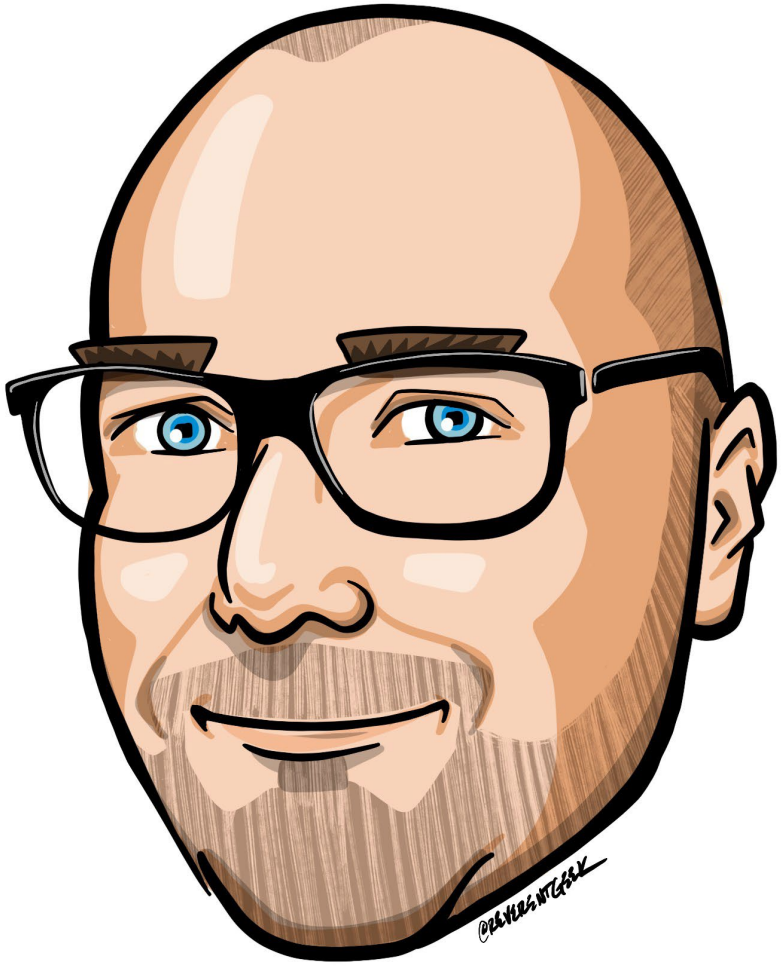
Lessons learned from enterprise cloud security programs

Karl Ots

Karl Ots

Head of Cloud Sec @ EPAM
CISSP. MVP, RD, LMGTFY

@karlgots



Agenda

- Introduction to cloud security
- Definition of a cloud security program
- Cloud security architecture components
- Lessons learned

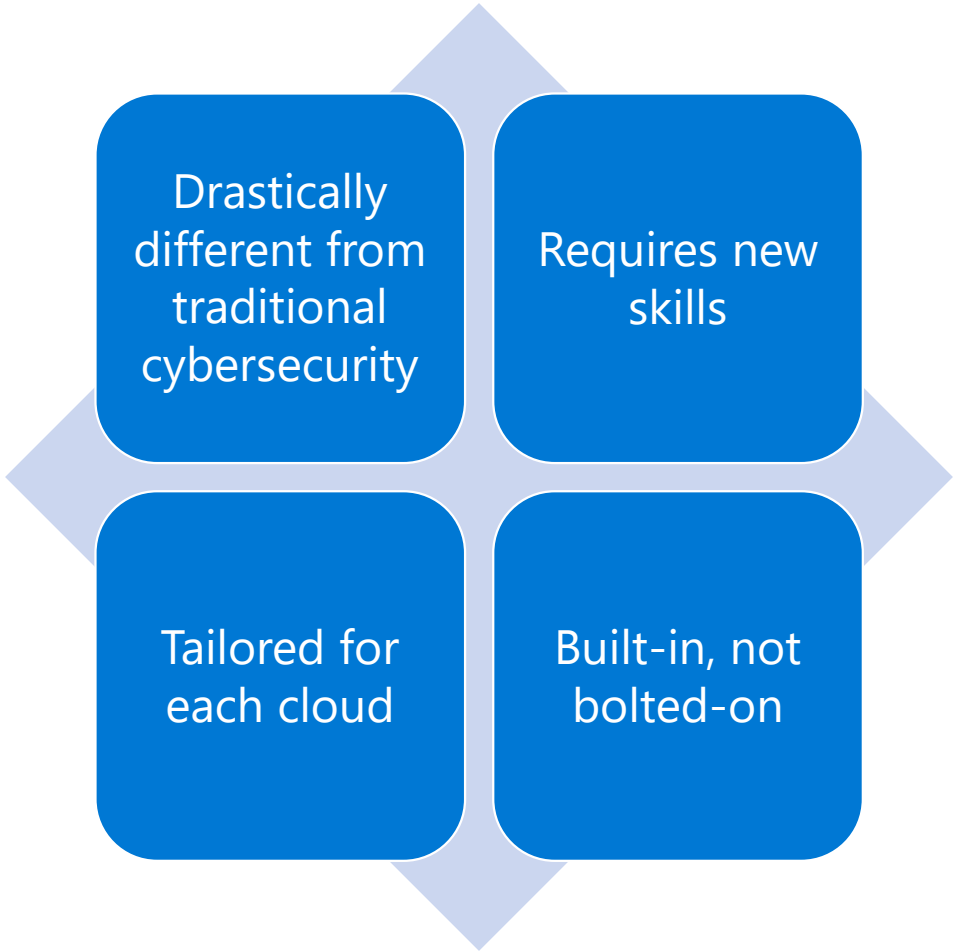
Agenda

- **Introduction to cloud security**
- Common cloud security programs
- Cloud security architecture components
- Lessons learned

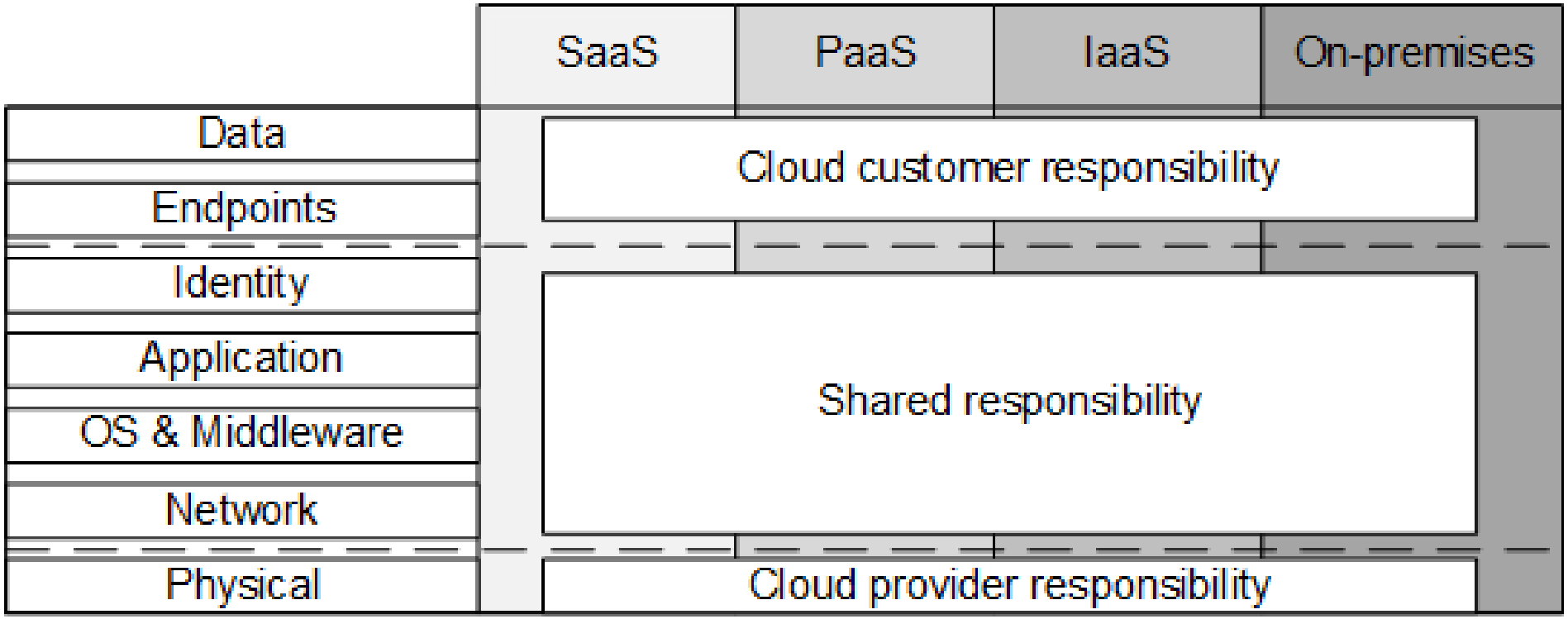
The pandemic validated cloud’s value proposition

We need **cloud native security**

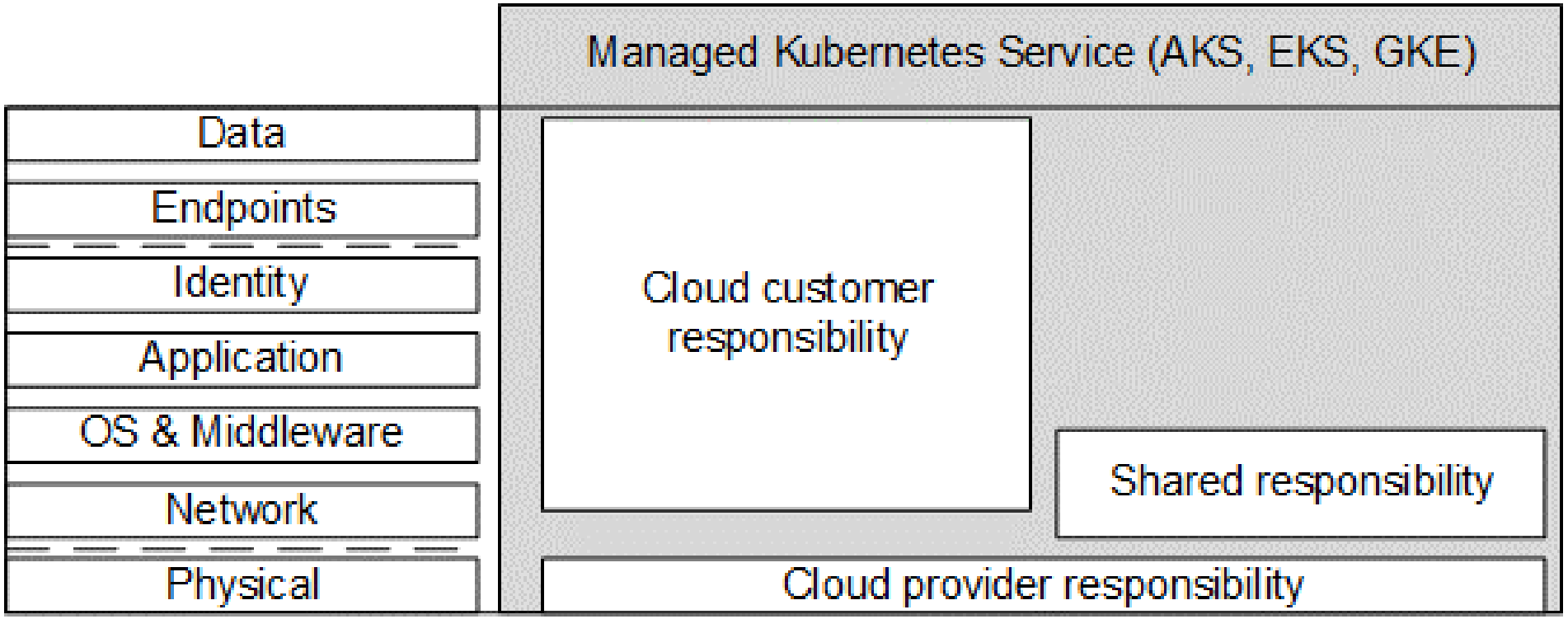
Cloud native security



Shared cloud security responsibility matrix



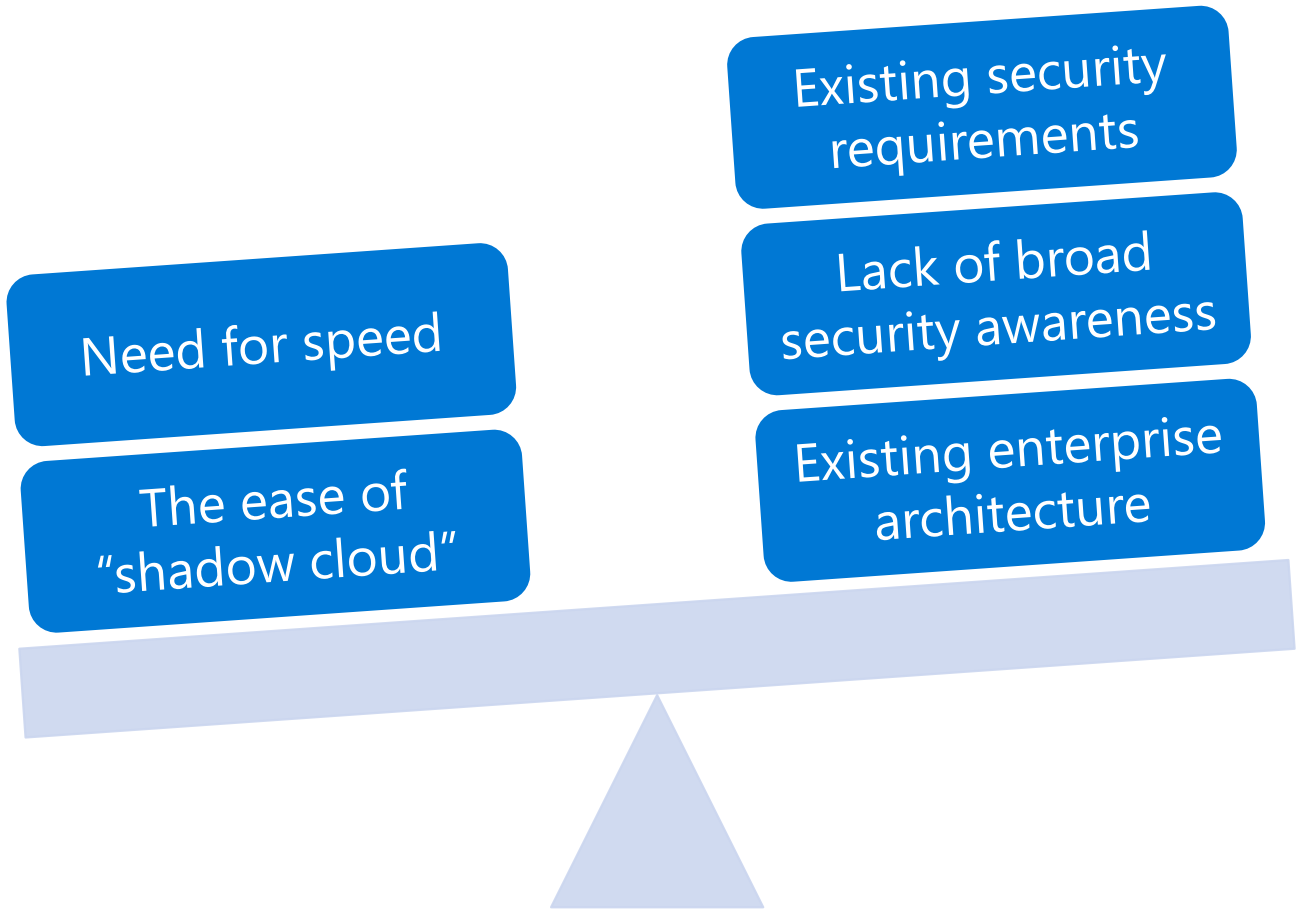
Customize the shared cloud security responsibility matrix for your services



Agenda

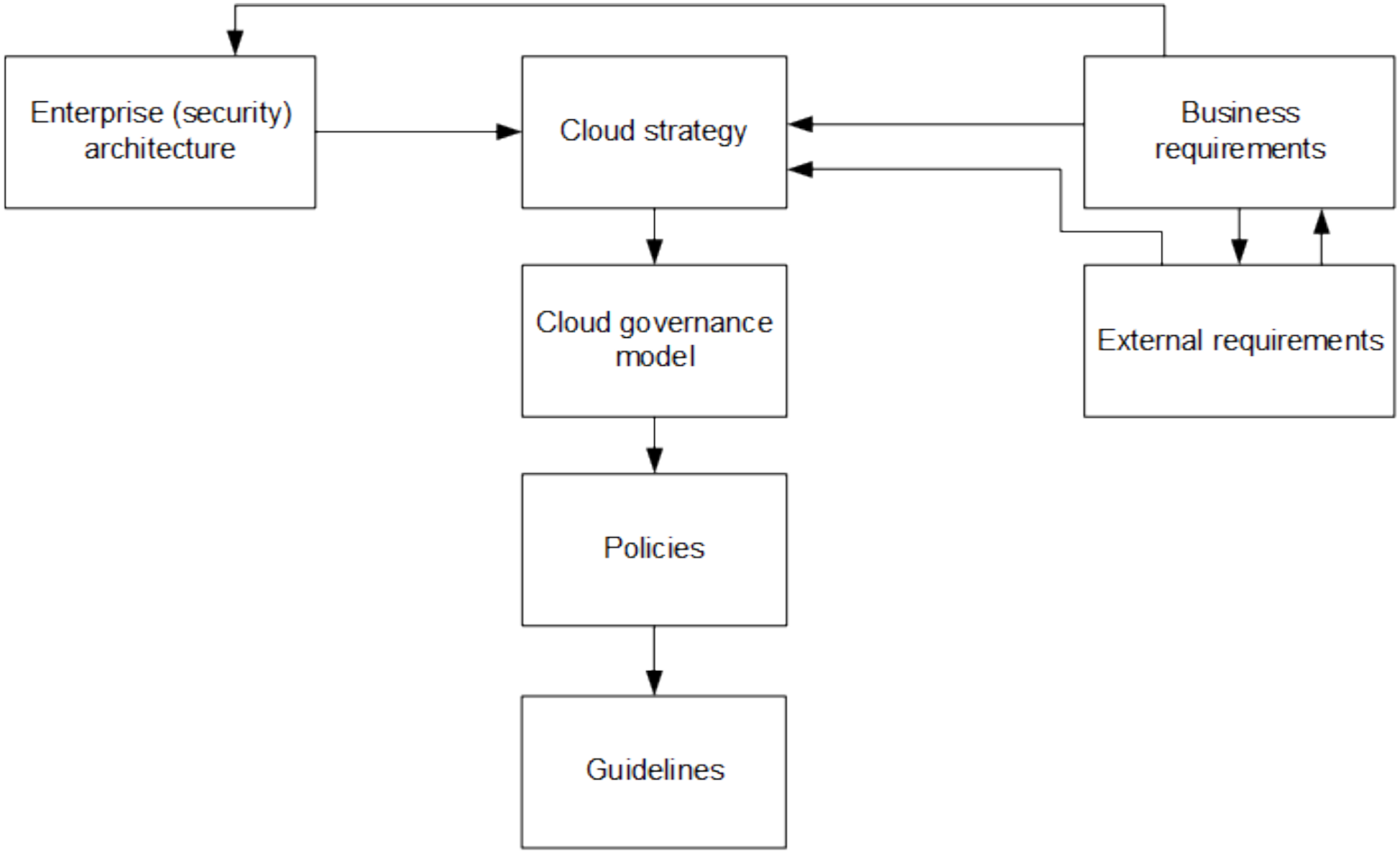
- Introduction to cloud security
- **Common cloud security programs**
- Cloud security architecture components
- Enterprise hiccups

The balance of enterprise cloud security



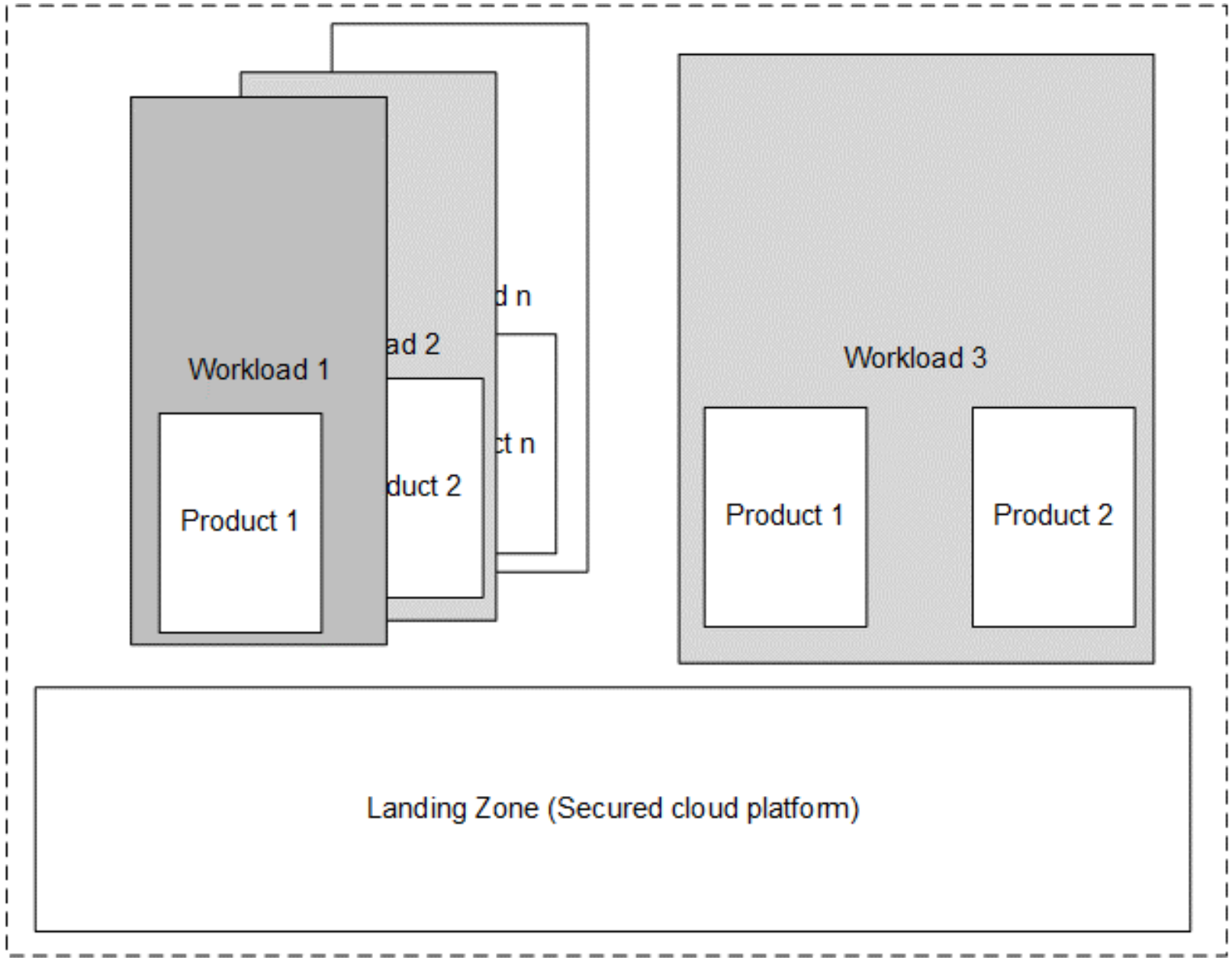
How can we agree on cloud security policies that keep us both **competitive & secure**?

A **cloud security program** defines the architecture, policies, and controls to secure your cloud environment.


Enterprise (security) architecture
Cloud strategy
Business requirements
Cloud governance model
External requirements
Policies
Guidelines

Agenda

- Introduction to cloud security
- Common cloud security programs
- **Cloud security architecture components**
- Enterprise hiccups


d n
ad 2
Workload 1
ct n
duct 2
Product 1
Workload 3
Product 1
Product 2
Landing Zone (Secured cloud platform)

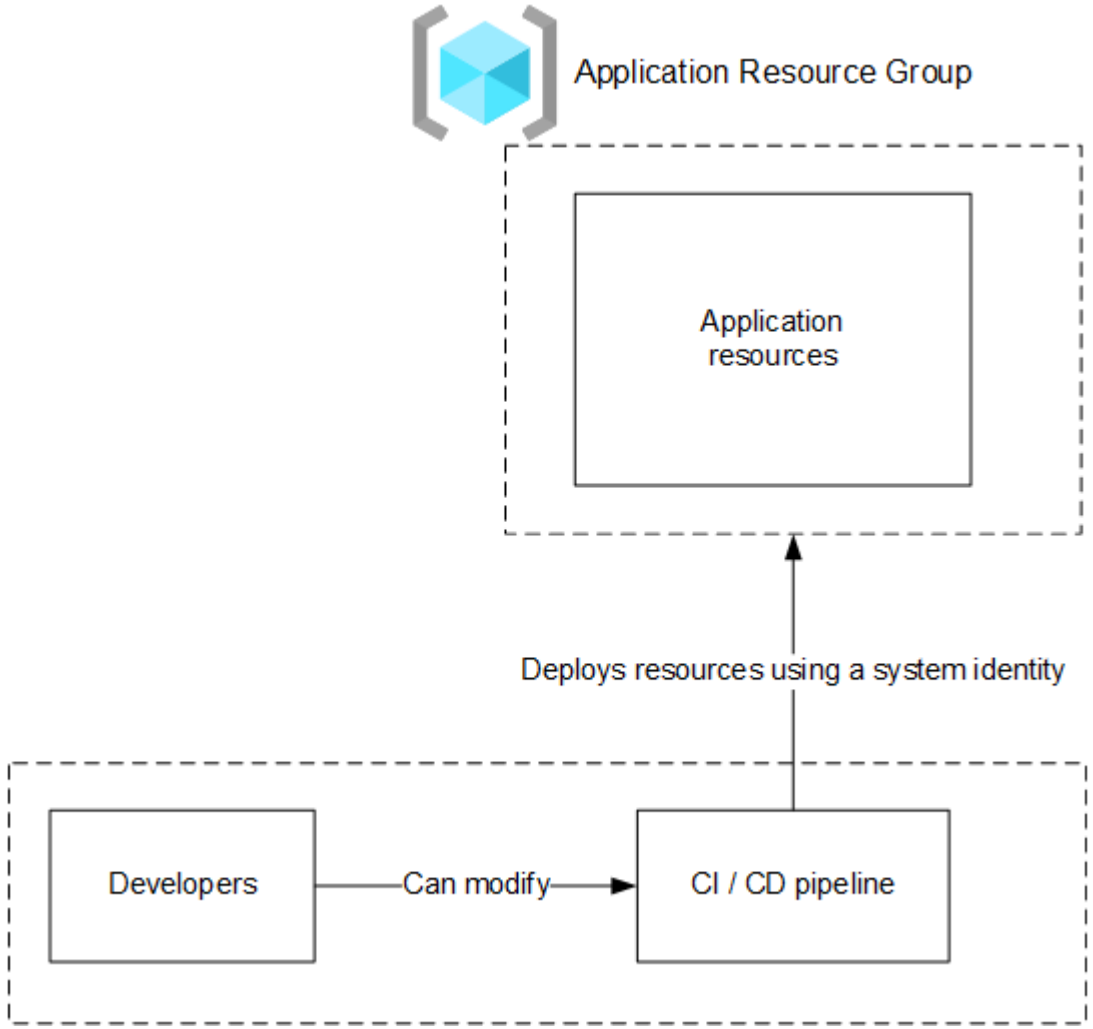
Identity and access management

Integration with existing IAM processes

Access control to the management and data plane

Access control through the SecDevOps life cycle

SecDevOps access control

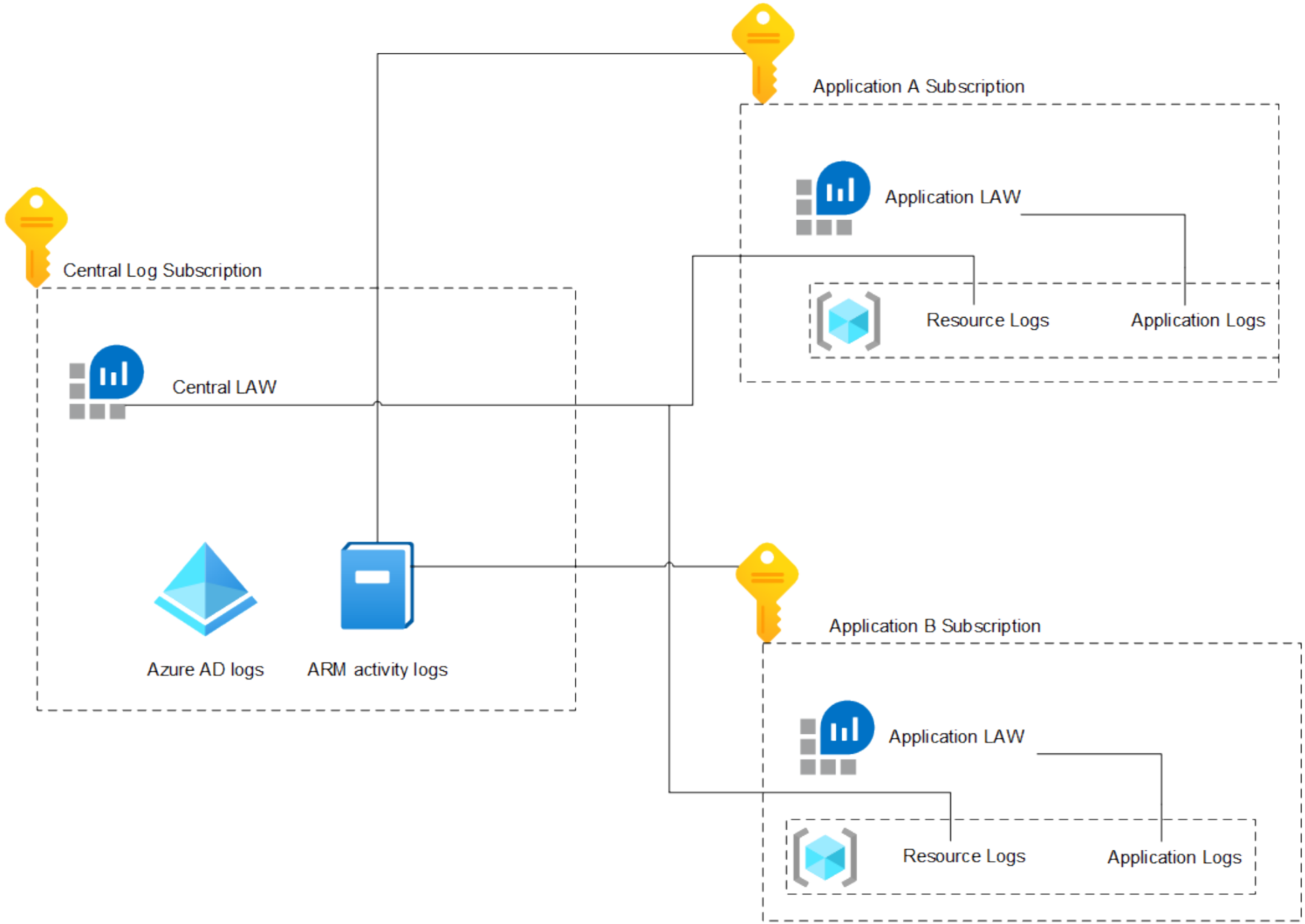


Detection and monitoring

Enforcing audit logging across the landing zone and any products or workloads deployed onto it

Integration with your SIEM and SOC

Centralized logging architecture


Application A Subscription
Application LAW
Central Log Subscription
Resource Logs
Application Logs
Central LAW
Azure AD logs
ARM activity logs
Application B Subscription
Application LAW
Resource Logs
Application Logs

Network security

Cross-subscription, cross-region, and cross-cloud traffic

Platform-as-a-Service and Infrastructure-as-a-Service traffic

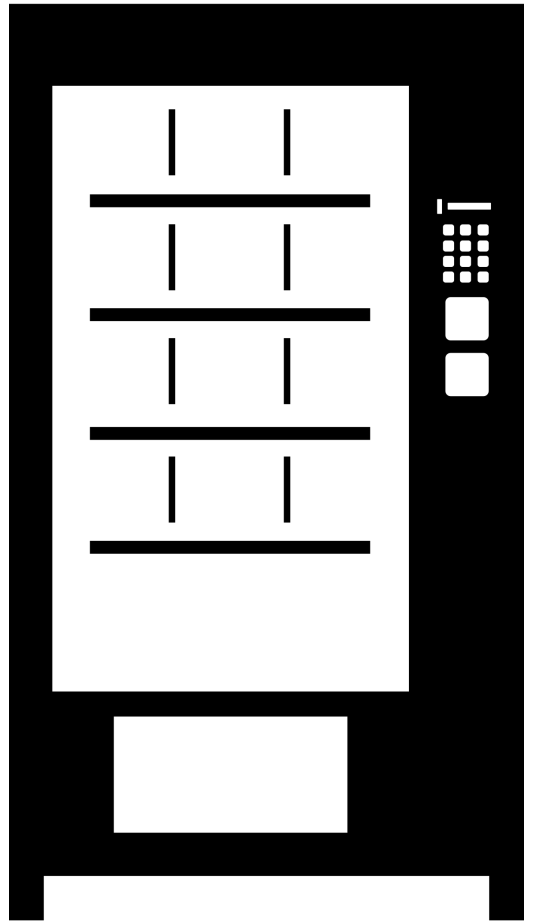
Application-level traffic

Agenda

- Introduction to cloud security
- Common cloud security programs
- Cloud security architecture components
- **Enterprise hiccups**

Identity and access management

- Integrating cloud with enterprise IAM
- Privileged, unmanaged and federated accounts
- Cloud account vending machines



Vulnerability management

- Multi-cloud inventory / asset management
- Containers
- CSP vulnerabilities
- New signals

Supply chain lifecycle

- Shared responsibility

Supply chain lifecycle

- Shared responsibility
- Dev is not out of scope for attackers

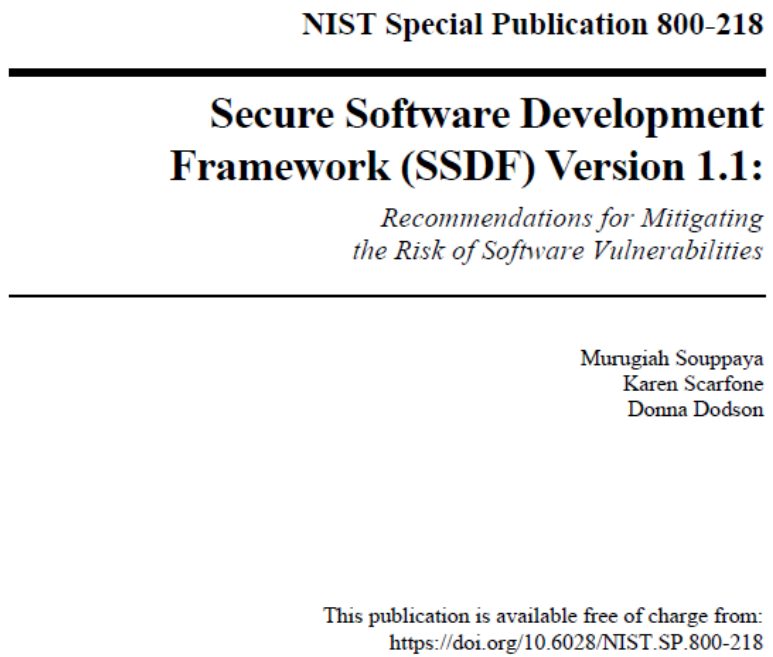
wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure

Supply chain lifecycle

- Shared responsibility
- Dev is not out of scope for attackers
- Impact of Software bill of materials EO?

Supply chain lifecycle

- Shared responsibility
- Dev is not out of scope for attackers
- Impact of Software bill of materials EO?



NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

Murugiah Souppaya
Karen Scarfone
Donna Dodson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-218

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Lessons learned from enterprise cloud security programs

Karl Ots