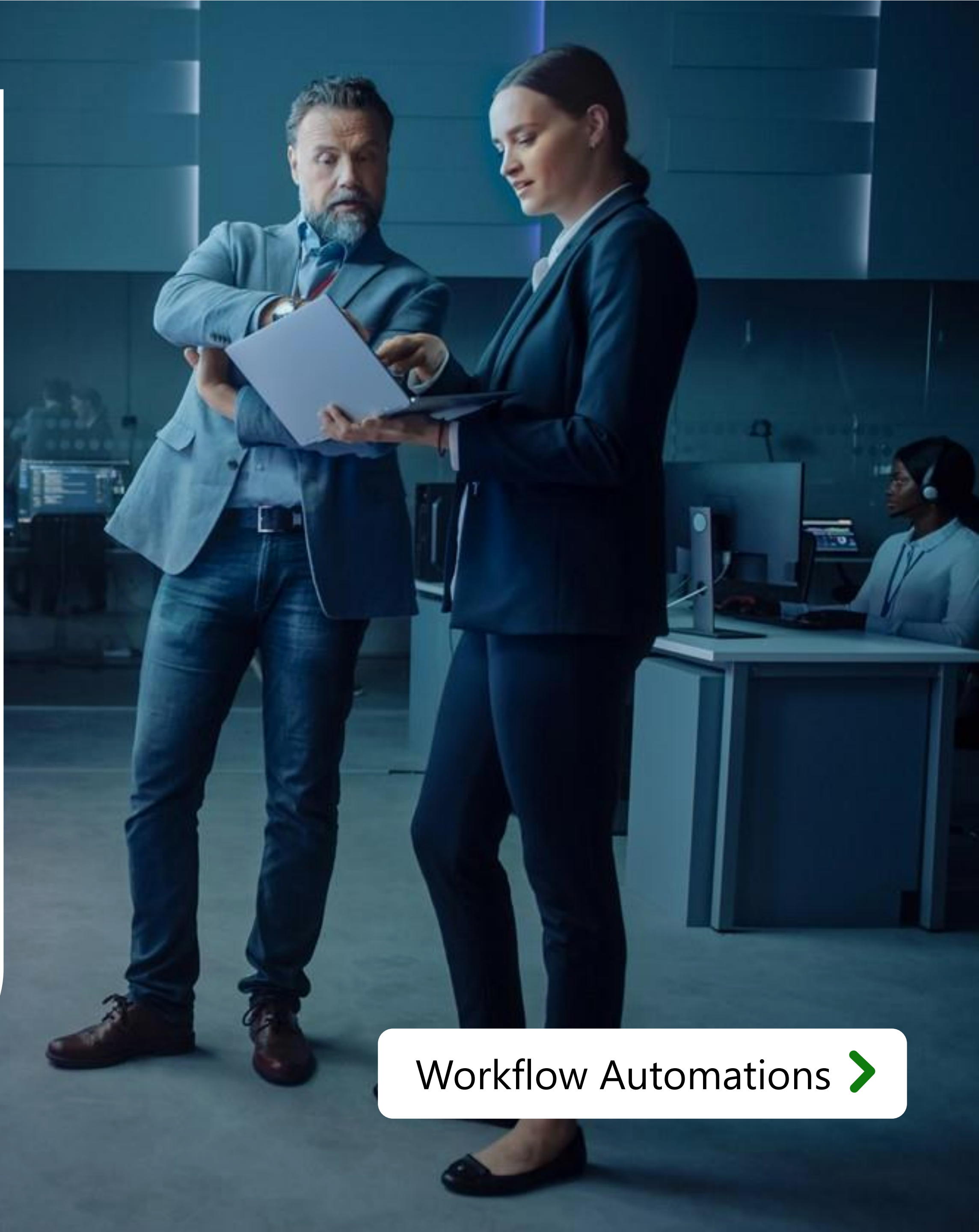
Use Cases:

- Security Team
- Cloud Infrastructure Operations Team
- Identity and Access Management Team



Use case: Security Team

- Monitor, assess and alert excessive permissions for human and workload identities including machines, serverless functions, access keys, bots, etc.
- Monitor access to infrastructure resources containing sensitive data
- Detect and respond to security anomalies
- Automate assessment, remediation, and monitoring



Workflow Automations >

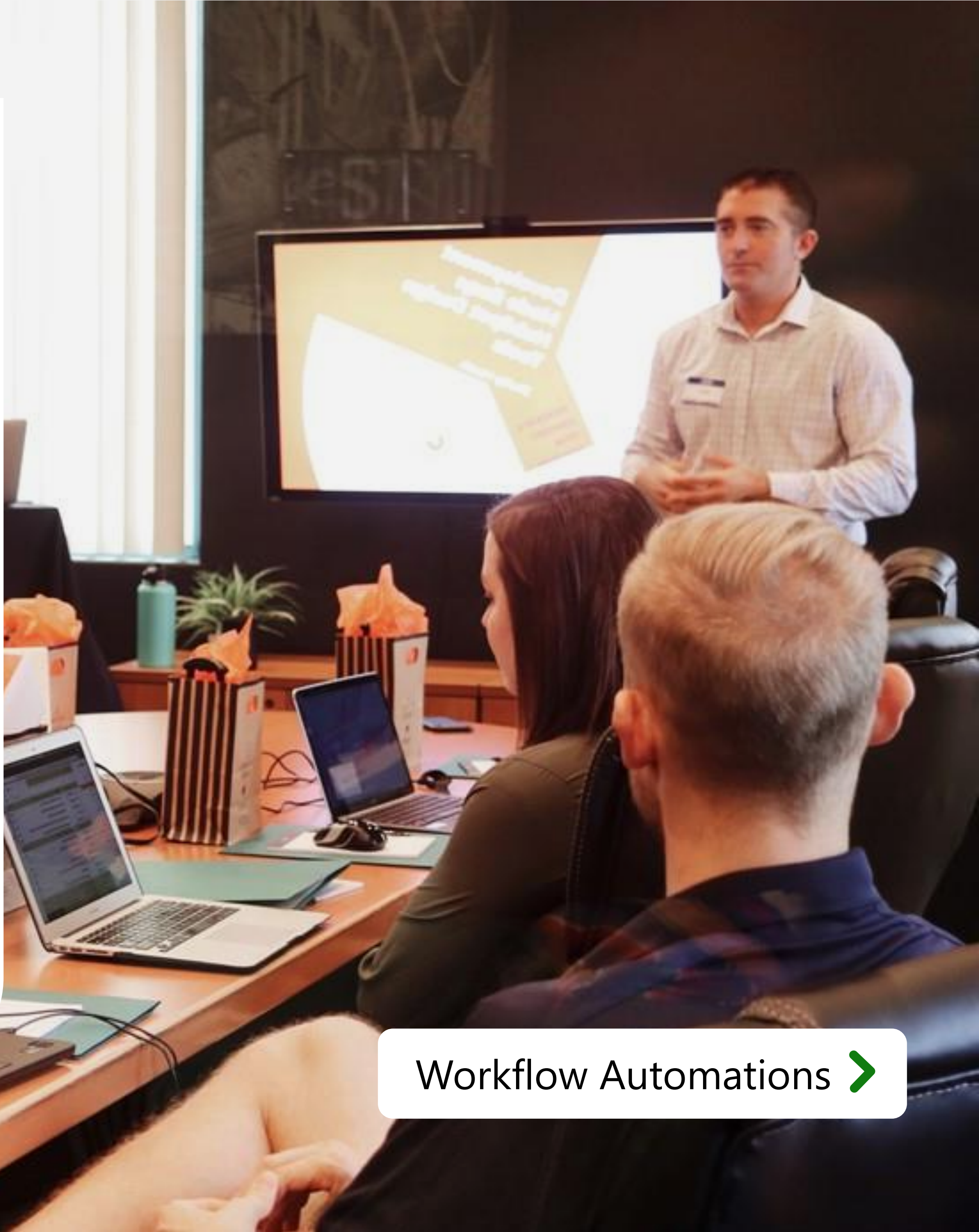
Use case: Cloud Infrastructure Operations Team

- Monitor access to infrastructure resources containing sensitive data
- Monitor and manage permissions of identities and resources across multicloud environments
- Detect, assess, alert and remediate anomalies and outliers across the three dimensions of identity, resource and action

Workflow Automations >

Use case: Identity and Access Management Team

- Implement least privilege policies for human and workload identities by right-sizing permissions based on usage
- Handle authorization and reviews for access requests
- Manage access recertification campaigns
- Manage access lifecycle for all identities



Workflow Automations >

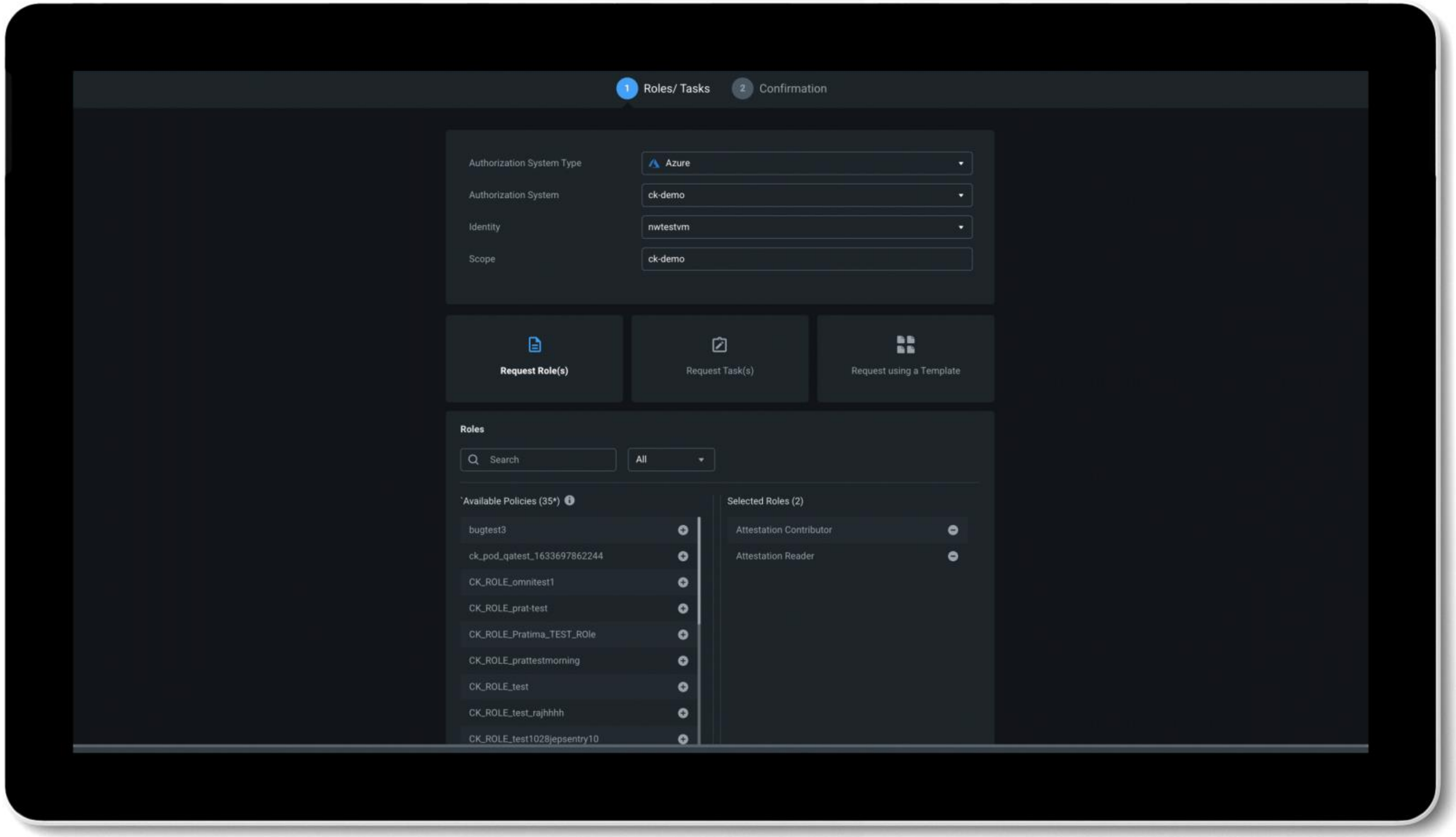
Workflow Automations

Best practice workflows for permissions on-demand

- **Requesting Delete Permissions:** No user will have delete permissions unless they request them and are approved.

- **Requesting Privileged Access:** High-privileged access is only granted through just-enough permissions and just-in-time access.

- **Requesting Periodic Access:** Schedule reoccurring daily, weekly, or monthly permissions that is time-bound and revoked at the end of period.



Authorization System Type: Azure
Authorization System: ck-demo
Identity: nwtestvm
Scope: ck-demo

Roles

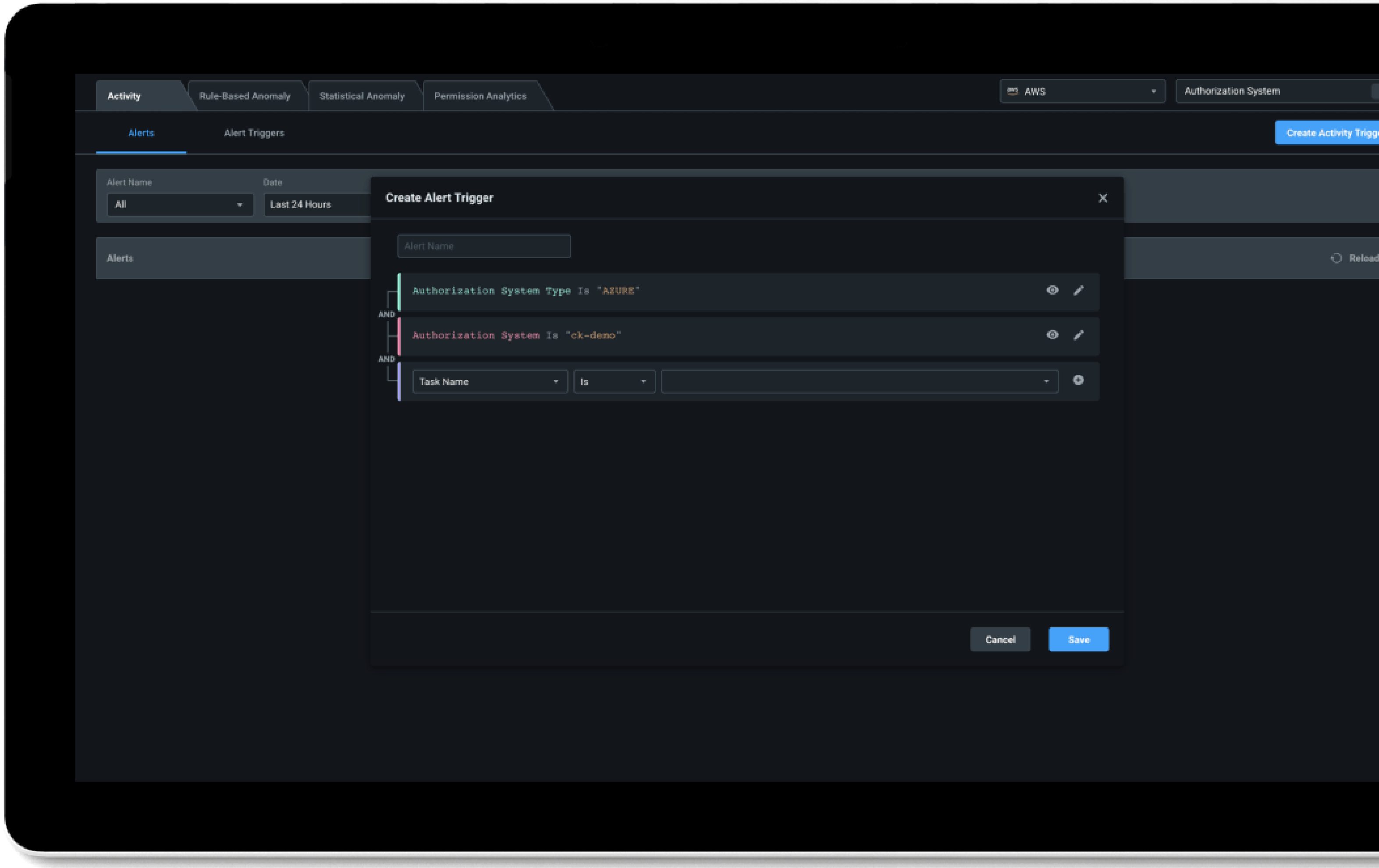
Search | All

`Available Policies (35*)
- bugtest3
- ck_pod_qatest_1633697862244
- CK_ROLE_omnitest1
- CK_ROLE_prat-test
- CK_ROLE_Pratima_TEST_ROle
- CK_ROLE_prattestmorning
- CK_ROLE_test
- CK_ROLE_test_rajhhhh
- CK_ROLE_test1028jepsentry10

Selected Roles (2)
- Attestation Contributor
- Attestation Reader

Best Practices for Custom Alerts

- Permission assignments done outside of approved administrators
- Access to critical sensitive resources
- Use of break glass accounts like root in AWS, global admin in azure AD accessing subscriptions, etc.



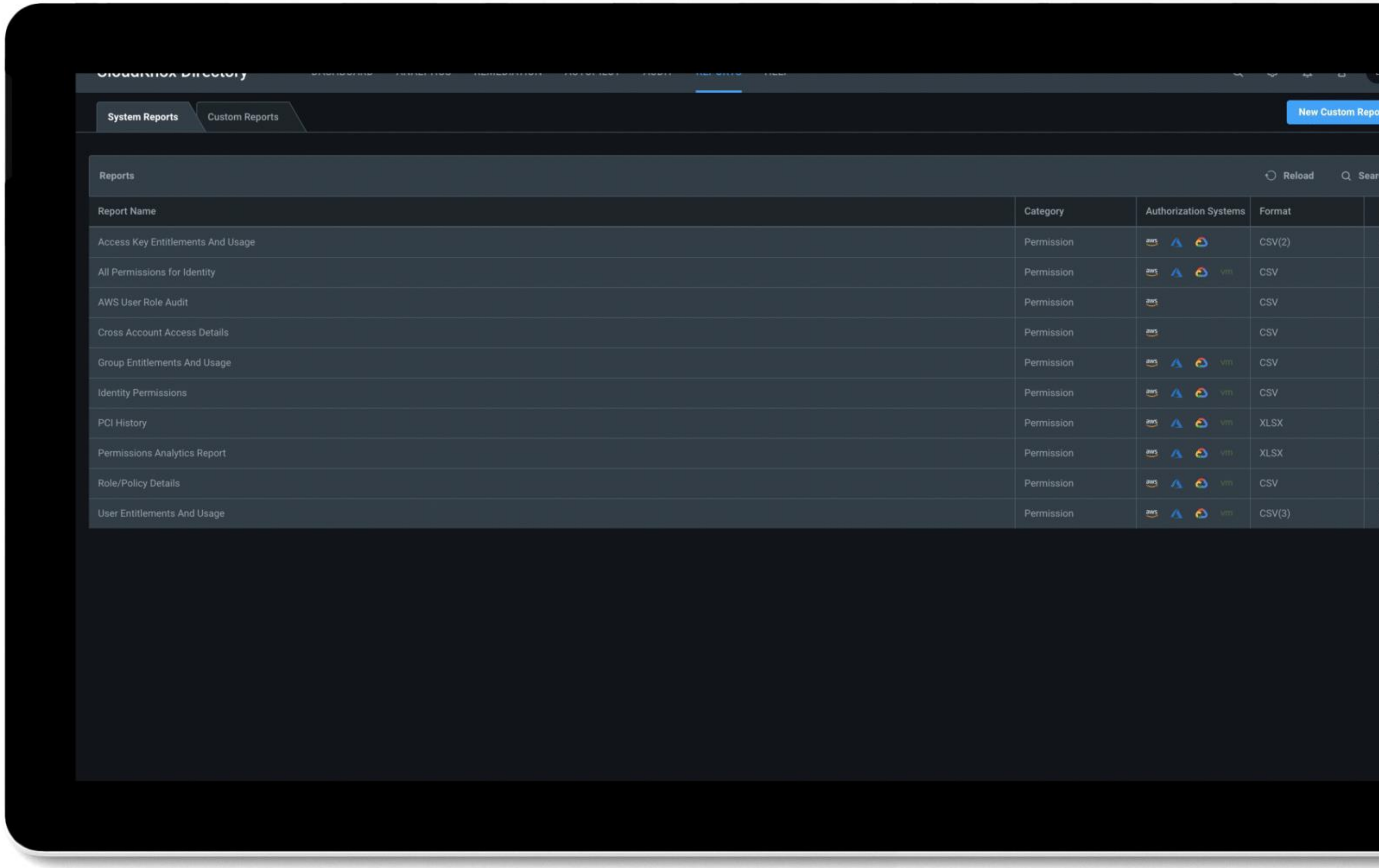
```
Authorization System Type Is "AZURE"
AND
Authorization System Is "ck-demo"
AND
Task Name  Is
```

Key Reports to Monitor

- **Permissions Analytics Report:** lists the key permission risks including Super identities, Inactive identities, Over-provisioned active identities, and more

- **Group entitlements and Usage reports:** Provides guidance on cleaning up directly assigned permissions

- Access Key Entitlements and Usage reports: Identifies high risk service principals with old secrets



Report Name	Category	Authorization Systems	Format
Access Key Entitlements And Usage	Permission	aws A ☁	CSV(2)
All Permissions for Identity	Permission	aws A ☁ vm	CSV
AWS User Role Audit	Permission	aws	CSV
Cross Account Access Details	Permission	aws	CSV
Group Entitlements And Usage	Permission	aws A ☁ vm	CSV
Identity Permissions	Permission	aws A ☁ vm	CSV
PCI History	Permission	aws A ☁ vm	XLSX
Permissions Analytics Report	Permission	aws A ☁ vm	XLSX
Role/Policy Details	Permission	aws A ☁ vm	CSV
User Entitlements And Usage	Permission	aws A ☁ vm	CSV(3)

Microsoft Security | Quadra

Thank you.