

Navigating the Challenges of Cloud Permissions: Ownership, Maturity, and Centralized Control



ACCESS



Sandy Bird
Co-Founder & CTO
Sonrai Security



Alex Shulman
Cloud Cybersecurity Leader
Ernst & Young LLP



EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.

The views expressed by the presenters are their own and not necessarily those of Ernst & Young LLP or other members of the global EY organization or Sonrai Security.

These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

Why is Cloud IAM Different?



Identity and access management (IAM) is the new cloud perimeter and creates a higher risk of public exposure of critical data if IAM, permissions or policies are misconfigured.



Cloud IAM provisioning is done by cloud, dev and DevOps teams and can't be manually reviewed.

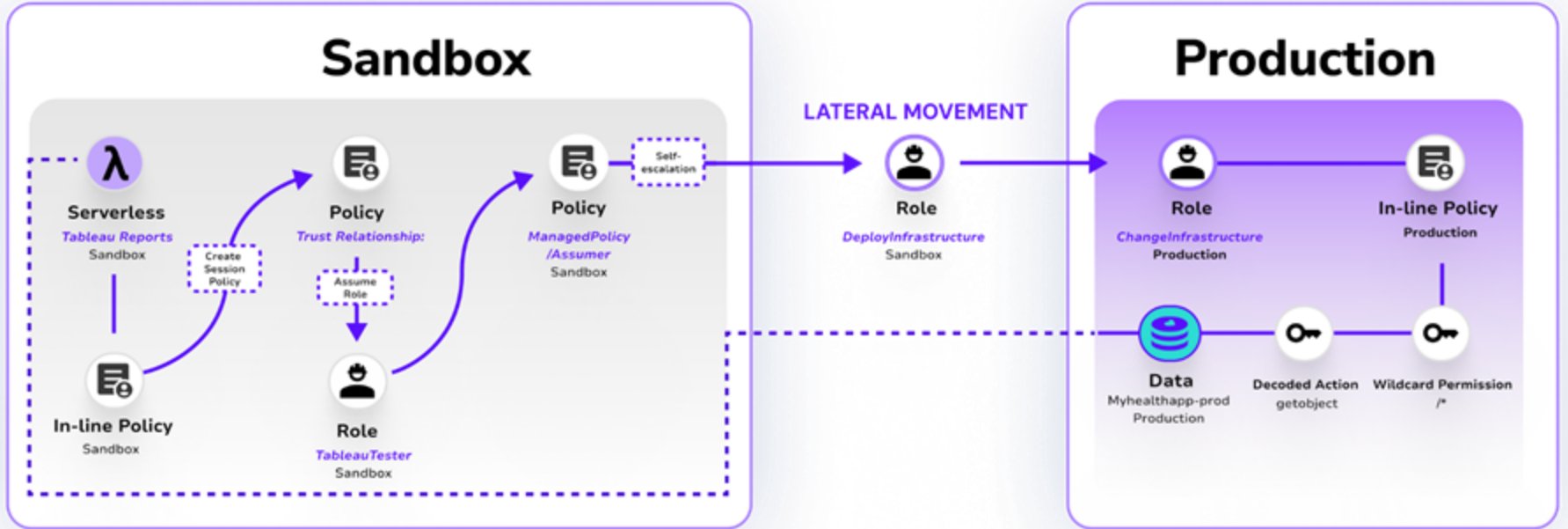


Cloud infrastructure entitlements are too granular for traditional IAM and privileged access management (PAM) tools.



Cloud scale and speed require automated detection and response.

Risk of Over Privileged Identities



WHAT CAN ACCESS THE IDENTITY?

WHAT CAN THE IDENTITY ACCESS?

State of Privileged Access



Complex

14,000+

Unique permissions
in AWS

Overprivileged

92%

Of identities have
excessive
permissions

Still Broken

30 mins

Per identity to fix

2-3

Different clouds with
separate IAM schema

61%

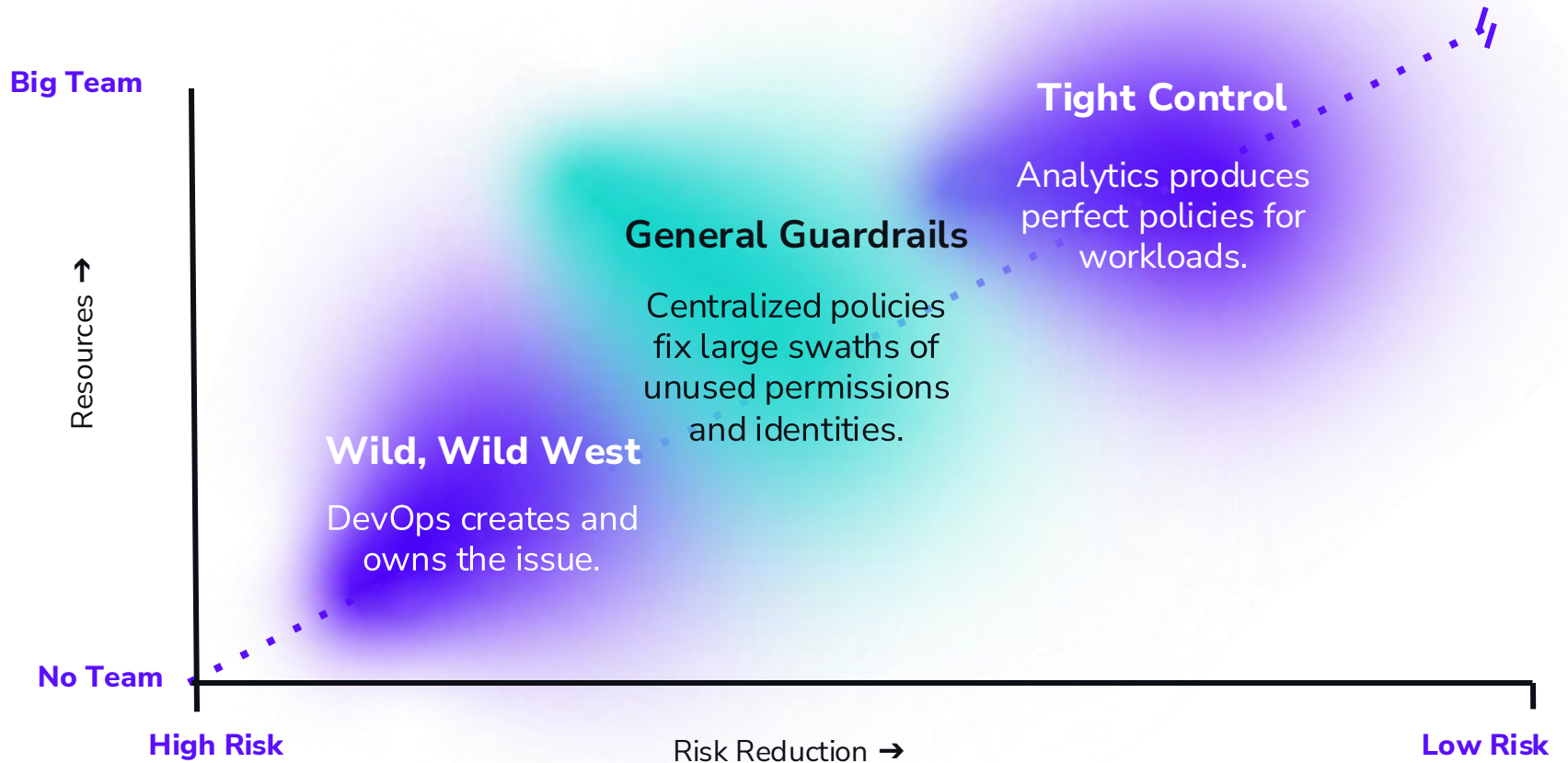
Of identities are
unused

10,000+

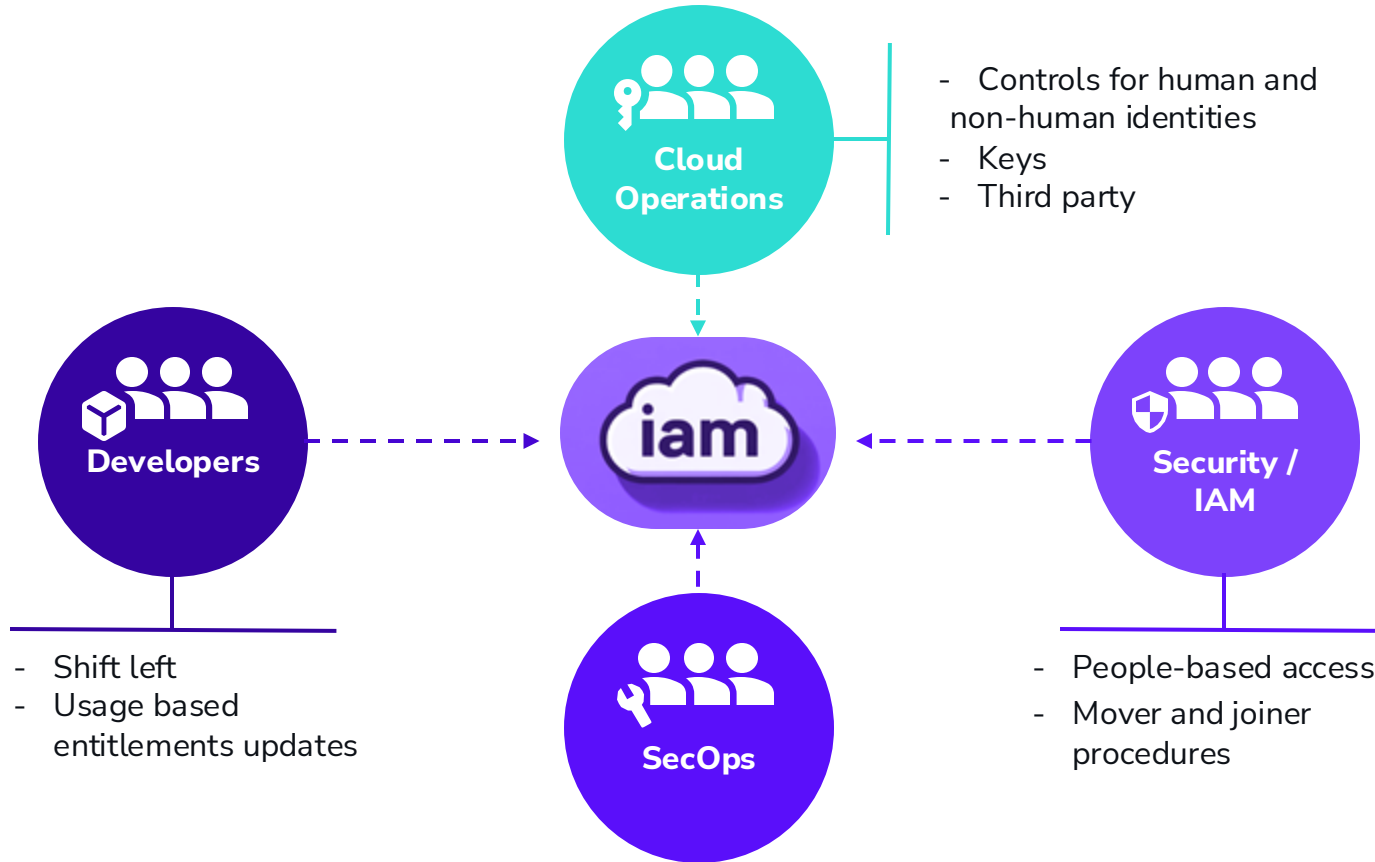
Average identities in
a corporate cloud

* Data collected in 2023 from enterprises in US and Canada. [Source](#): Sonrai Security.

Least Privilege Maturity Stages



Who is Responsible?



How Are Misconfigurations Handled?

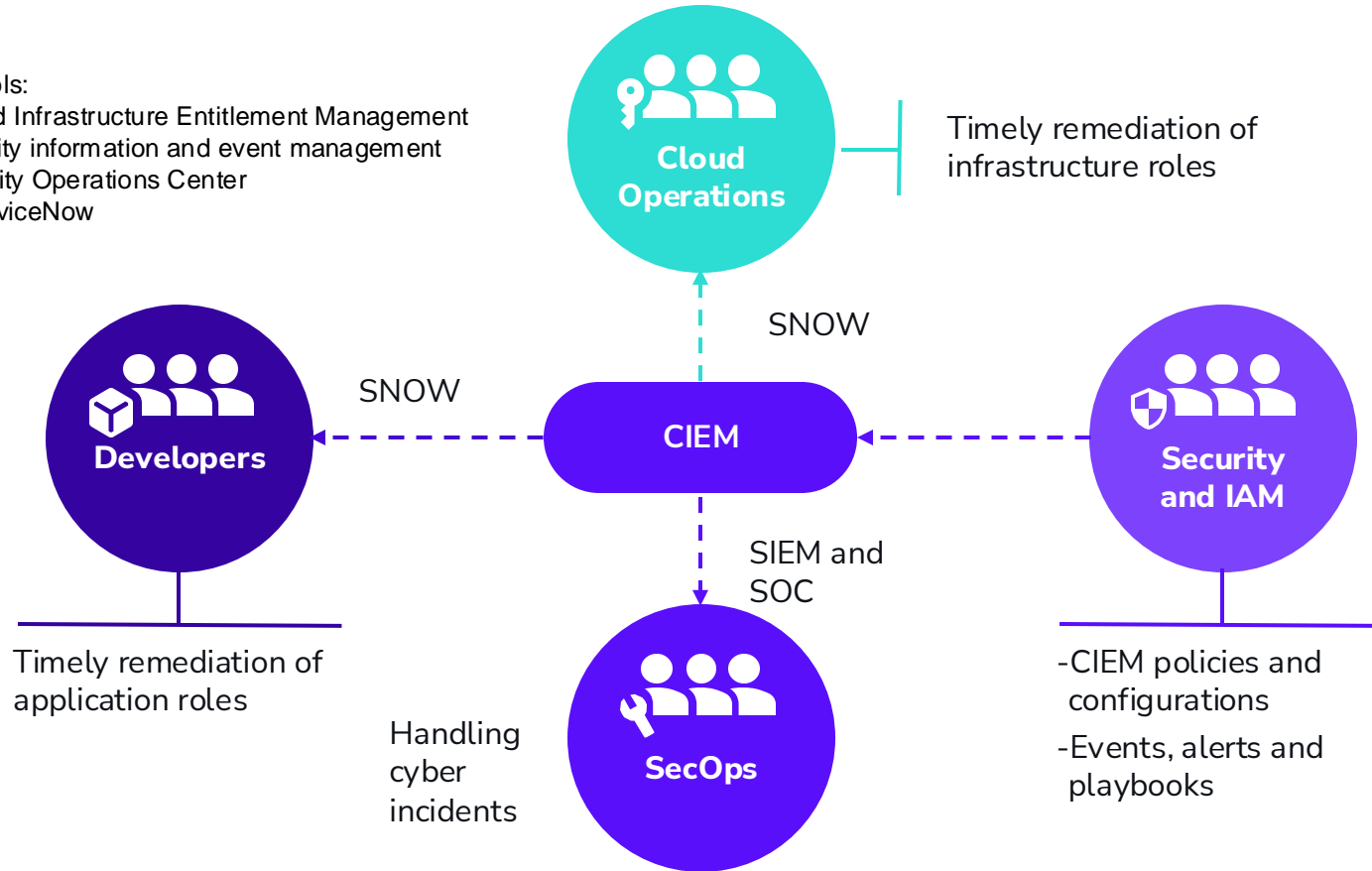
Common Tools:

CIEM – Cloud Infrastructure Entitlement Management

SIEM - security information and event management

SOC – Security Operations Center

SNOW – ServiceNow



Shift Left vs. Central Control?

Central Control

Global cloud policies
SSO federation by ops
Detect architectural flaws
caused by poor IAM
configuration

Shift Left

Follow basic linting advice
Granular RBAC by dev
Entitlements updated based
on actual usage

Good Enough Operating – Centralized Control



Secure the baseline ...

- 1 Secure 3,000+ sensitive permissions.
- 2 Review one global policy.
- 3 Deploy centrally.



Restrict
unused sensitive
permissions.



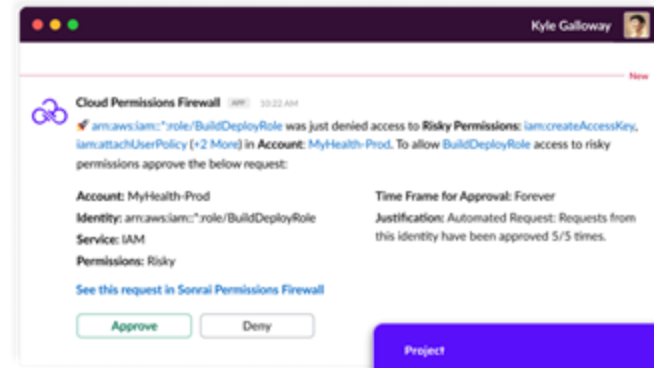
Quarantine
zombie
identities.



Disable
unused
services.

... and keep everyone happy

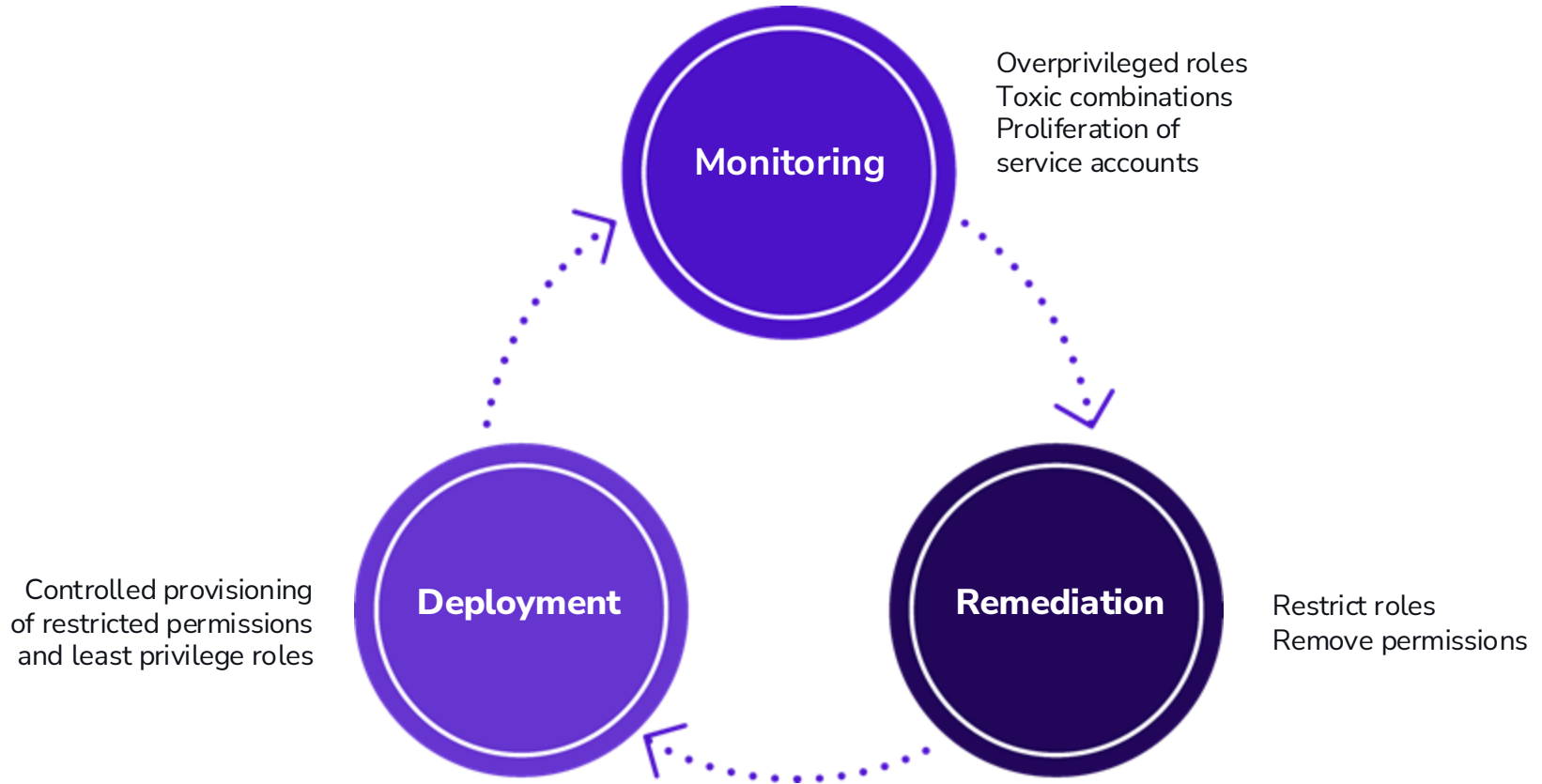
Permissions on demand



The right
exemptions

Project	Usage
AWS - MyHealth-Prod CloudFormation	5 Identities
Exemptions Add*	Last used
Build	7 days
Maurice Moss	7 days
Jen Barber	9 days
Roy Trenneman	4 months
Richmond Avenal	3 days

Cloud IAM Remediation Lifecycle



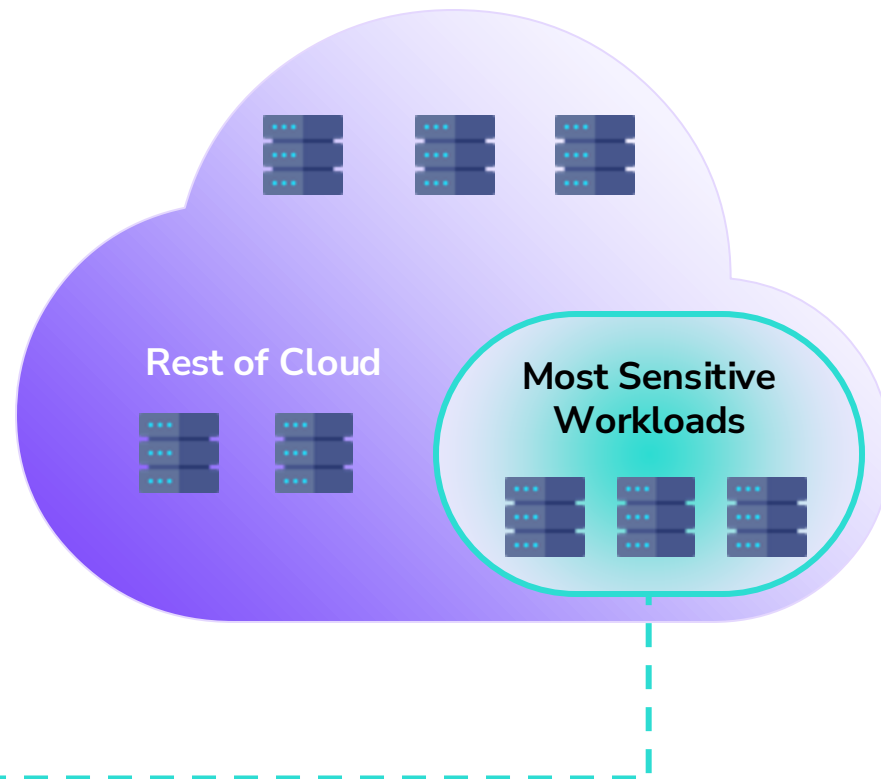
Recommendations

Good Enough

- Disable the unused identities (delete or quarantine).
- Disable the services and regions you don't use.
- Block tampering of security controls (requires break glass to circumvent).
- Uphold security best practices (prevent drift).
- Enforce encryption, block public access, etc.
- Prevent perimeter breaches and get control of third party.

Granular Least Privilege

- Use analytics and historical data to generate policies.
- Continually monitor and adjust.



ACCESS

Q&A



Sandy Bird
sandy.bird@sonraisecurity.com



Alex Shulman
alex.shulman@ey.com

Thank You!