AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

GPS314

Operating at scale: Lessons learned from AWS MSP Partners

Andy Reedy
Principal Partner Solutions Architect
AWS

Mike Deck
Sr. Manager – Differentiation Programs
AWS

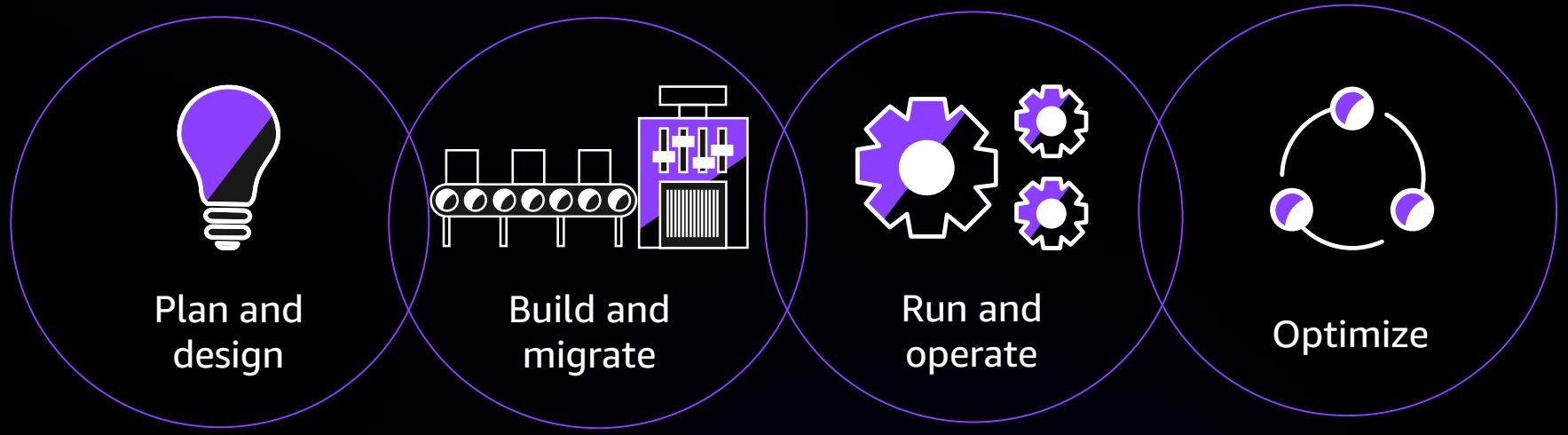
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The AWS Managed Service Provider Program

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

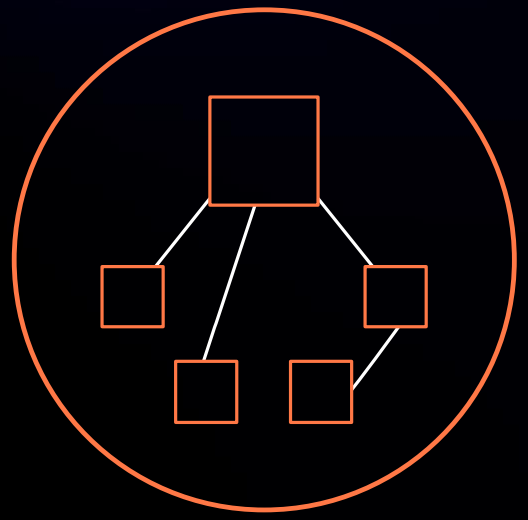
Evolution of AWS Managed Services

"I need help migrating, running, and optimizing my AWS workloads."



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

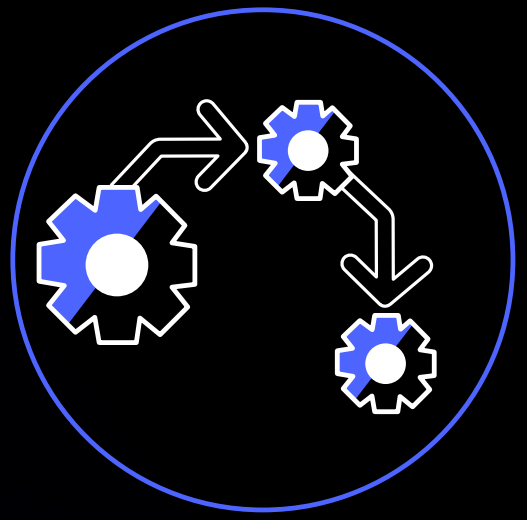
Managing at scale



Account management



Advanced monitoring



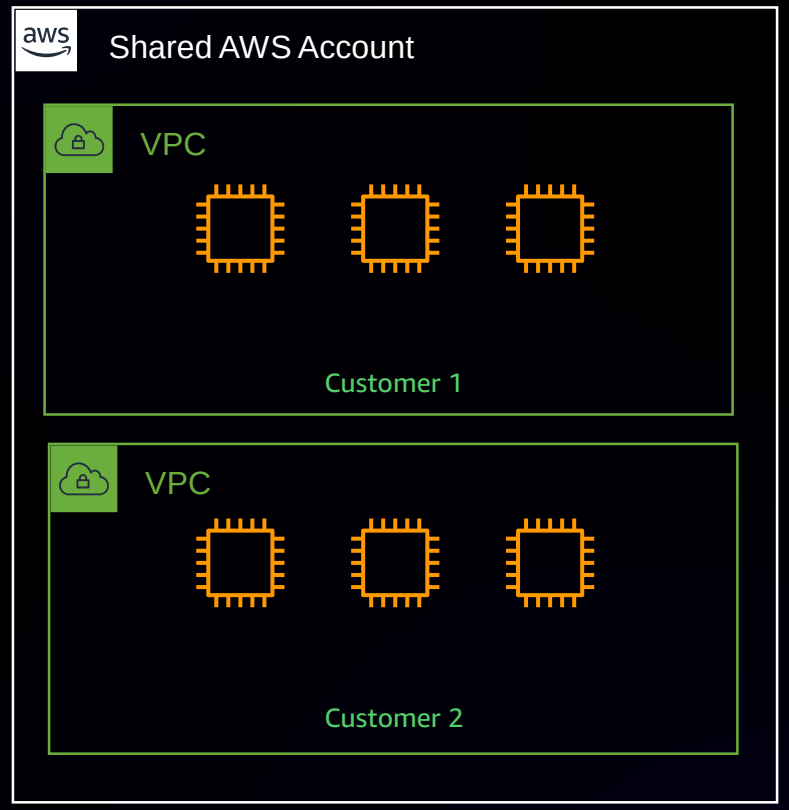
Automatic remediation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account ownership versus account management

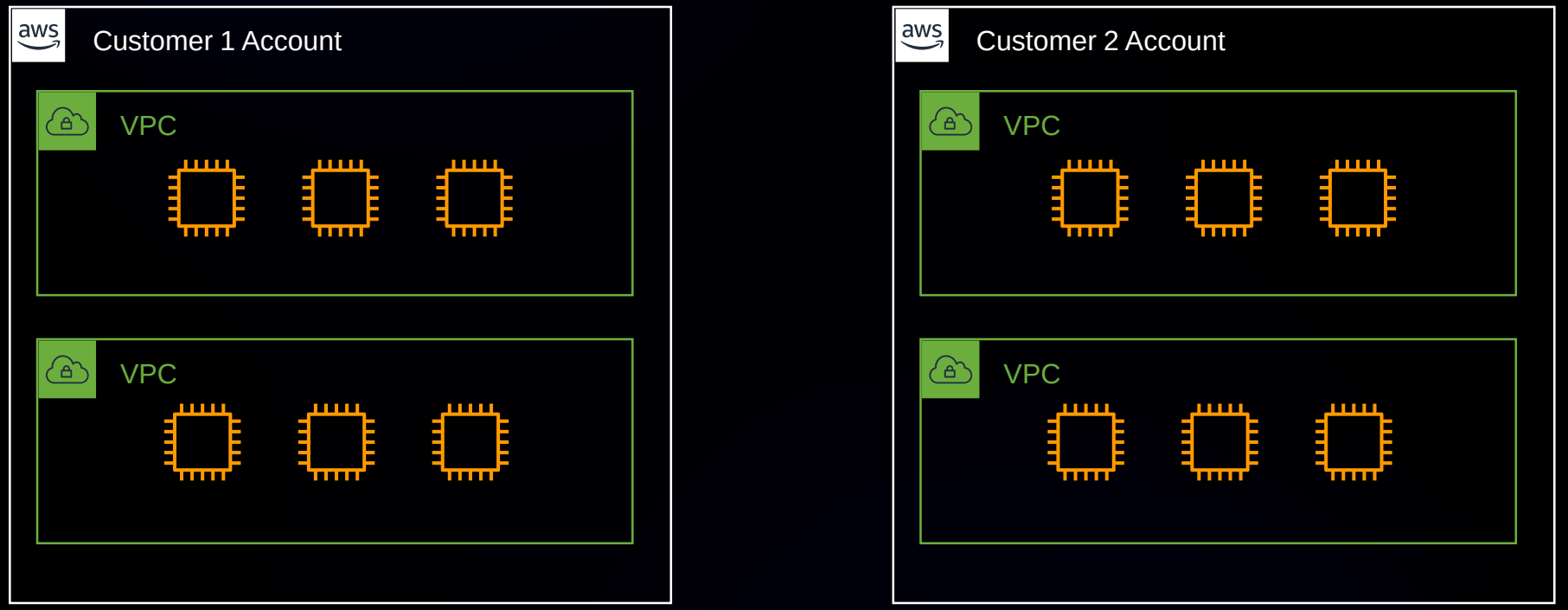
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Progression of MSP account management



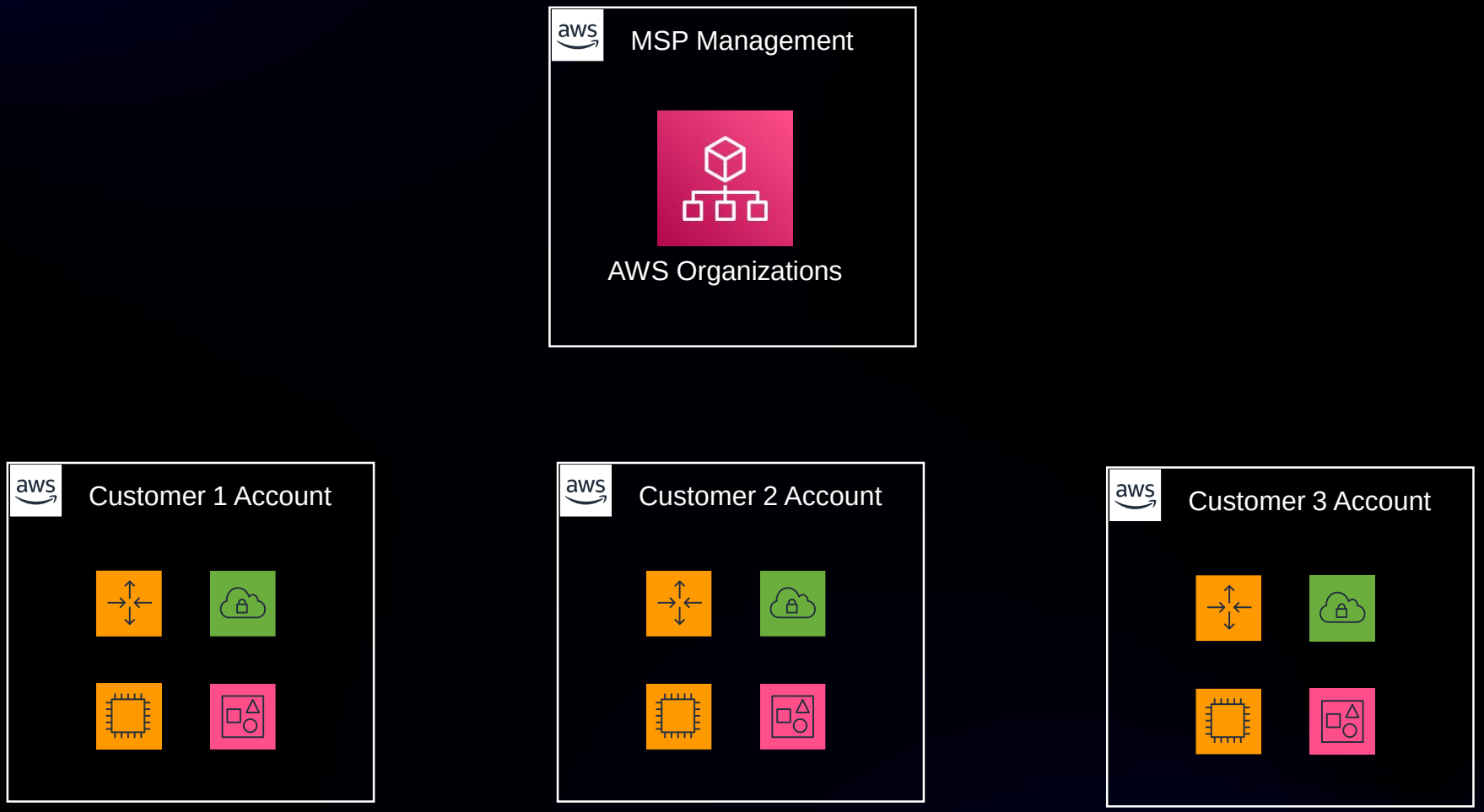
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Progression of MSP account management



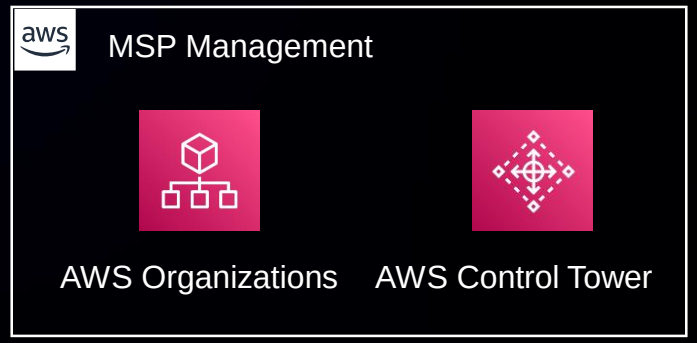
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Progression of MSP account management



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

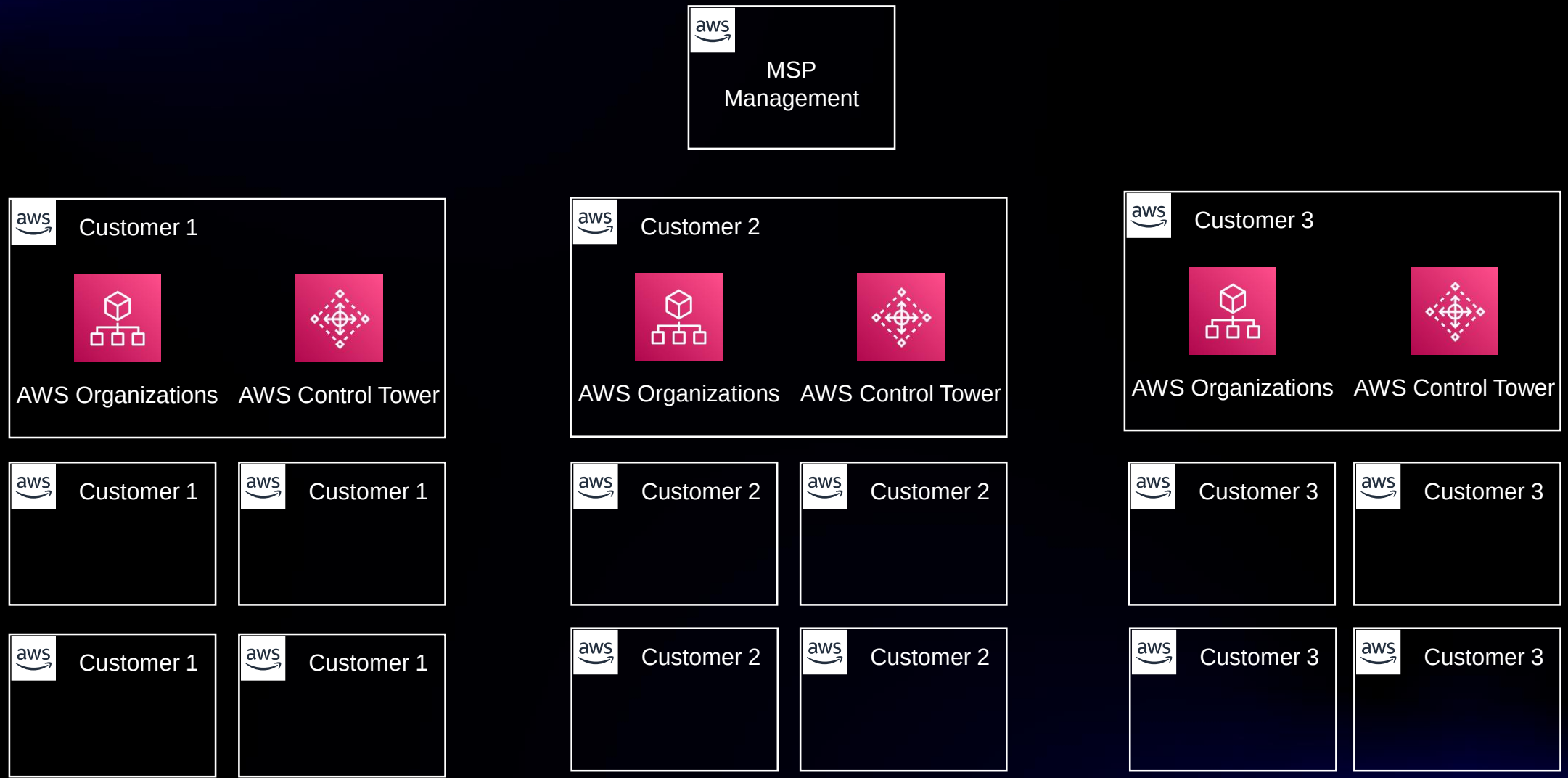
Progression of MSP account management





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Progression of MSP account management



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account management – Lessons learned

1. Embrace and plan for different management models
2. Embrace AWS Control Tower and AWS Organizations when possible and plan for outliers
3. Iterate your strategy as you grow
4. Inventory and state management is key!
5. Mentality: value versus traffic cop

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Advanced monitoring

Application performance monitoring

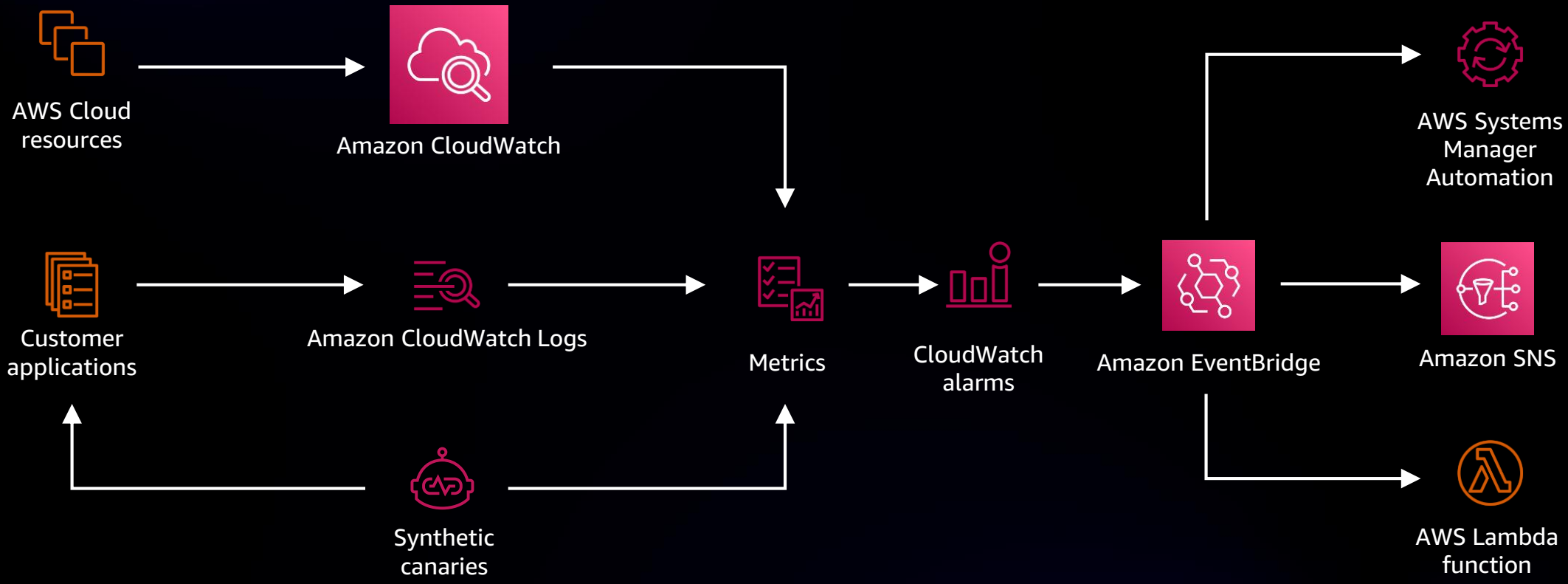
Synthetic testing

Application metrics and logs

Cloud resources

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring pattern



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Announcing Amazon CloudWatch cross account alarms

Posted On: Aug 5, 2021

Amazon CloudWatch announces cross account alarms, a new feature that enables customers to set alerts and take actions based on changes to metrics in other AWS accounts. Cross account alarms provide alerting based on trends in metrics in different AWS accounts and can be used in combination with existing cross account dashboards to setup operational visibility in a centralized monitoring account. With cross account alarms, you can be alerted when a trending metric in a different AWS account indicates that further investigation is required before the trend starts to cause operational issues or impacts the end user experience.

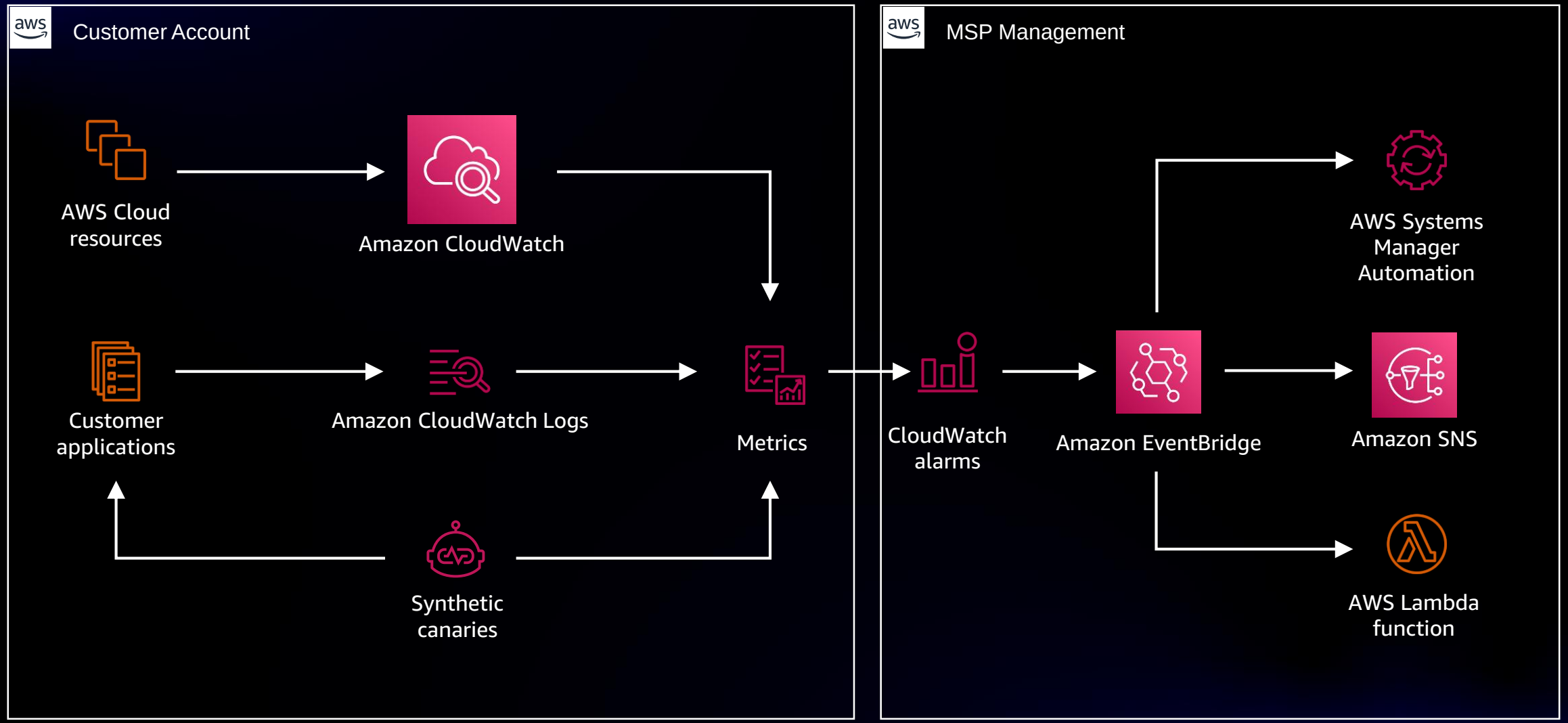
For example, you dedicate an AWS account as a monitoring account that your team uses to monitor and troubleshoot a number of different AWS accounts that run your production application. Cross account alarms can be used to notify your team when average or max CPUUtilization across EC2 instances in all production accounts exceeds some acceptable threshold, like 80%. You can combine metrics from different accounts using Metric Math and organize cross account alarms into hierarchies using composite alarms in the monitoring account.

Cross account alarms are now available in all commercial AWS Regions, standard CloudWatch alarm pricing applies – see pricing page for details. To get started, first enable cross account permissions to give your monitoring account visibility on metrics in other AWS accounts. Then navigate to the CloudWatch alarms console and click Create Alarm. You will be able to search and select metrics from accounts you have granted permissions to view.

To get started with Cross Account Alarms please refer to our documentation.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring pattern



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

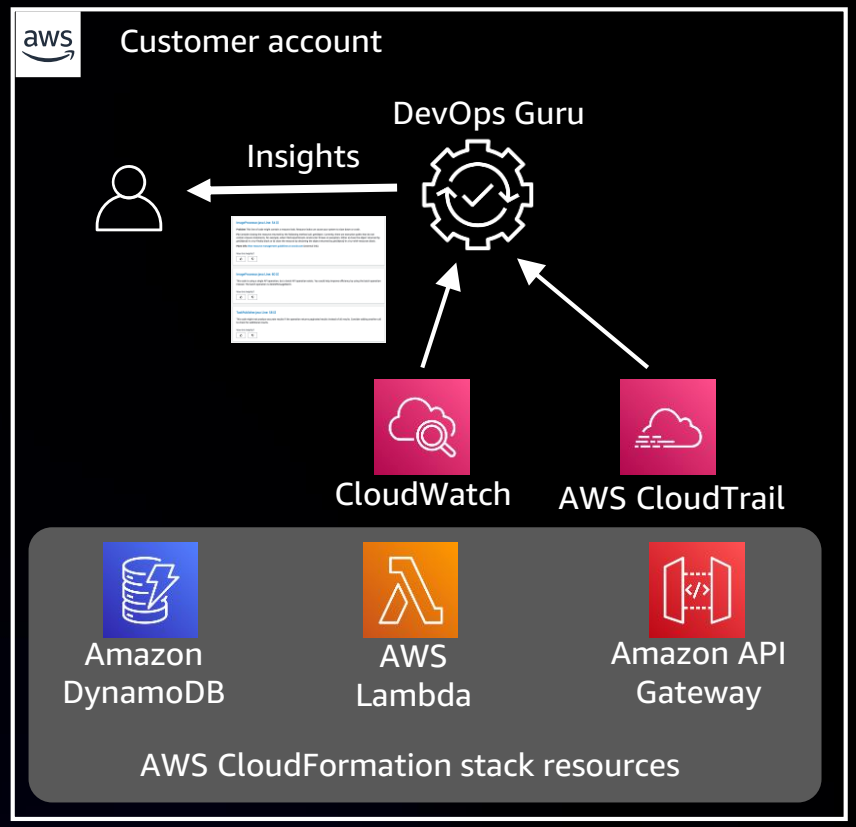
Anomaly detection

Amazon CloudWatch anomaly detection

- No static thresholds
- Account for seasonality and trend changes
- Works with custom metrics (applications)

Amazon DevOps Guru

- ML-based anomaly detection
- Automatically detect operational issues
- Self-tuning – **reduced alarm fatigue**



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Advanced monitoring – Lessons learned

1. Monitoring tiers – Not all accounts and services are the same
2. Start with the least common denominator
3. Anomaly detection versus threshold-based alarms
4. Distributed metrics, centralized alarms (and actions)
5. Relentless focus on signal to noise

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automatic remediation

Automatic remediation

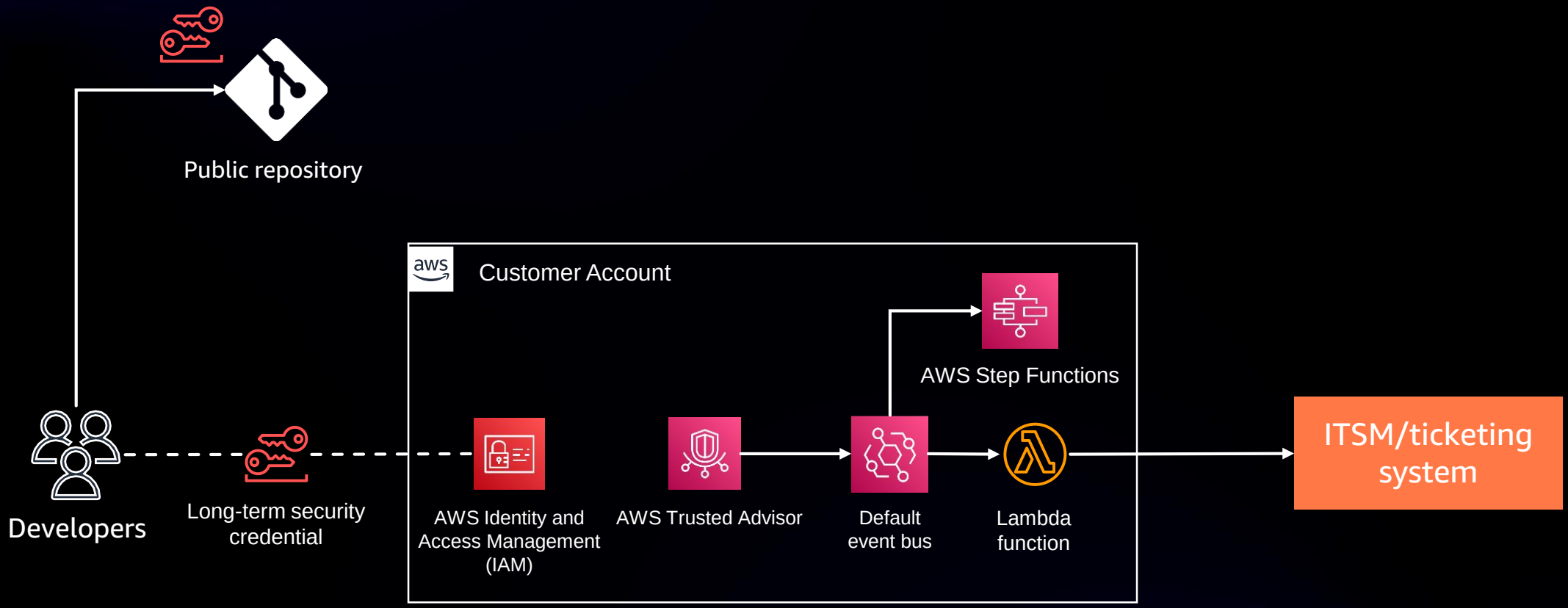
Ticketing/ITSM integration

Amazon SNS/email

Events

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Health risk notifications



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rackspace case study

62,000+ SSM-enabled instances and virtual machines (3,616 non-AWS)

September 2021:

- 23,000 incidents including 7,400 CloudWatch alarms
- 6,780 automated responses

764 person-hours saved in one month

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automatic remediation – Lessons learned

1. Start small and simple – develop the skillset
2. Use metrics to identify the frequent/recurring events
3. Leverage AWS Config and AWS Security Hub
4. Close the feedback loop
5. Recognize this is not optional at scale

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.