
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

BWP301

# How Buy with Prime built a resilient multi-tenant SaaS architecture


Jiwon Yeom (she/her)

Solutions Architect, Buy with Prime
Amazon

Joseph Decena (he/him)

Solutions Architect, Buy with Prime
Amazon

Ryan Lohan (he/him)

Principal Engineer, Buy with Prime
Amazon



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

1. What is Buy with Prime?
2. Identity and Isolation
3. Noisy neighbors
4. Conclusion

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

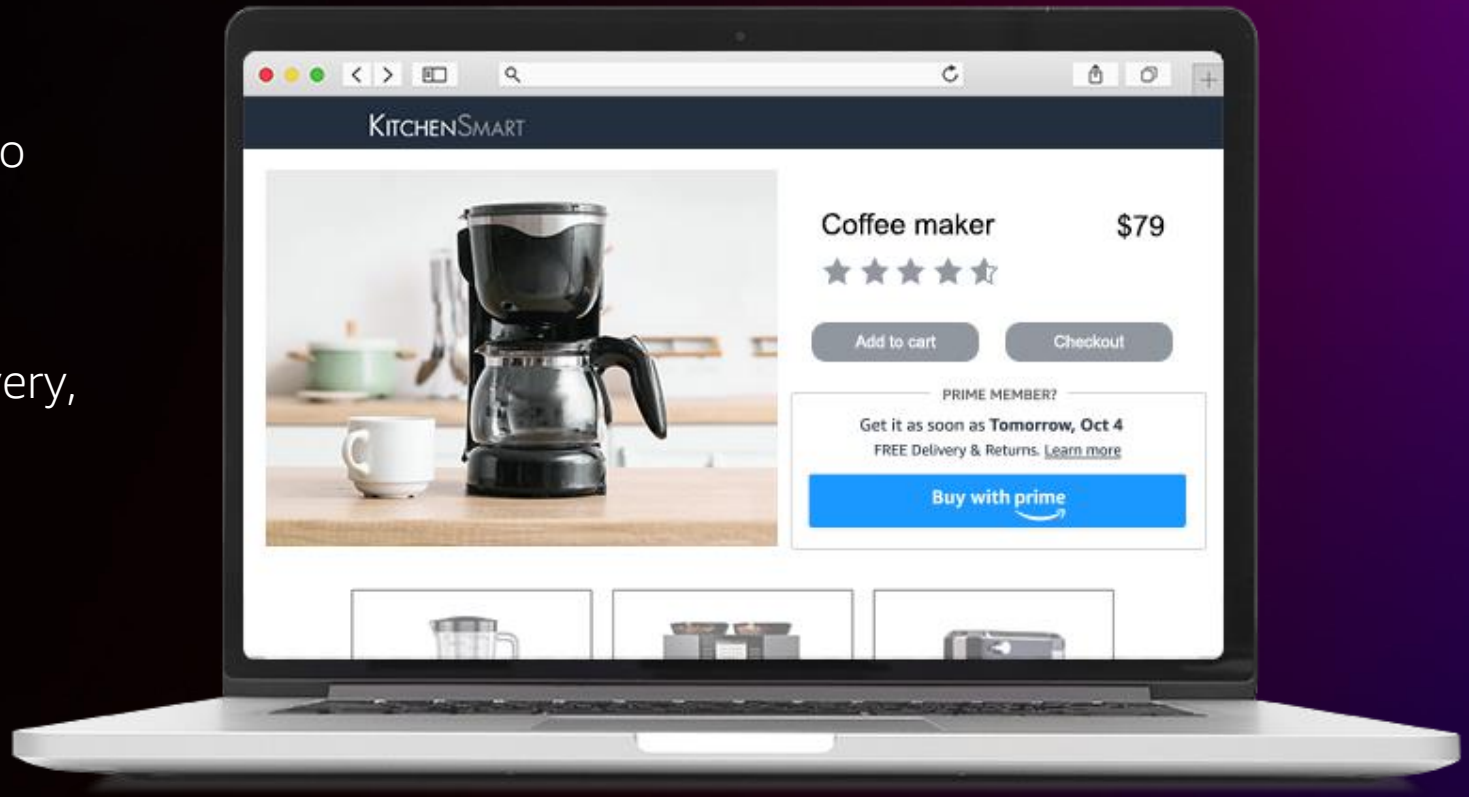



# What is Buy with Prime?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Buy with Prime

Buy with Prime empowers merchants to grow their direct-to-consumer (DTC) business by letting millions of Prime members shop directly from their site, while enjoying the same fast, free delivery, easy returns, and seamless checkout experience Prime members trust on Amazon.com.




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How to use Buy with Prime

## Buy with Prime Button Install



Use merchant console to import your catalog and enable products for Buy with Prime. Install the Buy with Prime button code one time on your site.

## Buy with Prime API



Our API enables deeper and flexible integration for the merchants and Buy with Prime Partners.

## Buy with Prime Developer Tools



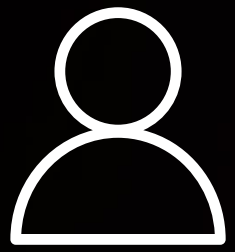
Use Partner Portal and upcoming developer tools to build integrations against Buy with Prime for new business opportunities.

Coming soon!

aws

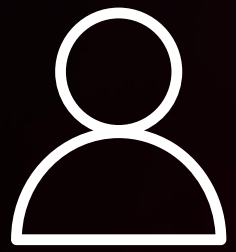
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Key stakeholders



Shopper

Shop, checkout, and get post-purchase support on a merchant's site



Merchant

Build and manage Buy with Prime integration within an existing or new DTC site



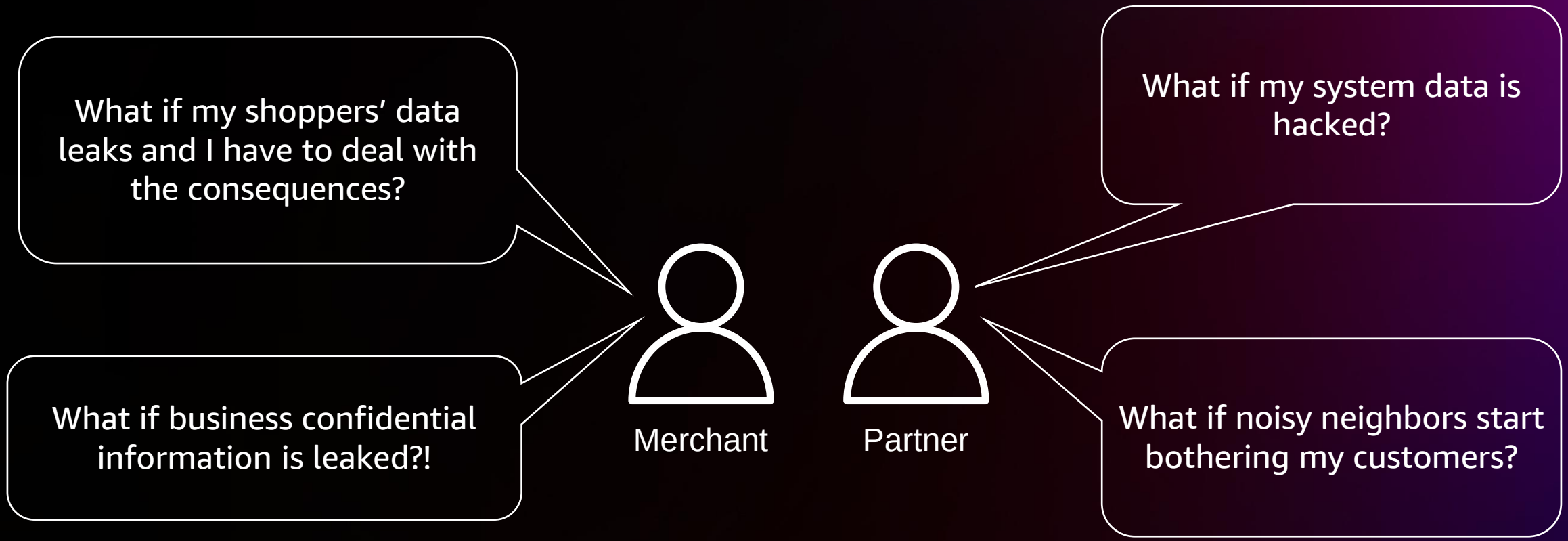
Partner

Publish tools, assets, apps, and services for merchants

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Key concerns of merchants and partners




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

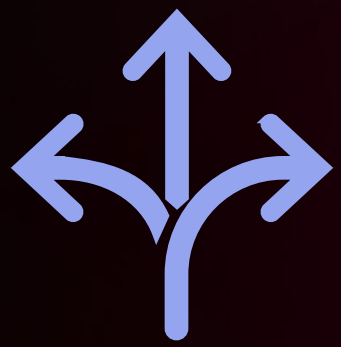
# Challenges as a service provider



Security



Scalability



Flexibility



Cost efficiency

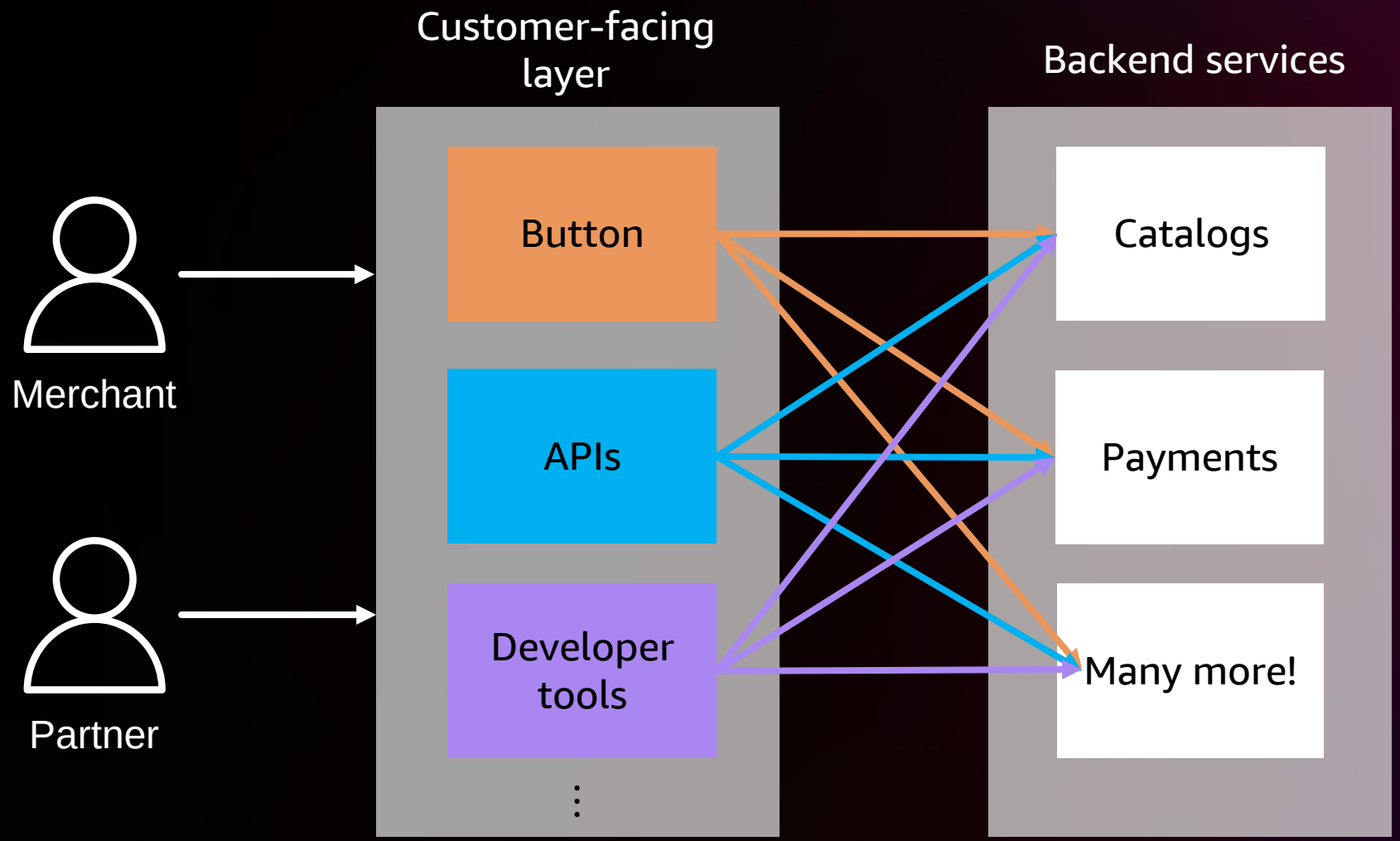
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Identity and isolation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

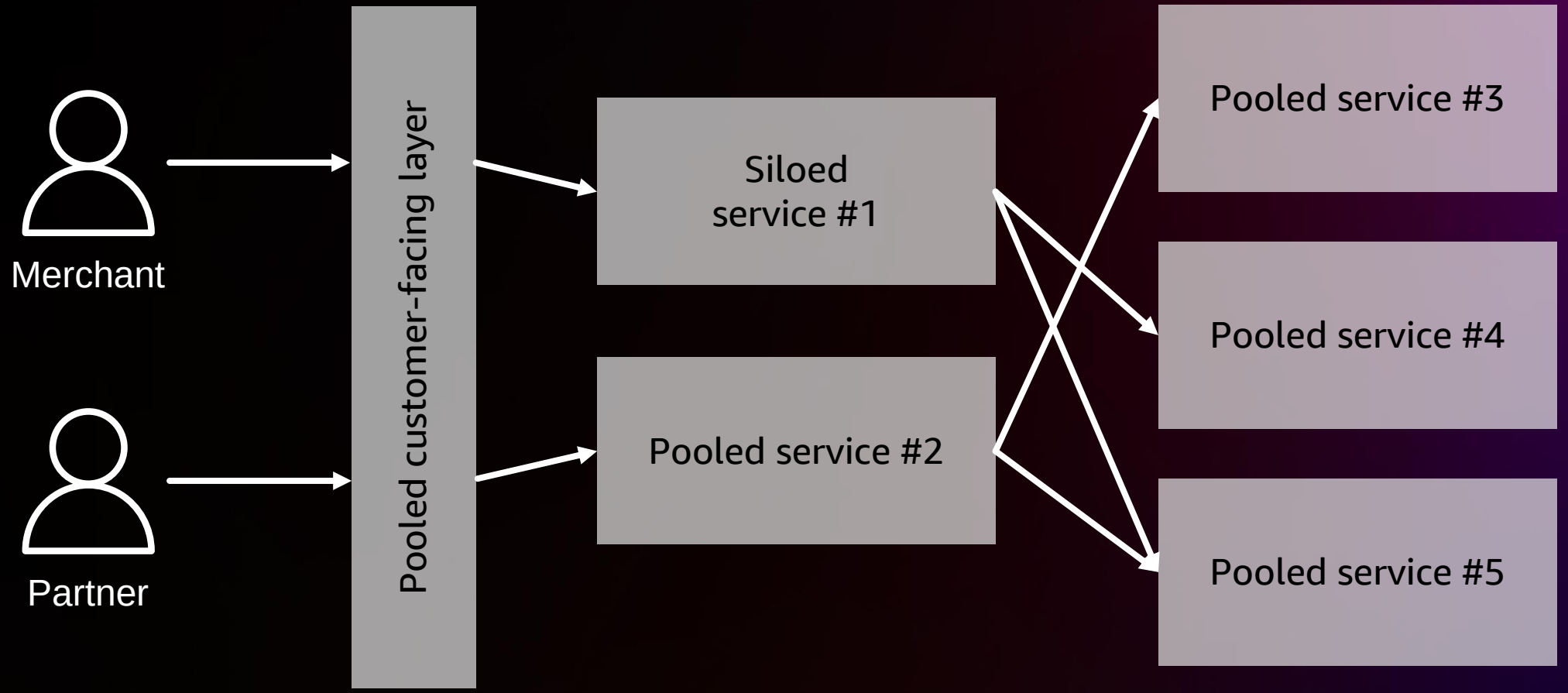
# Buy with Prime architecture from 50,000 ft




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Buy with Prime architecture from 30,000 ft

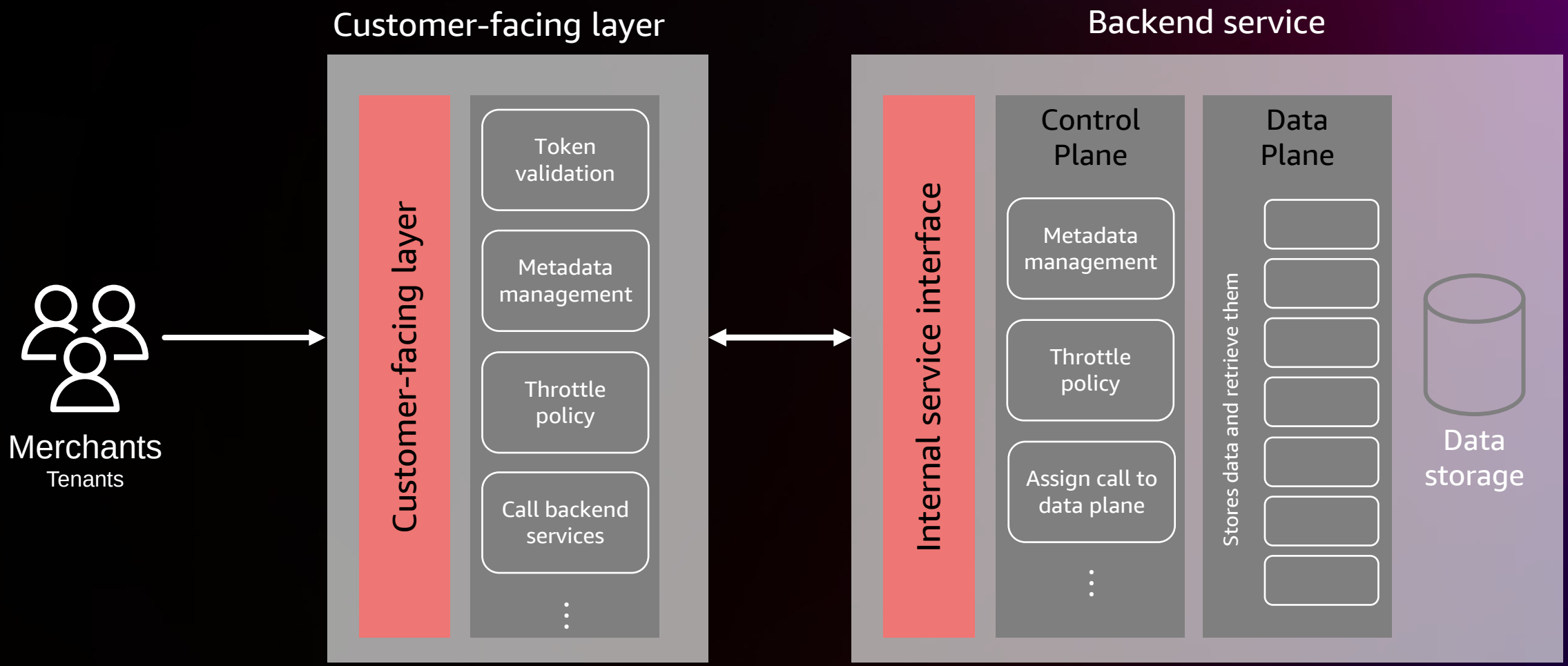
MIXTURE OF TENANT MODELS




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Buy with Prime architecture from 20,000 ft

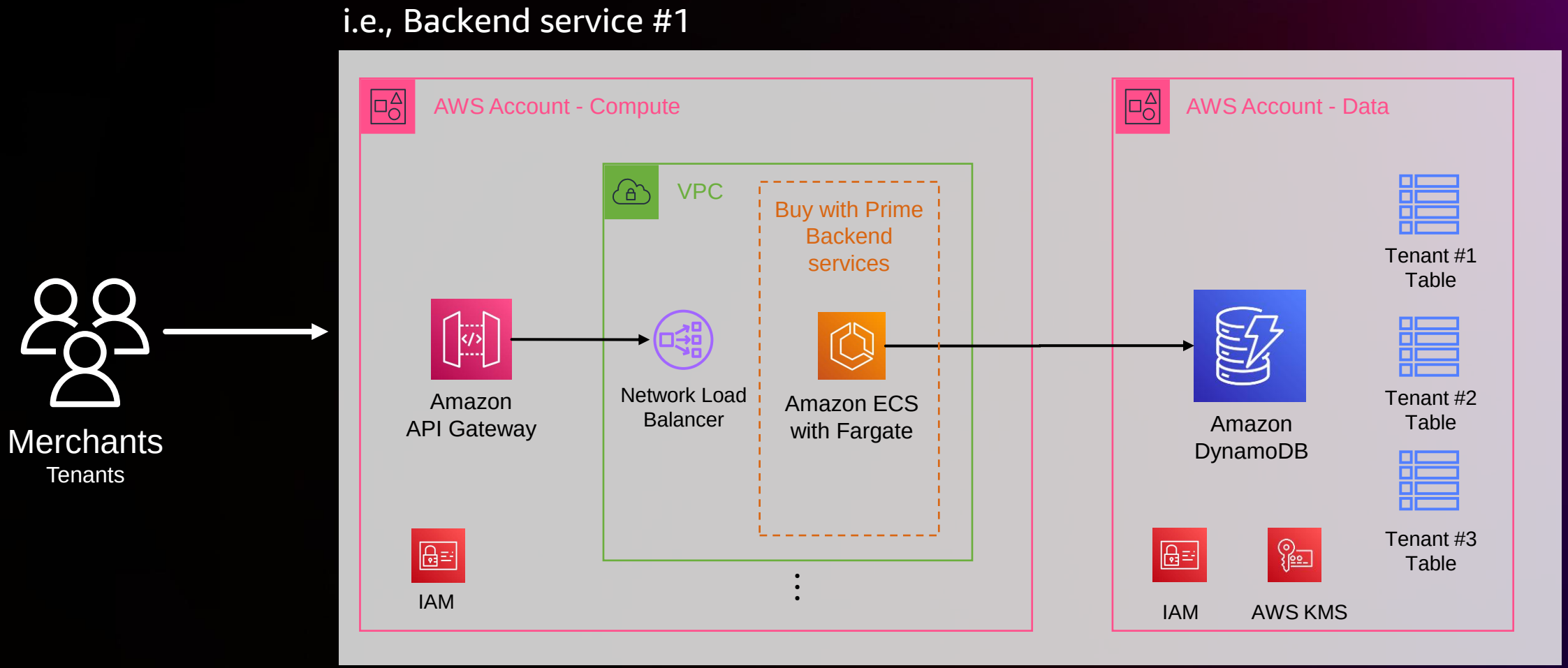
MICROSERVICES – HIGH-LEVEL DESIGN




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Buy with Prime architecture from 10,000 ft

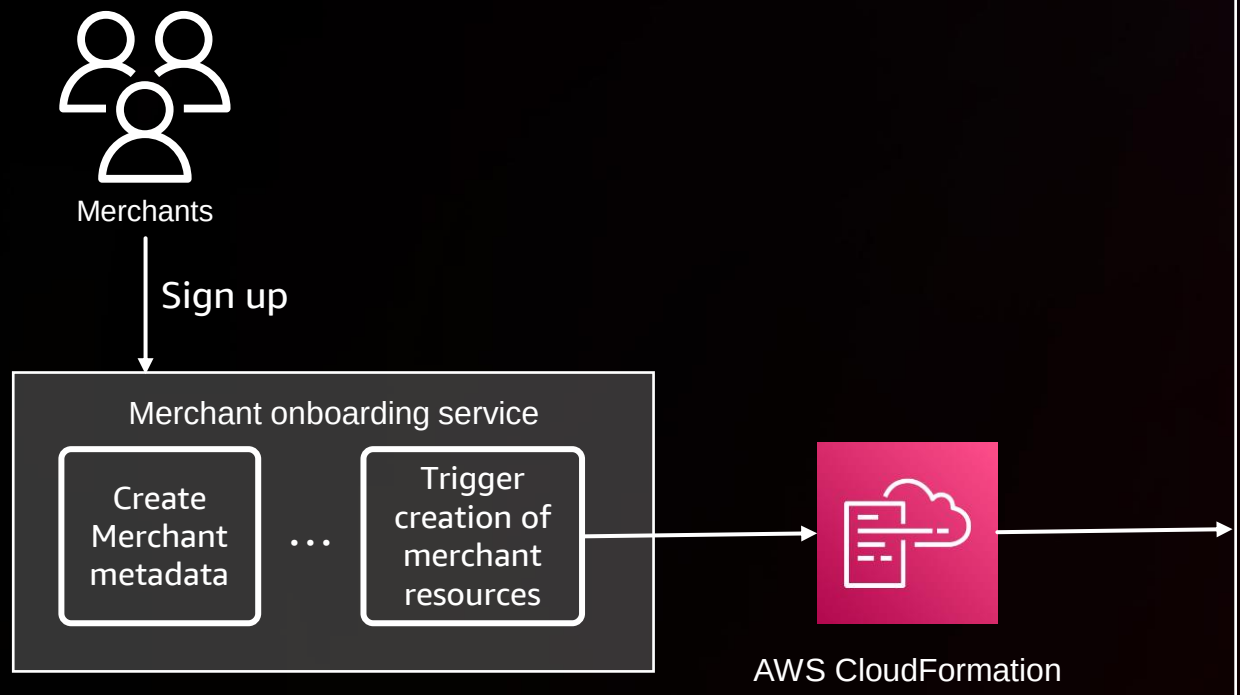
MULTI-TENANCY IN ACTION AT LOW LEVEL




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Onboarding to Buy with Prime

HOW YOUR BUILT-IN SECURITY STARTS




CloudFormation Template

```
{
 "Parameters": {
  "tenantId": {
   "Type": "String",
   "Description": "Merchant owner ID"
  }
 },

 "Resources": {
  "Resource1": {
   "Type": "Amazon::BwP::CatalogInstance",
   "Properties": {
    "TenantId": {"Ref": "tenantId"}
   }
  },

  "Resource2": {
   "Type": "Amazon::BwP::OrderInstance",
   "Properties": {
    "TenantId": {"Ref": "tenantId"}
   }
  },
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

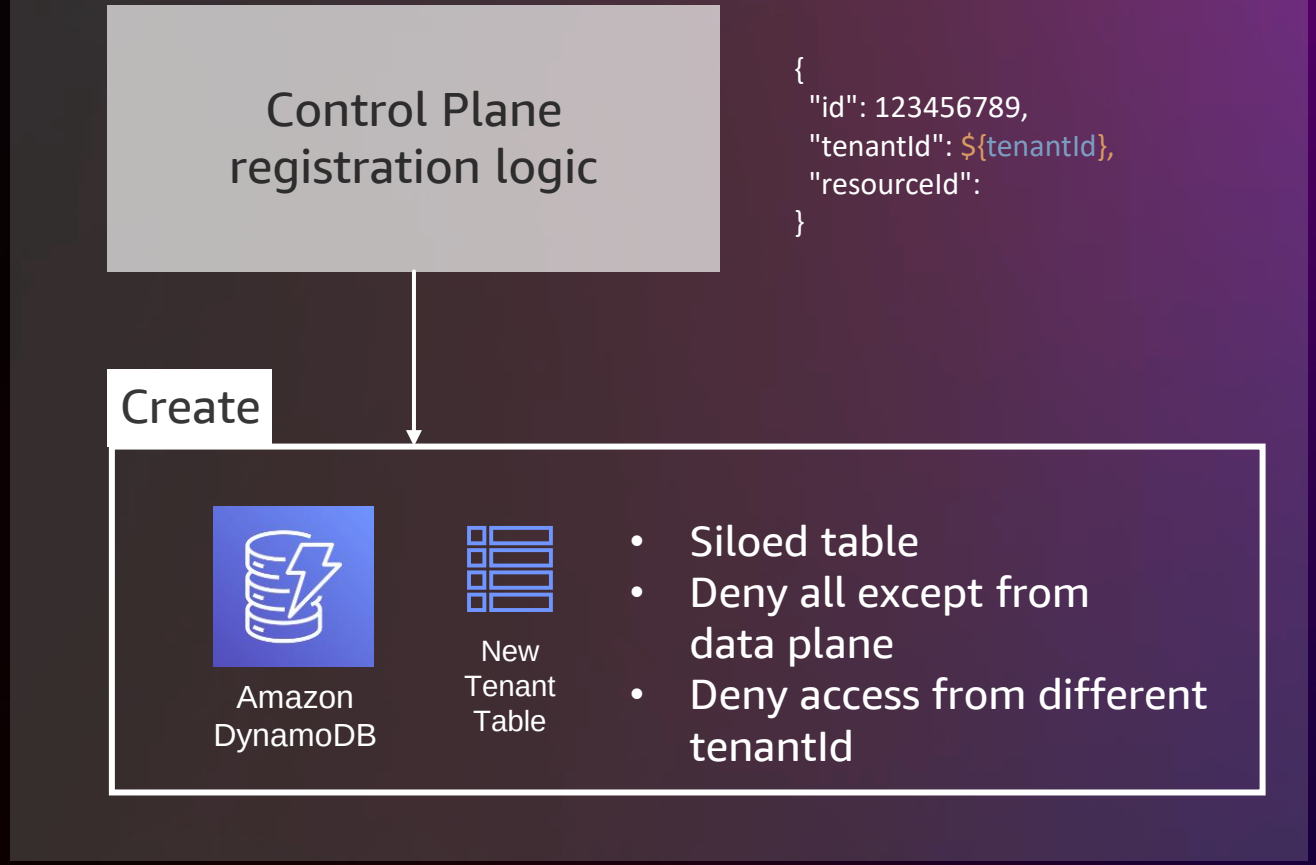
# Onboarding to Buy with Prime

HOW YOUR BUILT-IN SECURITY STARTS

```
{
 "Parameters": {
  "tenantId": {
   "Type": "String",
   "Description": "Merchant owner ID"
  }
 },

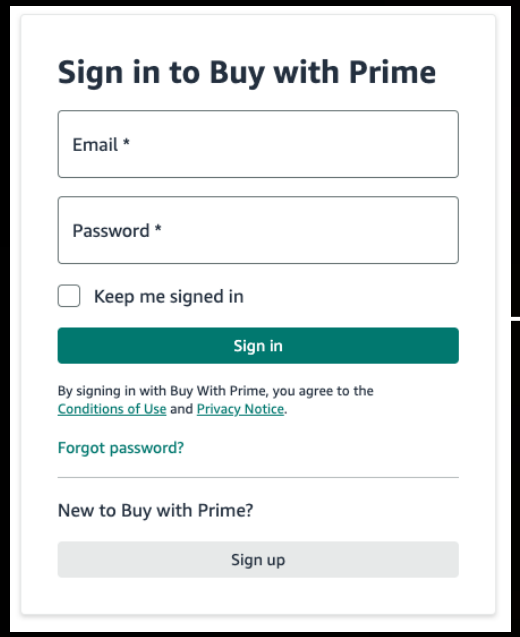
 "Resources": {
  "Resource1": {
   "Type": "Amazon::BwP::CatalogInstance",
   "Properties": {
    "TenantId": {"Ref": "tenantId"}
   }
  },

  "Resource2": {
   "Type": "Amazon::BwP::OrderInstance",
   "Properties": {
    "TenantId": {"Ref": "tenantId"}
   }
  \ },
}
```




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Vending identities for tenants




Buy with Prime Identity service

Credentials

IAM STS

```
GetCredential
( ResourceContext =
{ "aws:bwp:owner":
  ”userID”} )
```

```
AssumeRole
(policy=A-Business-Role-Policy,
  Tags={tenantId: userID})
```

```
{
  "StringEqualsIfExists": {
     "aws:bwp:owner":
   ${aws:PrincipalTag/tenantId}
     }
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Vending identities for tenants



Tenant-aware / Scoped-down temporary credential

Buy with Prime backend service

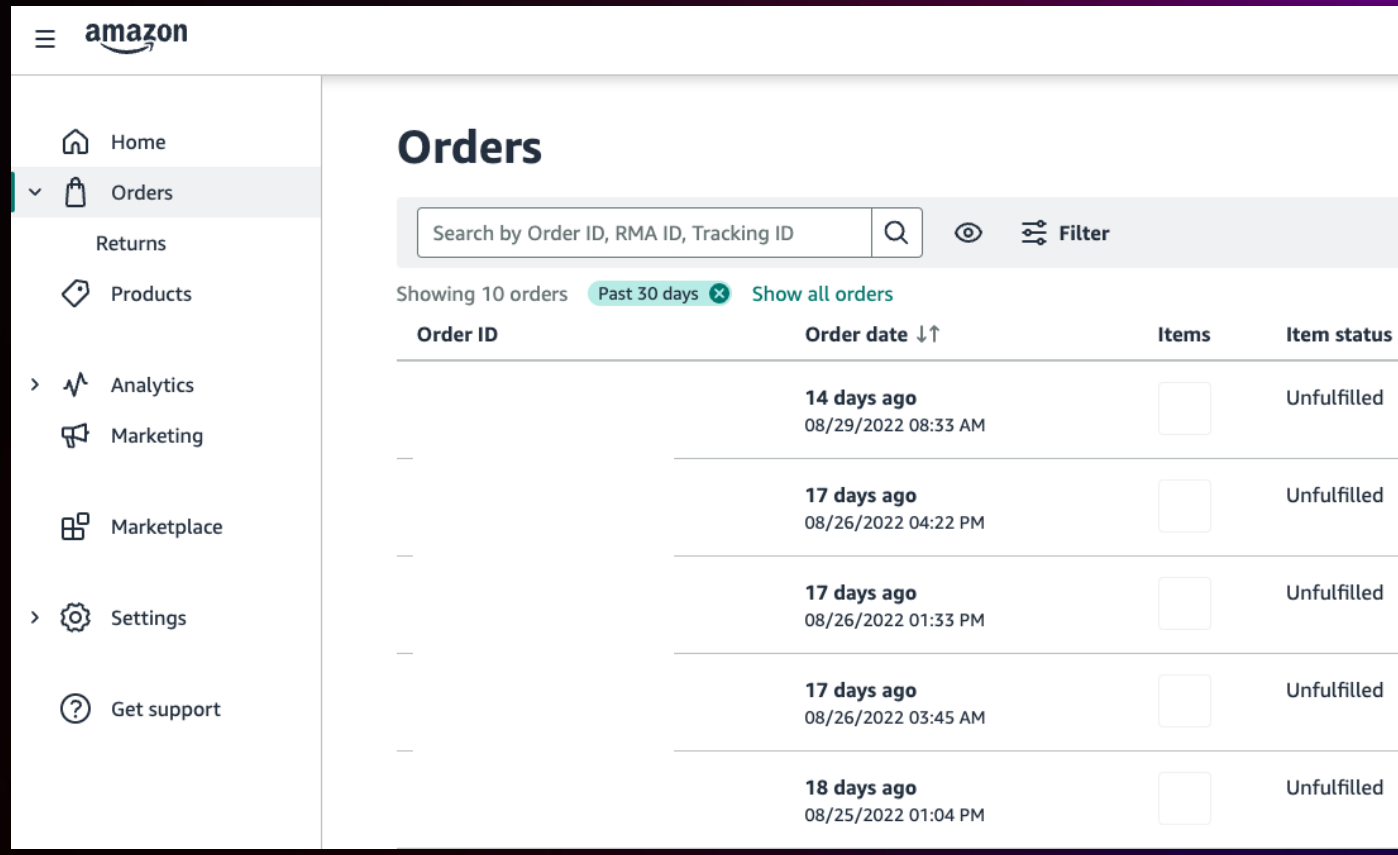
Compare resourceContext & Policies



IAM



Control Plane Database




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Real test cases for identity and isolation

## Key Tenant ID test cases

1. An authorized caller can successfully call
2. A caller from a different AWS account cannot access the resource even if they have a user policy permitting access for the Tenant ID of the resource
3. A caller from a different AWS account cannot access the resource, even if they have “Administrator” user permissions
4. A caller from the same AWS account with a user policy restricting by Tenant ID cannot access a resource with a different Tenant ID

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Noisy neighbors

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Dealing with noisy neighbors



Prevent



Monitor

aws

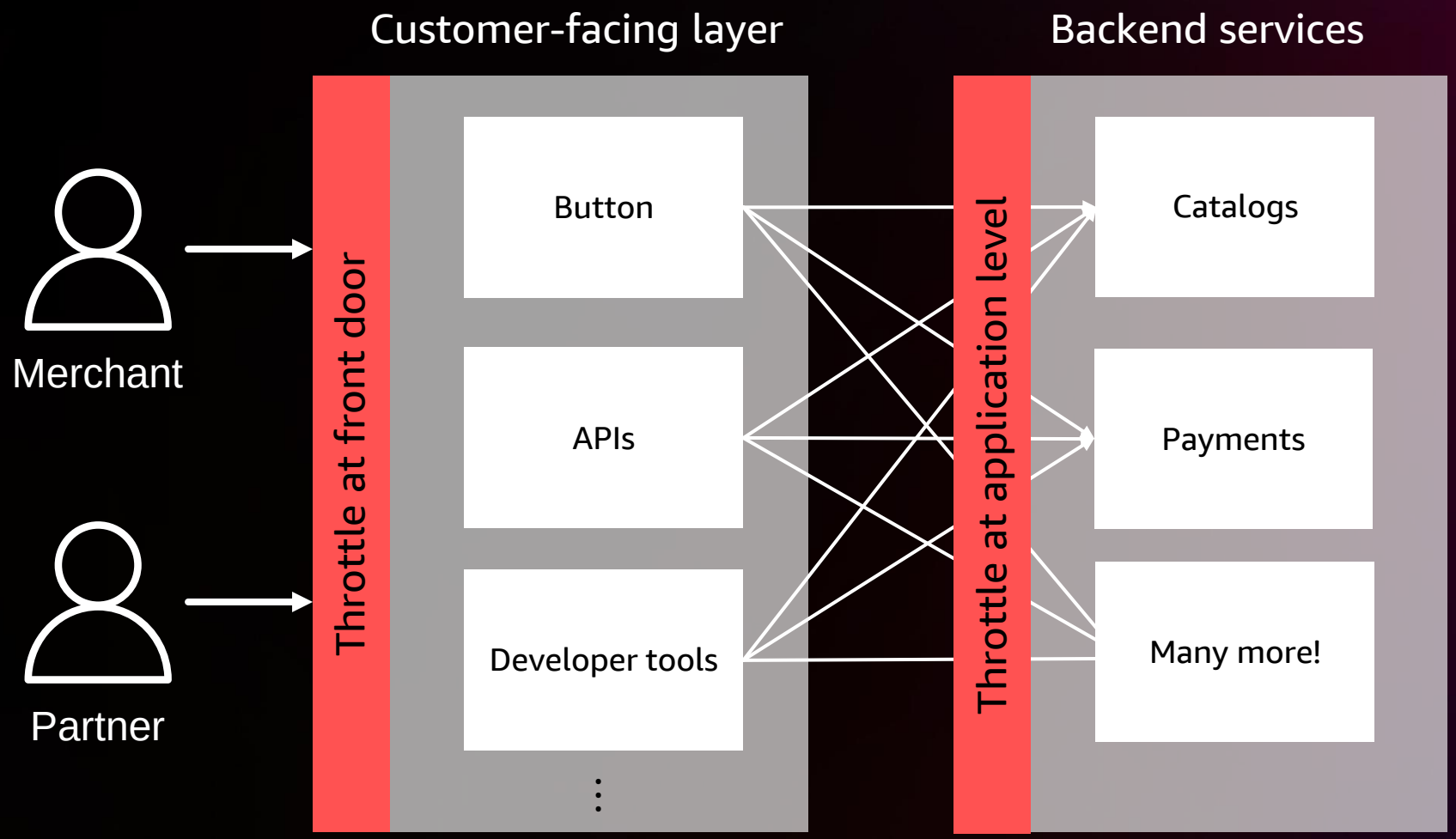
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Preventing noisy neighbors

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

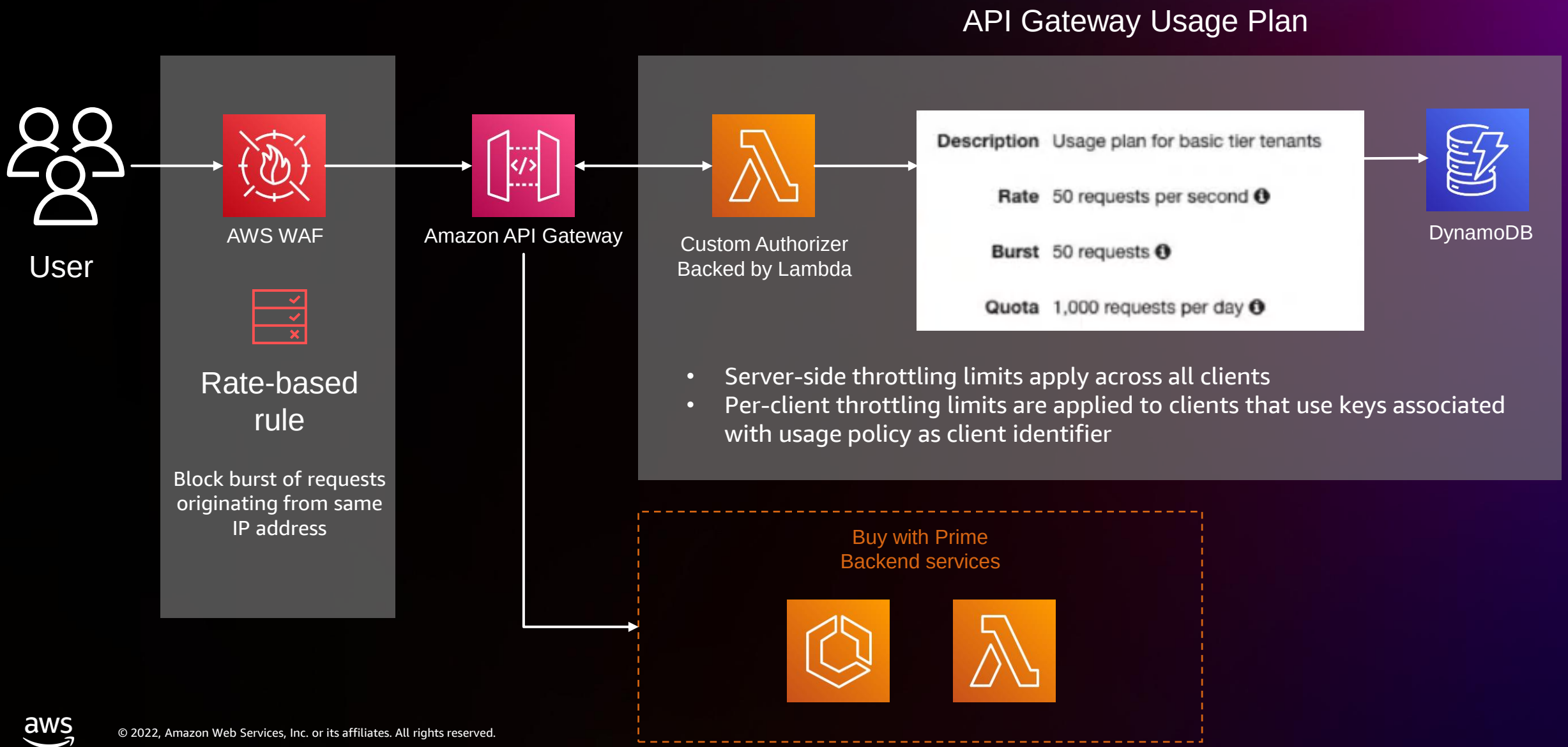
# Preventing noisy neighbors

HIGH-LEVEL OVERVIEW WHERE THROTTLING OCCURS



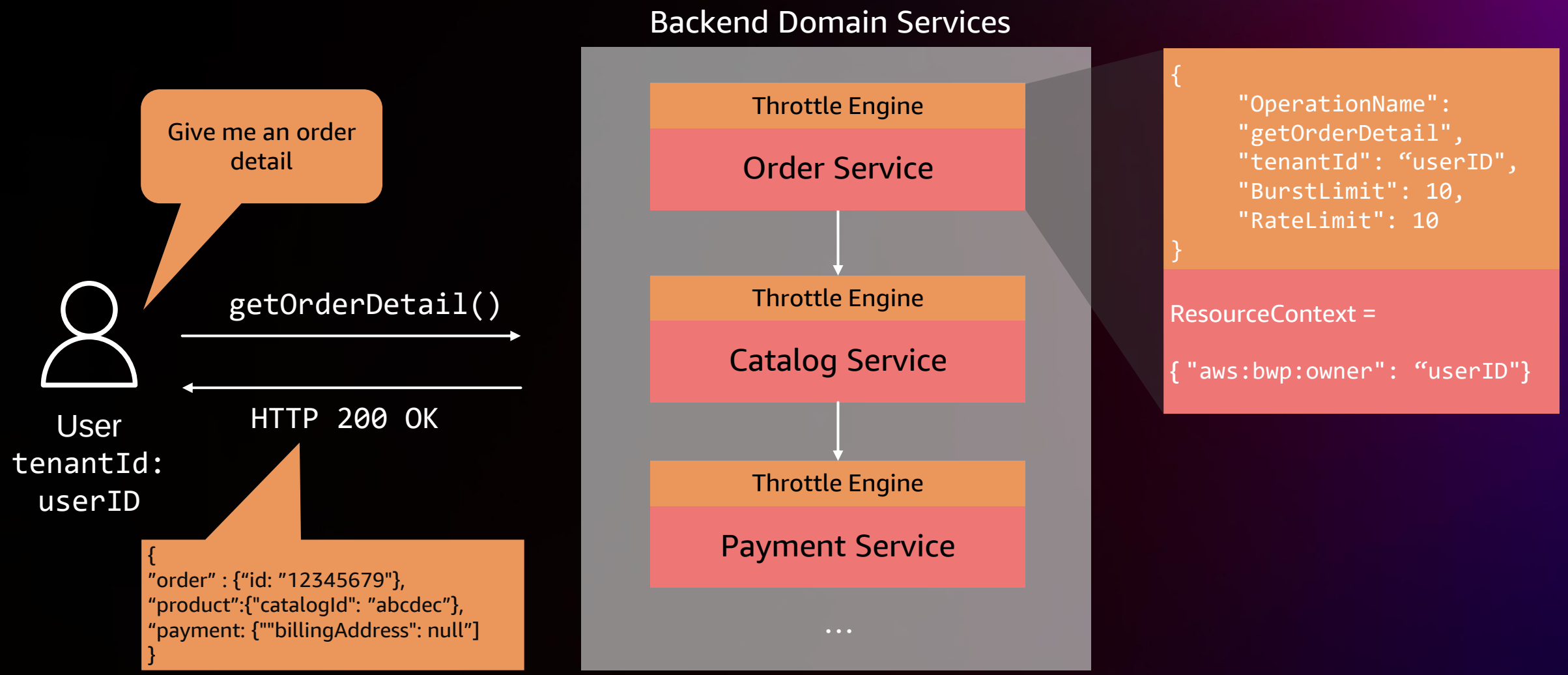

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Throttle at front door



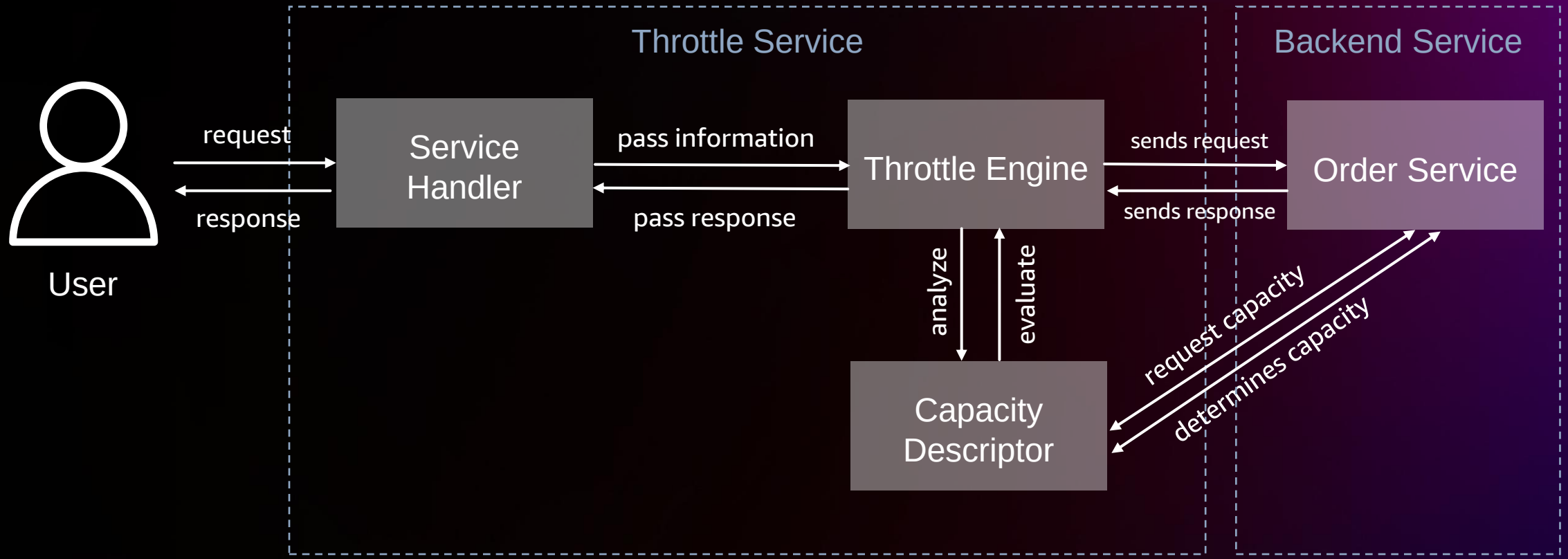

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Throttle at application level




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Let’s dive deeper into our throttling engine

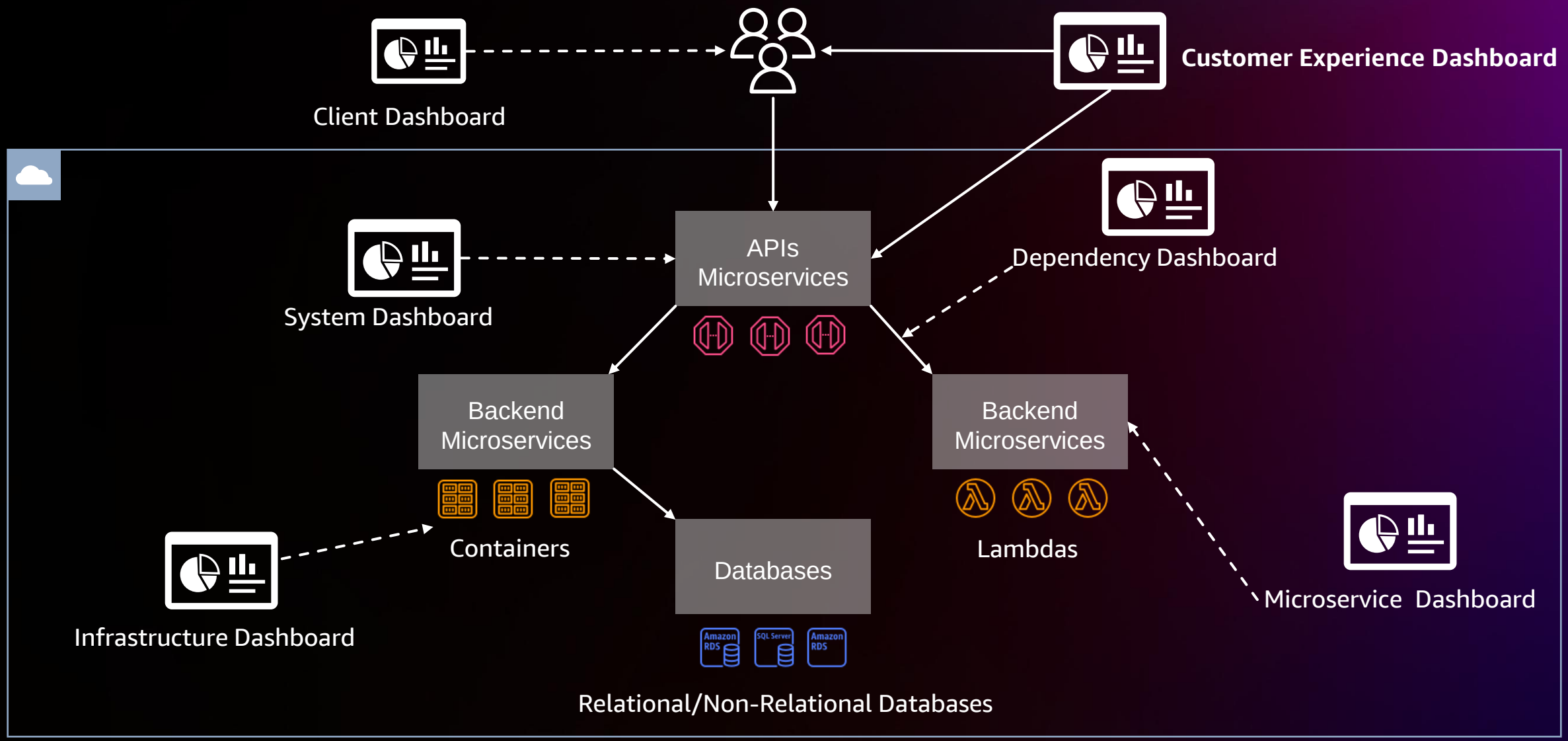



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Monitoring noisy neighbors

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Tenant activity & insights




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Our tools



CloudWatch Dashboards



CloudWatch metrics
and alarms



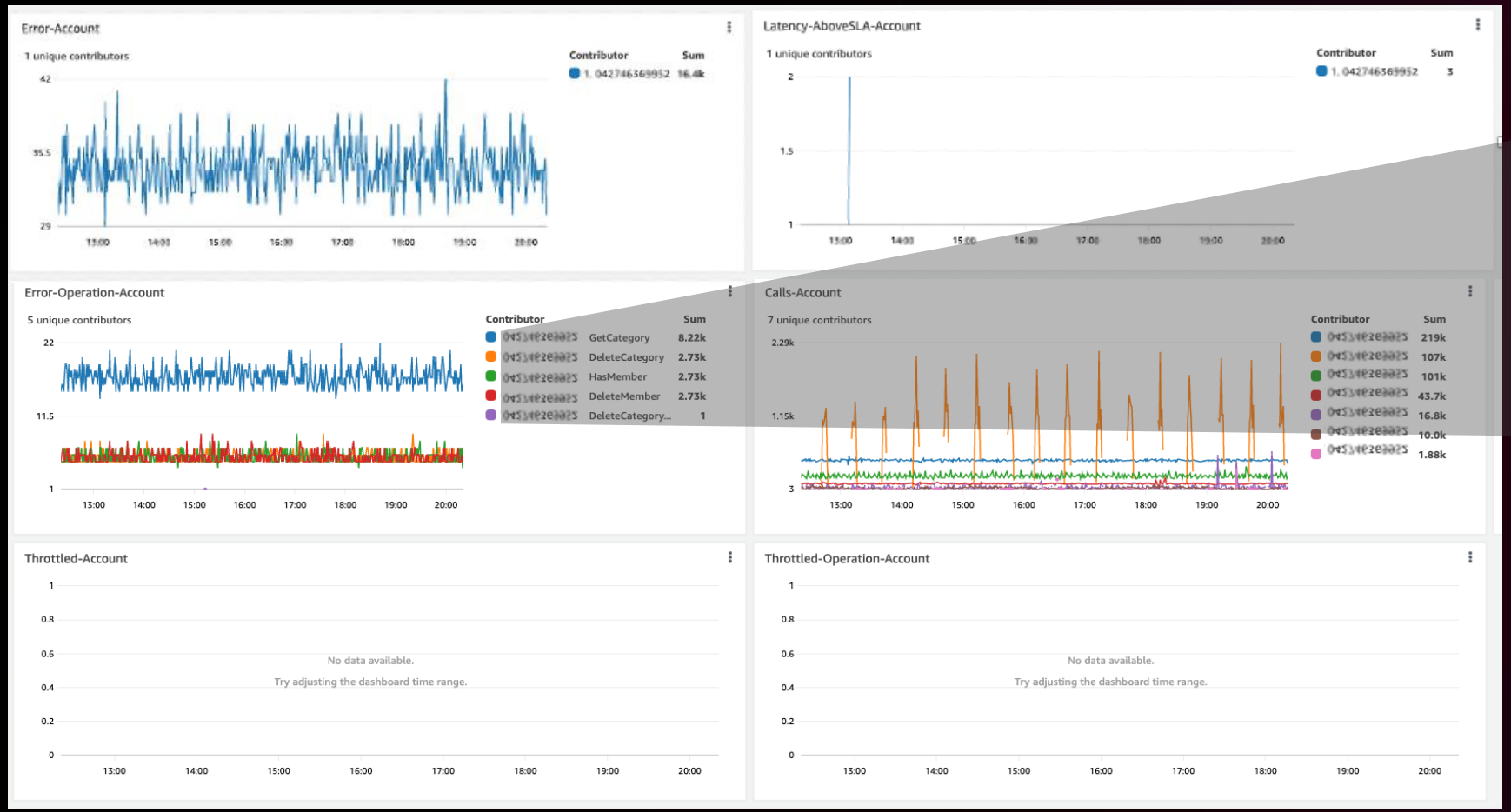
CloudWatch Logs/
Log Insights

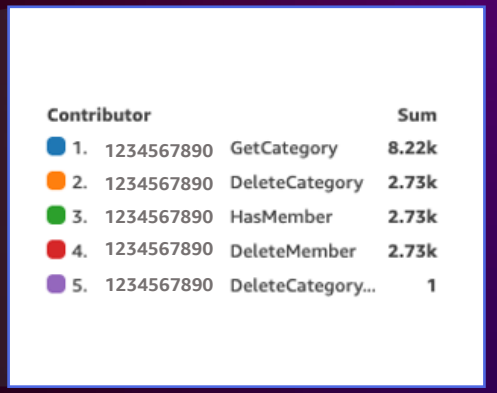


Buy with Prime
CloudWatch Logs CLI

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Account-level dashboard

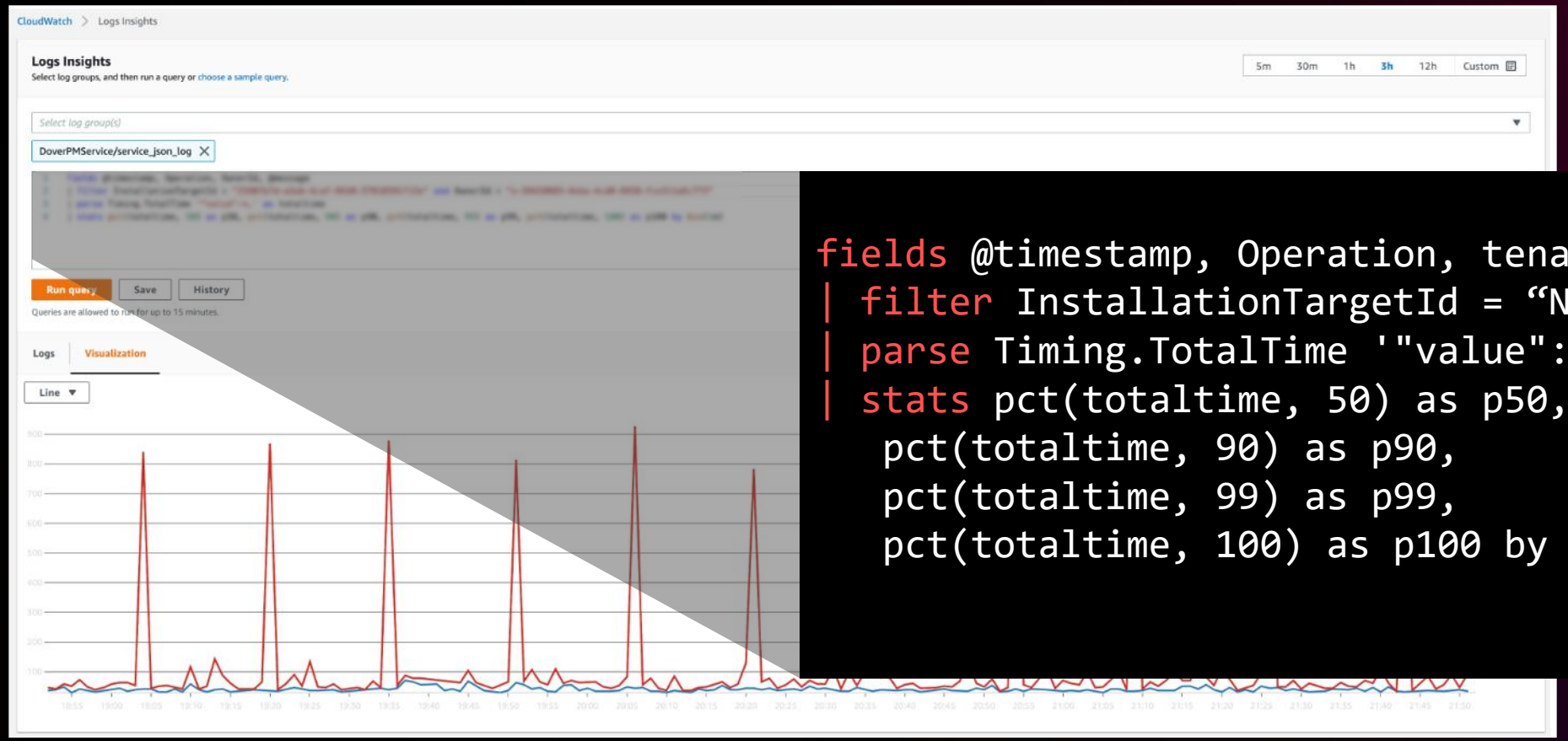



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Log Insights and Queries

Log insights to view response time for our backend services and tenantId




```
fields @timestamp, Operation, tenantId, @message
| filter InstallationTargetId = “N" and tenantId = ”Y"
| parse Timing.TotalTime '"value":*,' as totaltime
| stats pct(totaltime, 50) as p50,
   pct(totaltime, 90) as p90,
   pct(totaltime, 99) as p99,
   pct(totaltime, 100) as p100 by bin(1m)
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Finding the noisy neighbor

Customer impact list with total fault occurrence for specific API call

```
fields AwsAccountId, tenantId
| filter Operation = <Operation name>
| filter Fault = 1
| stats count() as @Occurrence by AwsAccountId
, tenantId, Operation
| sort @Occurrence desc
```

Customer impact list with latency impact for specific API call

```
fields tenantId, AwsAccountId, @timestamp, @message
| filter Time >= <Time>
| filter Operation = <Operation name>
| stats count() as @Occurrence by AwsAccountId ,
tenantId
| sort @Occurrence desc
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Buy with Prime CloudWatch Log CLI

Get the full context of a request **without clicking through different links, accounts, etc.**
Significantly **cut down the time to find logs we need.** (Usually within 1 minute)
Easily **pipe different queries together** to search across different log groups and more.

```
buywithprime-logs customer-impact –
service buywithprime
```




Catalog Service – Account 1

Order Service – Account 2

Payment Service – Account 3

The following command will retrieve the top merchants that were impacted in the past hour.

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Key takeaways

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Key takeaways

1. Let the resources track the owner for flexible and scalable architecture
2. All of the requests to each microservice should contain a tenant id for 1) tenant isolation and 2) effective noisy-neighbor isolation
3. Tenant isolation should be automatically tested throughout all the phases of development lifecycle
4. To contain noisy neighbors' impact, your architecture should throttle at multiple layers
5. Use telemetry to identify noisy neighbors

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What's next

- Learn more about Buy with Prime in the AWS Demo theater
- Join the Buy with Prime community to be part of the new ecommerce world



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

Jiwon Yeom
jiwony@amazon.com

Joseph Decena
decen@amazon.com

Ryan Lohan
ryanloha@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.