How can cloud permission risks impact your organization?

As more organizations adopt multicloud infrastructures, identity permissions have exploded across the 3 leading cloud platforms: Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

The shift to multicloud presents new permission challenges

- 40,000+ permissions across major clouds and counting
- >5% of permissions are actually used
- 50% of these permissions are considered high-risk
- 95% of permissions are unused and represent potential high-security risks

The rise of human & workload identities increases complexity across clouds

- Ratio of user identities vs. workload identities:
  - 1.5 today
  - 120 in five years

As services continue to expand, super identities expose your infrastructure to unnecessary risk

- Increase of cloud services across major cloud infrastructures: +10%
- Average number of services went from 15 to 150 annually per cloud platform

How can you prevent your cloud permissions from expanding your attack surface?

- Assess your permission risks and identify what identity has been doing what, where they’ve been doing it, and when they’ve been doing it.
- Grant permissions on-demand and just-in-time to ensure the principle of least privilege.
- Continuously monitor permissions usage across clouds to prevent security threats.

Learn more about multicloud permissions management at https://aka.ms/PermissionsManagement.

©2021 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.