Microsoft Entra Permissions Management

Introduction

Agenda

- What is a CIEM?
- Securing Cloud Infrastructure
- What are the challenges Microsoft Entra Permissions Management can help me overcome?
- Why should you care?
- Next steps and Proof of Concept

Microsoft Entra Product Family

Identity & access management

- Microsoft Entra ID
- Microsoft Entra ID Governance
- Microsoft Entra External ID

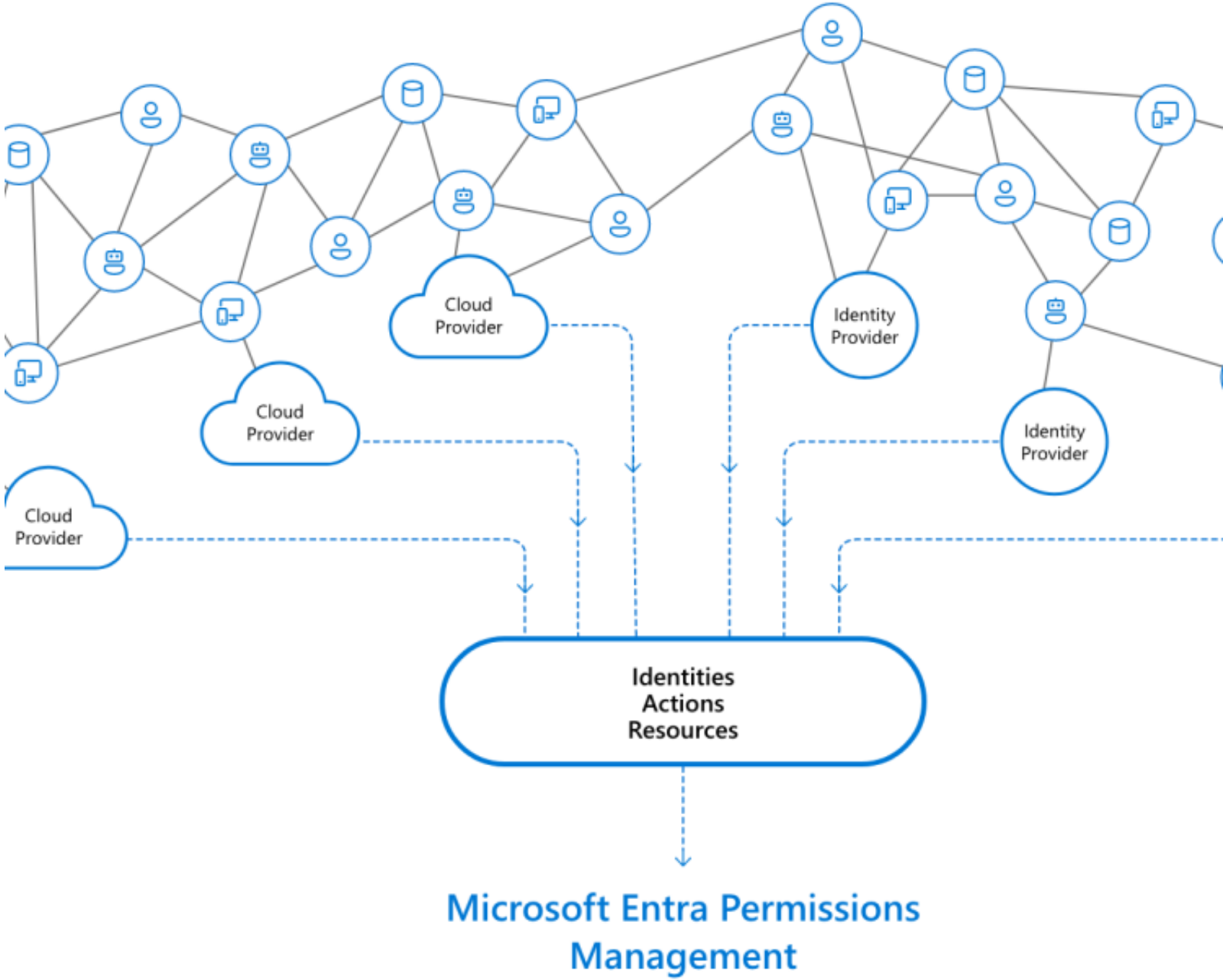
New Identity categories

- Microsoft Entra Verified ID
- Microsoft Entra Permissions Management
- Microsoft Entra Workload ID

Network Access

- Microsoft Entra Internet Access
- Microsoft Entra Private Access

What is a CIEM?



What is a CIEM?

- CIEM: Cloud Infrastructure Entitlement Management

How does it help organizations

Risk

CIEM tools help organizations manage cloud access risks via administration-time controls for the governance of entitlements in hybrid and multicloud infrastructure as a service (IaaS).

Analytics

They use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges and dormant and unnecessary permissions.

Enforcement

CIEM ideally provides enforcement and remediation of least-privilege approaches. Some CIEM tools can extend entitlement controls to SaaS applications and identity providers (IdPs) like Microsoft Azure Active Directory, and also provide basic threat discovery, incident response and forensics.

What is a CIEM?

"The challenge of managing privileges in IaaS is worsening, with thousands of services added in recent years by cloud providers. Security and risk management leaders must combine traditional IAM approaches with CIEM to achieve efficient **identity-first security** management results."

- Gartner

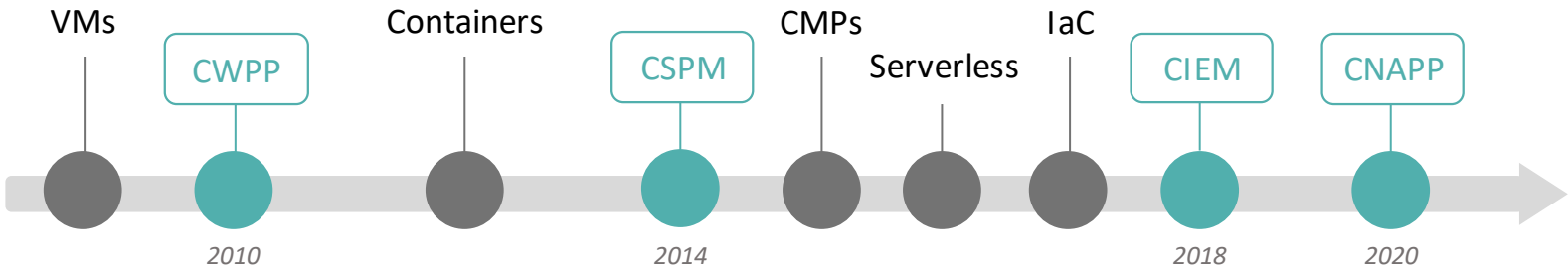
Cloud infrastructure entitlement management (CIEM) offerings are:

- Specialized identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for the governance of entitlements in **hybrid and multicloud** IaaS.
- Typically use analytics, machine learning (ML) and other methods to **detect anomalies** in account entitlements, like **accumulation of privileges**, **dormant and unnecessary entitlements**.
- CIEM ideally provides remediation and enforcement of **least privilege** approaches.

- Gartner

How did we get here?

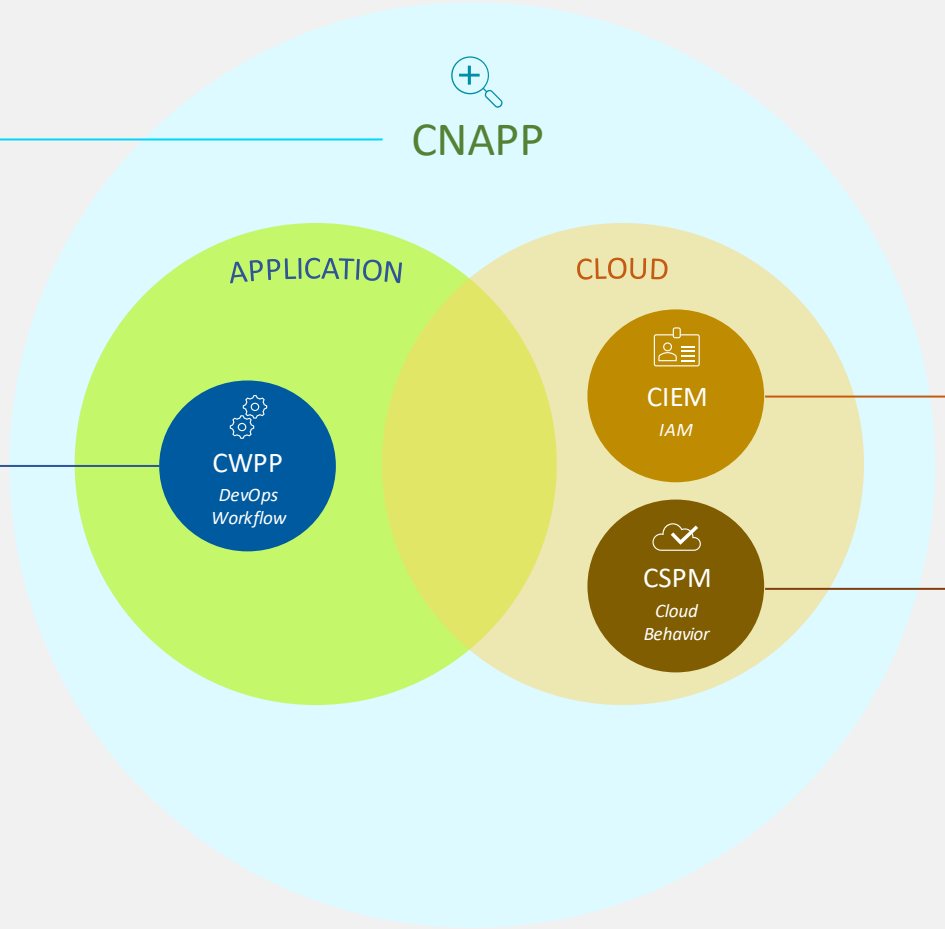
A brief history of cloud security technologies



Cloud Native Application Protection Platforms
Provides a holistic view of cloud security risks by scanning workloads and configurations in development and protecting them at runtime. Secures applications by identifying, assessing, prioritizing, and adapting to risk in cloud-native applications, infrastructures, and configurations.

Cloud Workload Protection Platform
Endpoint protection solutions tailored to server workloads wherever they are running today (VMs, public cloud IaaS, PaaS, etc.).

Microsoft Defender for Cloud



Cloud Infrastructure Entitlement Management
Manages identities and access privileges in multi-cloud environments, applying the principle of least privilege access to cloud infrastructure and services while identifying anomalies in account entitlements.

Microsoft Entra Permissions Management

Cloud Security Posture Management
Leverages native API integrations with IaaS cloud service providers to discover and assess risks of cloud assets and configuration.

Microsoft Defender for Cloud

Securing Cloud Infrastructure

Confusion…?

- Lots of cloud security products, all doing related, but different things
- SASE, CASB, CIEM, SIEM, CNAPP, the list goes on
- Microsoft has several of these offerings:
  - Entra Permissions Management
  - Defender for Cloud
  - Defender for Cloud Apps
  - Sentinel
  - Etc.
- What should you be using, and for what purpose?

Securing Cloud Infrastructure

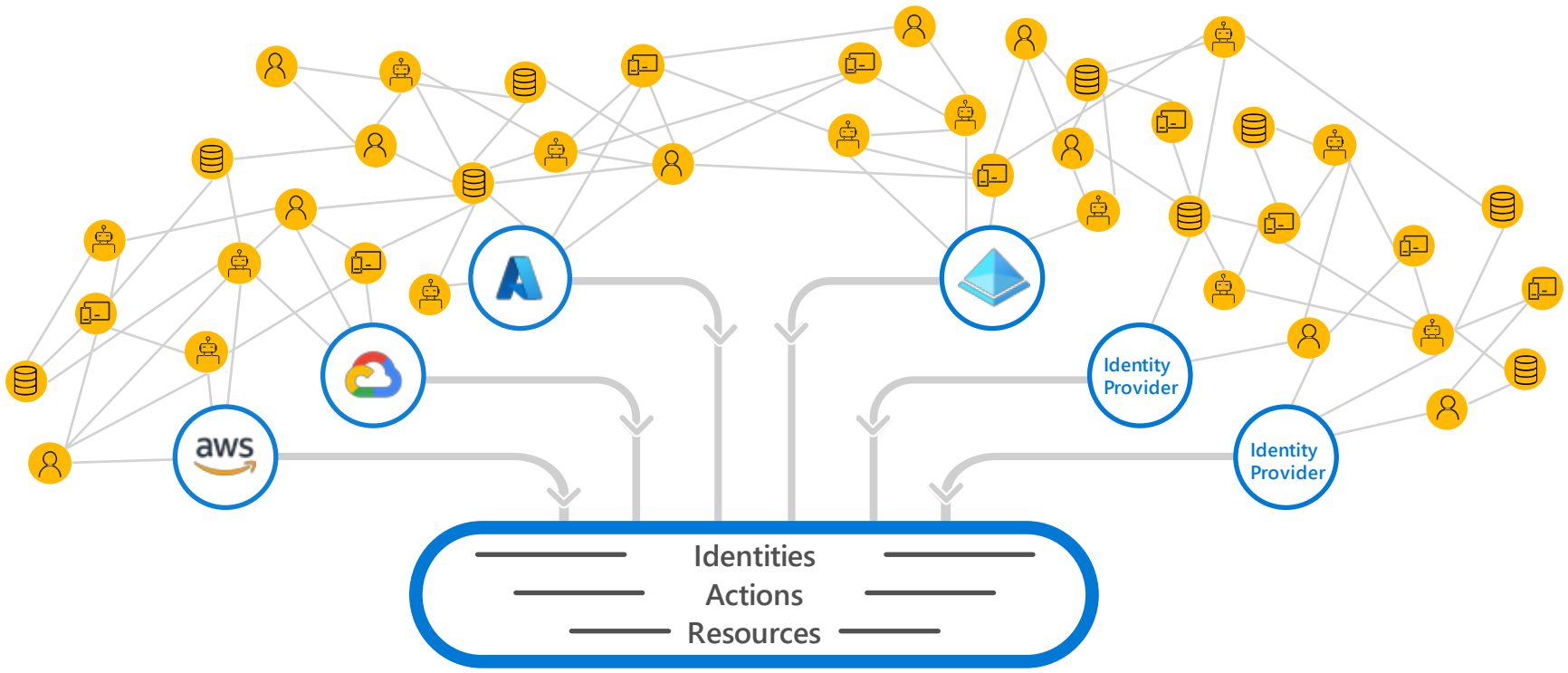
Big Picture of Products and Capabilities

Microsoft Defender for Cloud (CSPM)

- Patch level
- Ports
- Hardening
- & more

Microsoft Defender for Endpoint (through MDC) (CWPP)

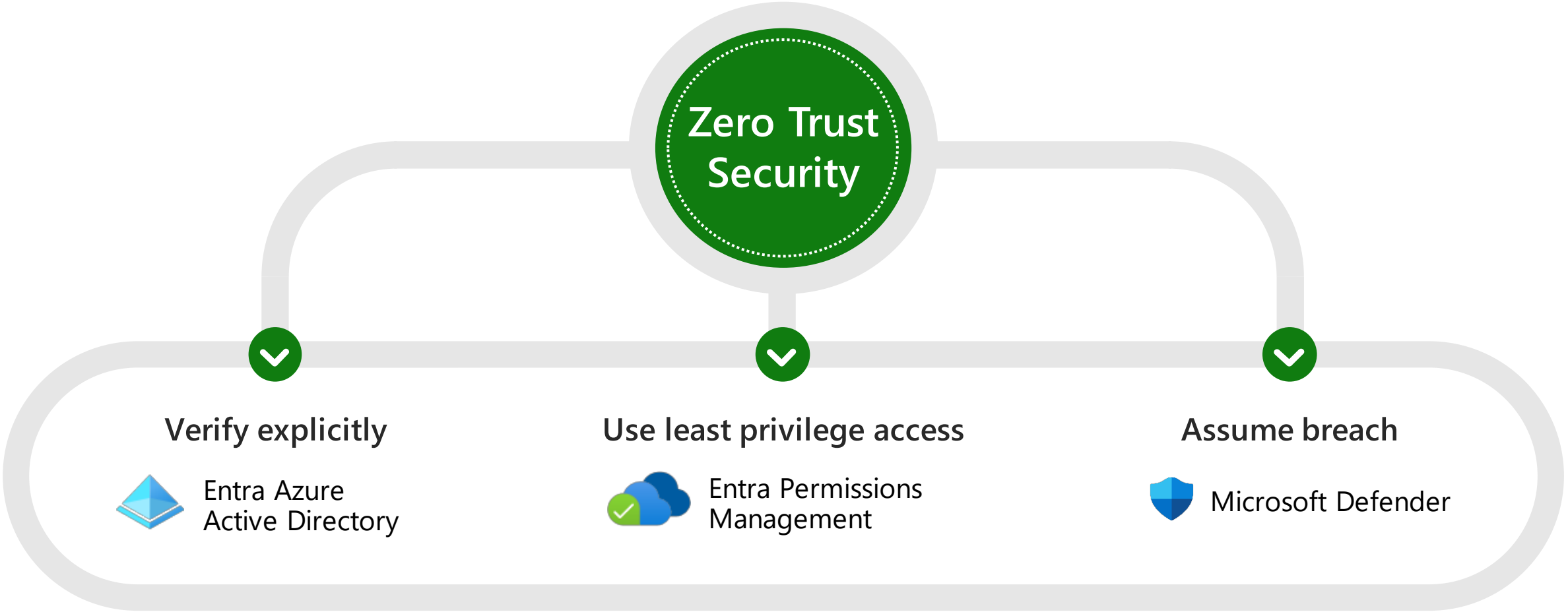
- Malicious execution patterns
- Anomalous processes
- & more



Microsoft Entra Permissions Management (CIEM)

- Over-privileged identities
- Irregular permission pattens
- Unused permissions
- & more

Entra Permissions Management empowers Zero Trust

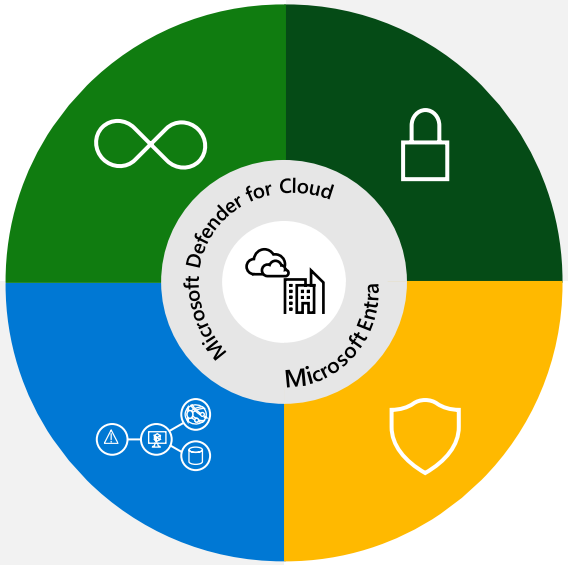


Multicloud | Multi-Platform

Microsoft's cloud-native application protection platform (CNAPP)

DevSecOps

Unify your DevOps security management across multi-pipelines



Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM

Cloud security posture management

Visibility and contextual insights to identify and help remediate your most critical risk

Cloud workload protection

Help detect and respond to modern threats across your cloud workloads in runtime

Integrated to protect across your cloud infrastructure

Microsoft Purview (Data Security)

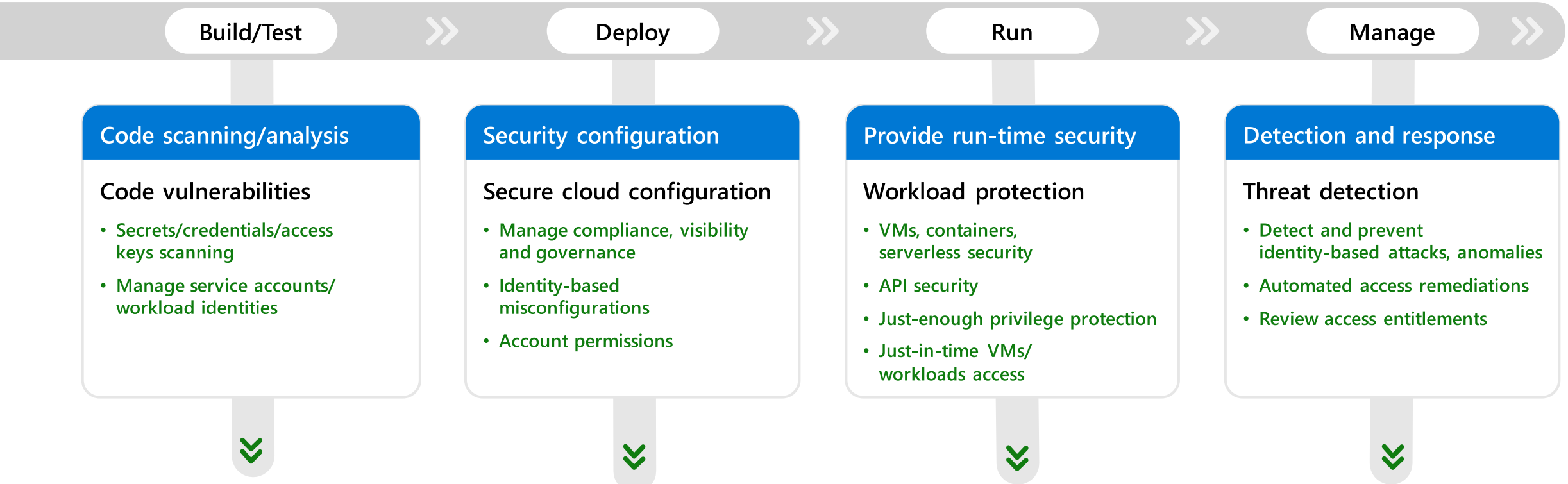
Microsoft Defender External Attack Surface Management (EASM)

Azure Network Security

Microsoft Sentinel (SOAR)

CIEM: Managing identities and permissions for CNAPP

Cloud infrastructure entitlements management offers protection of identities and access throughout a cloud workload's lifecycle



Securing Cloud Infrastructure

Two complementary products

Defender for Cloud

- Cloud security posture management for protecting workloads *running in the cloud*
- Examples:
  - Ensure monitoring agents are installed on VMs
  - VM disks should be encrypted
  - Network Security Groups should restrict most ports
  - Endpoint protection software should be installed on VMs

Microsoft Entra Permissions Management

- Evaluate permissions for the *cloud control plane*
- Examples:
  - Azure admins that manage storage accounts should only have the Storage Administrator role, not Subscription Contributor
  - Storage accounts should not allow anonymous access
  - Developers should not have standing access to AWS VMs

What are the challenges Permissions Management can help you overcome?

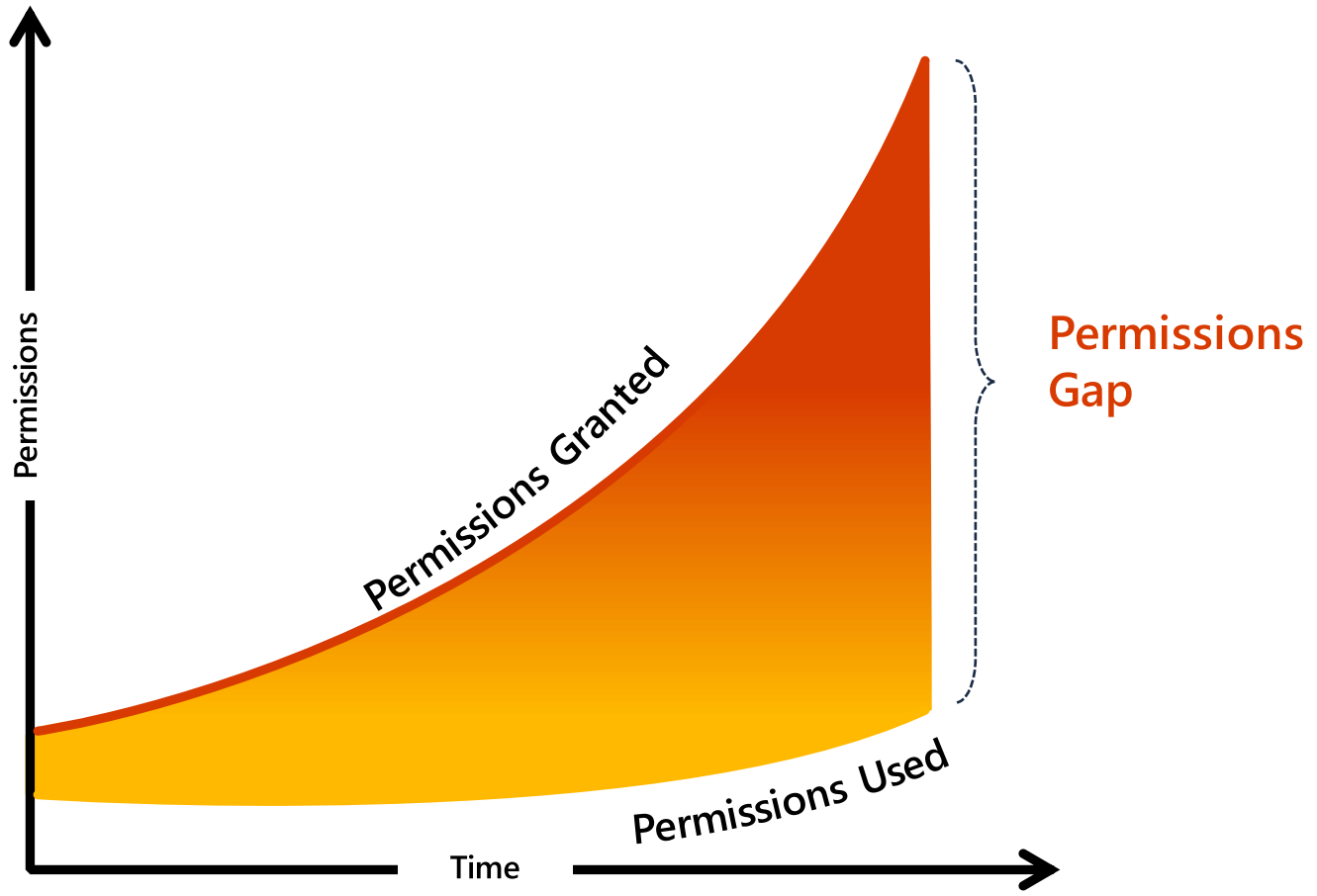
(Multi-)cloud adoption brings new permission challenges

Exponential growth of identities, machines, functions, and scripts operating in the cloud infrastructure

>90% of identities are using **<5% of permissions** granted

>50% of permissions are high-risk and can cause catastrophic damage

Unmanaged permissions are expanding the attack surface



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

Managing permissions across multicloud environments requires a new approach

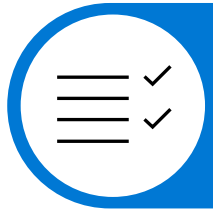
Today's static, outdated approach

~~Grants permissions based on job roles and responsibilities~~

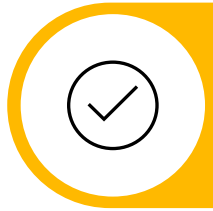
~~IAM admins manually grant permissions which are not time-bound~~

~~Permission clean-up is done manually on an as-need basis~~

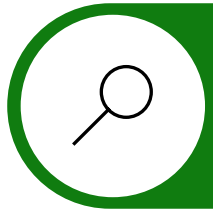
A new, *dynamic* approach



Grants permissions based on historical usage and activity



Allow temporary access to high-risk permissions on-demand



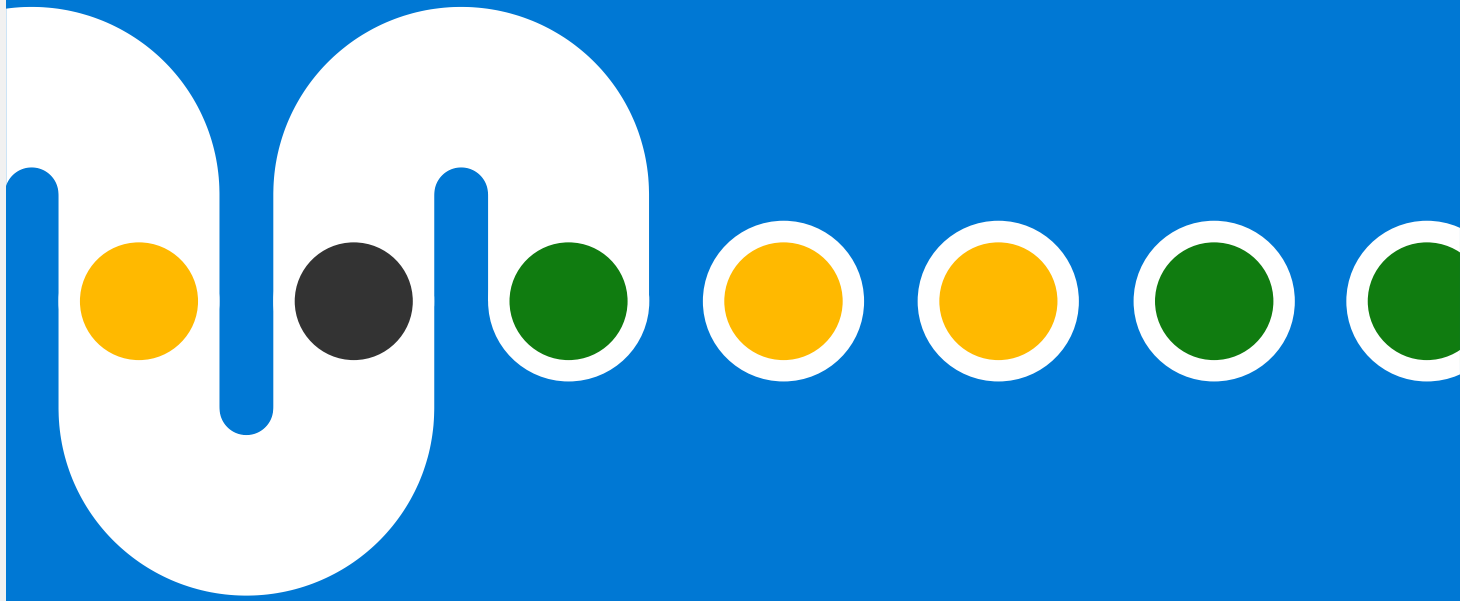
Continuously monitor and right-size identities to prevent privilege creep

What are the *common* challenges?

- Permissions granted based on broad job roles and responsibilities
  - Common to grant broadest permissions that could ever be needed by a role or team
  - Not based on what tasks each person will *actually perform*
- IAM admins manually grant permissions which are not time-bound
  - Permission requirements *change over time* – not enough admins in the world to keep up with the pace of change in most enterprises. Users will naturally accrue more and incorrect permissions as time goes on
  - Compromised account can be used to wreak havoc, especially if attacker can phish an MFA credential
- Permission clean-up is done manually on an as-needed basis
  - Access review processes are manual, time-consuming, and usually *all or nothing*
  - Hard to gain deep enough insights into actual usage to do real *least privilege* right-sizing
  - Hard to operationalize if processes are too manual – permission right-sizing not performed frequently enough

How various teams can leverage EPM

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

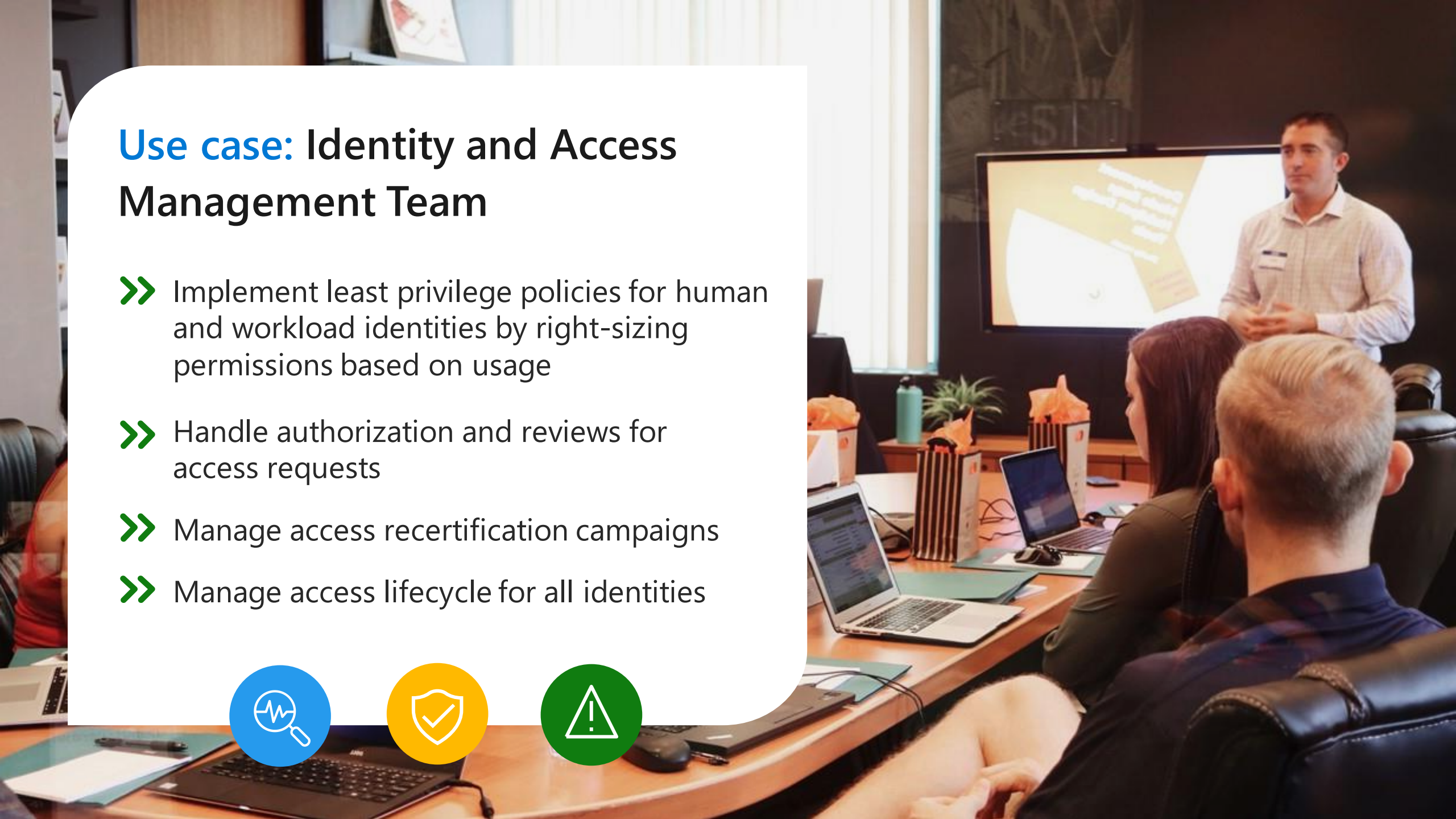


Use case: Cloud Infrastructure Operations Team

- 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

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



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

Business Benefits and ROI

What does your business get out of EPM?

- Alignment with your Zero Trust journey
  - ZT Principles: Verify Explicitly, Use **Least-Privilege Access**, **Assume Breach**
    - These principles sound good, but are hard to live by without the right tooling and automation

- More than just neat technology, you get concrete ROI:
  - Reduced blast radius when accounts are compromised
  - Automated right-sizing of roles reduces manual remediation work
  - Monitor and alert on cloud-native asset types, such as machine identities and serverless functions
  - Reporting to the business
    - Are you reducing your risk over time?
    - What is your overall risk across all Cloud Solution Providers?
    - Are you able to provide evidence for auditors of just enough access?

NIST Zero Trust Goal and Principles (NIST SP.800-207)

Goal:

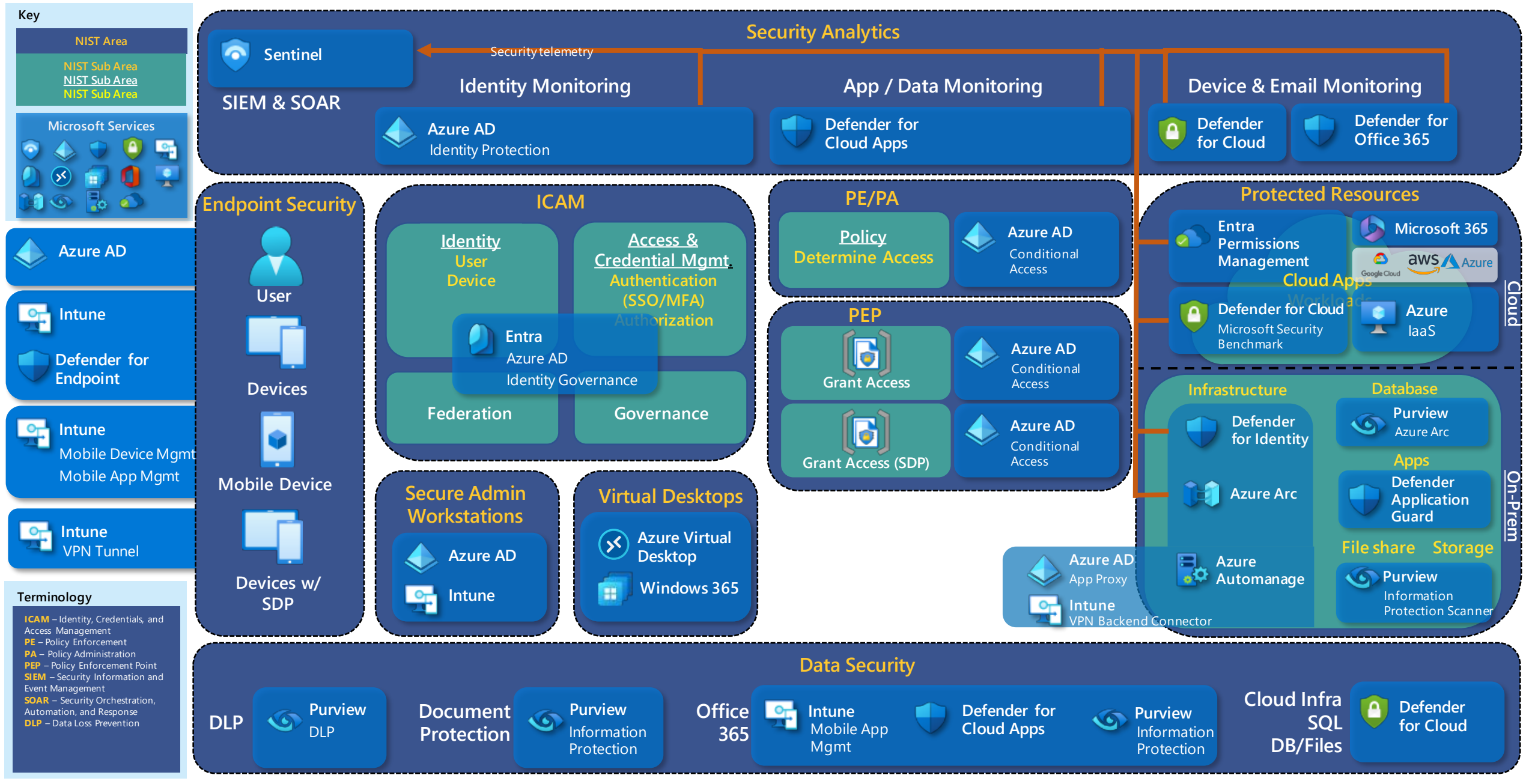
Protect data, computing services (infrastructure), and business functions by "eliminating unauthorized access, coupled with making the access control enforcement as granular as possible."

Principles:

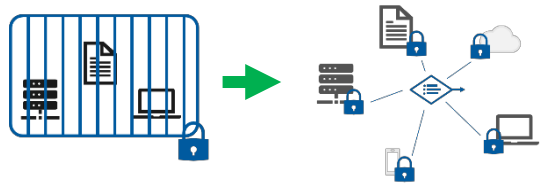
- Network is hostile
- Continued risk analysis and evaluation (never trust and always verify)
- Enact protections to mitigate risk
    - **Minimize access to resources to only those who are validated as needing access**
    - Continuously authenticating the identity and security posture of each access request
    - Access is granted through a Policy Decision Point (PDP) and Policy Enforcement Point (PEP)

Ref: Zero Trust Architecture (nist.gov)

Microsoft Overlay - NIST ZT architecture



Business Benefits of Zero Trust



Line of Business

- **Business Agility –** for continuous business environment changes:
  - Business Models and Partnerships
  - Technology Trends
  - Regulatory, Geopolitical, Cultural Forces
  - Disruptive Events
  - Paradigm Shift to Remote Work
- **Accelerate digital transformation** initiatives and lower risk

Business Support

(Finance, HR, etc.)

- **Accelerate process modernization** using cloud technologies
- **Rapidly apply policy** as people change roles

  Employee ←→ supplier ←→ partners
- **Better business risk visibility & mitigation** for acquisitions and new ventures

IT & Security

- **Simpler architectures** are more cost effective, easier to support, and reduce the threat surface
- **Less policy exceptions** and escalations to manage
- **Better visibility** into technical risks
- **Better prevention** of common security risks

Business Benefits of Entra Permissions Management

ZT Benefits EPM contributes to

Line of Business

- **Business Agility** – for continuous business environment changes:
  - Business Models and Partnerships
  - Technology Trends
  - Regulatory, Geopolitical, Cultural Forces
  - Disruptive Events
  - Paradigm Shift to Remote Work
- **Accelerate digital transformation** initiatives and lower risk

Business Support

(Finance, HR, etc.)

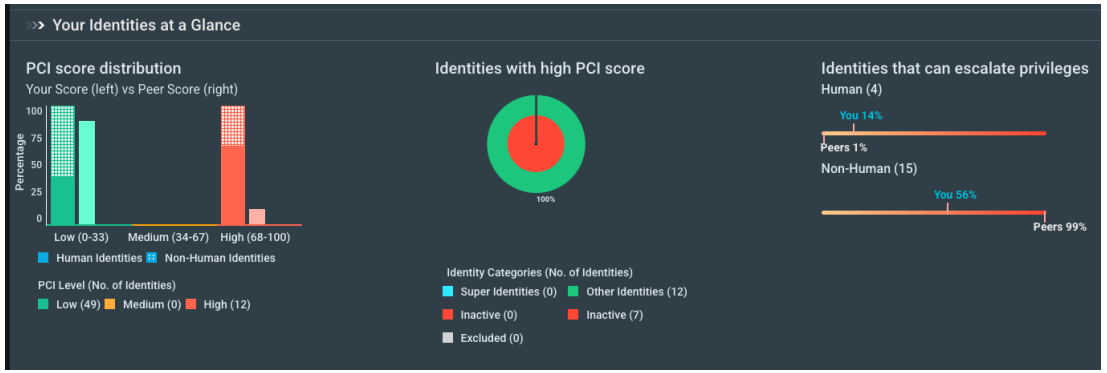
- **Accelerate process modernization** using cloud technologies
- **Rapidly apply policy** as people change roles

  Employee ←→ supplier ←→ partners
- **Better business risk visibility & mitigation** for acquisitions and new ventures

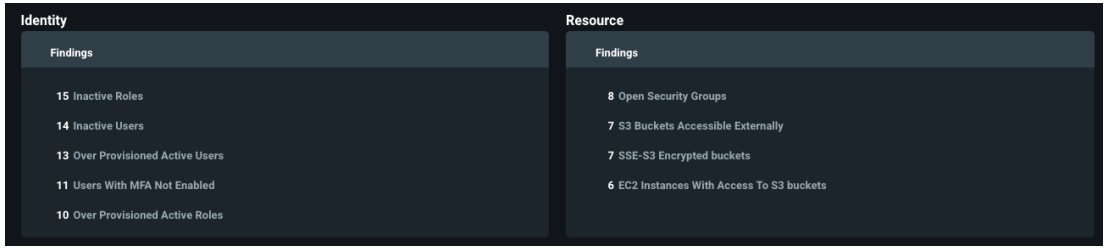
IT & Security

- **Simpler architectures** are more cost effective, easier to support, and reduce the threat surface
- **Less policy exceptions** and escalations to manage
- **Better visibility** into technical risks
- **Better prevention** of common security risks

Reporting on Overall Security to the Business



- Glanceable and scheduled reports that can provide business leaders insight into risk and improvement over time



- Identity and Resource centric views of risk

Reporting on Overall Security to the Business

What do executives care about when it comes to cloud security?	How does EPM Address this concern?
Overall Risk Exposure	Reduce permissions to only what's needed
Cost per incident	Decrease blast radius of an incident through reduction of permissions
Improvement over time	Permissions Creep Index historical report, other reports

Next Steps and POC

Where do we go from here?

- Continue the workshop, of course…
  - Onboard some production Azure Subscriptions, AWS Accounts, and/or GCP Projects into Entra Permissions Management with read-only permissions
  - Investigate initial “quick win” findings discovered in POC
  - Understand automation and alerting capabilities
    - Turn on automation for test resources?
- Purchase? – Talk to us and your account team if you want to keep going
- Deploy what you own
  - Transition from read-only mode to report only and manage mode, use automation and alerting
  - Use permissions on demand
  - Enhance – integrate with your SOC, SIEM, and ServiceNow
- Provide product feedback

Workshop FAQ

- What's the intended outcome?
  - For you to go from 0 to deployed with EPM, understand the value it brings to your organization, and to have a clear plan on what to "go do" moving forward
- How long will this POC be?
  - We'll go through the workshop content in a couple of hours
- What will Microsoft own vs what will you own?
  - We'll offer deployment guidance and best practices we've seen other customers leverage. You will need to operate EPM. If you'd like deeper assistance, we can connect you with a partner for more hands-on guidance
- What does success look like?
  - That you're up and running with EPM, understand what it can do, and have a path forward on what to do next
- Any other questions before we continue?

Thank you!

Microsoft Security

Common Risk Assessment Key Findings

Finding	Implication	Best Practices
>90% of identities using <5% of permissions granted	Excessively permissioned active identities are exposed to credential theft risks	Remove inactive roles/ policies and identities to avoid unauthorized access to resources
Cross-account access is frequently granted to external identities	Cross-account access enables identities to access all resources in target accounts, leading to data leakage or malicious service disruption	Right-size permissions based on the past activities of these identities and grant additional permissions on an on-demand basis
Lack of separation of duties: Users with excessive roles/policies in both development and production subscriptions/accounts	Leveraging the same roles/policies and permissions in development and production environments exposes your infrastructure to insider threats and malicious external threats	Right-size permissions in development environments and clone permissions into production only as a starting point, then rightsize permissions to tighten controls
Workload identities are over-provisioned and >40% inactive	Inactive identities leave organizations open to credential misuse or exploitation for malicious activities	Right-size scope of roles/ policies to access limited resources and limit access to specific identities in other accounts