
AWS
re:Inforce
JULY 26 – 27, 2022 | BOSTON, MA

NIS331

Architecting for ransomware protection on AWS

Kiaan Sumeet

Senior Security Consultant
AWS

Koen van Blijderveen

Principal EMEA Security SSA
AWS

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

Introduction



Koen van Blijderveen
Principal EMEA Security Specialist SA
AWS Worldwide Specialist Organization



Kiaan Sumeet
Senior Security Consultant
AWS Professional Services BDSI

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

Agenda

Evolution of ransomware

NIST Cybersecurity Framework (CSF)

AWS services and ransomware

Q&A and practical scenarios

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

Ransomware threats

75% of IT organizations will face one or more **ransomware threats by 2025**

Gartner, "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware"

"Hackers are locking people out of their networks and demanding big payments to get back in. New data shows just how common and damaging the attacks have become."

The New York Times

Scripps enters fourth week of ransomware attack

The San Diego Union-Tribune

DHS to issue first cybersecurity regulations for pipelines after Colonial hack

"Two directives will seek oversight of the industry after ransomware attack upended gas availability in the Southeast for 11 days"

The Washington Post

Ransomware attack on Bose exposes employee SSNs and financial information

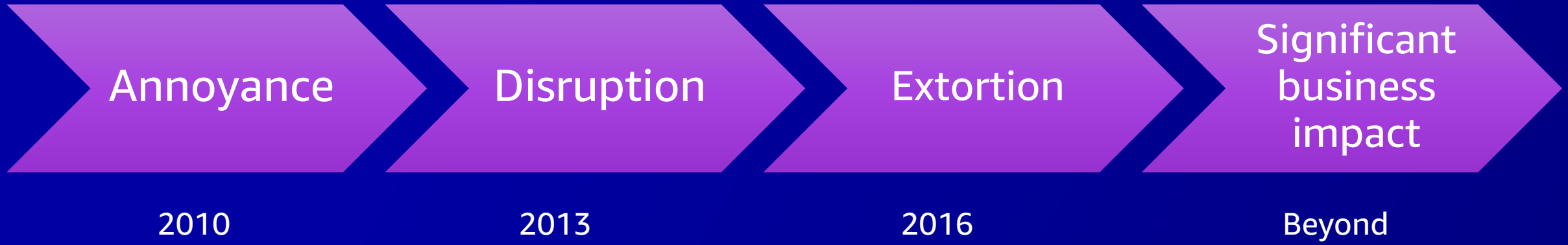
"The company was forced to notify New Hampshire officials after employees in the state had their information accessed"

ZDNet

aws

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

Evolution of ransomware



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

Who here has experience preventing or responding to ransomware?

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

Lessons from ransomware evolution

- Increased incident rates and sophistication
- Skyrocketing recovery costs
- Early detection is key
- Preventive controls go a long way
- Automation
- Education, training, and awareness

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

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)



IDENTIFY

Identify an organization's critical functions, assets, and processes and how cybersecurity risks could disrupt them



PROTECT

Define safeguards necessary to protect critical infrastructure services



DETECT

Implement the right measures to identify threats and cyber-risks promptly



RESPOND

Define the measures necessary to react to an identified threat



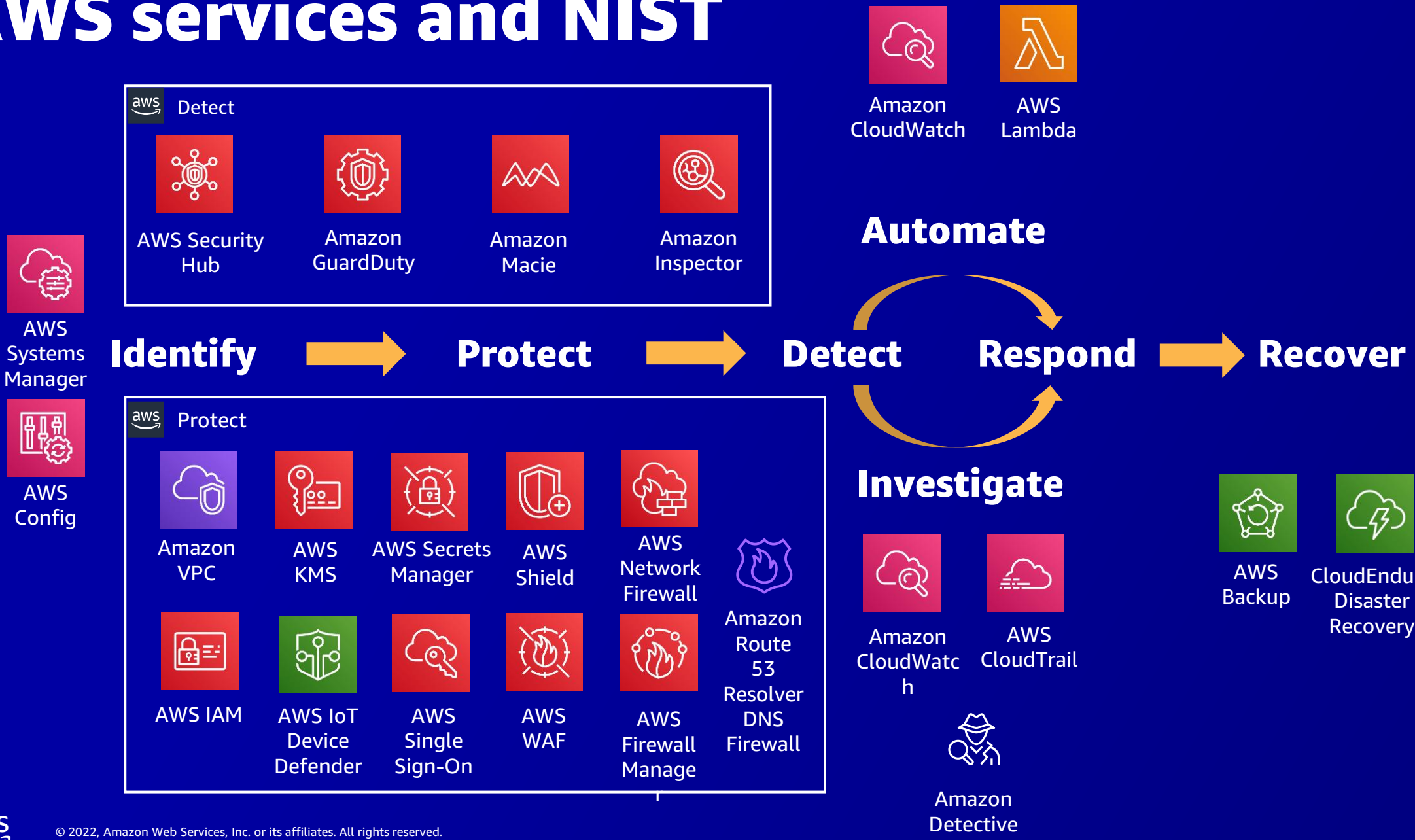
RECOVER

Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

aws

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

AWS services and NIST



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

5 AWS security best practices for ransomware protection

1. Monitor and control outgoing traffic including DNS
2. Leverage MFA where possible (MFA delete on Amazon Simple Storage Service bucket)
3. Turn off direct remote access (SSH/RDP)
4. Make data immutable using AWS Backup vaults and other options
5. Turn on automated detection services including Amazon GuardDuty for Amazon S3

aws

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

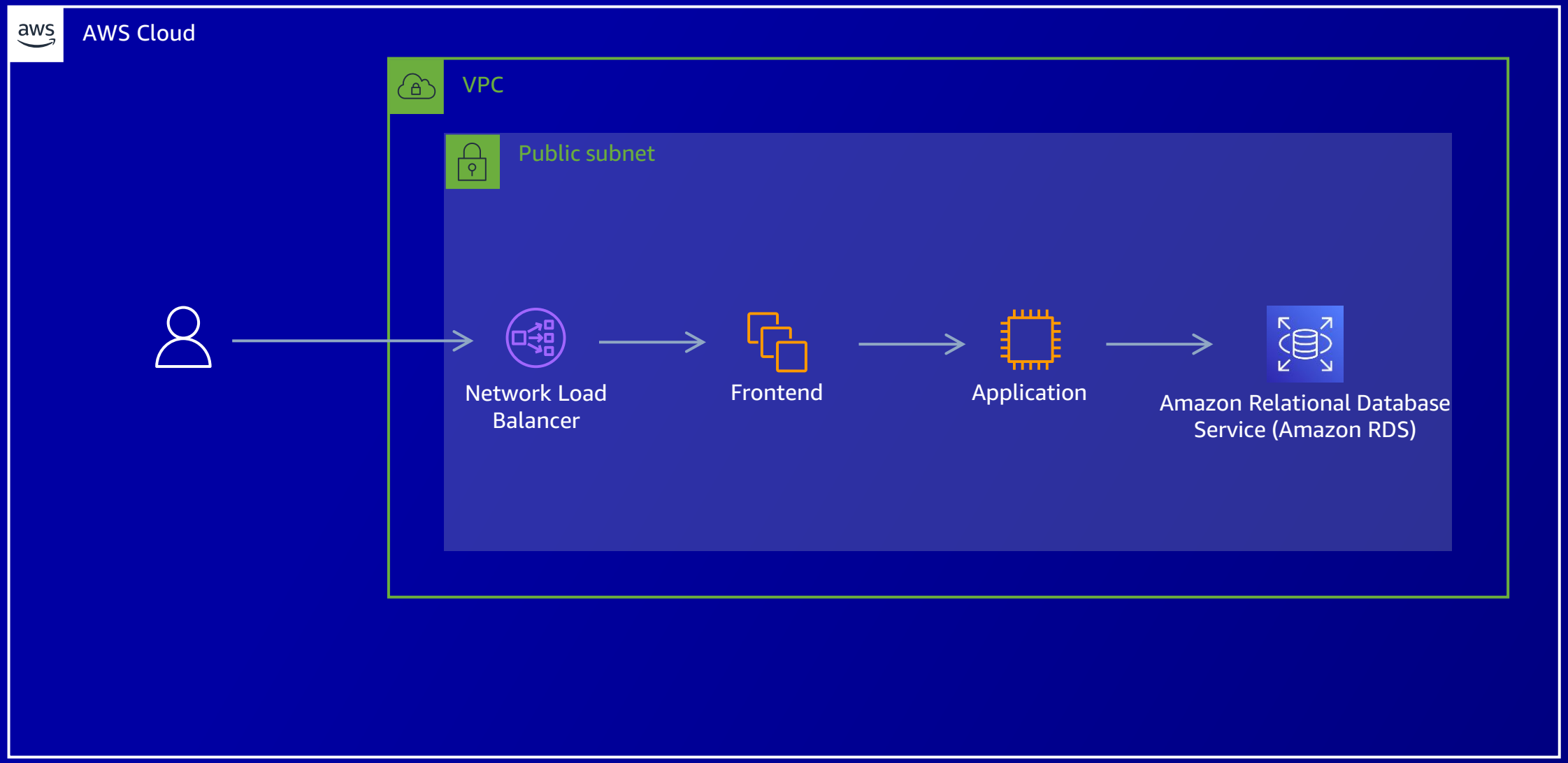
What challenges did you run into while preparing or responding to ransomware on AWS?

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

Scenarios

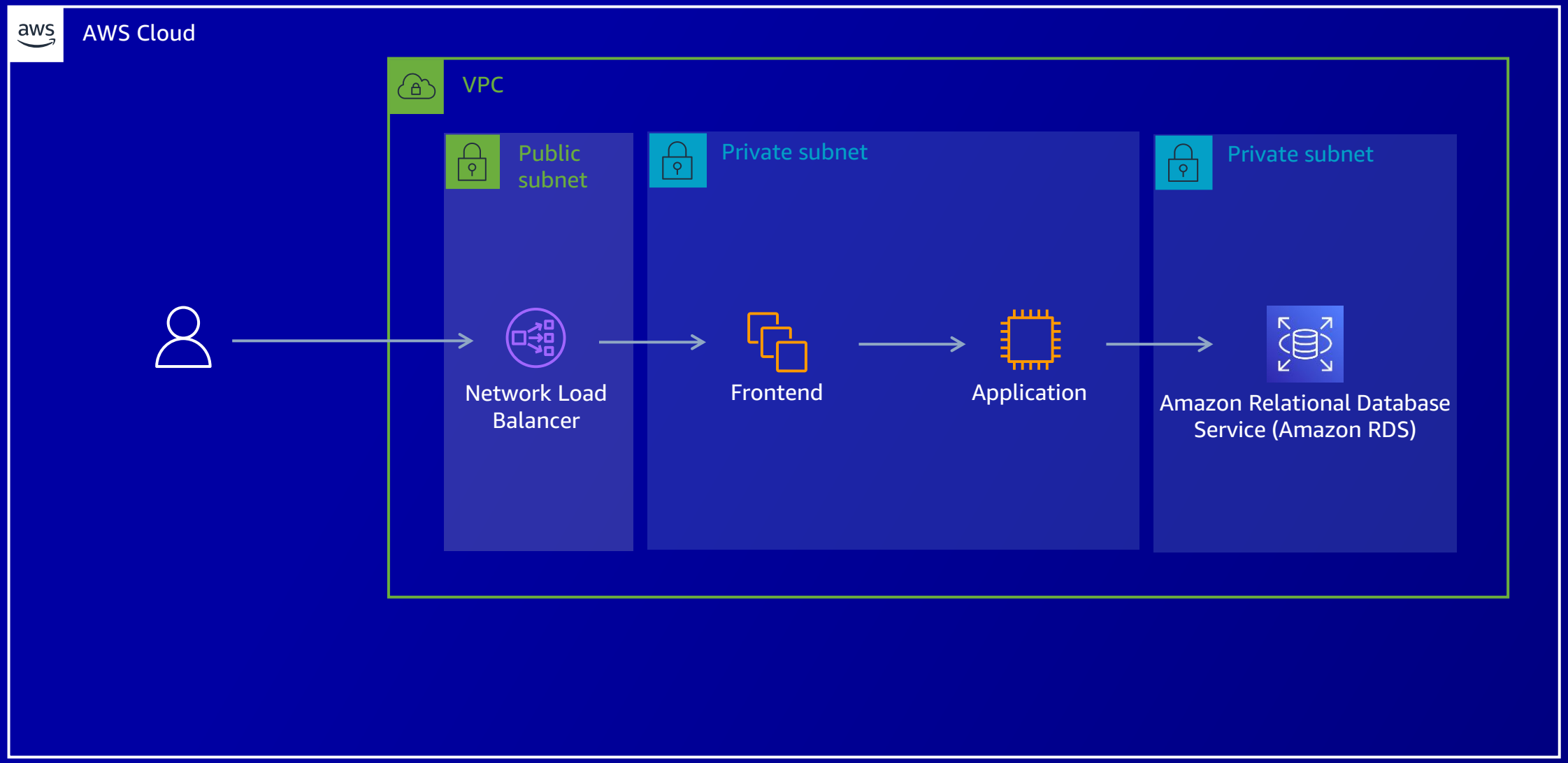
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1



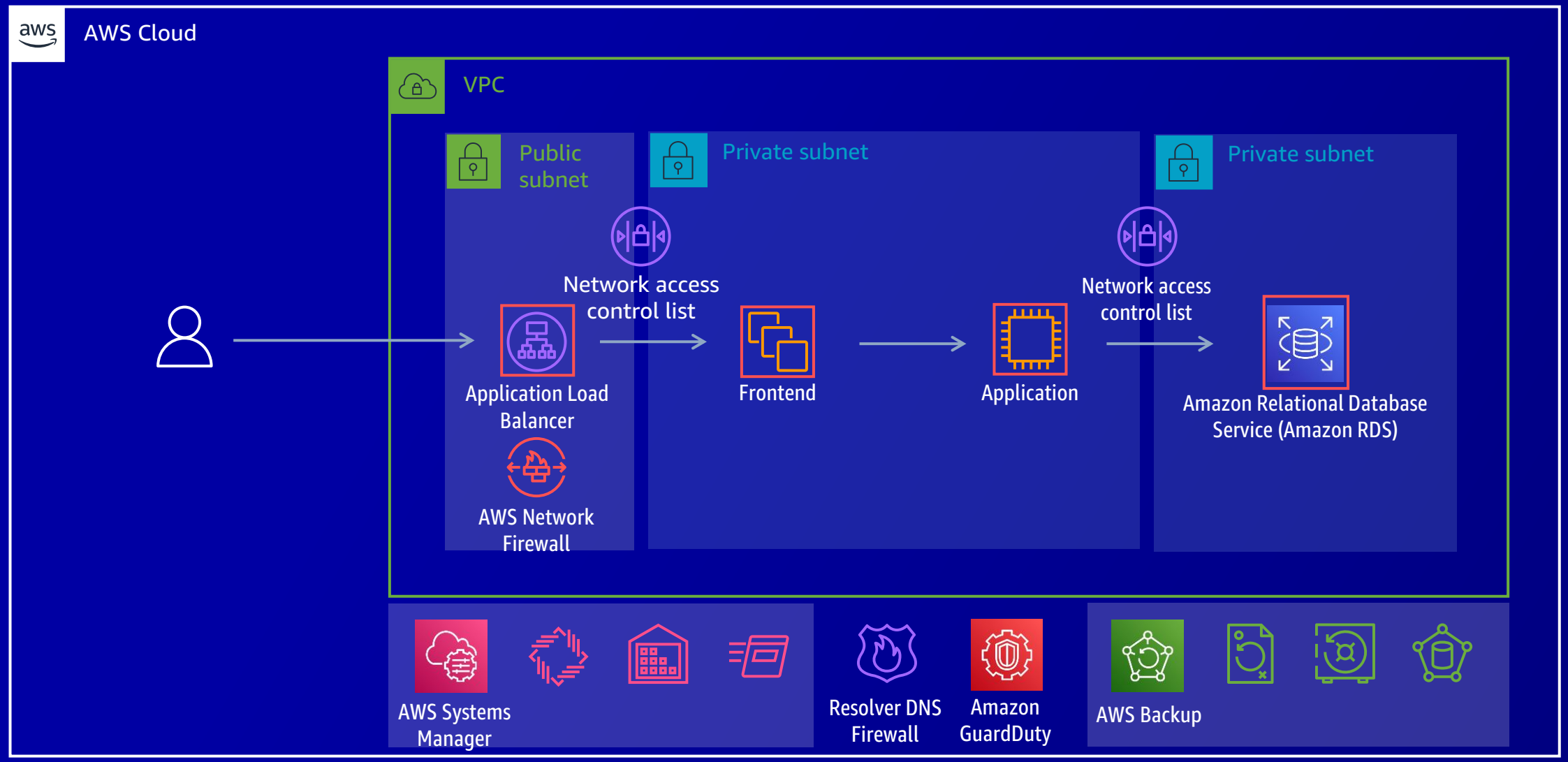
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1



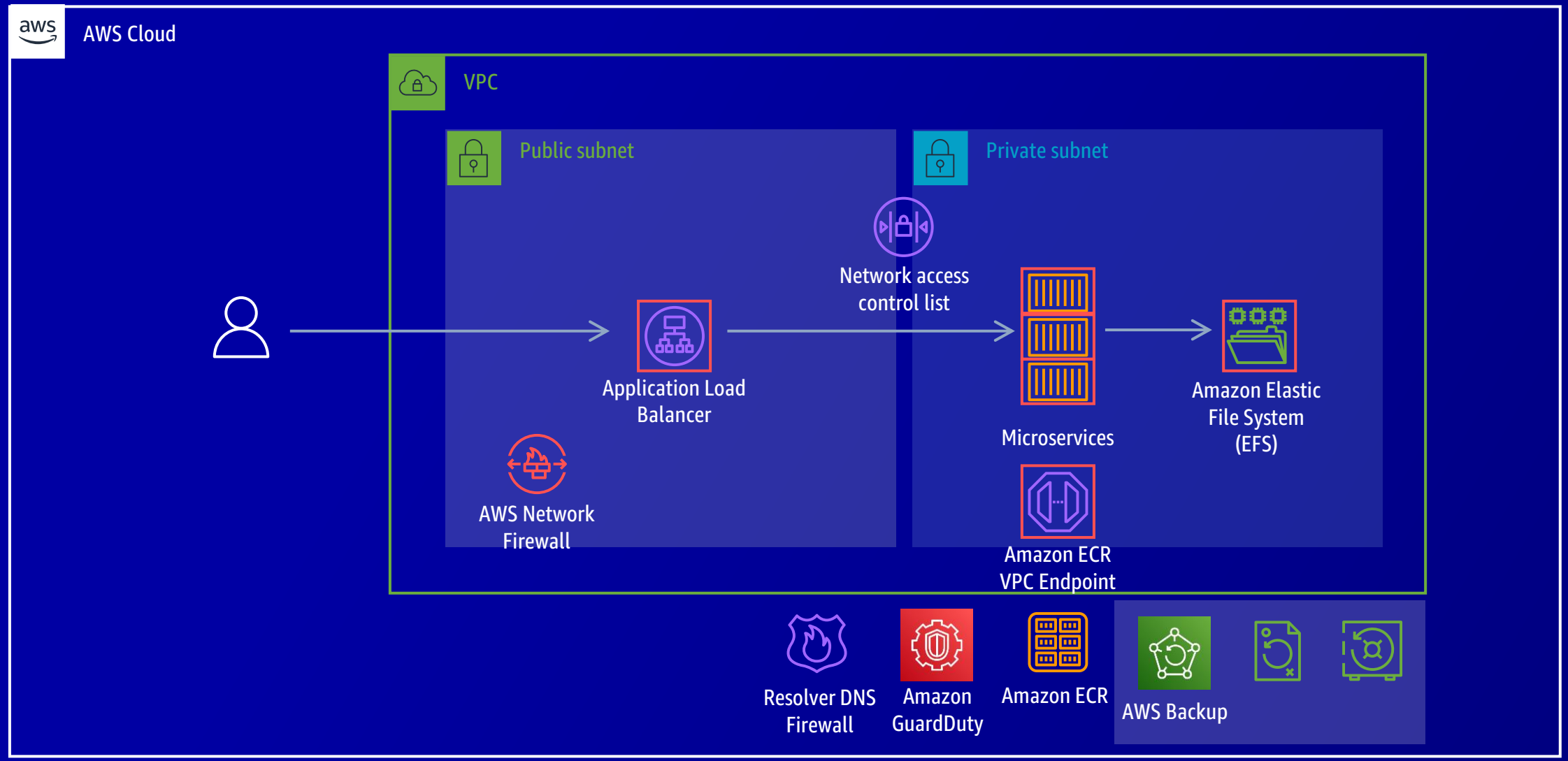
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1



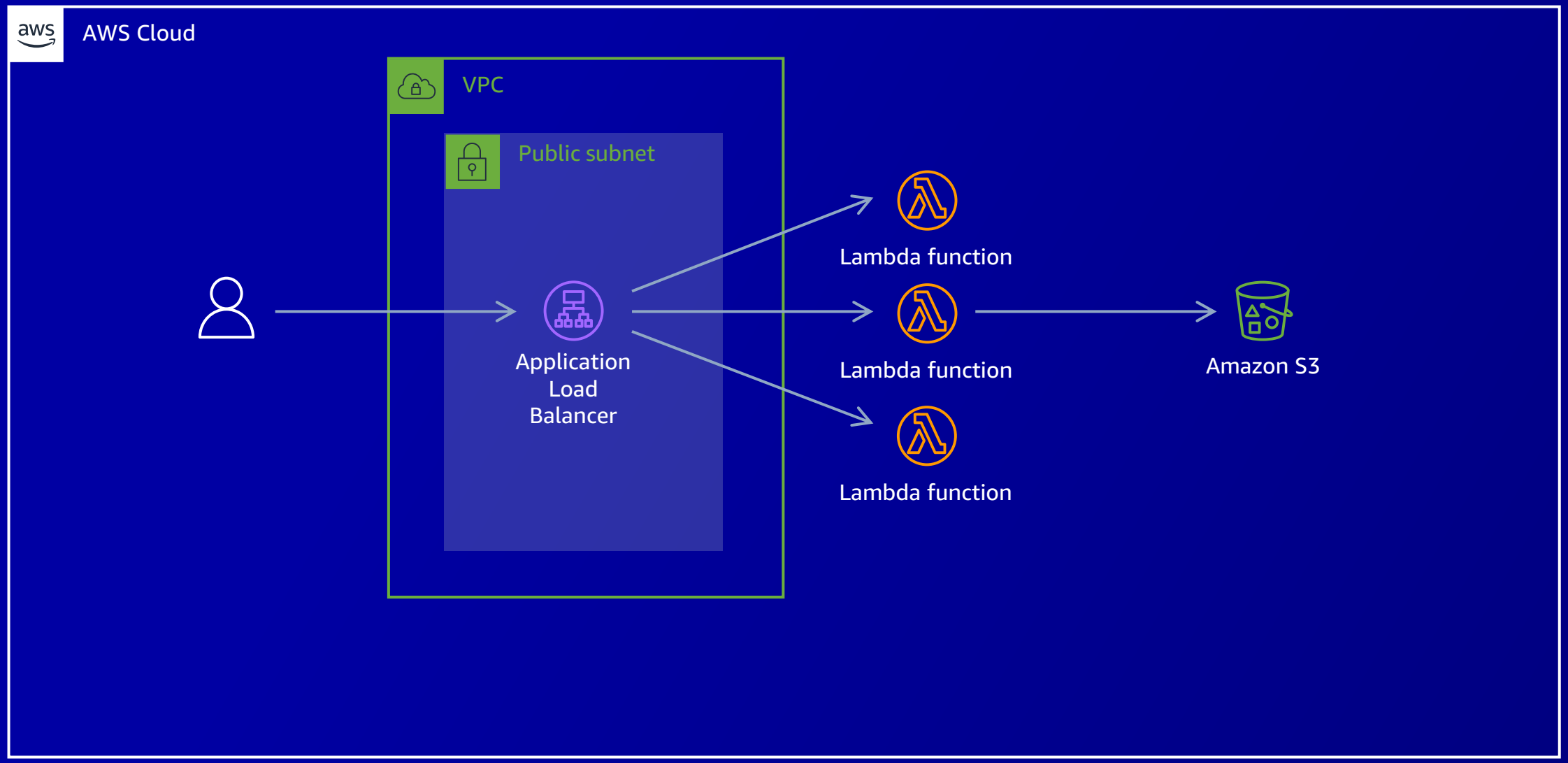
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 2



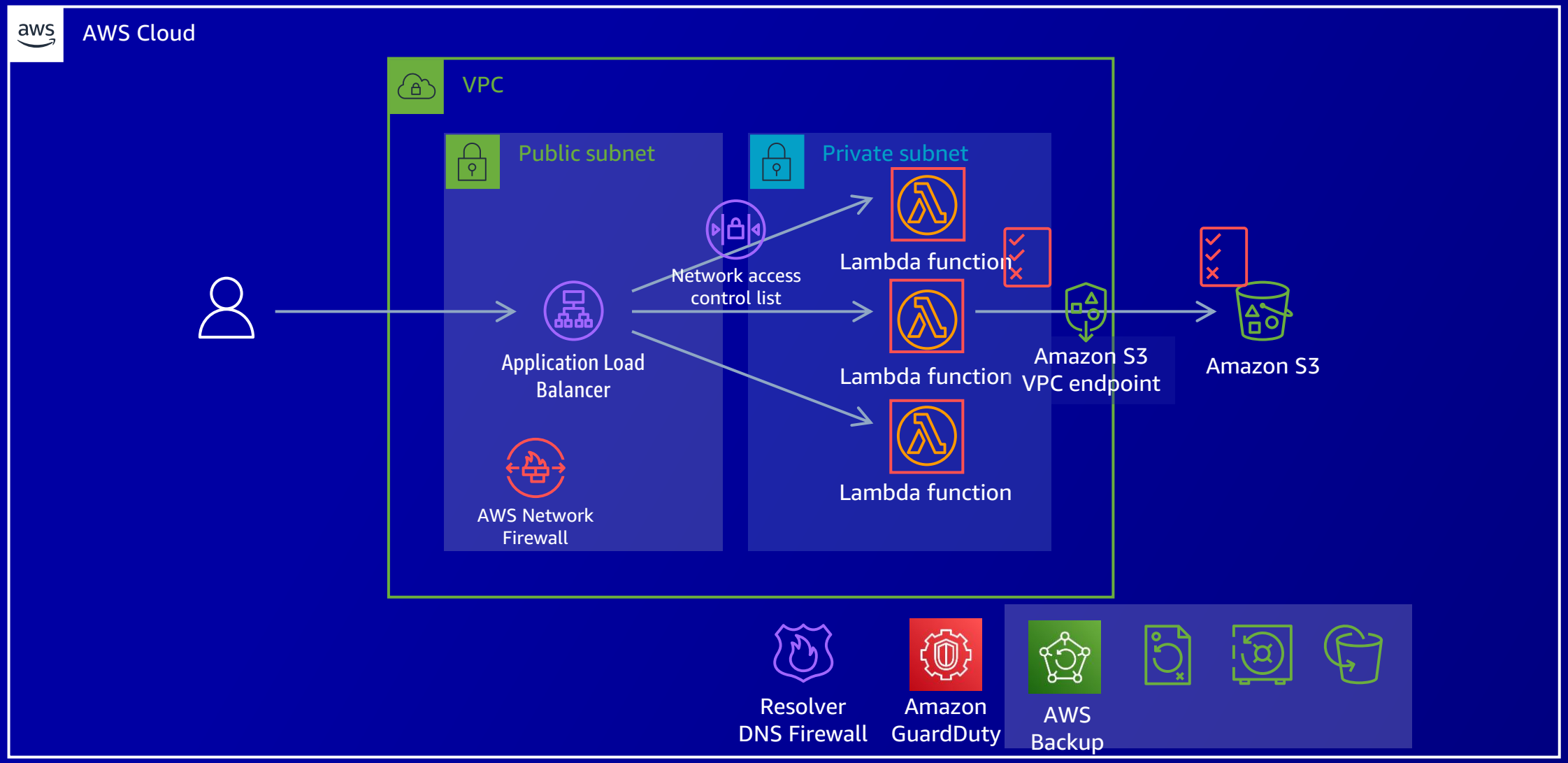
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 3



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

Scenario 3



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

Other sessions

- NIS306 – 7/27/2022 2:00pm Breakout session
  300 – Advanced – Automating patch management and compliance using AWS

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

Thank you!

Kiaan Sumeet
sumeetks@amazon.co.uk

Koen van Blijderveen
kvb@amazon.nl

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