Securing Multi-vendor Clouds Part 3 – CIEM with Entra Permissions Management

23 June 2022 from 1300 BST

Please complete our poll

https://aka.ms/SecuringMVC3-Poll

Today’s Agenda

13:00	Introductions and housekeeping
13:05	Introducing Microsoft Entra Permissions Management
13:20	Challenges of managing permissions across multiple cloud services
	Getting started with Entra PM
	Visibility into over-permissioned access
13:50	Break
14:00	Remediating over-permissioned access
14:50	Wrap up + Live Q&A
15:00	Event ends

Meet the Team

Cassandra Browning
Cloud Solutions Architect
Azure and multi-cloud security

Shelley Hill
Technical Specialist
Microsoft Entra Permissions Management

Hugo Rubirosa Rodriguez
Partner Engagement Manager
Microsoft Entra

Housekeeping

There will a break & speaker changes throughout

This is a one-way speaker to attendees audio, so please ask any questions in the Q&A

This will be recorded and links sent to you

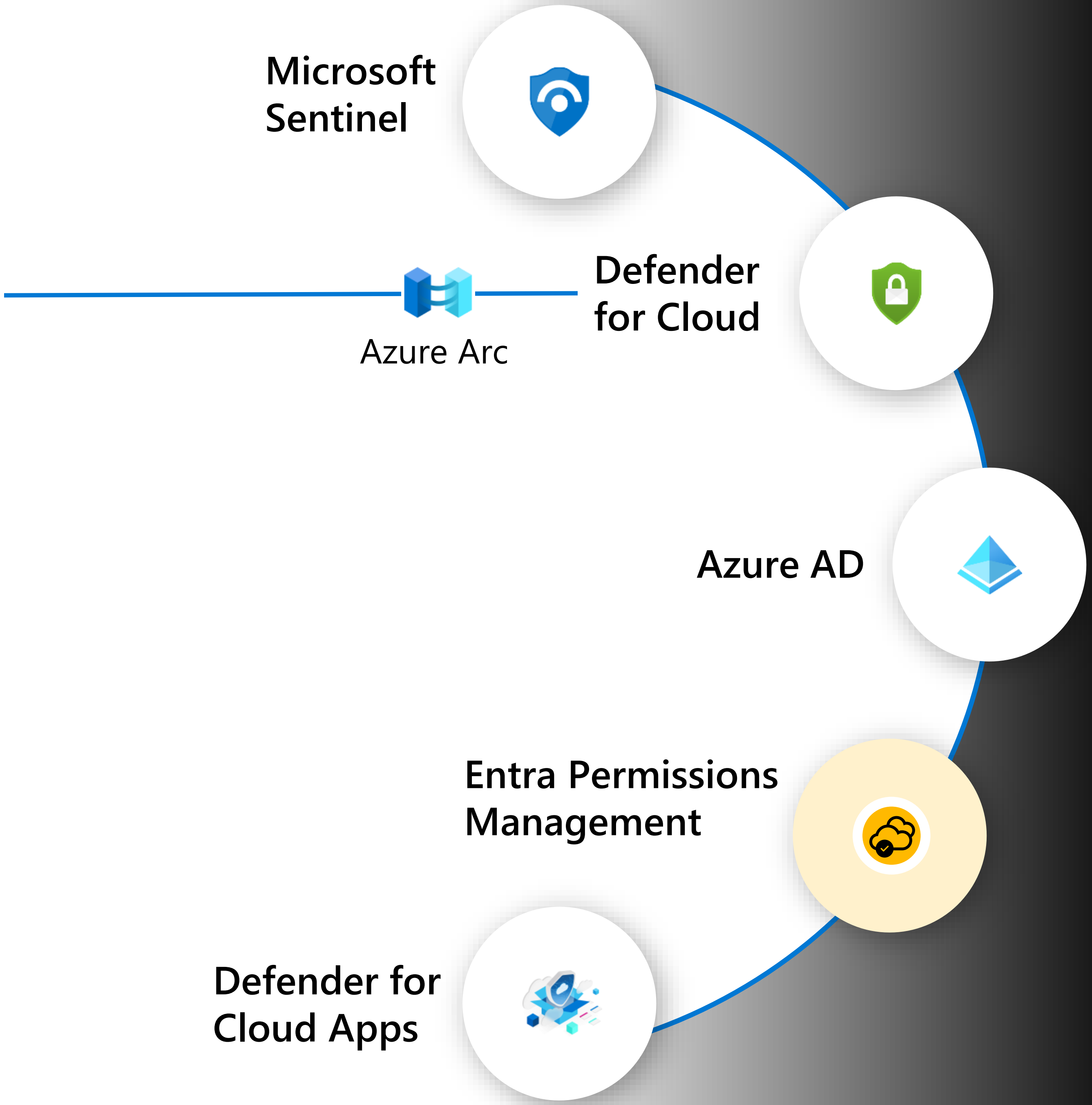
Feedback – https://aka.ms/SecuringMVC3-Feedback

These Resources will be shared with you (to share with others at your company)

All content is under your partnership NDA

Securing aws and ☁ with Microsoft

- Threat protection and response
- Visibility
- Security posture and compliance
- Governance and control
- Single sign-on
- Identity Governance
- Permissions Management



In case you missed Parts 1 or 2

- Part 1 – Identity - Slides and Labs: https://aka.ms/SecuringMVC-Repo
- Part 2 – Posture Management and Threat Protection - Slides and Labs: https://aka.ms/SecuringMVC2-Repo

Microsoft Security

Microsoft Entra

Secure access for a connected world

Microsoft Entra

Secure access for a connected world.

Azure Active Directory

Protect your users, apps, workloads, and devices.

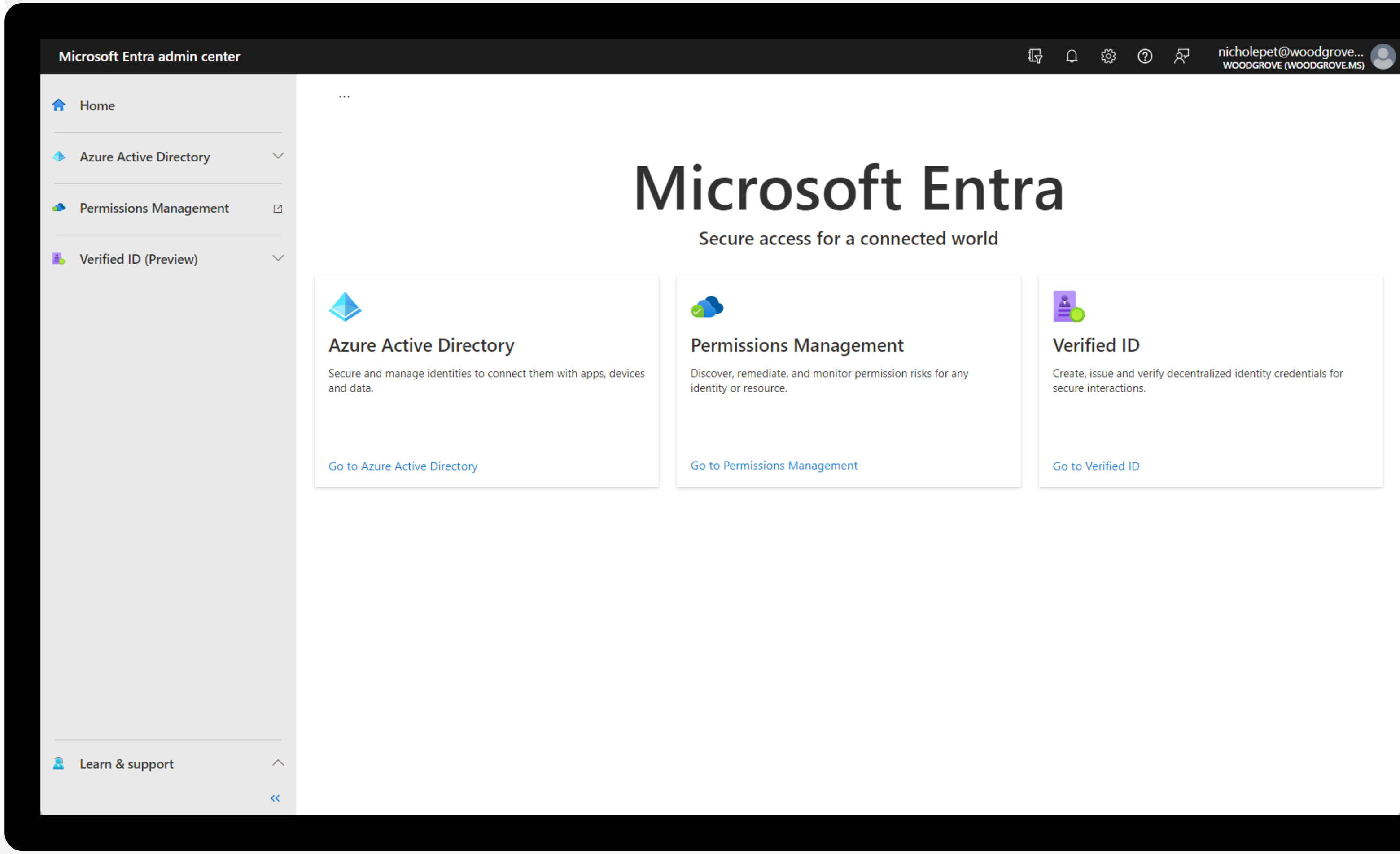
Permissions Management

One unified model to manage permissions of any identity across any cloud.

Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

All in one place:
Microsoft Entra admin center



Microsoft Entra

Secure access for a connected world

Azure Active Directory

Secure and manage identities to connect them with apps, devices and data.

Go to Azure Active Directory

Permissions Management

Discover, remediate, and monitor permission risks for any identity or resource.

Go to Permissions Management

Verified ID

Create, issue and verify decentralized identity credentials for secure interactions.

Go to Verified ID

Microsoft Entra

Secure access for a connected world

Azure Active Directory

Protect your users, apps, workloads, and devices.

Permissions Management

One unified model to manage permissions of any identity across any cloud.

Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

Permissions Management

One unified model to manage permissions of any identity across any cloud.

Discover

Get a **comprehensive view** of every action performed by **any identity** on any resource.

Remediate

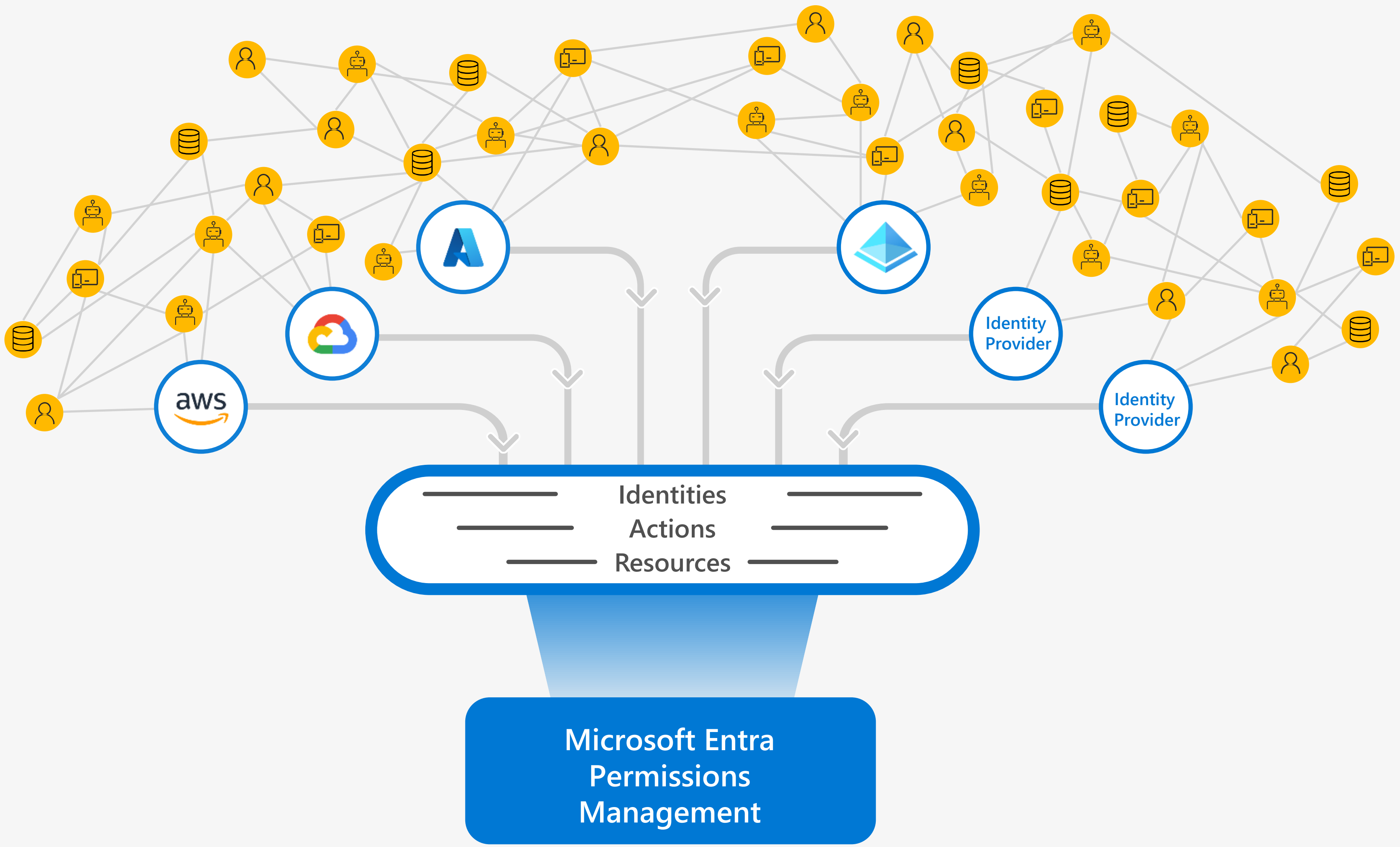
Right-size permissions based on usage and activity and enforce **permissions on-demand** at cloud scale.

Monitor

Detect **anomalous permission usage** and generate detailed **forensic reports**.

Microsoft Entra Permissions Management

Manage permissions based on historical usage and activities



Microsoft Security

The challenges of managing permissions across multiple cloud services

Multi-cloud adoption brings new access control challenges

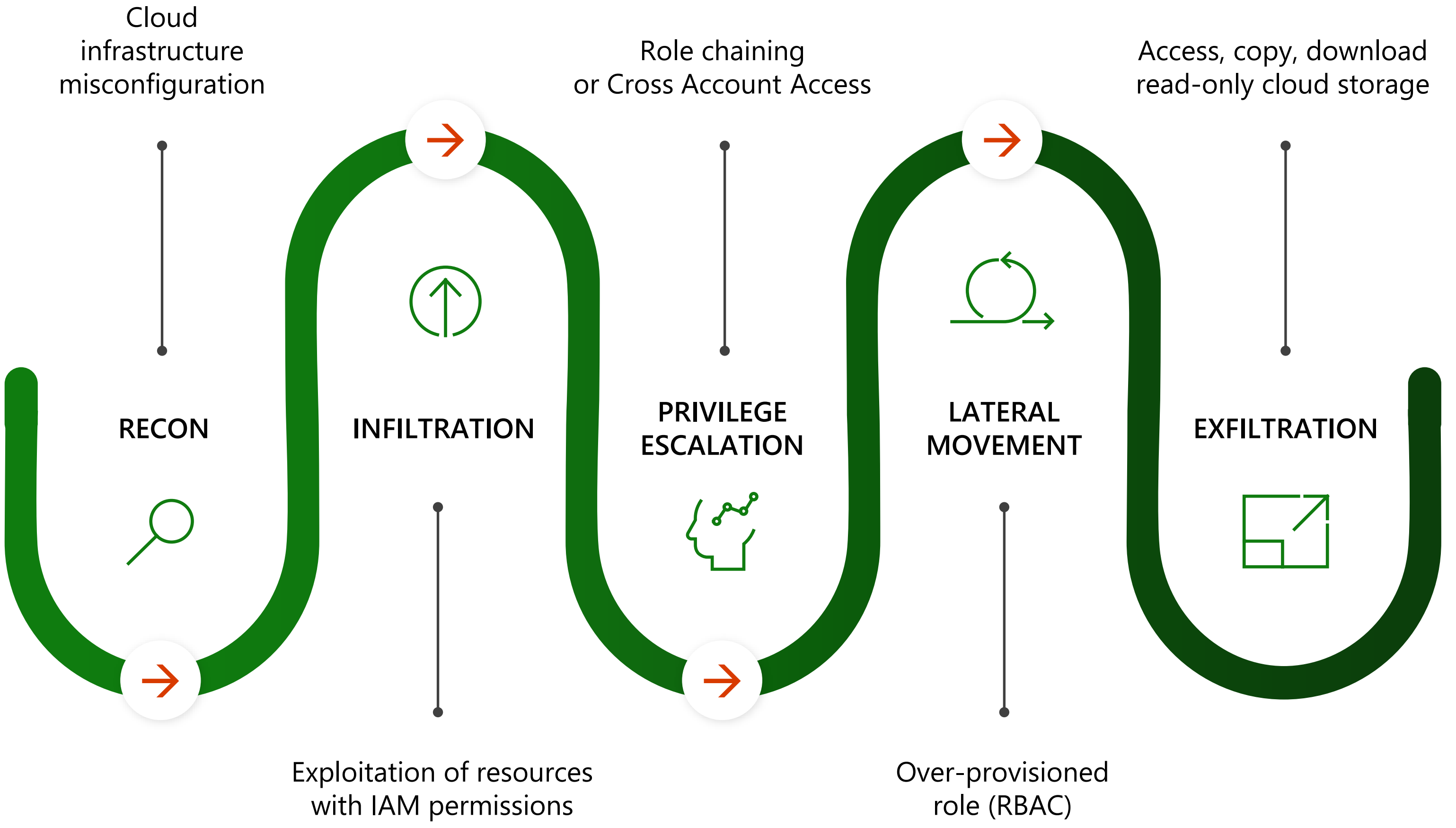
>90%	Identities can adversely impact infrastructure
50%	Increase in identities accessing cloud infrastructure
<5%	Permissions granted are *actually* used

Implications

- Lack of visibility across clouds
- Increased complexity to implement consistent access policies
- Increased risk of security breach

Cloud Infrastructure Kill Chain Analysis

What's the risk?



RECON

Cloud infrastructure misconfiguration

INFILTRATION

Exploitation of resources with IAM permissions

PRIVILEGE ESCALATION

Role chaining or Cross Account Access

LATERAL MOVEMENT

Over-provisioned role (RBAC)

EXFILTRATION

Access, copy, download read-only cloud storage

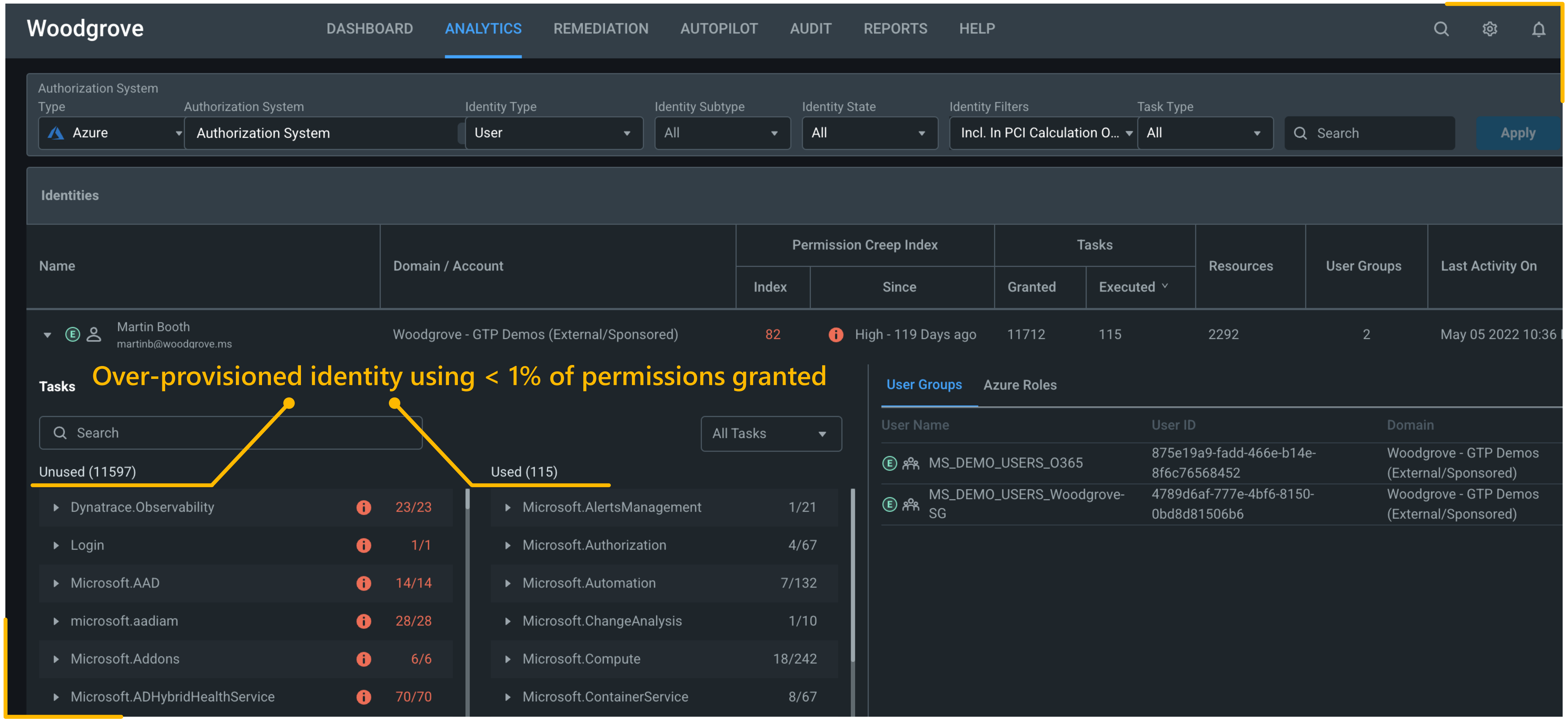
2nd Generation Cloud Breach TTPs

Top Threats to Cloud Computing: Egregious Eleven Deep Dive

A case study analysis for 'The Egregious 11: Top Threats to Cloud Computing' and a relative security industry breach analysis

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Design and Human error by an internal cloud team	**EE1** *Data Breach:* Compromise of AWS server instance and AWS access key in production AWS, which led to an exposure of a database snapshot containing sensitive data	**EE2** *Misconfiguration and Inadequate Change Control –* A server with access to sensitive database snapshots was configured to be internet accessible.	**EEI** *Data Breach:* Subset of Incapsula customers' email addresses, passwords, API keys and certificates were disclosed.	**Financial** • No data available	**Preventive** • DSI-05 • EKM-04 • IVS-07 • IVS-06
		Undisclosed Server Vulnerability – The attacker was able to pivot from an internet facing cloud server, meaning he was able to compromise it via some undisclosed vulnerability or gross misconfiguration.	*Cloud Instance Compromised:* An attacker was able to compromise an AWS EC2.	**Operational** • Marketing, Security & Operations teams incident response • Re-issuing and rerolling tens Of thousands of customer certificates, passwords and API keys	**Detective** • IVS-06 • IVS-01 • TVM-02
External • Unknown threat actor • Undisclosed bug bounty hunter	*Cloud Server and Credentials Compromise:* An attacker was able to compromise an AWS EC2 service instance and abuse credentials that he found on that server	**EE3** Lock of Cloud Security Architecture and Strategy – A server with access to production database snapshot was used for testing. It was internet facing and used AWS API keys rather than roles (temporary credentials).	*Cloud Access Key Credentials Compromised*	**Compliance** • GDFR driven breach notifications issued	**Corrective** • AIS-04 • CCC-03 • GRM-02 • IAM-08
				Reputational N/A	

https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/



Woodgrove

Authorization System Type: Azure

Authorization System: Authorization System

Identity Type: User

Identity Subtype: All

Identity State: All

Identity Filters: Incl. In PCI Calculation O...

Task Type: All

Identities

Name	Domain / Account	Permission Creep Index		Tasks		Resources	User Groups	Last Activity On
		Index	Since	Granted	Executed			
Martin Booth martinb@woodgrove.ms	Woodgrove - GTP Demos (External/Sponsored)	82	High - 119 Days ago	11712	115	2292	2	May 05 2022 10:36

Tasks

Over-provisioned identity using < 1% of permissions granted

Unused (11597)	
Dynatrace.Observability	23/23
Login	1/1
Microsoft.AAD	14/14
microsoft.aadiam	28/28
Microsoft.Addons	6/6
Microsoft.ADHybridHealthService	70/70

Used (115)	
Microsoft.AlertsManagement	1/21
Microsoft.Authorization	4/67
Microsoft.Automation	7/132
Microsoft.ChangeAnalysis	1/10
Microsoft.Compute	18/242
Microsoft.ContainerService	8/67

User Groups | Azure Roles

User Name	User ID	Domain
MS_DEMO_USERS_O365	875e19a9-fadd-466e-b14e-8f6c76568452	Woodgrove - GTP Demos (External/Sponsored)
MS_DEMO_USERS_Woodgrove-SG	4789d6af-777e-4bf6-8150-0bd8d81506b6	Woodgrove - GTP Demos (External/Sponsored)

Managing permissions across multicloud environments requires a new approach

Today's static, outdated approach	A new, dynamic approach
~~Grants permissions based on job roles and responsibilities~~	Grants permissions based on historical usage and activity
~~IAM admins manually grant permissions which are not time-bound~~	Allow temporary access to high-risk permissions on-demand
~~Permission clean-up is done manually on an as-need basis~~	Continuously monitor and right-size identities to prevent privilege creep

Microsoft Security

Getting started with Entra Permissions Management

1 *Deploy*
< 30 minutes

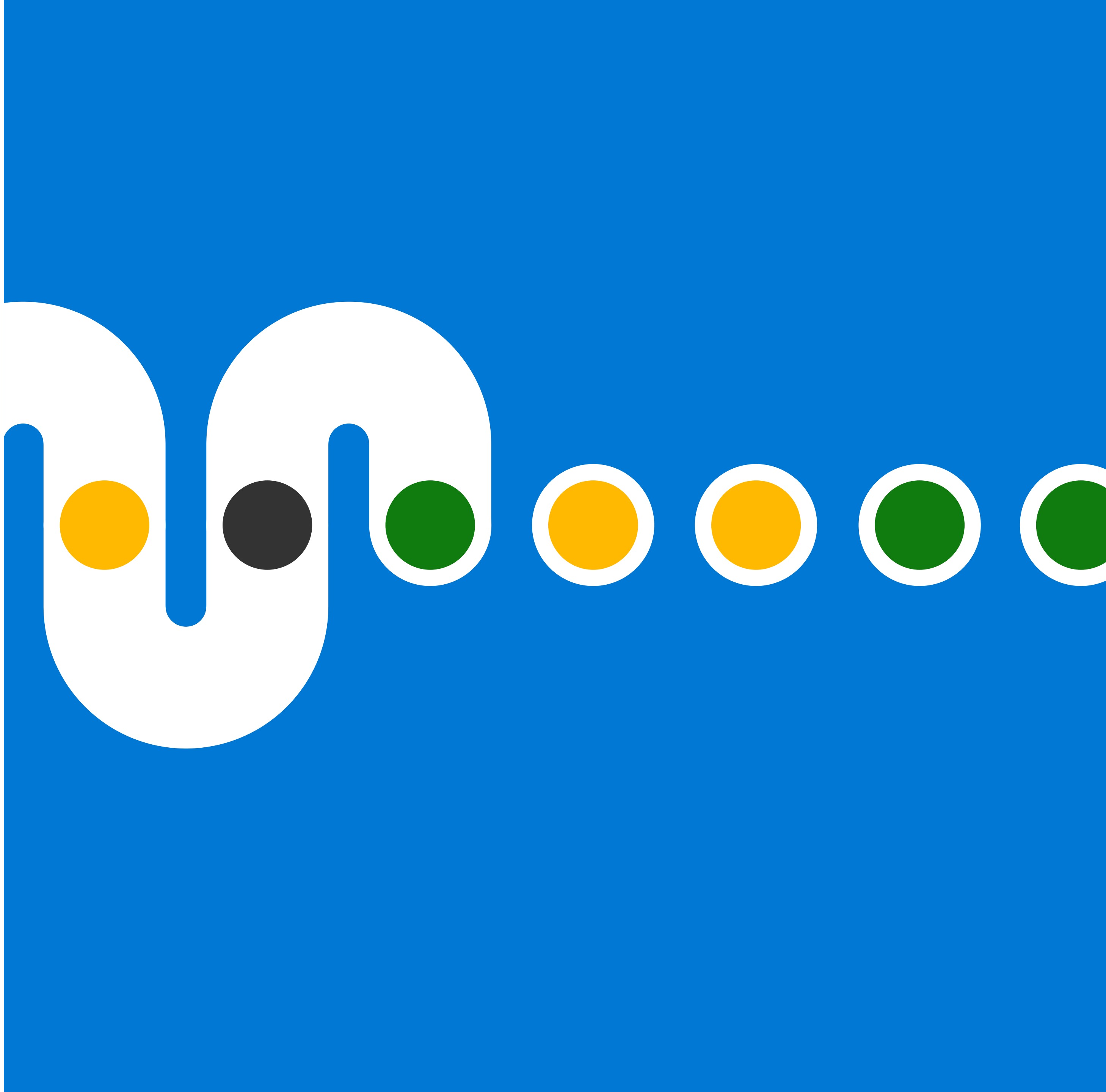
2 *Data collection*
< 24 hours

3 *Operational*
< 1 day

Microsoft Security

Visibility into over-permissioned access across cloud vendors

Demo



Break

Please return at 1400 BST

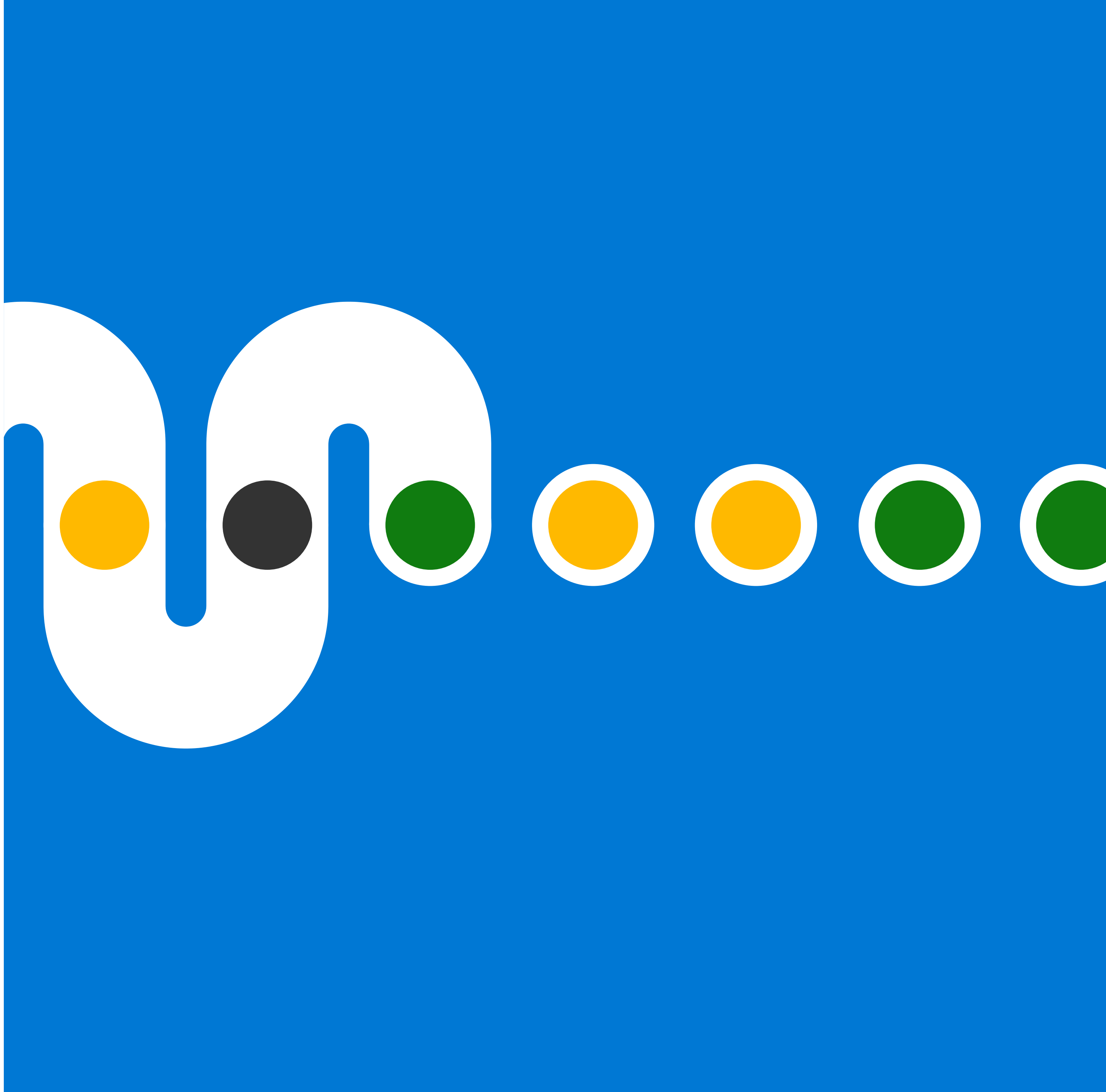
Please complete the poll if you haven't already

https://aka.ms/SecuringMVC3-Poll

Microsoft Security

How to use Entra Permissions Management to remediate over-permissioned access

Demo



Mitigation Strategies

- Disable inactive identities, groups or convert them to “read-only” status
- Remove all high-risk permissions that have not been used over 90 days
- Remediate issues identified in the Permissions Analytics Report – eg old Access Keys, resources externally available

- Create (customize) least privileged roles/policies
- Continuously monitor active identities to prevent permissions creep/sprawl
- Allow temporary access to high-risk permissions on demand or just-in-time (resource and time bound)

Managing permissions across multicloud environments requires a new approach

Today’s static, outdated approach	A new, dynamic approach
~~Grants permissions based on job roles and responsibilities~~	Grants permissions based on historical usage and activity
~~IAM admins manually grant permissions which are not time-bound~~	Allow temporary access to high-risk permissions on-demand
~~Permission clean-up is done manually on an as-need basis~~	Continuously monitor and right-size identities to prevent privilege creep

Cloud Permissions Activities Hygiene

- Determine what high-risk permissions have been assigned (policies that have been created and attached to roles) – **What and Where**
- Determine who’s assigned to those roles and consider revising the policies to remove unnecessary permissions (get to Least Privileges) - **Who**
- Generate your new least privilege policies and assign, allowing removal of high-risk permissions – **How**
- Anomaly & Outlier Detection
- Rinse and repeat on an ongoing basis

Good Practices

Microsoft Azure

- **Remove all inactive users** and service principals to avoid unauthorised access to resources.
- **Replace high-risk contributor roles** with lower-risk right-sized roles leveraging activity-based authorisation.

aws

- **Restrict broad access** to all resources for applications on EC2 instances.
- **Regularly review** all identity policies for any privilege escalation possibilities.

Google Cloud

- **Service account keys** should be rotated every 90 days to ensure the data can’t be accessed with old keys that may be compromised.
- **Replace high-risk owner/editor roles** with lower-risk roles leveraging activity-based authorisation to right-size all service accounts.

Microsoft Security

Q&A

Resources

Web

aka.ms/PermissionsManagement

Docs

aka.ms/CIEM

Datasheet

aka.ms/PermissionsManagementDataSheet

Microsoft Entra Announcement Blog

aka.ms/EntraAnnouncement

Solution Brief

aka.ms/PermissionsManagementSolutionBrief

White Paper

aka.ms/CIEMWhitePaper

Infographic

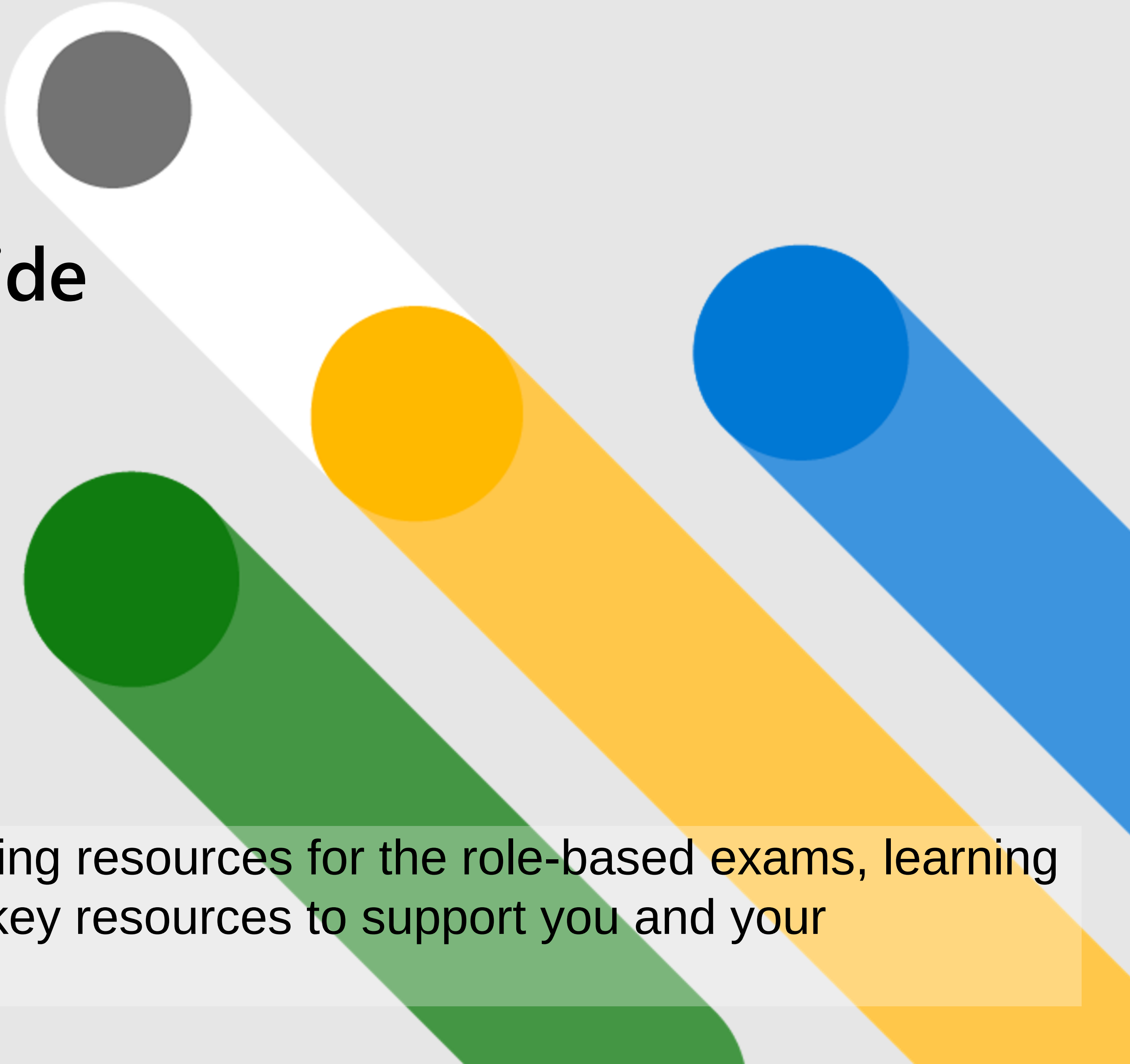
aka.ms/PermissionsRisksInfographic

2021 State of Cloud Permissions Risks Report

aka.ms/PermissionsRisksReport

Microsoft Security

Security, Compliance, Identity Enablement Guide for Partners



Access the latest partner-facing version here:
https://aka.ms/scipartnerenablement

Simplified Guide to SCI Partner training resources for the role-based exams, learning journeys across Security, and other key resources to support you and your organization on your skilling journey.

ACTION PLAN

- Create an **Entra Permissions Management Risk Assessment offer** and publish in the marketplace
- Pass the **SC-300 Microsoft Identity and Access Management administrator exam**
- **Share the training** and materials with others at your organization – slides will be in the event’s GitHub repository.
- **Help your customers** with their security needs across the Microsoft security stack

Contact your local GPS Team to get started!
UK – protectanddefend@microsoft.com

Share your thoughts, **feedback** via our survey!

https://aka.ms/SecuringMVC3-Feedback

Microsoft Security

Thank you.