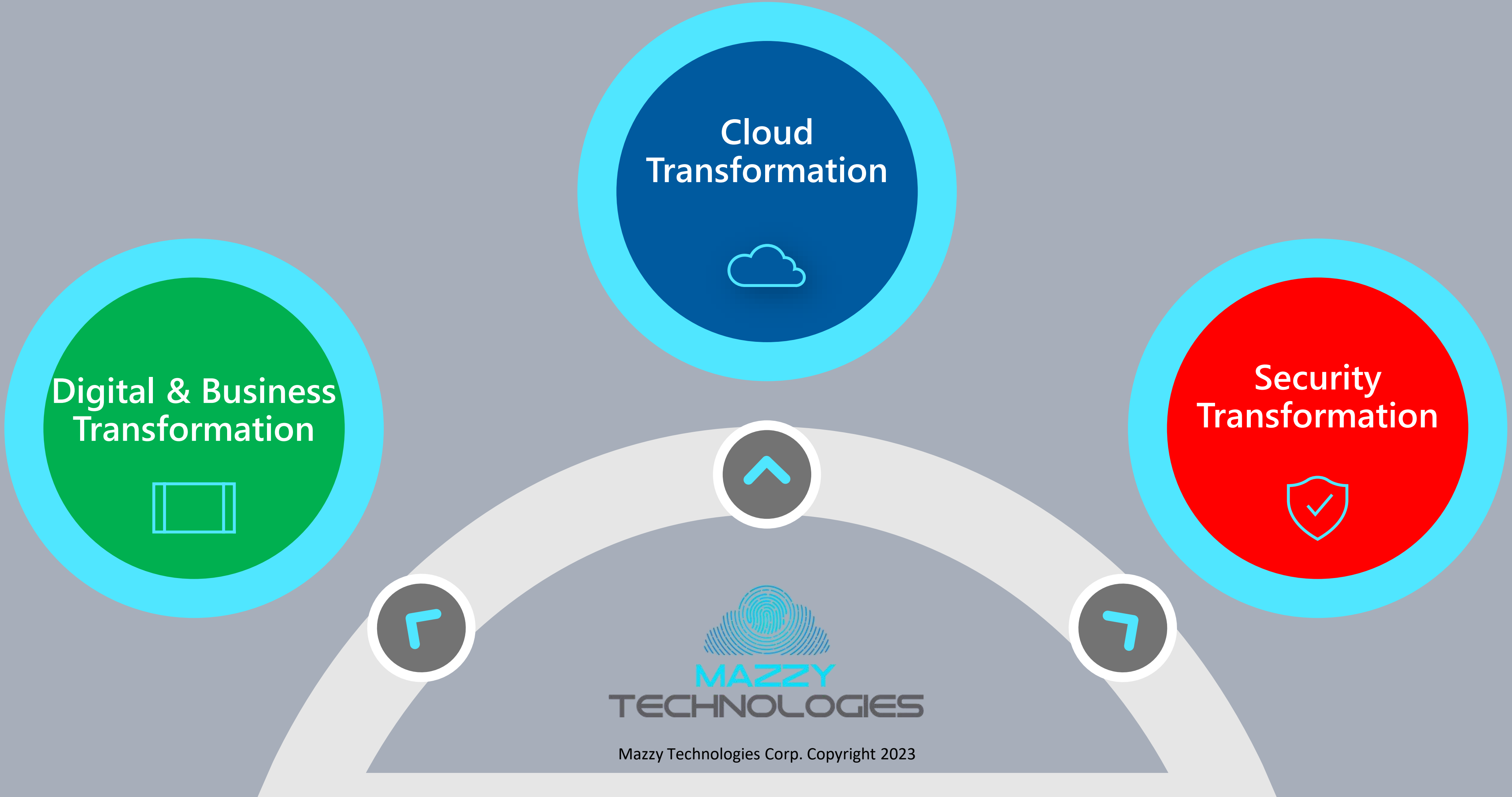
MAZZY
TECHNOLOGIES

Entra Permission Management Risk Assessment

Know who has access to your cloud resources…

Transformation

As the world goes through amazing transformation so are enterprises and governments.



Mazzy Technologies Corp. Copyright 2023

Transformation requires Security Transformation

In modern-day enterprises & governments, there has been a growing transition to cloud-based environments and IaaS, PaaS, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring several challenges to organizations when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud.

Security threats have become more advanced as the digital landscape continues to evolve.

This is why MT suggests the implementation of a **Zero Trust Framework**.

Mazzy Technologies Corp. Copyright 2023

Zero Trust defined

Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to:

“never trust, always verify.”

Every access request is fully authenticated, authorized, and encrypted before granting access. Micro-segmentation and least-privilege access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time.

Mazzy Technologies Corp. Copyright 2023

Zero Trust principles

Verify

Verify explicitly - Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use

Use least-privilege access - Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume

Assume breach - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Mazzy Technologies Corp. Copyright 2023

MAZZY
TECHNOLOGIES

What is CIEM?

Cloud Infrastructure Entitlement Manage (CIEM) solutions automate the process of managing user entitlements and privileges in cloud environments. This makes them an integral part of an organization's identity and access management and cloud security posture management (CSPM) infrastructure.

Get full visibility - Discover what resources every identity is accessing across your cloud platforms.

Automate the principle of least privilege - Use usage analytics to ensure identities have the right permissions at the right time.

Unify cloud access policies - Implement consistent security policies across your cloud infrastructure.

Mazzy Technologies Corp. Copyright 2023

MAZZY TECHNOLOGIES

Microsoft Entra Permissions Management

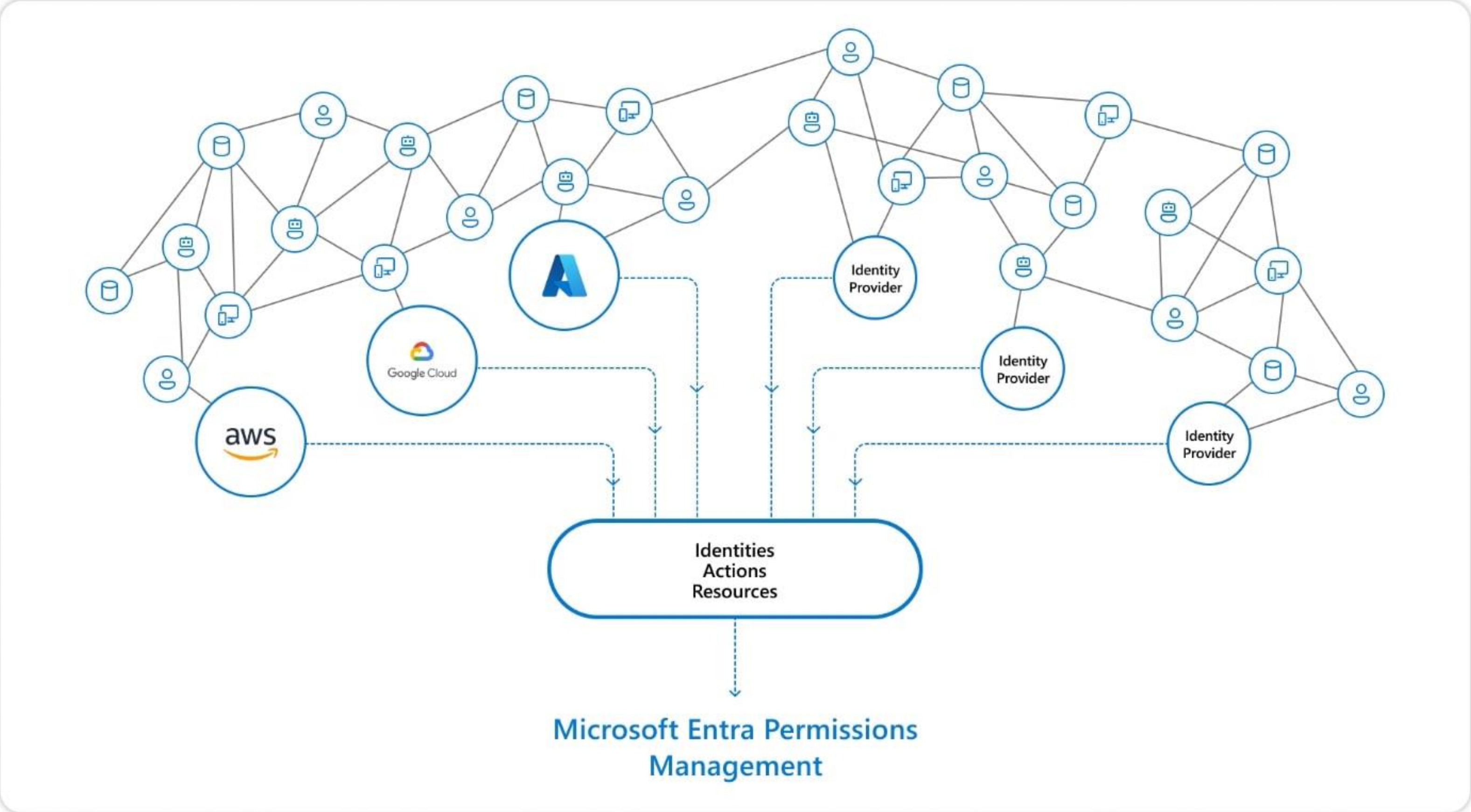
Permissions Management allows you to:

- Get a multi-dimensional view of your risk by assessing identities, permissions, and resources.
- Automate least privilege policy enforcement consistently in your entire multi-cloud infrastructure.
- Prevent data breaches caused by misuse and malicious exploitation of permissions with anomaly and outlier detection.

Mazzy Technologies Corp. Copyright 2023

MAZZY TECHNOLOGIES

Microsoft Entra Permissions Management



Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all user and workload identities, actions, and resources across cloud infrastructures and identity providers. It detects, right-sizes, and monitors unused and excessive permissions and enables Zero Trust security through least privilege access in Azure and other public clouds

Mazzy Technologies Corp. Copyright 2023

MAZZY TECHNOLOGIES

Entra Permissions Management Risk Assessment

Mazzy Technologies will audit entitlement permissions posture across your multi-cloud infrastructure, using Entra Permissions Management

MT will provide risks associated with Permissions Creep Index, and define a plan to right-size unused and excessive permissions and enable Just-Enough-Privilege for zero trust security

Mazzy Technologies Corp. Copyright 2023

Entra Permissions Risk Assessment Timeline

Pre-engagement Call

- Engagement overview
- Define Scope (public clouds and subscriptions)
- Identify stakeholders
- Schedule kick-off meeting

Kick-off

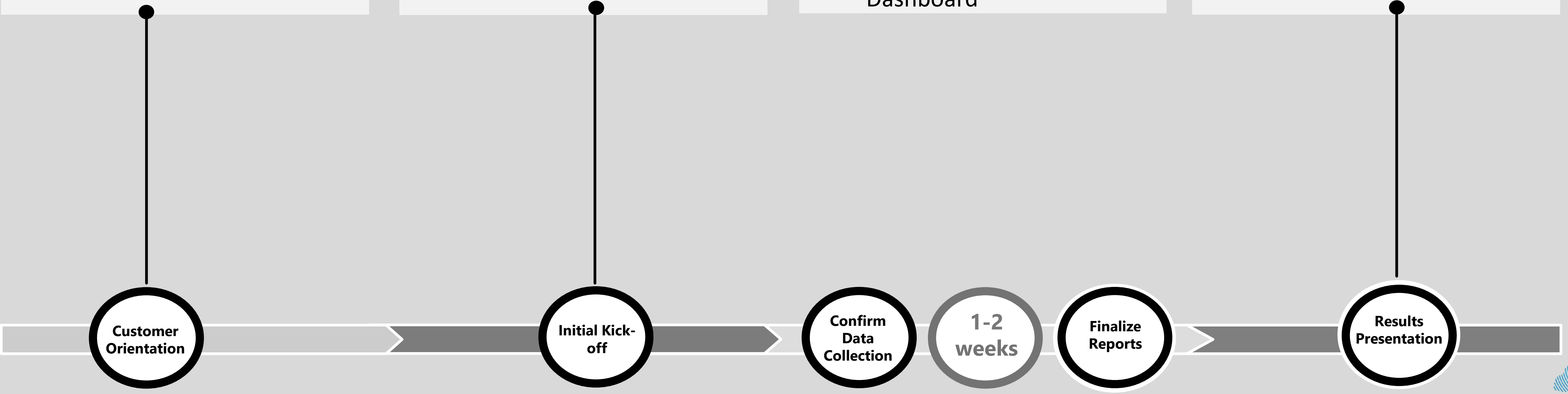
- Review goals, scope & deliverables
- Review access requirements
- Scheduling working sessions
- CPOR / PAL designation
- Review expectations and deployment next steps

Technical Setup

- Enable Entra Permissions Management on Azure AD
- Configure data collection settings
- Setup Cloud connectors
- Confirm data flow to Permissions Management Dashboard

Results Presentation

- Review deliverables
  - Executive report
  - Analytics dashboard
  - Technical details
- Discuss future actions



Customer Orientation

Initial Kick-off

Confirm Data Collection

1-2 weeks

Finalize Reports

Results Presentation

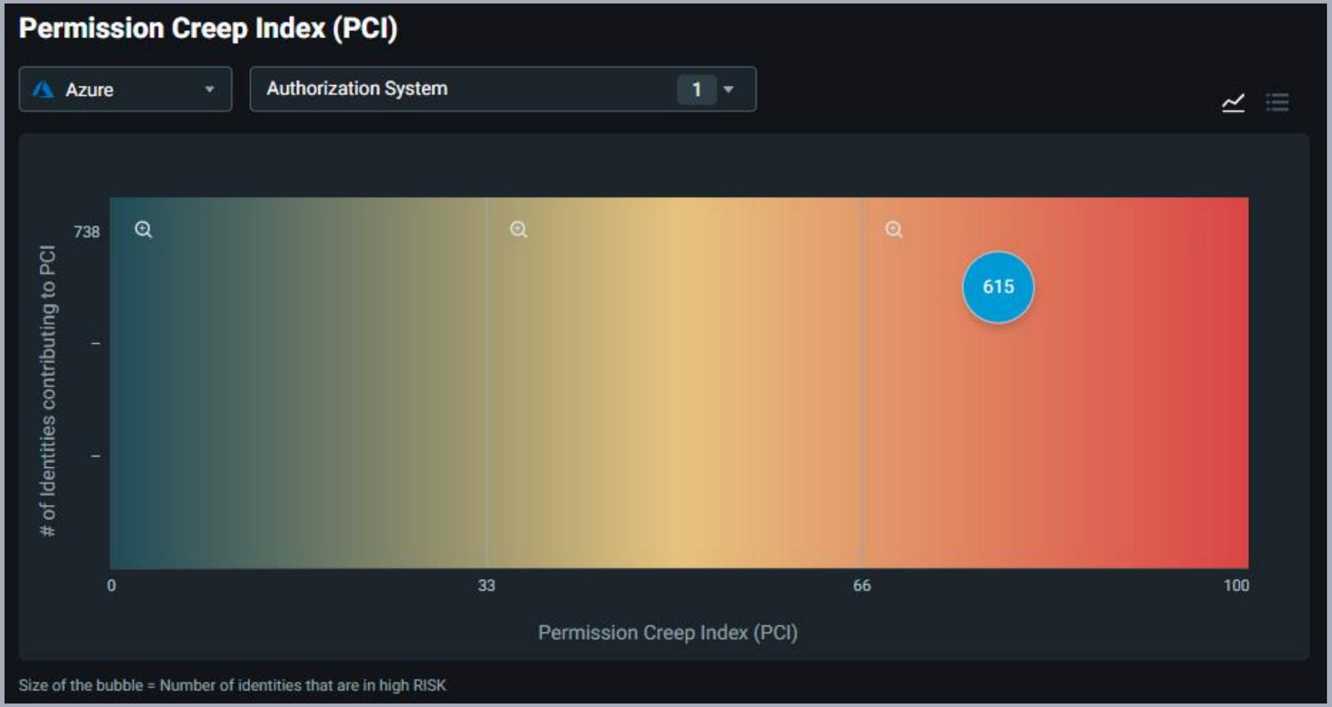
Mazzy Technologies Corp. Copyright 2023

MAZZY TECHNOLOGIES

The PCI Heat Map

The Permission Creep Index heat map shows the incurred risk of users with access to high-risk permissions, and provides information about:

- Users who were given access to high-risk permissions but aren't actively using them. High-risk permissions include the ability to modify or delete information in the authorization system.
- The number of resources a user has access to, otherwise known as resource reach.
- The high-risk permissions coupled with the number of resources a user has access to produce the score seen on the chart.



Permission Creep Index (PCI)

Azure

Authorization System 1

738
# of Identities contributing to PCI
615
0
33
66
100
Permission Creep Index (PCI)

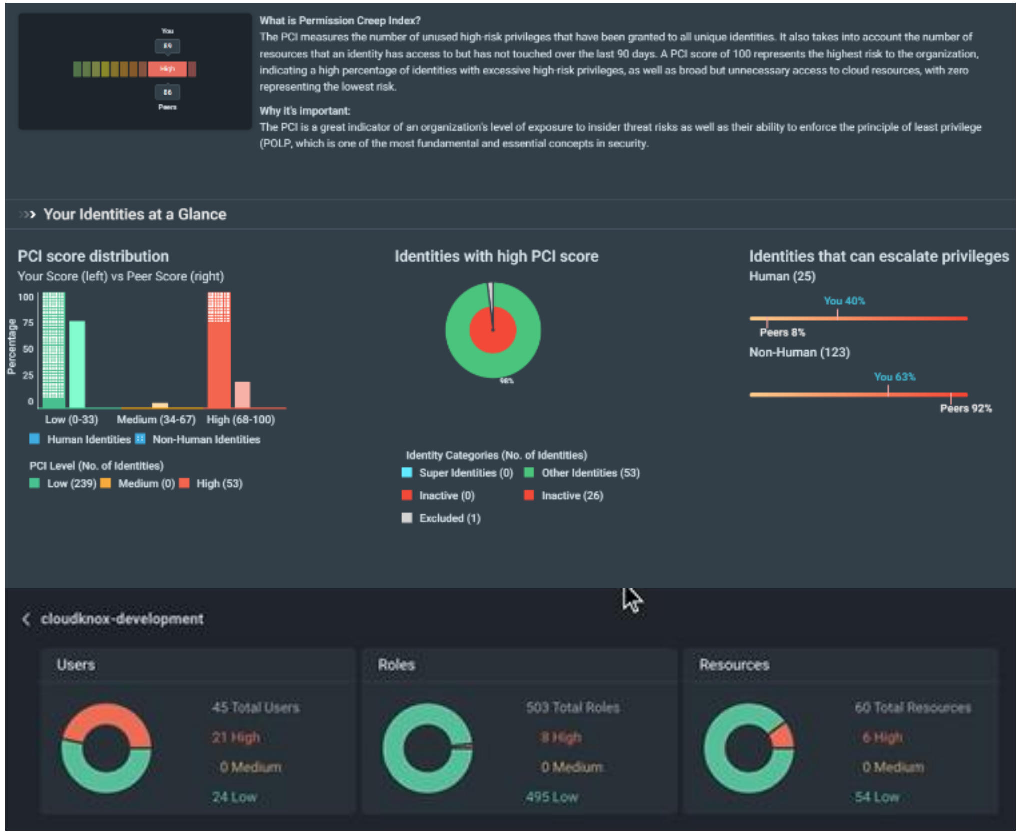
Size of the bubble = Number of identities that are in high RISK

Mazzy Technologies Corp. Copyright 2023

Entra Permissions Management Risk Assessment Deliverables

Both executive reports and detailed reports are delivered so that your organization can take immediate action to remediate risk and right-size permissions based on usage, grant new permissions on-demand, and automate just-in-time access for cloud resources.

- Permission Creep Index (PCI): An aggregated metric that periodically evaluates the level of risk associated with the number of unused or excessive permissions across your identities and resources. It measures how much damage identities can cause based on the permissions they have.
- Permission usage analytics: Multi-dimensional view of permissions risk for all identities, actions, and resources.


You
High
Peers
PCI score distribution
Your Score (left) vs Peer Score (right)
Percentage
100
75
50
25
0
Low (0-33)
Medium (34-67)
High (68-100)
🟦 Human Identities ▦ Non-Human Identities
PCI Level (No. of Identities)
🟩 Low (239) 🟧 Medium (0) 🟥 High (53)
Identities with high PCI score
Identity Categories (No. of Identities)
🟦 Super Identities (0) 🟩 Other Identities (53)
🟥 Inactive (0) 🟥 Inactive (26)
⬜ Excluded (1)
Identities that can escalate privileges
Human (25)
You 40%
Peers 8%
Non-Human (123)
You 63%
Peers 92%

What is Permission Creep Index?

The PCI measures the number of unused high-risk privileges that have been granted to all unique identities. It also takes into account the number of resources that an identity has access to but has not touched over the last 90 days. A PCI score of 100 represents the highest risk to the organization, indicating a high percentage of identities with excessive high-risk privileges, as well as broad but unnecessary access to cloud resources, with zero representing the lowest risk.

Why it's important:

The PCI is a great indicator of an organization's level of exposure to insider threat risks as well as their ability to enforce the principle of least privilege (POLP, which is one of the most fundamental and essential concepts in security.

›› Your Identities at a Glance

‹ cloudknox-development

Users

45 Total Users
21 High
0 Medium
24 Low

Roles

503 Total Roles
8 High
0 Medium
495 Low

Resources

60 Total Resources
6 High
0 Medium
54 Low

Mazzy Technologies Corp. Copyright 2023

Thank you!

Contact us:

Phone: **1.888.992.1062**

info@mazzytechnologies.com

https://mazzytechnologies.com

MAZZY TECHNOLOGIES

Mazzy Technologies Corp. Copyright 2023