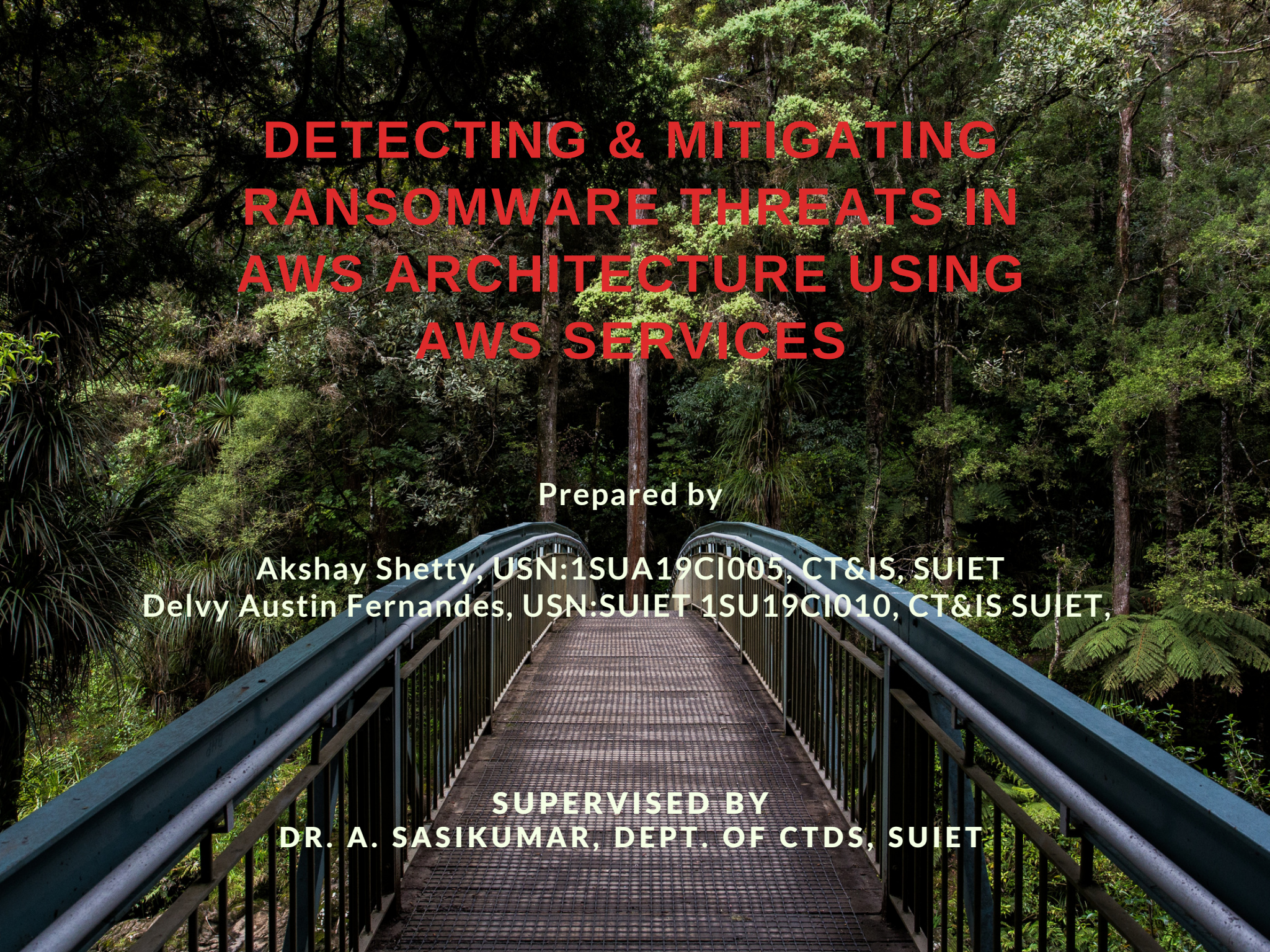


DETECTING & MITIGATING RANSOMWARE THREATS IN AWS ARCHITECTURE USING AWS SERVICES

Prepared by

Akshay Shetty, USN:1SUA19CI005, CT&IS, SUIET
Delvy Austin Fernandes, USN:SUIET 1SU19CI010, CT&IS SUIET,

SUPERVISED BY
DR. A. SASIKUMAR, DEPT. OF CTDS, SUIET

Agenda

IN THIS PROJECT WE WILL DO THREE THINGS:

1. Protect: Use AWS Systems Manager to update and configure our EC2 instances – to mitigate system vulnerabilities.
2. Detect: Use Guard Duty, Security Hub, and Systems Manager to detect malicious behavior by an EC2 instance and investigate it further for the presence of ransomware.
3. Respond: Use Systems Manager automation to gather data from an affected system, snapshot it, and isolate it. This enables the incident response team to do further investigation and forensic work.

Abstract

Protect, Detect, and Respond

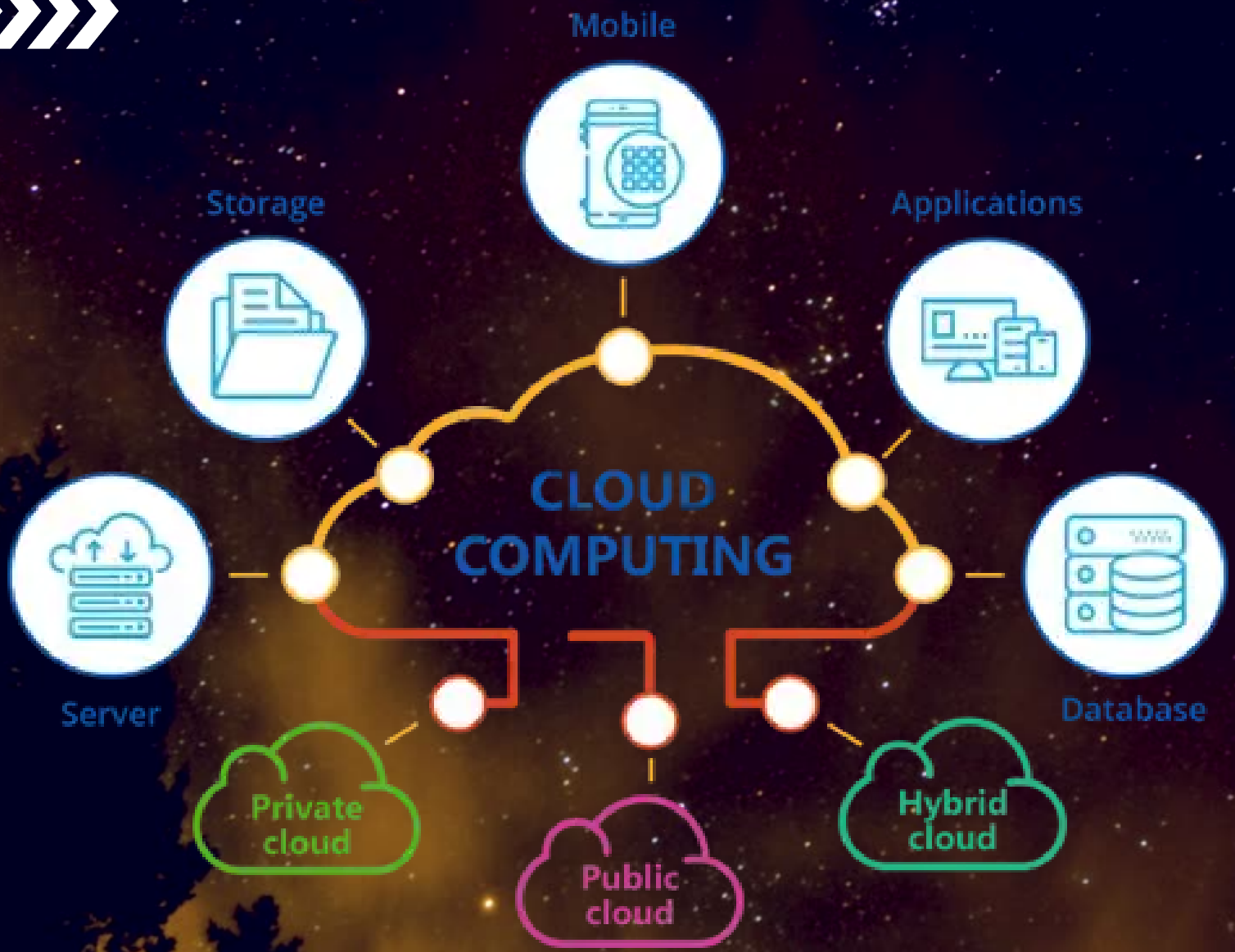
Threat detection can continuously monitor our AWS accounts and workloads for malicious activity and deliver detailed security findings for visibility and remediation. Early detection of anomalous network activity is key to mitigating ransomware threats and their impact.

INTRODUCTION

Criminal organizations use sophisticated methods to compromise their victims' systems and encrypt the data, usually with the goal of extorting money from the victim. An AWS customer, benefits from AWS data centers and network infrastructure, which are architected to protect the information, identities, and applications.

Project Domain

<u>Cloud computing</u>:
where the sky is not the limit but the gateway to infinite possibilities, scalability, and seamless collaboration.



Amazon Web Services

IN THE VAST LANDSCAPE OF CLOUD SERVICES, AWS STANDS TALL, DELIVERING THE TOOLS AND INFRASTRUCTURE TO FUEL DIGITAL TRANSFORMATION AND DRIVE SUCCESS.

ACCORDING TO GARTNER, BY 2025, RANSOMWARE ATTACKS ARE EXPECTED TO INCREASE BY 700% AND AT LEAST 75% OF IT ORGANIZATIONS WILL FACE ONE OR MORE ATTACKS.

Gartner, “Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware”, January 2021.”, January 2021.

Misconfigurations Leading to AWS S3 Ransomware Exposure

ermetic

S3 buckets are advertised by AWS as extremely durable.

Recent Ermetic research found that misconfigurations of S3 buckets and access-related factors made exposure to potential ransomware in the real-world sample studied extremely common.

This potential risk calls for organizations to take urgent action to correct any such S3 bucket misconfigurations and access-related factors.

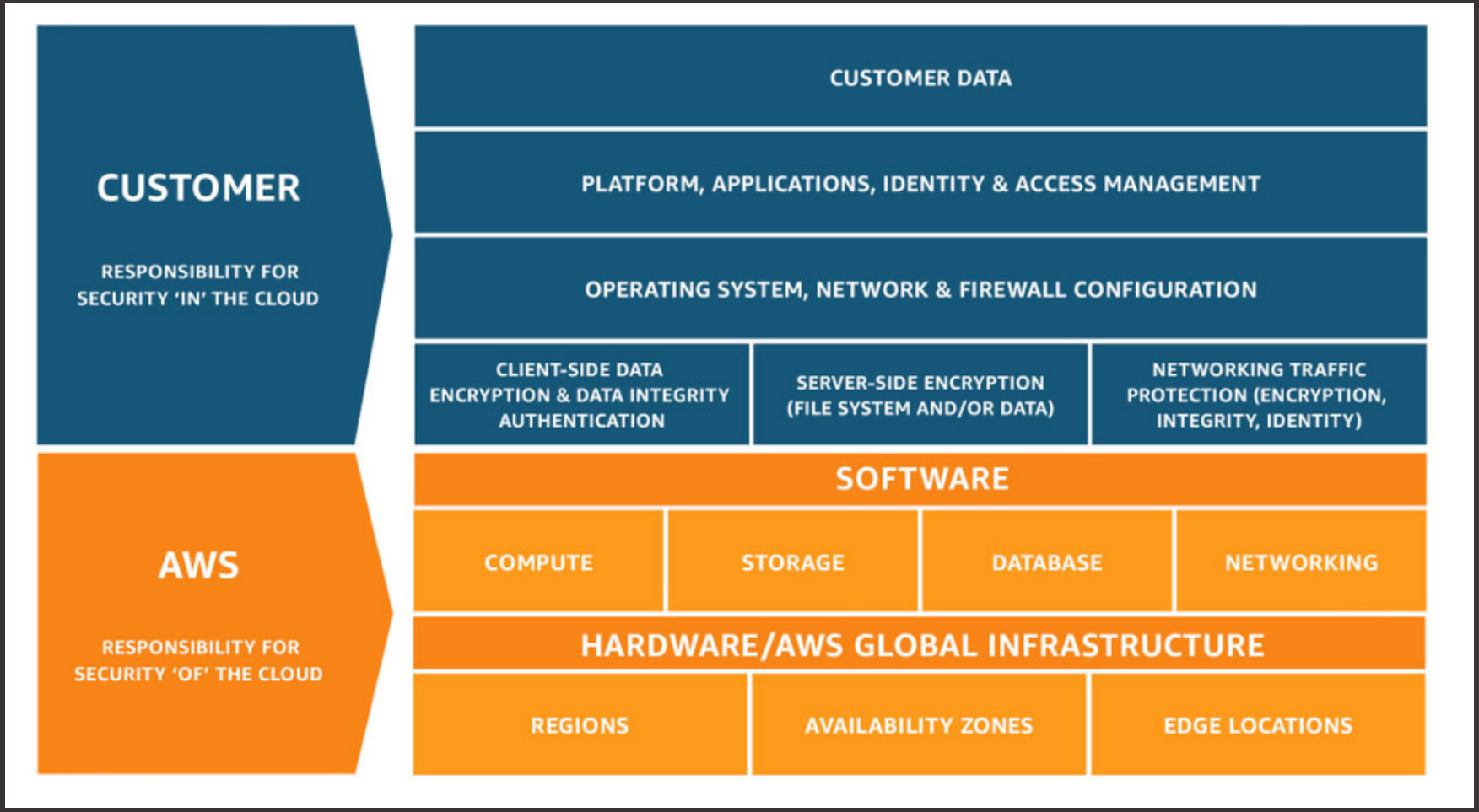
The Vulnerability Aspect

RUNNING IN AWS ALONE, HOWEVER, IS NOT ENOUGH TO PROTECT THE SYSTEMS FROM RANSOMWARE OR OTHER CYBERSECURITY THREATS.

USER RETAINS THE RESPONSIBILITY FOR SECURING THE ASPECTS OF THE ENVIRONMENT ONE CONTROLS IT. (CONCEPT OF AWS SHARED RESPONSIBILITY MODEL)

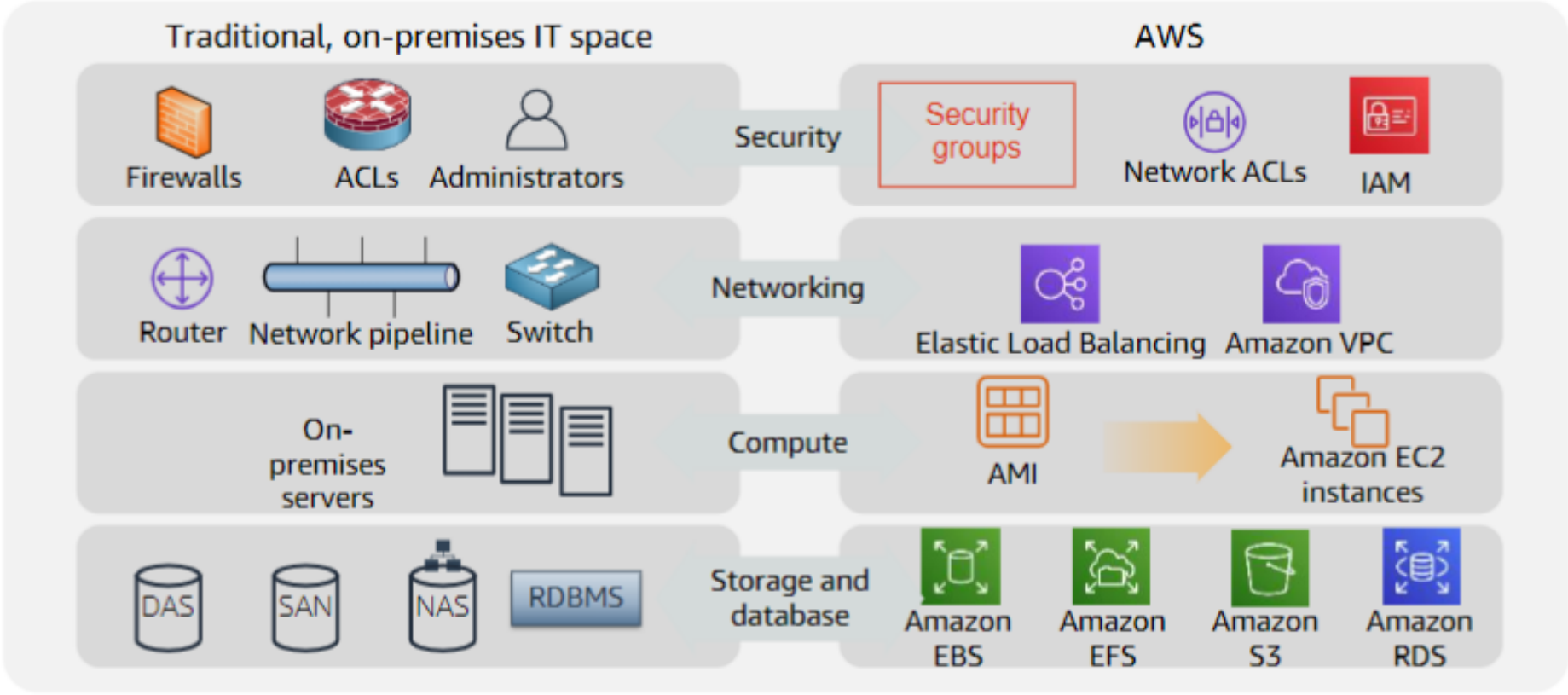
AWS PROVIDES USERS WITH A ROBUST SET OF TOOLS TO KEEP THEIR ENVIRONMENT SECURE AT SCALE. IN THIS PROJECT WE WILL EXPLORE HOW SOME OF THESE TOOLS CAN ENHANCE OUR ABILITY TO PROTECT AGAINST RANSOMWARE, DETECT MALICIOUS ACTIVITY, AND RESPOND TO MALICIOUS ACTIVITY IF IT IS DETECTED.

Concept of Shared Responsibility Model in AWS



The Comparison

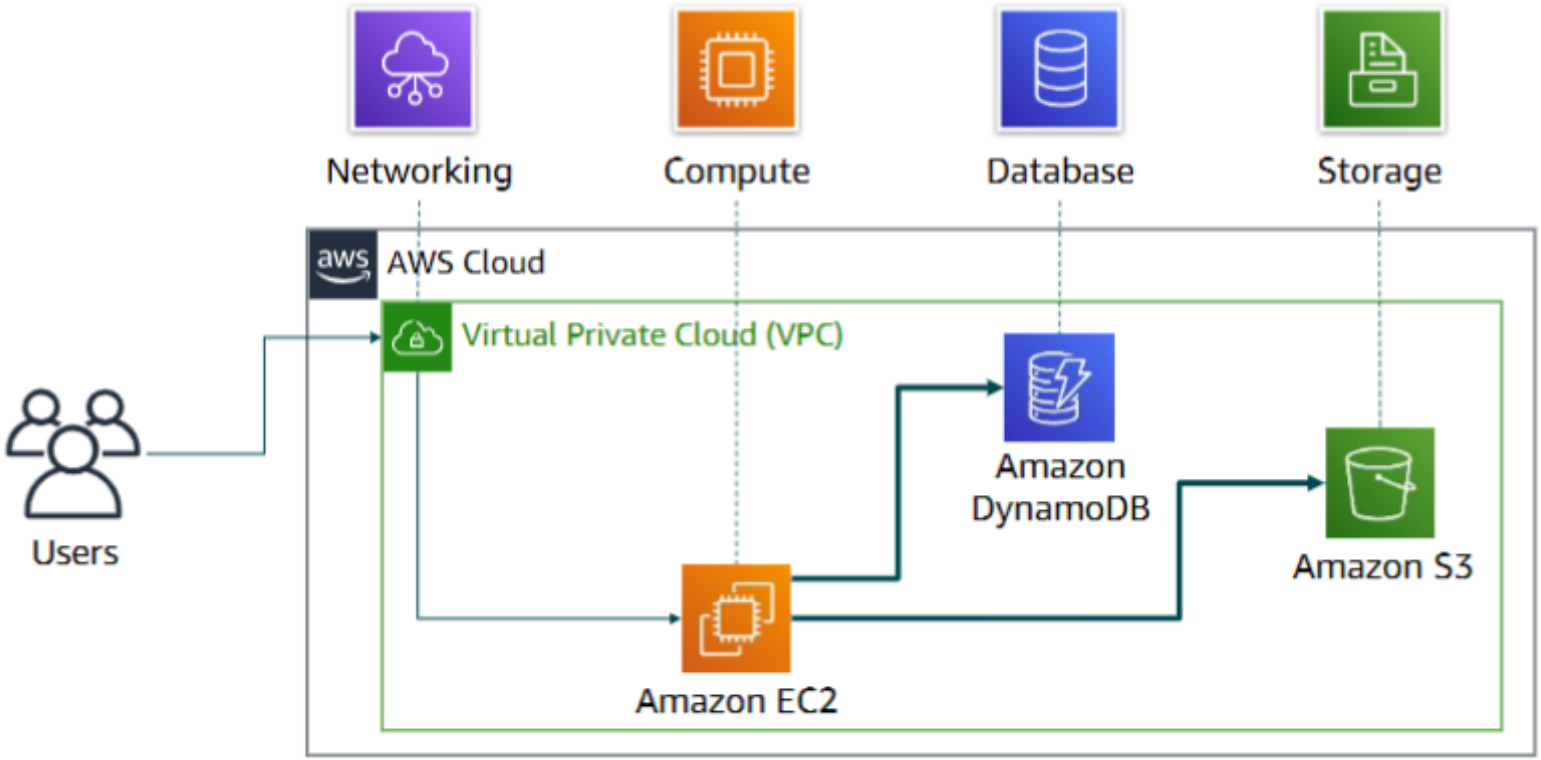
Similarities between AWS and traditional IT



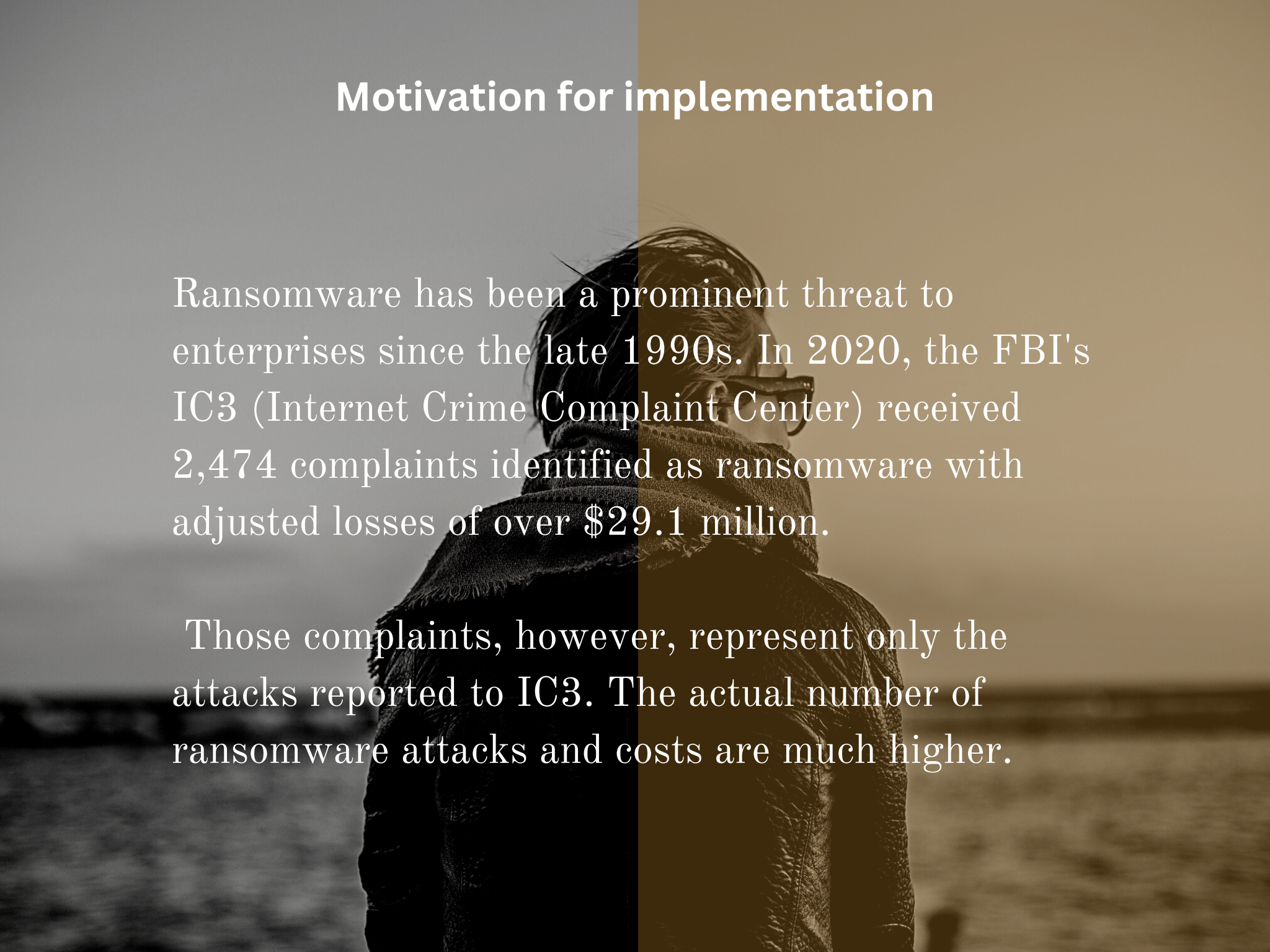
aws

A Simple Architecture

Simple solution example



Motivation for implementation



Ransomware has been a prominent threat to enterprises since the late 1990s. In 2020, the FBI's IC3 (Internet Crime Complaint Center) received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million.

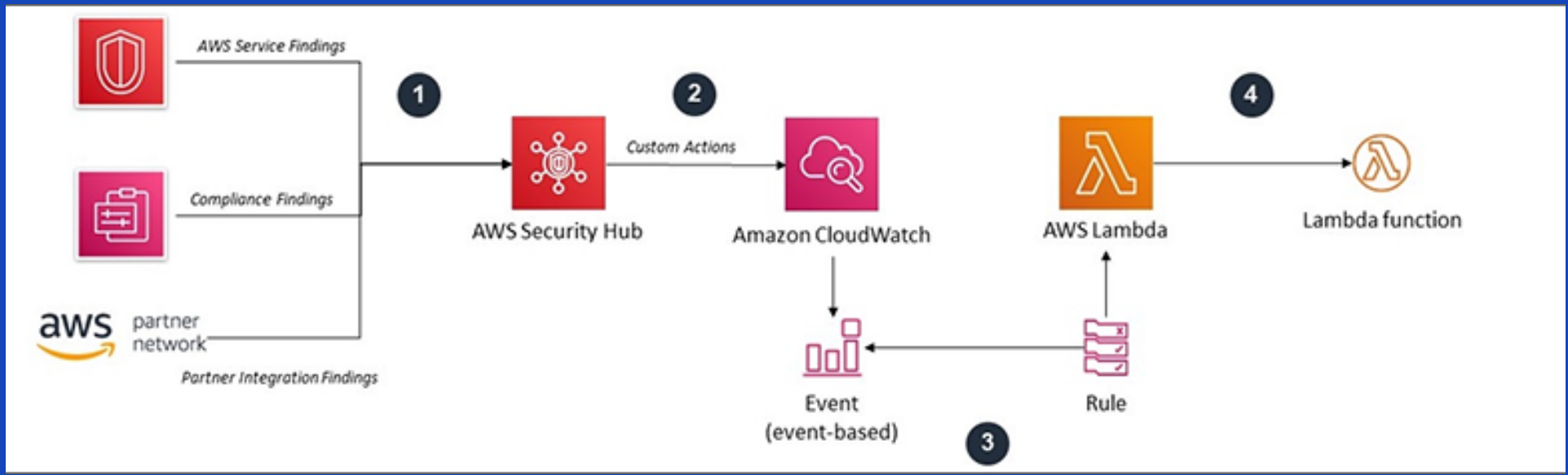
Those complaints, however, represent only the attacks reported to IC3. The actual number of ransomware attacks and costs are much higher.

Cloud security at AWS is the highest priority. AWS has technology that helps customers protect and recover their systems from ransomware attacks, including services and features that provide infrastructure and data backups, the AWS-Well Architected Tool, and strong security controls using AWS security services.

AWS Services to be Used

AWS Security Hub

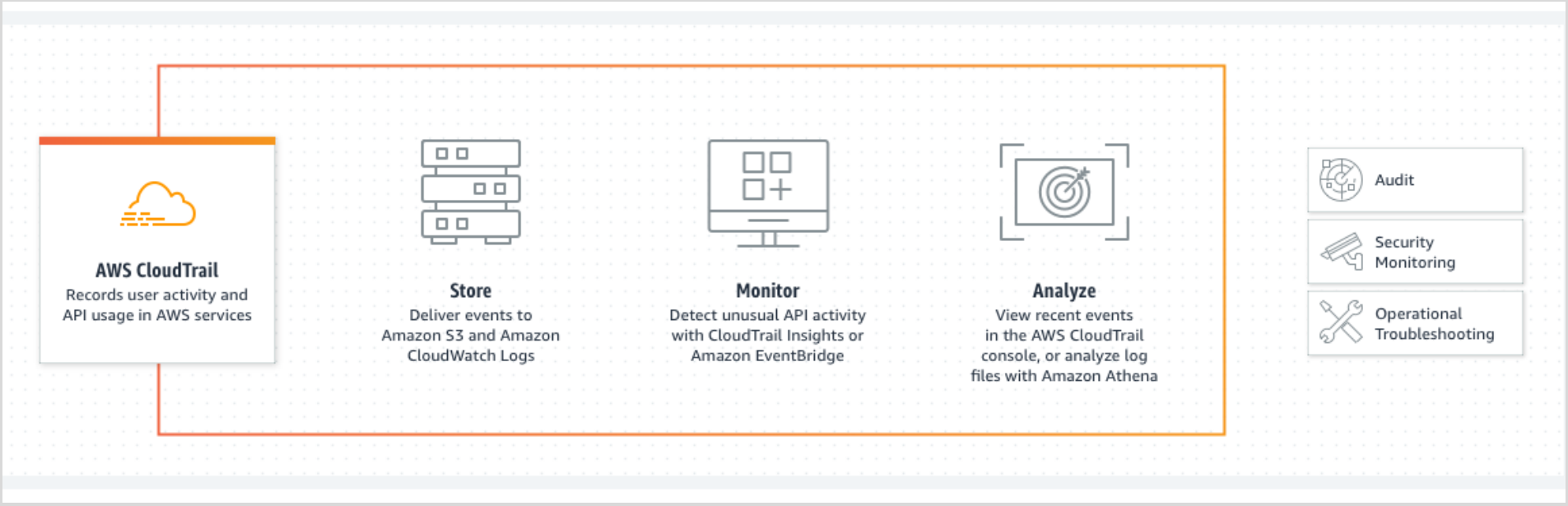
→ Automates Response and Remediation.



AWS CLOUDTRAIL

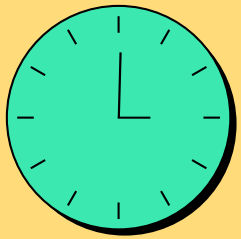
TRACKS USER ACTIVITY AND API USAGE

AWS CLOUDTRAIL MONITORS AND RECORDS ACCOUNT ACTIVITY ACROSS YOUR AWS INFRASTRUCTURE, GIVING YOU CONTROL OVER STORAGE, ANALYSIS, AND REMEDIATION ACTIONS.



AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)

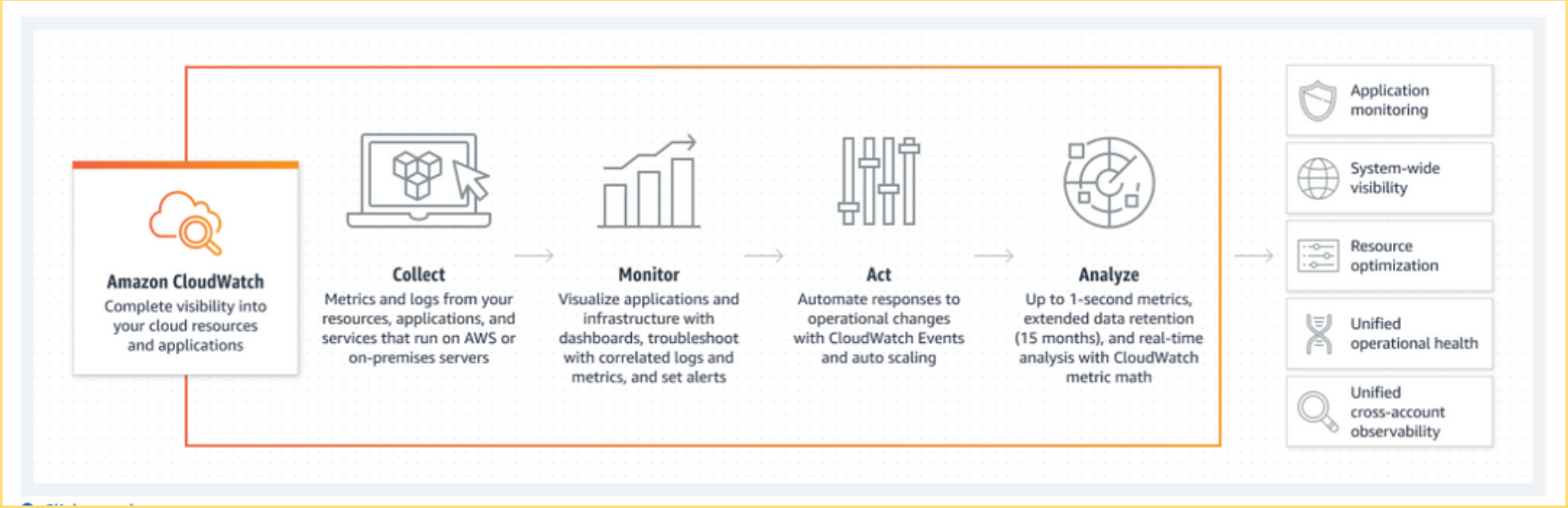
AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC) GIVES FULL CONTROL OVER OUR VIRTUAL NETWORKING ENVIRONMENT, INCLUDING RESOURCE PLACEMENT, CONNECTIVITY, AND SECURITY.



AMAZON CLOUDWATCH

IT OBSERVES AND MONITORS RESOURCES AND APPLICATIONS ON AWS, ON-PREMISES, AND ON OTHER CLOUDS.

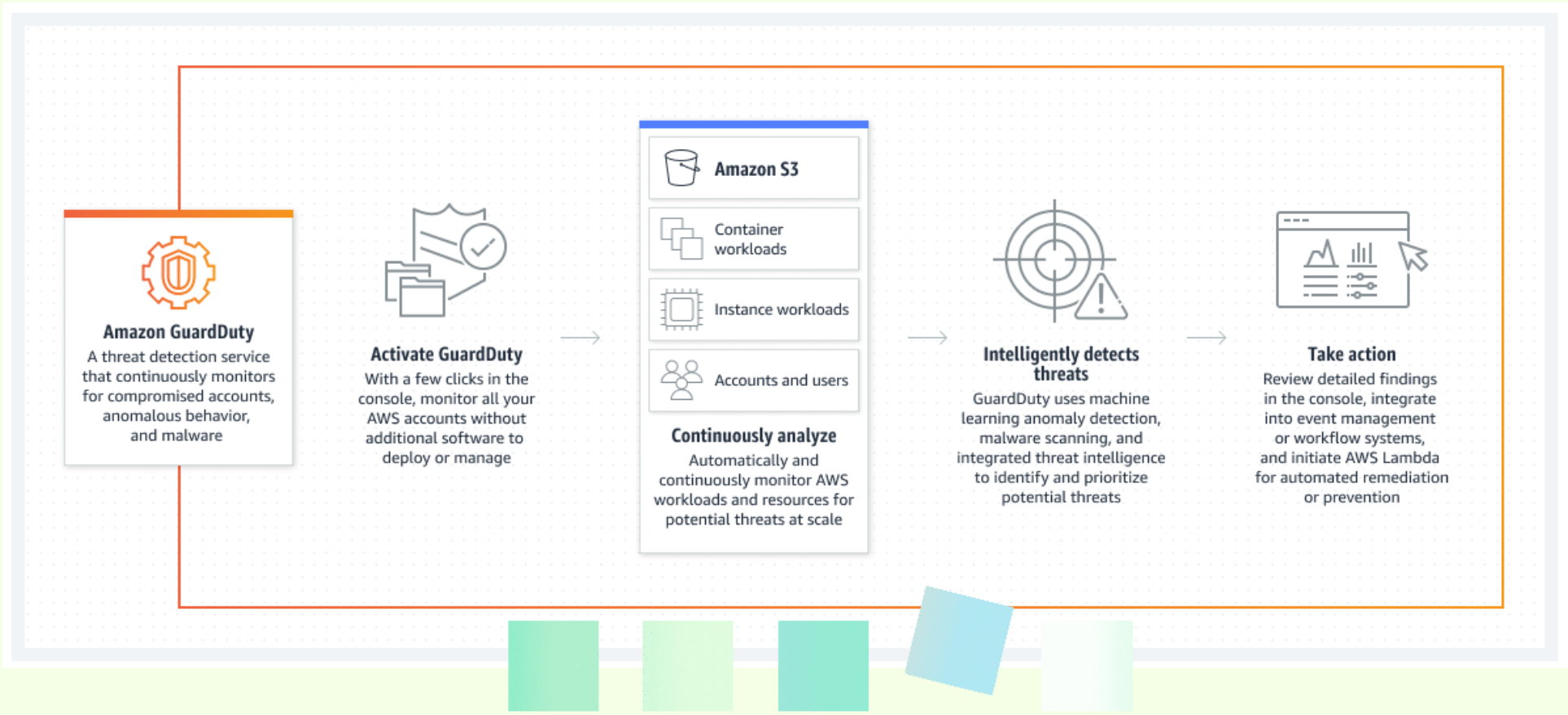
AMAZON CLOUDWATCH COLLECTS AND VISUALIZES REAL-TIME LOGS, METRICS, AND EVENT DATA IN AUTOMATED DASHBOARDS TO STREAMLINE OUR INFRASTRUCTURE AND APPLICATION MAINTENANCE.



AMAZON GUARDDUTY

IT PROTECTS AWS ACCOUNTS WITH INTELLIGENT THREAT DETECTION.

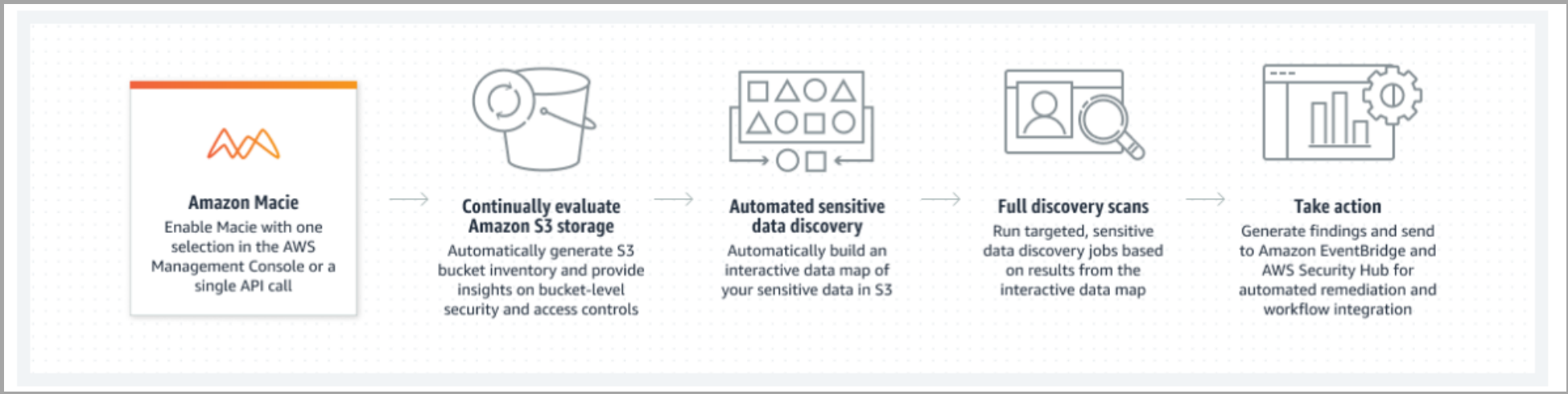
AMAZON GUARDDUTY IS A THREAT DETECTION SERVICE THAT CONTINUOUSLY MONITORS YOUR AWS ACCOUNTS AND WORKLOADS FOR MALICIOUS ACTIVITY AND DELIVERS DETAILED SECURITY FINDINGS FOR VISIBILITY AND REMEDIATION.



AMAZON MACIE

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE

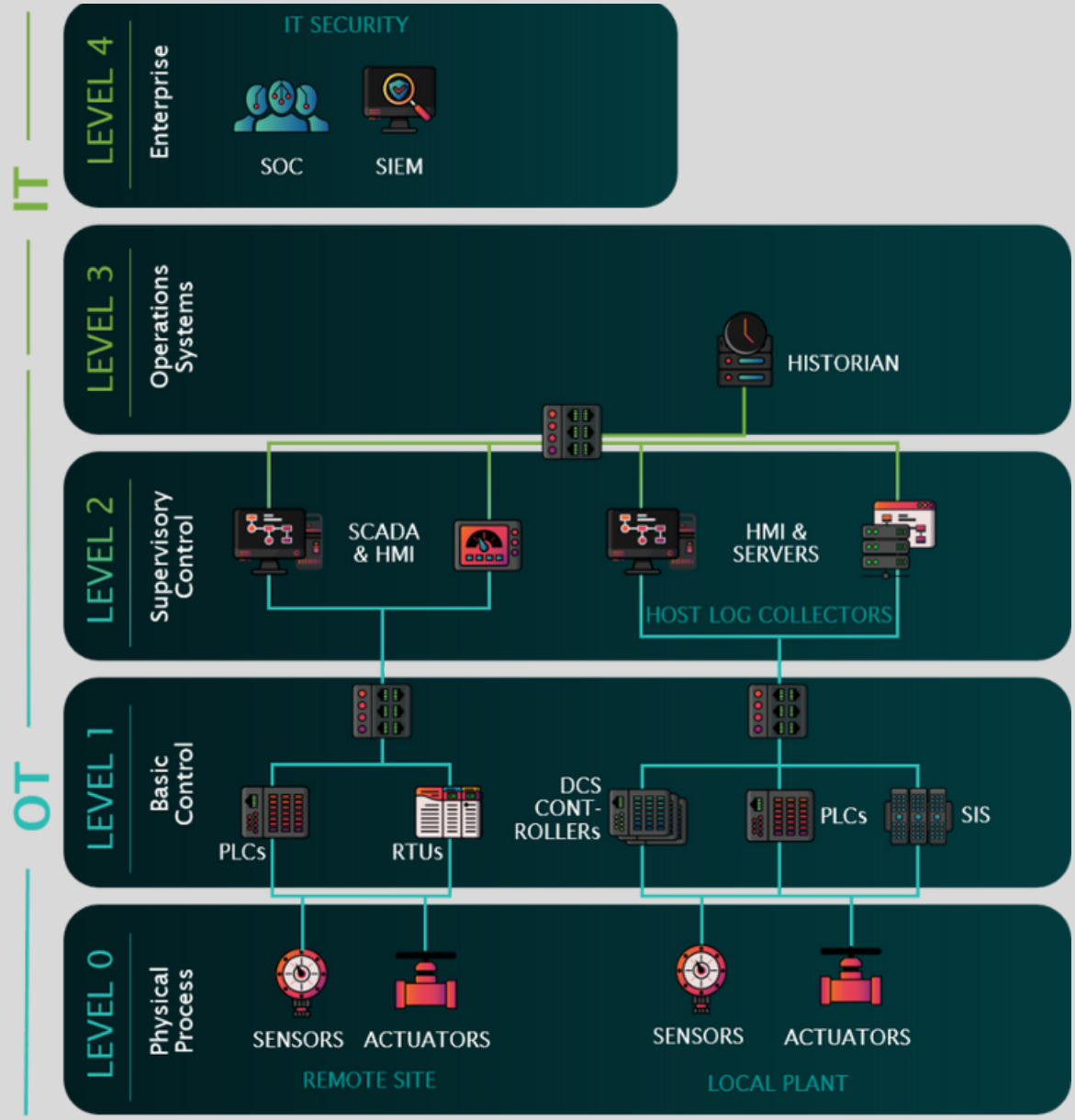
AMAZON MACIE IS A DATA SECURITY AND DATA PRIVACY SERVICE THAT USES MACHINE LEARNING (ML) AND PATTERN MATCHING TO DISCOVER AND PROTECT YOUR SENSITIVE DATA.



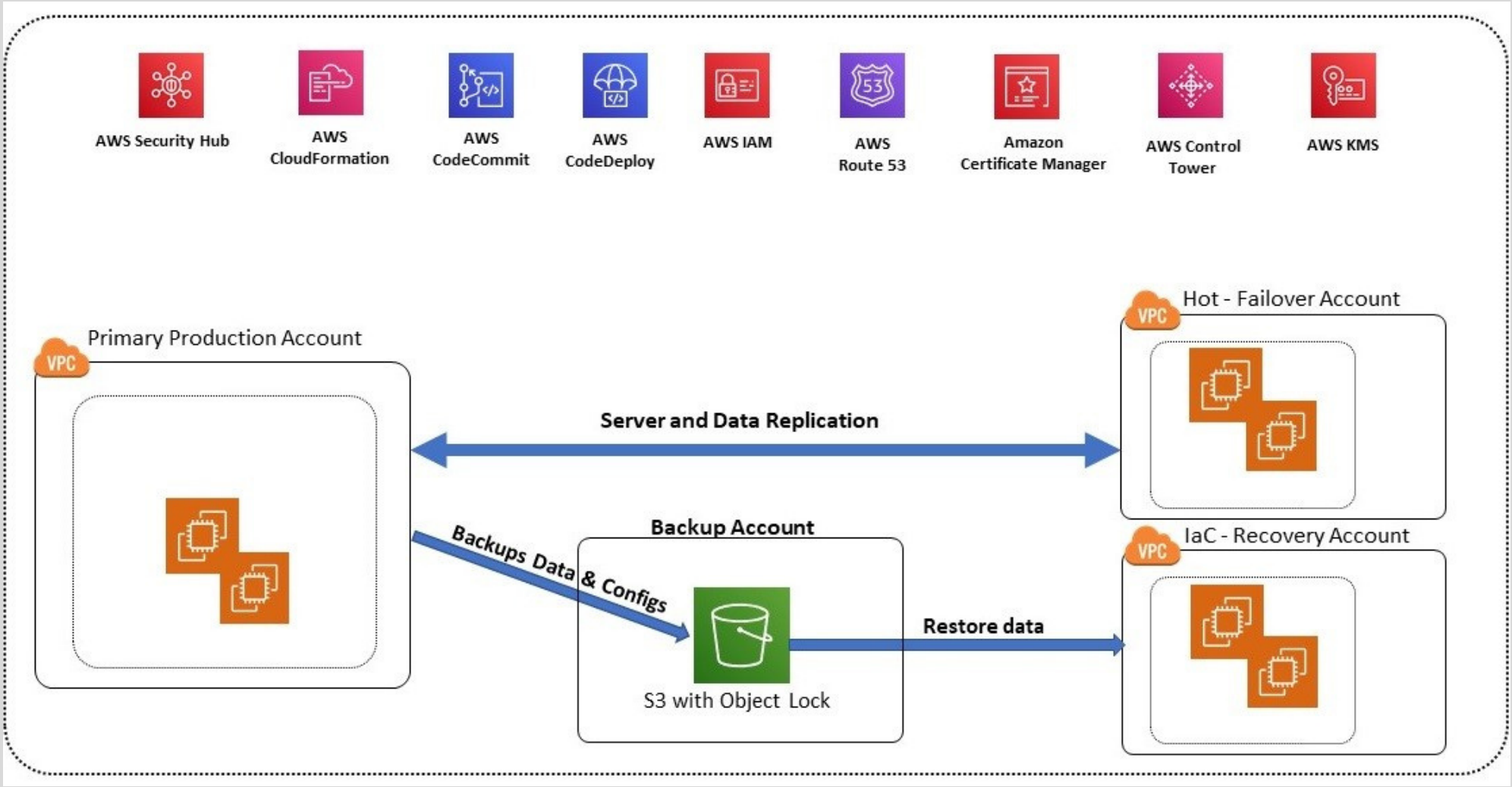
Security and compliance resources

- AWS Security Reference Architecture (AWS SRA)
- The European Union Agency for Cybersecurity (ENISA)
- U.S. Cybersecurity & Infrastructure Security Agency (CISA)

How energy and utility companies can recover from ransomware and other disasters using infrastructure as code on AWS



Infrastructure as a code recovery view



USEFUL LINKS

SECURING YOUR AWS CLOUD ENVIRONMENT FROM RANSOMWARE

HTTPS://D1.AWSSTATIC.COM/WWPS/PDF/AWSPS_RANSOMWARE_EBOOK_APR-2020.PDF

RANSOMWARE RECOVERY

AWS ELASTIC DISASTER RECOVERY | RANSOMWARE RECOVERY | AWS (AMAZON.COM)

BEST PRACTICES FOR SECURITY, IDENTITY, & COMPLIANCE

SECURITY, IDENTITY & COMPLIANCE | AWS ARCHITECTURE CENTER (AMAZON.COM)

AWS SECURITY INCIDENTRESPONSE GUIDE

HTTPS://D1.AWSSTATIC.COM/WHITEPAPERS/AWS_SECURITY_INCIDENT_RESPONSE.PDF

CLASSIC INTRUSION ANALYSIS FRAMEWORKS FOR AWS ENVIRONMENTS: APPLICATION AND ENHANCEMENT

CLASSIC INTRUSION ANALYSIS FRAMEWORKS FOR AWS ENVIRONMENTS: APPLICATION AND ENHANCEMENT - AWS WHITEPAPERS (AMAZON.COM)

REFERENCES

Base paper

https://aws.amazon.com/blogs/apn/protect-detect-and-respond-to-ransomware-with-presidios-ransomware-mitigation-kit/

AWS White Paper

Security Pillar - AWS Well-Architected Framework - Security Pillar (amazon.com)


THANK YOU!