

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC214-L

What we can learn from customers: Accelerating innovation at AWS Security

CJ Moses

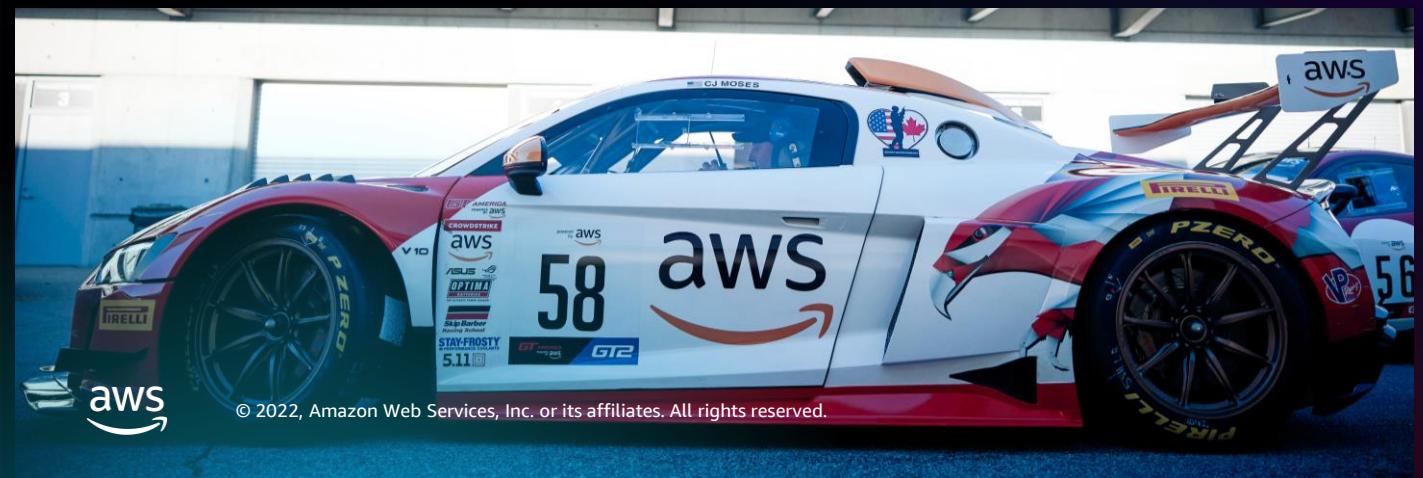
Chief Information Security Officer
Amazon Web Services



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



Every one of us
is a **builder**



aws

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

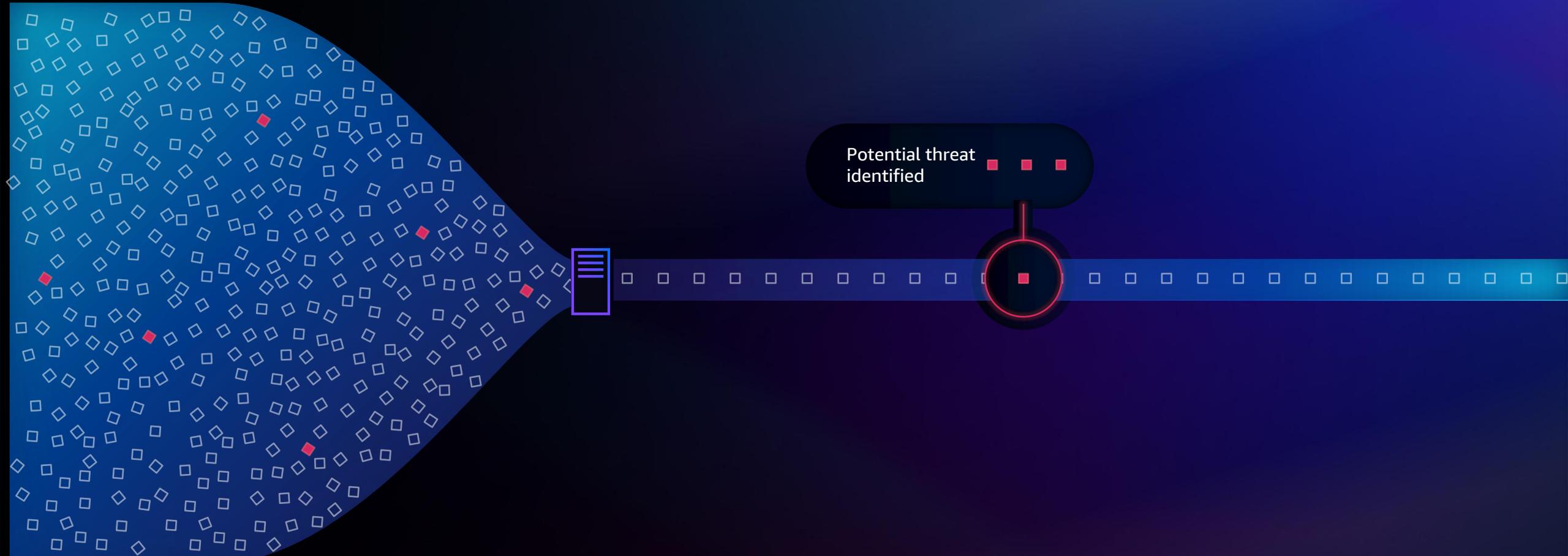
**“Customers are
always wonderfully,
beautifully unsatisfied.”**

Jeff Bezos

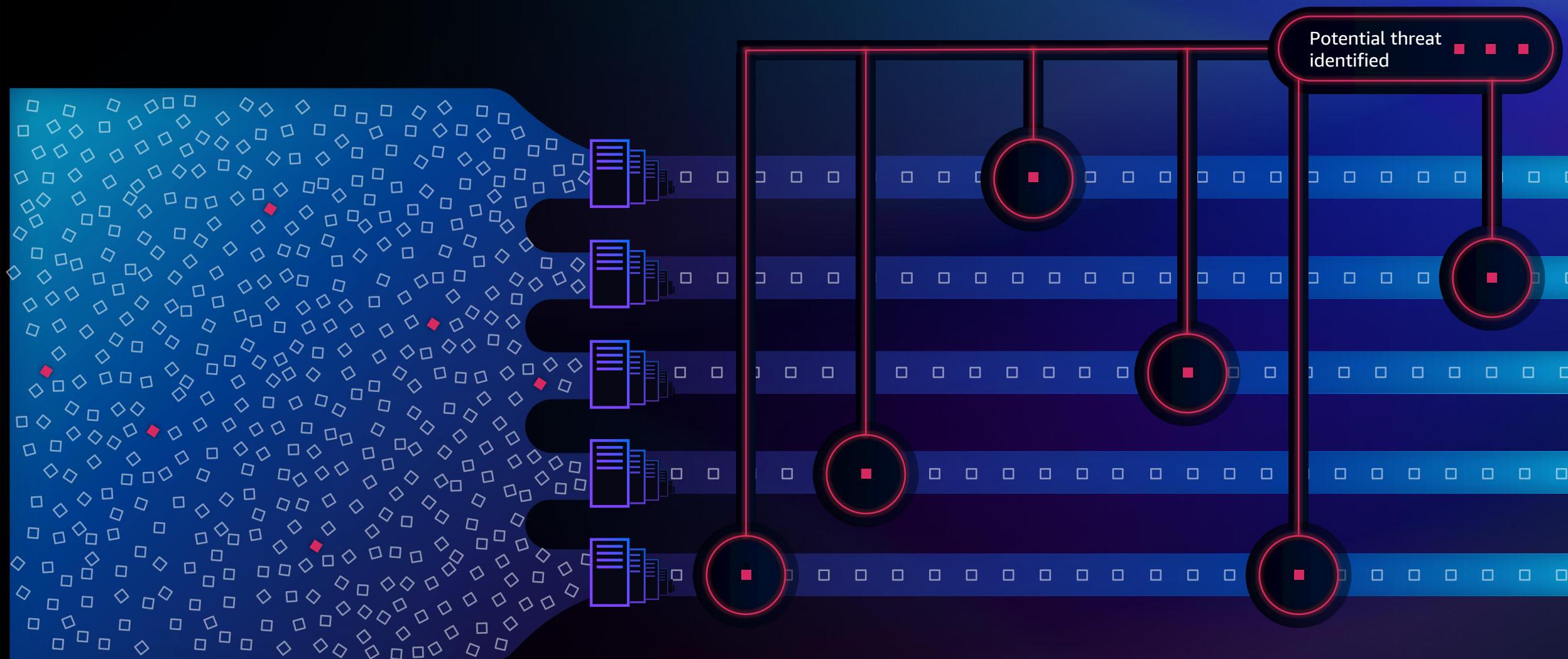


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Potential threats hiding in massive amounts of data



Threat identification at scale



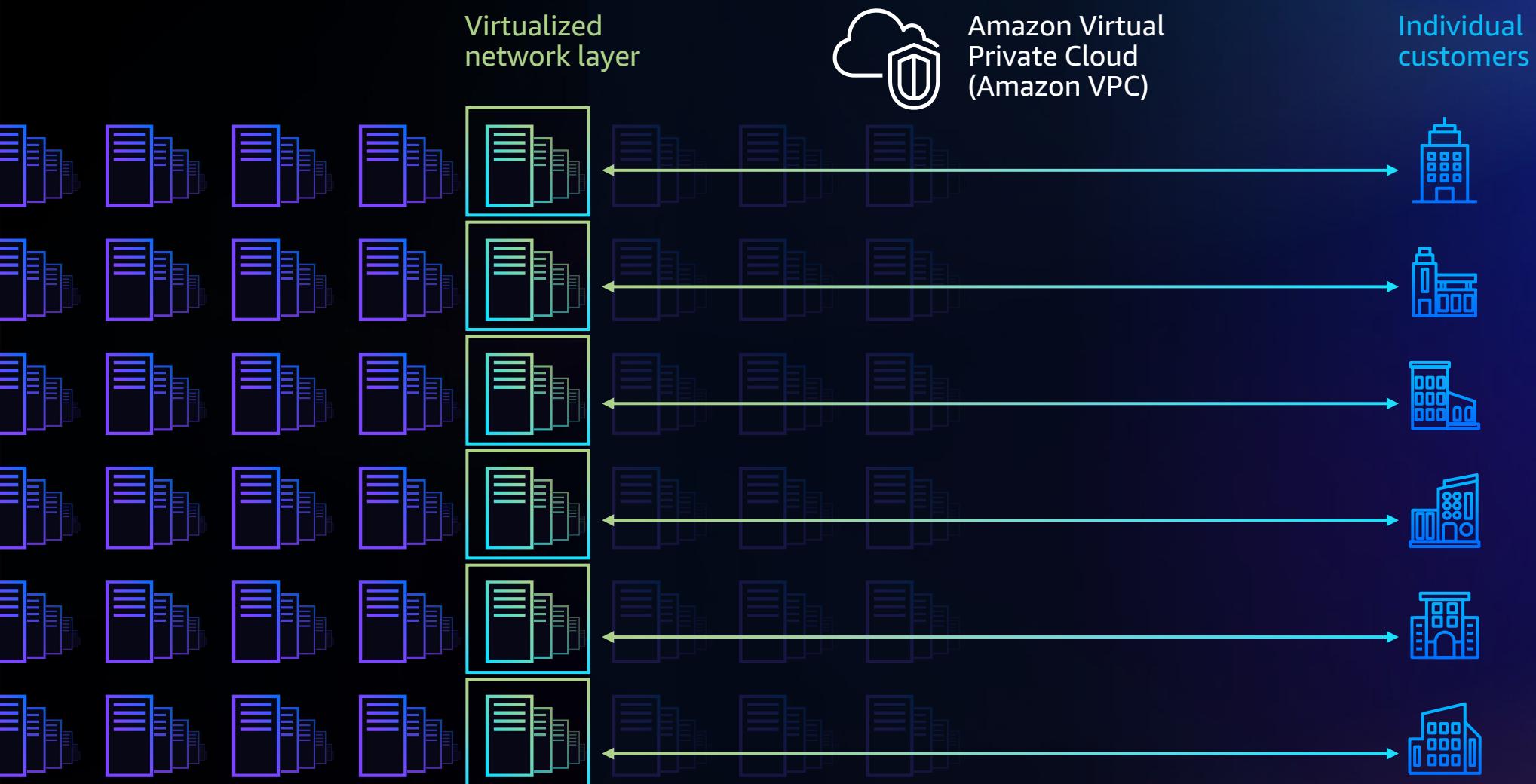
DECEMBER

2007



**“That's your space –
make it the way you want.”**





Unmatched scale and experience

200+

services

1M+

customers

\$82B

annual run rate

AWS global network

1,000,000,000,000,000



Shared responsibility model

AWS

RESPONSIBLE FOR SECURITY **OF** THE CLOUD

Software



Compute



Storage



Database



Networking

Hardware/AWS Global Infrastructure



AWS Regions



Availability Zones



Edge Locations

CUSTOMER

RESPONSIBLE FOR SECURITY **IN** THE CLOUD



Customer Data



Platform, Applications,
Identity & Access Management



Operating System,
Network & Firewall Configuration



Client-side Data
Encryption & Data
Integrity Authentication



Server-side Encryption
(File System and/
or Data)



Networking Traffic
Protection (Encryption,
Integrity, Identity)

Common threats continue to proliferate



DDoS



Threat actors



Ransomware

DDoS remains a common security threat

35%

increase of
DDoS events

256%

increase in
compromised instances

106K

DDoS attacks
prevented

Build DDoS- resilient architecture



AWS Shield

Maximize application availability
and responsiveness with
managed DDoS protection



AWS WAF

Protect your web applications
from common exploits

Threat actors are continuously deploying malware

AWS sensors processed

>224M

malware samples in six months

AWS distilled them down into

28,673

unique types of malware

Protect EC2 instances



Amazon GuardDuty

Protect your AWS accounts with
intelligent threat detection

Unintended disclosure of **security credentials**

A photograph of a man with dark hair and glasses, wearing a red button-down shirt. He is seated at a desk, looking down at a silver laptop. The background is blurred, showing what appears to be a cityscape or office environment.

Protect against unintended disclosure of credentials



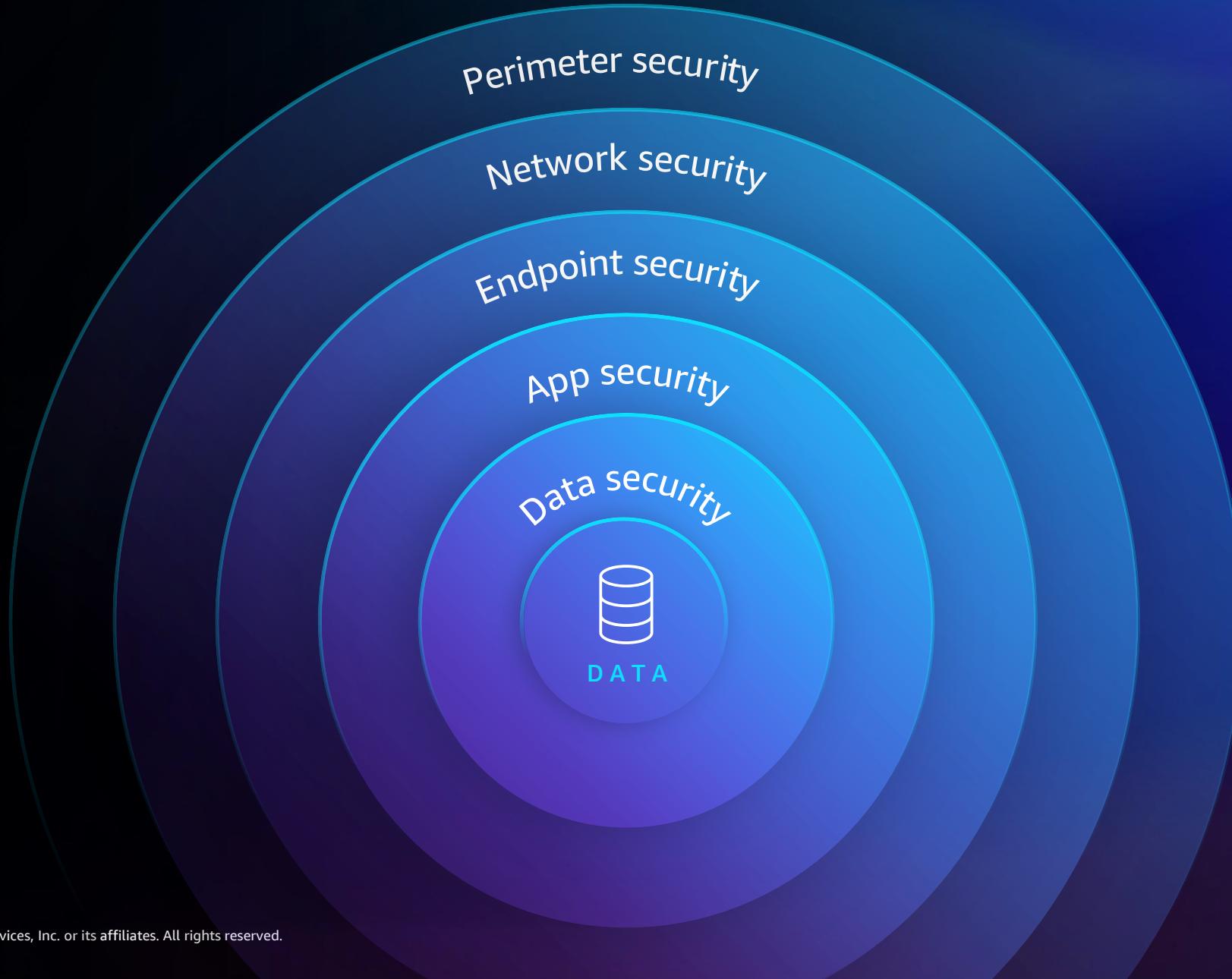
AWS IAM Identity Center

Centrally manage workforce
access to multiple AWS
accounts and applications



AWS Security Hub

Automate AWS security
checks and centralize
security alerts



Six learnings

- 1
- 2
- 3
- 4
- 5
- 6

AS AWS CISO



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

1

Educate **everyone**
about security



2

Security-first culture

Product Managers



C-Suite



Developers



Business Leaders



Front-Office Employees



A photograph of a man and a woman looking down at a tablet device. The man, on the left, has dark hair and a beard, wearing a blue button-down shirt. The woman, on the right, has long dark hair and is wearing a blue and white striped shirt. They are both focused on the screen of the tablet.

3

Hire and develop
the best

4



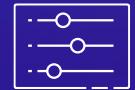
Ideation



Architecting



Coding



Testing



Security review



Production

Shift left and automate

4



Ideation



Architecting



Coding



Testing



Production

Shift left and automate

5

Invest in a **dynamic workforce**



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

6

Make security the
department of
“yes, and...”

Six learnings

AS AWS CISO

1

Educate **everyone** about security

2

Security-first culture

3

Hire and develop **the best**

4

Shift left and automate

5

Invest in a **dynamic workforce**

6

Make security the department of "**yes, and...**"

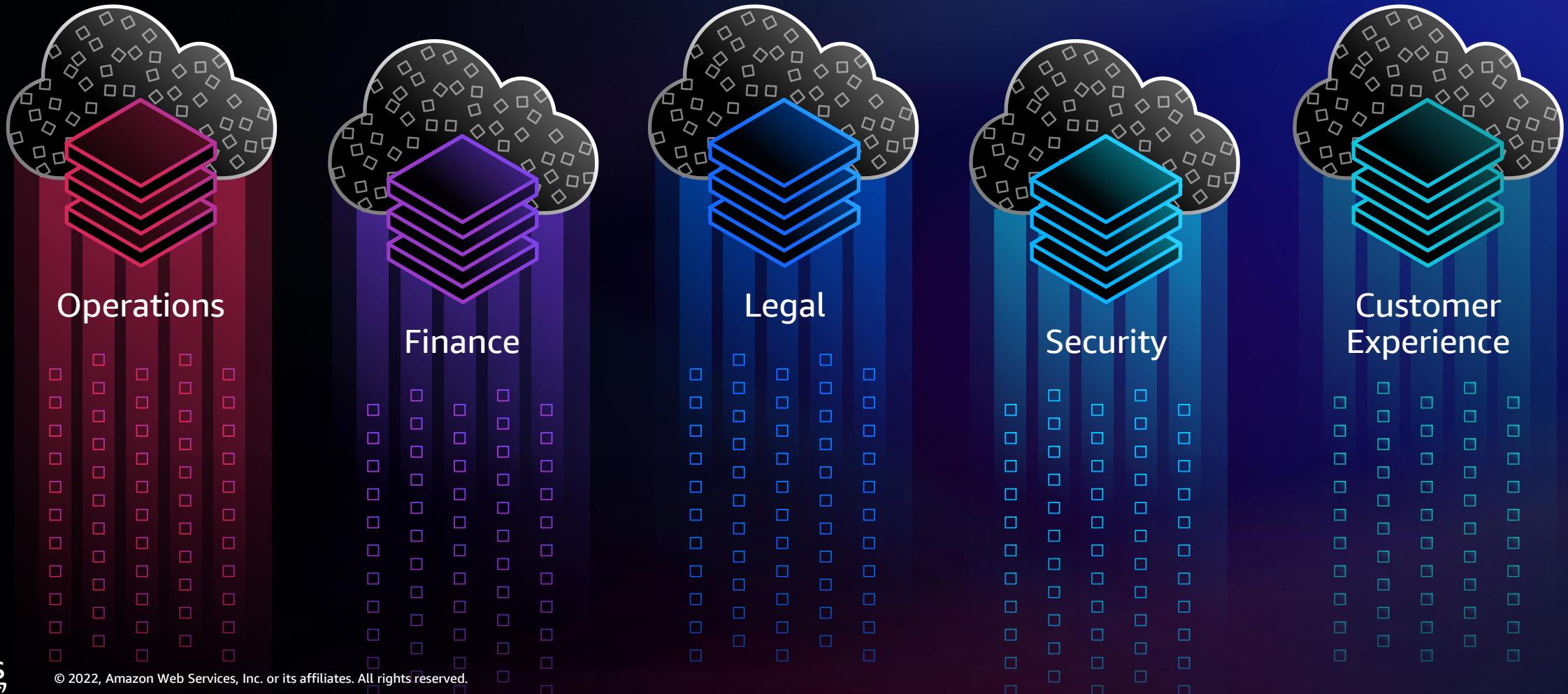
Predictions for 2023

THE OUTLOOK FOR NEXT YEAR



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

Increasing threats continue to drive the shift to the cloud



NEW

Amazon Security Lake

PREVIEW AVAILABLE TODAY



Analyze data using your preferred analytics tools while retaining control and ownership of your security data



Centralize data from cloud, on-premises, and custom security sources across accounts and Regions



Normalize data to an industry standard to easily share and use with multiple analytics tools



Optimize and manage security data for more efficient storage and query performance

A photograph of four diverse women laughing together while looking at a tablet. They are all smiling and appear to be in a casual, friendly environment. The woman in the center-right is wearing glasses and a light-colored button-down shirt, holding a tablet. The woman to her right has dark hair in braids and is resting her chin on her hand. The woman to her left is wearing a white top and has her arm around the center woman. The woman on the far left is partially visible, wearing glasses and a dark patterned top.

The growing need for **security professionals**



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

Automation in cloud security



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



```
private void defaultCommunityIndexStrategy(
    CommunityRepository communityIndexRepository,
    CommunityIndexer communityIndexer,
    CommunityDocumentPopulator communityDocumentPopulator,
    CommunityService communityService,
    DefaultCommunityIndexStrategy strategy
) {
    this.communityIndexRepository = communityIndexRepository;
    this.communityIndexer = communityIndexer;
    this.communityDocumentPopulator = communityDocumentPopulator;
    this.communityService = communityService;
    this.strategy = strategy;
}

@Override
public void defaultCommunityIndexStrategy(
    CommunityRepository communityIndexRepository,
    CommunityIndexer communityIndexer,
    CommunityDocumentPopulator communityDocumentPopulator,
    CommunityService communityService,
    DefaultCommunityIndexStrategy strategy
) {
    this.communityIndexRepository = communityIndexRepository;
    this.communityIndexer = communityIndexer;
    this.communityDocumentPopulator = communityDocumentPopulator;
    this.communityService = communityService;
    this.strategy = strategy;
}

@Override
public void collectDocuments(Collection<Community> communities) {
    Collection<Community> documents = communities.stream()
        .map(communityIndexer::index)
        .collect(Collectors.toList());
    documents.forEach(document -> communityDocumentPopulator.convert(CommunityDocument.of(document), community));
    communityIndexRepository.updateIndex();
}

@Override
public Collection<Community> searchCommunityByQuery(
    String query,
    Collection<Community> documents = communityIndexRepository.getDocuments()
) {
    List<Community> result = new ArrayList();
    documents.stream().filter(document -> communityIndexer.isMatch(query, document))
        .forEach(result::add);
    return result;
}

@Override
public void searchCommunityByQuery(
    String query,
    Collection<Community> documents = communityIndexRepository.getDocuments()
) {
    documents.stream().filter(document -> communityIndexer.isMatch(query, document))
        .forEach(result -> communityDocumentPopulator.convert(CommunityDocument.of(result), community));
}
```

```
package com.ds.ucd.be.before.solr;

import ...

public final class LocationUtils {

    /**
     * Parses Point from it's String representation.
     * @param locationString - String that represents location, as 2 double values split with coma. Accepts space after/before comma.
     * @return org.springframework.data.solr.core.geo.Point instance
     */
    public static Point parseLocation(String locationString) {
        Preconditions.checkNotNull(locationString, errorMessage: "Location String should not be null");
        Preconditions.checkArgument(locationString.contains(","), errorMessage: "Location must be split with coma");
        locationString = locationString.trim();

        if (locationString.contains(" ,")) {
            locationString = locationString.replaceAll(regex: " ,", replacement: ",");
        }

        if (locationString.contains(", ")) {
            locationString = locationString.replaceAll(regex: ", ", replacement: ",");
        }

        String[] location = locationString.split(regex: ",");
        Preconditions.checkArgument(expression: location.length >= 2, errorMessage: "Location should consist at least 2 Double parameters");
        double lat = Double.parseDouble(location[0]);
        double lon = Double.parseDouble(location[1]);

        return new Point(lat, lon);
    }
}
```

In 2020, we created
1.7 megabytes
of data every second

150 exabytes

of data has traversed the internet since its **creation**





By **2026, we will have tripled** that amount to

463 exabytes

NEW

Amazon Macie introduces automated data discovery

GENERALLY AVAILABLE TODAY



Discover and protect your sensitive data at scale



Gain cost-efficient visibility into sensitive data stored in Amazon S3, with one click



Use the interactive S3 data map to continually strengthen your data security posture



Reduce triage time with actionable reporting of sensitive data and sensitivity score for each bucket

Interactive data map



NEW

External Key Store (XKS) for AWS KMS

GENERALLY AVAILABLE TODAY



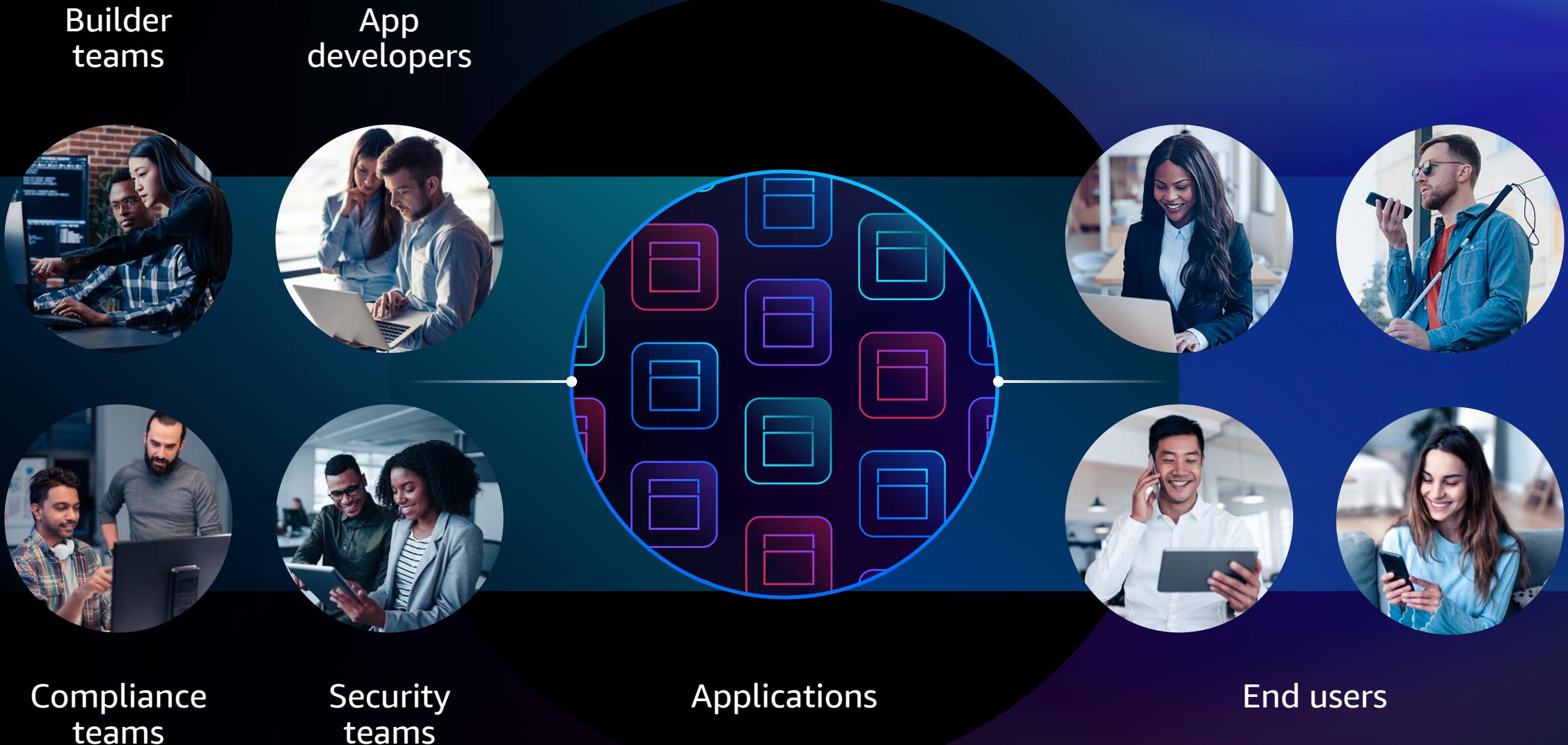
Protect your data with encryption keys stored in an external key management system



Provides the ability to externally track and control every cloud encrypt and decrypt request



Works with over 100 AWS services



Amazon Verified Permissions

NEW

PREVIEW AVAILABLE TODAY



Accelerate application development by decoupling authorization from business logic in your application



Save time and resources with centralized permissions and policy lifecycle management



Simplify compliance audits at scale using automated analysis to confirm permissions work as intended



Build applications that support Zero Trust architectures with dynamic, real-time authorization decisions

A close-up photograph of a person's hands typing on a laptop keyboard. The person is wearing a light blue ribbed sweater. In the background, there is a blurred view of a window with a cityscape, a white mug, and some papers on a desk.

Multimodal forms of authentication

NEW

Multiple MFA for AWS Identity and Access Management (IAM)

GENERALLY AVAILABLE TODAY



Add up to 8 MFA devices to AWS account root users and IAM users



Raise the security bar and limit access management to highly privileged principals

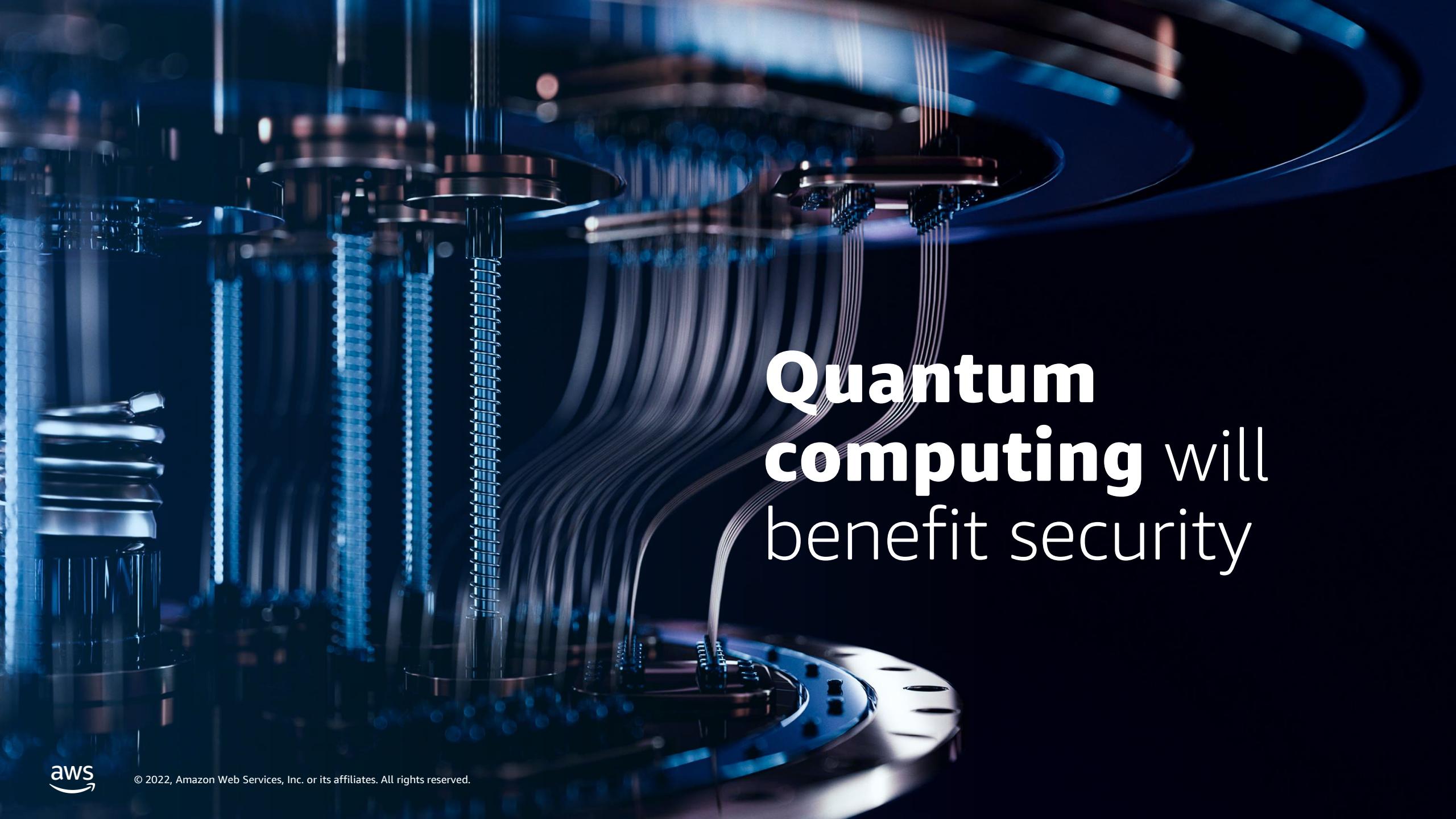


Use multiple types of MFA methods to secure your organization



Free MFA keys

BOOTH 1335 IN THE VILLAGE



**Quantum
computing will
benefit security**

Hybrid post-quantum key agreement

Working on post-quantum standards within
the Internet Engineering Task Force



Fireside chat

CJ Moses

Chief Information Security Officer
Amazon Web Services

Deneen DeFiore

Chief Information Security Officer
United Airlines





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

Thank you!

CJ Moses

Chief Information Security Officer
Amazon Web Services

Deneen DeFiore

Chief Information Security Officer
United Airlines



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