Microsoft

Azure Sentinel Level 400

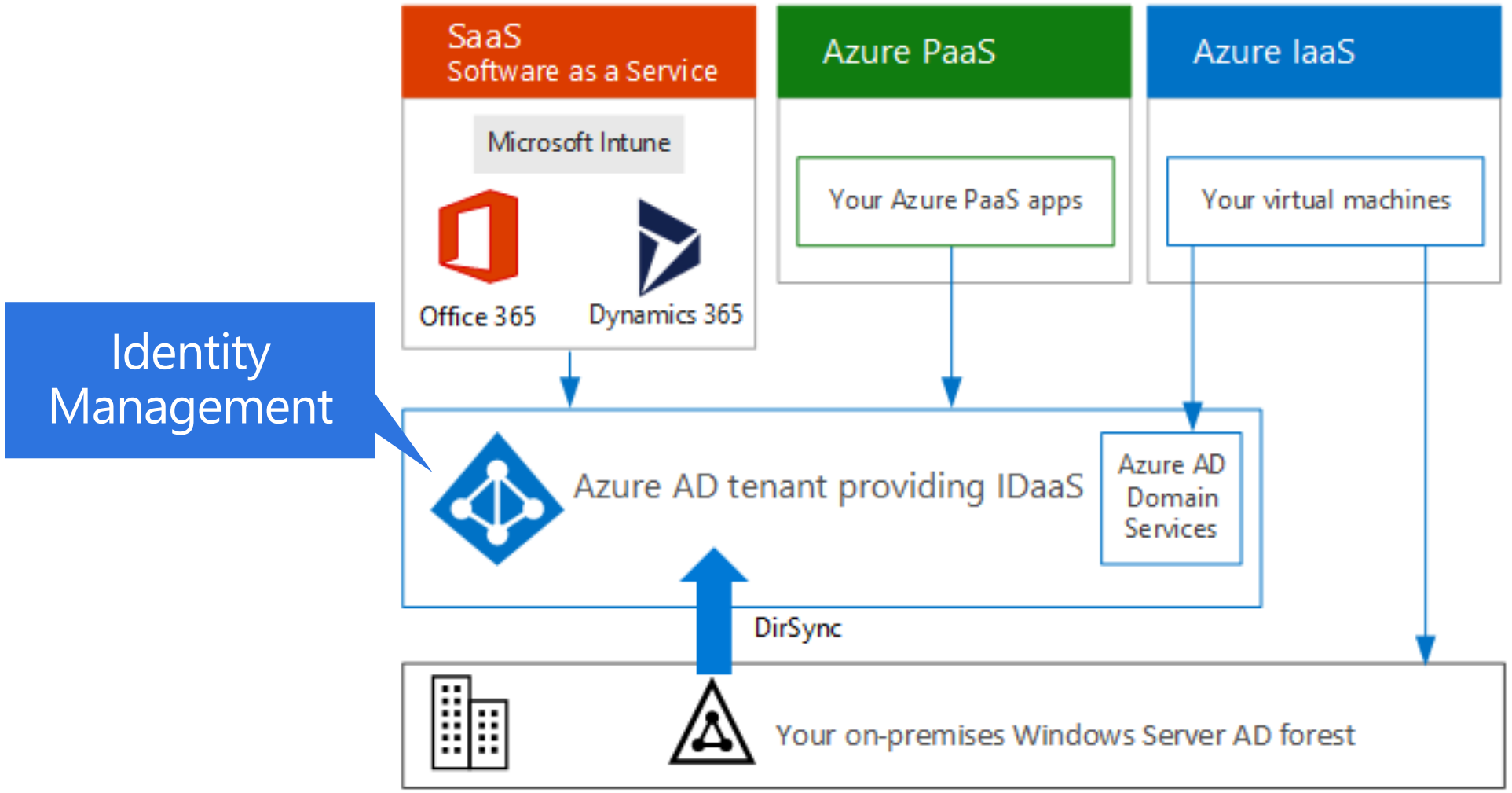
Cloud architecture

Agenda

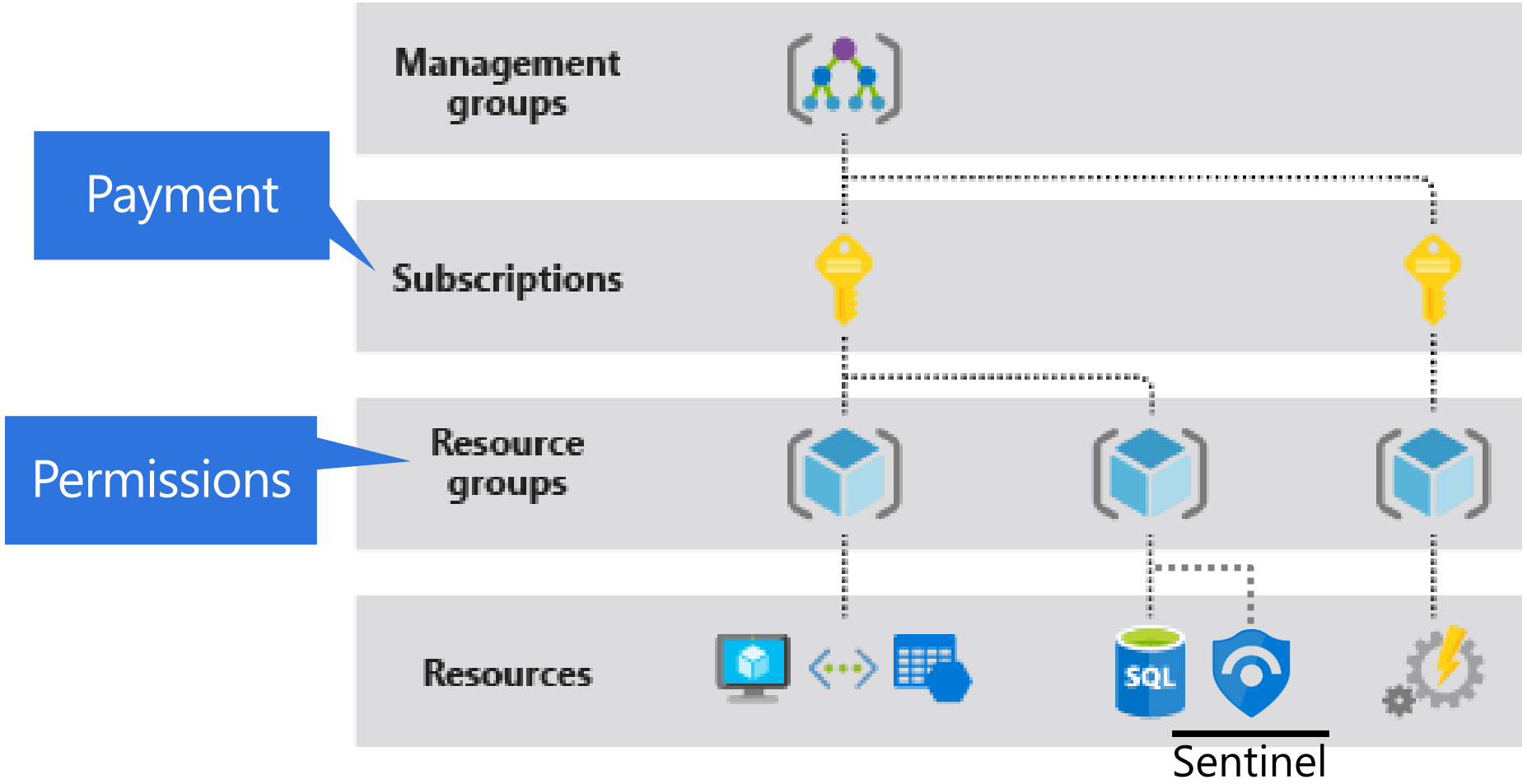
1. Azure: tenants, subscriptions, workspace etc.
2. The Sentinel workspace
3. Multi-workspace best practices

Azure Basics

Microsoft AAD Tenant



Azure subscriptions and resources



Regions and geos

- Any Azure region, supporting LA with some exceptions, can be used
- Most, but not all, data at rest stays in region
- Some data may go to EU West (EU), US East (Elsewhere)

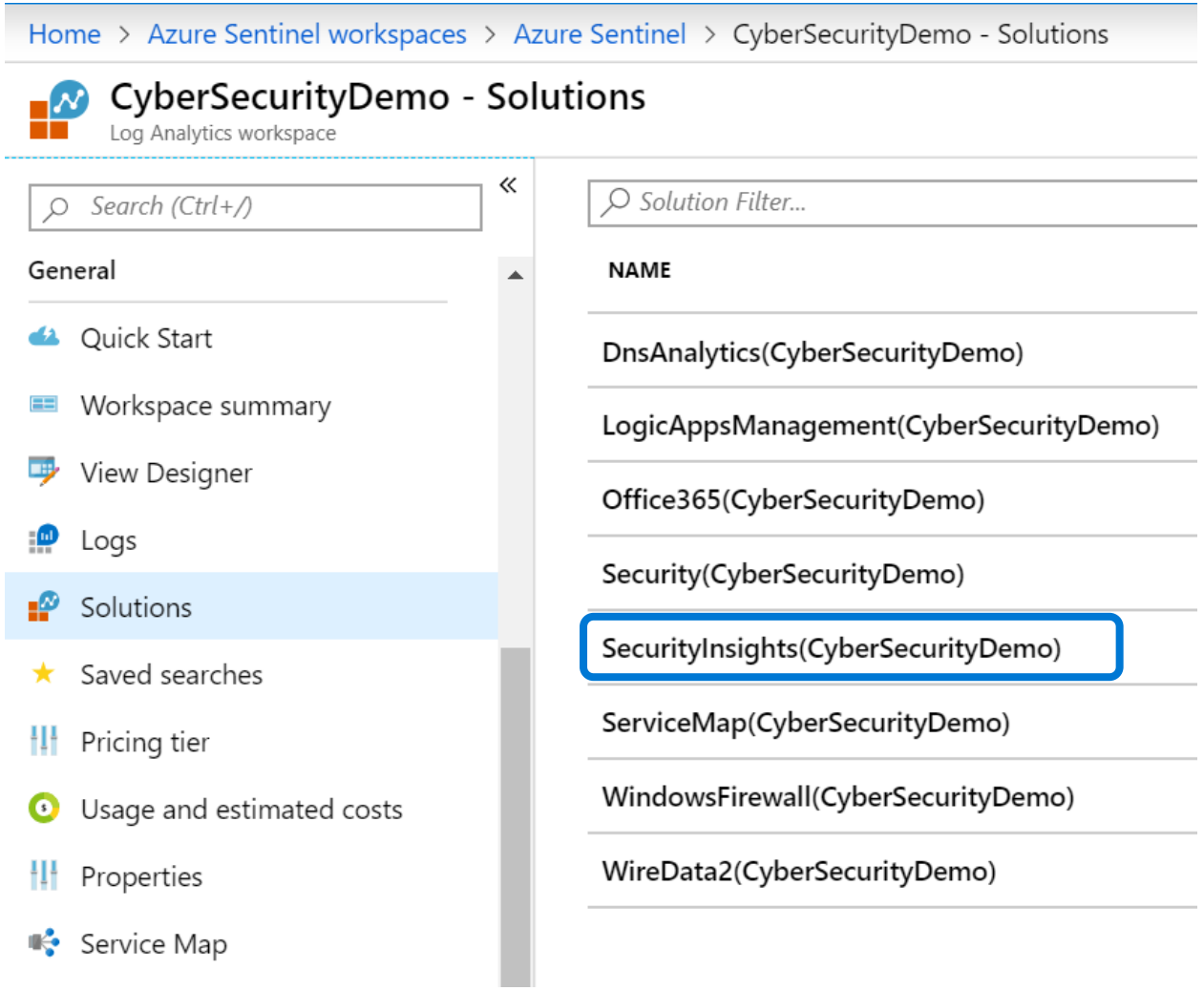
The Workspace

The Sentinel workspace

- The Azure resource container for Sentinel
  - The event database
  - Rules
  - Incidents
- But not
  - Playbooks

Fully compatible with Log Analytics

- Essentially a Log Analytics solution.
- Can be accessed as a Log Analytics workspace
- Whatever works for Log Analytics, works for Sentinel



Multi-Workspace best practices

Why will you need multiple workspaces?

- Data owners need access to their data ← Use resource RBAC
- Global SOC and Local SOCs (or MSSP and customers)
- Data ownership or sovereignty compliance
- Multiple Azure tenants

Use multiple workspaces

Additional multi-workspace considerations

Fine grained retention setting

Use table level retention

Multi-workspace Legacy architecture

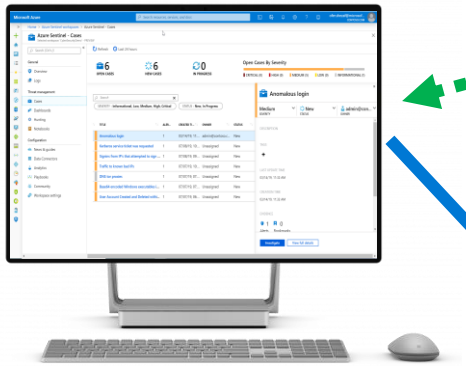
Migrate to less workspaces

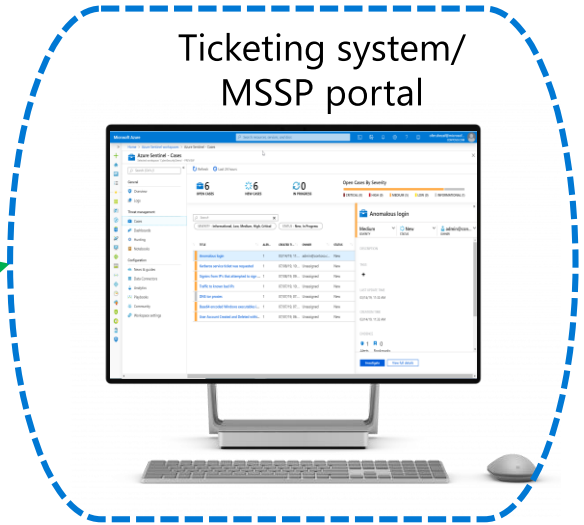
Separate billing

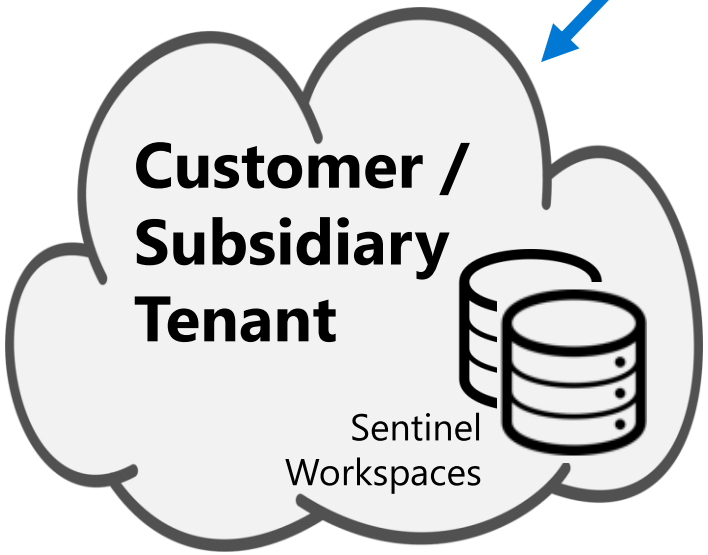
Use billing reporting

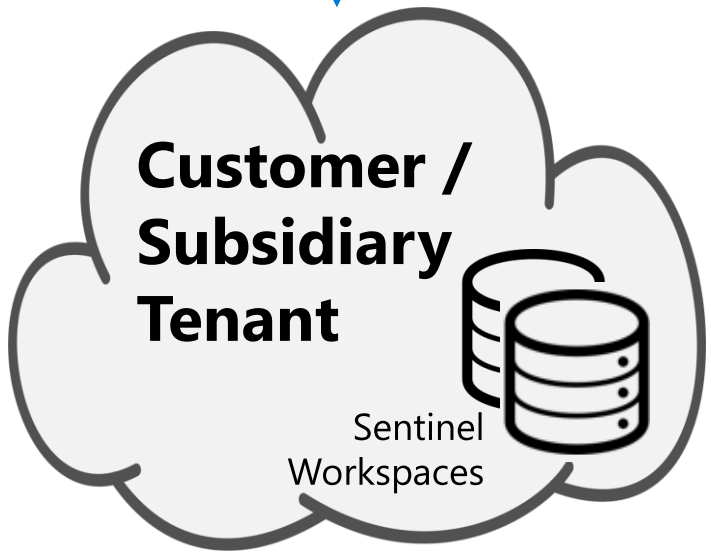
Hybrid multi-workspace/tenant model

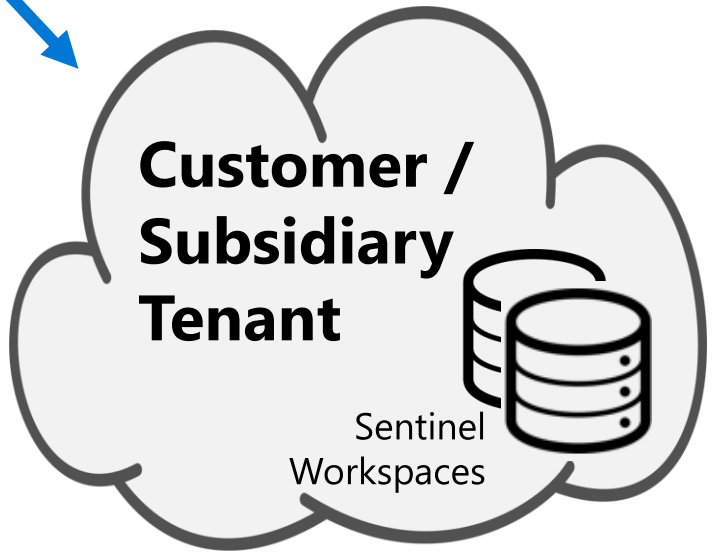
- Data stays at the customer's/subsidiary's tenant
- Central monitoring and management











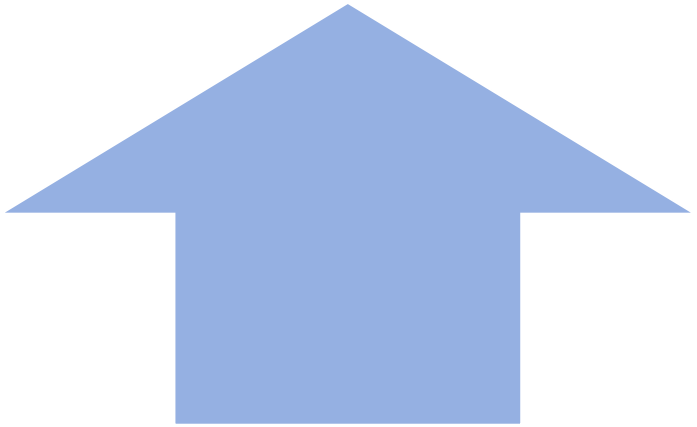
The hybrid model differences

Advantages:

- Flexible Global/MSSP and subsidiary/customer role management
- No data ownership & data privacy challenges
- Minimize network latency & charges
- Easy onboarding and offboarding

But how do you do?

- Central monitoring
- Central deployment and cofiguration
- IP protection



Workspaces rule of thumb

Use one workspace for each tenant, Azure region and subsidiary

Implementing

1. Consolidate workspaces
2. Use resource RBAC
3. Use cross-workspace queries and workbooks
4. Implement automation for deployment and configuration
5. Use Azure Lighthouse to extend to workspaces across regions
6. (optional) Integrate with a ticketing system

#1: Consolidate workspaces

- Modify sources to send events to a central workspace:
  - Agents
  - Other Azure sources
  - Current solutions in original workspace may need to be migrated
  - Supported across subscriptions
- Modify ASC default workspace to a central workspace
  - Does not affect ASC functionality
  - Supported across subscriptions

#2A: What is resource RBAC?

- The SOC team has full data access to the workspace.
  - Different SOC roles can still have limited access to features within the workspace
- Other teams get access to data using the “logs” option

#2B: Implementing resource RBAC

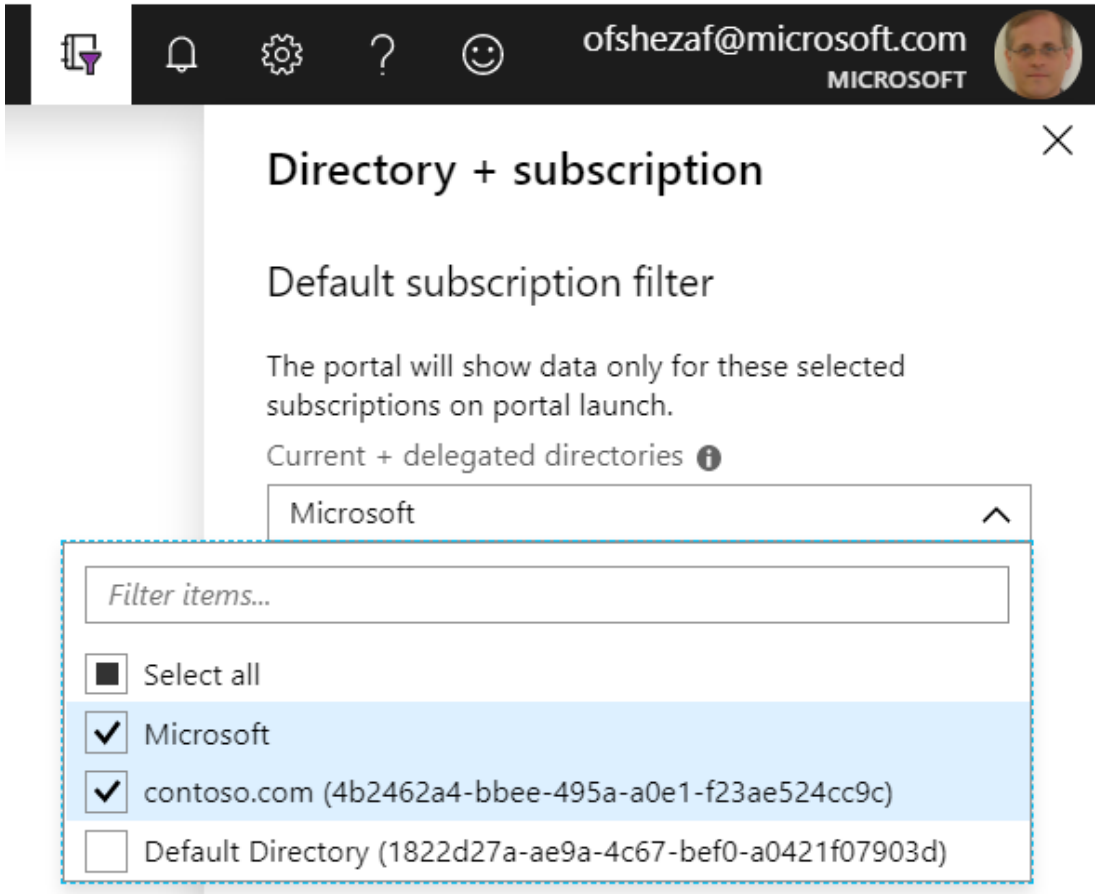
#2: Use resource RBAC

- Table base RBAC
  - Limit access to sensitive data such as Office logs
  - Viewable from the workspace.
- Resource centric RBAC
  - Enable resource owners' access to their data.
  - Now supports on-prem servers using Azure Arc.

#2: Implement Azure Lighthouse

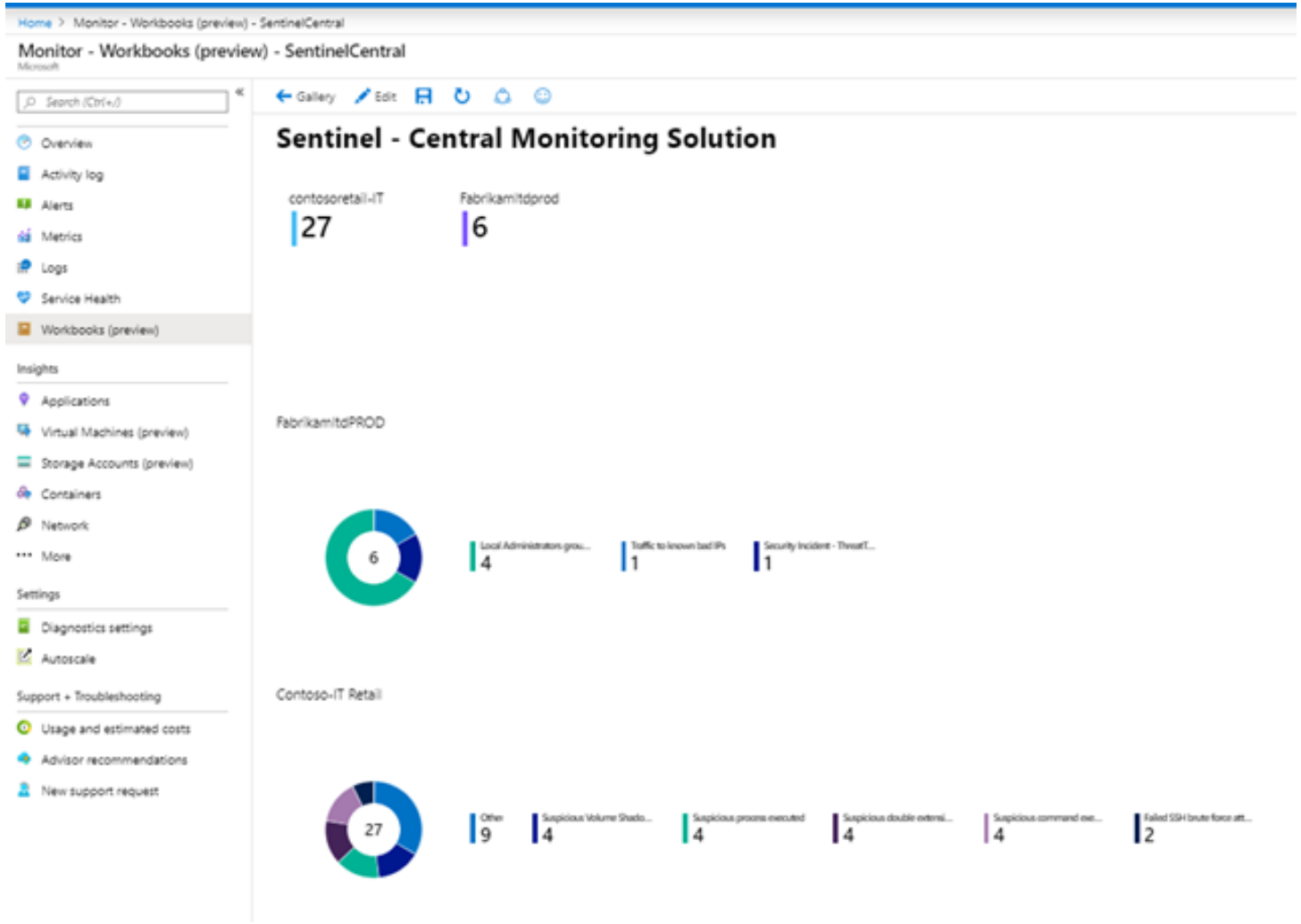
Cross Tenants / Workspaces:

- Search
- Workbooks
- Hunting



#3: Create cross tenant workbooks

- Alerts
- Connector status



#4: Replicate content and config

Use API and ARM templates to replicate:

- Onboard (API)
- Alert rules, Hunting queries (API) – Thanks Wortell for the AzSentinel PS module
- Playbooks (ARM)
- Workbooks (ARM)
- Saved searches (API)
- Permissions (API)
- Connectors (API, Partial)