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

SEC327

Zero-privilege operations: Running services without access to data

Colm MacCárthaigh

VP/Distinguished Engineer
Amazon Web Services

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

“Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.”

Jerome Saltzer

Communications of the ACM, 1974

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

The era of broad access is dead

1970s – 2010s	2010s –
A common industry norm for trusted system administrators and support personnel to have broad access	Recognition from customers, regulators, and compliance authorities that access must be limited to what is truly needed
Coarse-grained permissions	Fine-grained permissions, especially on the cloud
Encryption was not pervasive	Pervasive encryption is accessible

aws

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

Zero-privilege operations

Limit access to absolute least privilege needed – **zero**

Rethink access controls to limit human and system privileges

Provide a workable approach to capture goals and measure progress

Lower the costs and barriers to entry for increased security

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

Calling AWS Support

We love to help people

AWS Support can’t access your EC2 Instances, or your data

Customers have to explicitly grant access



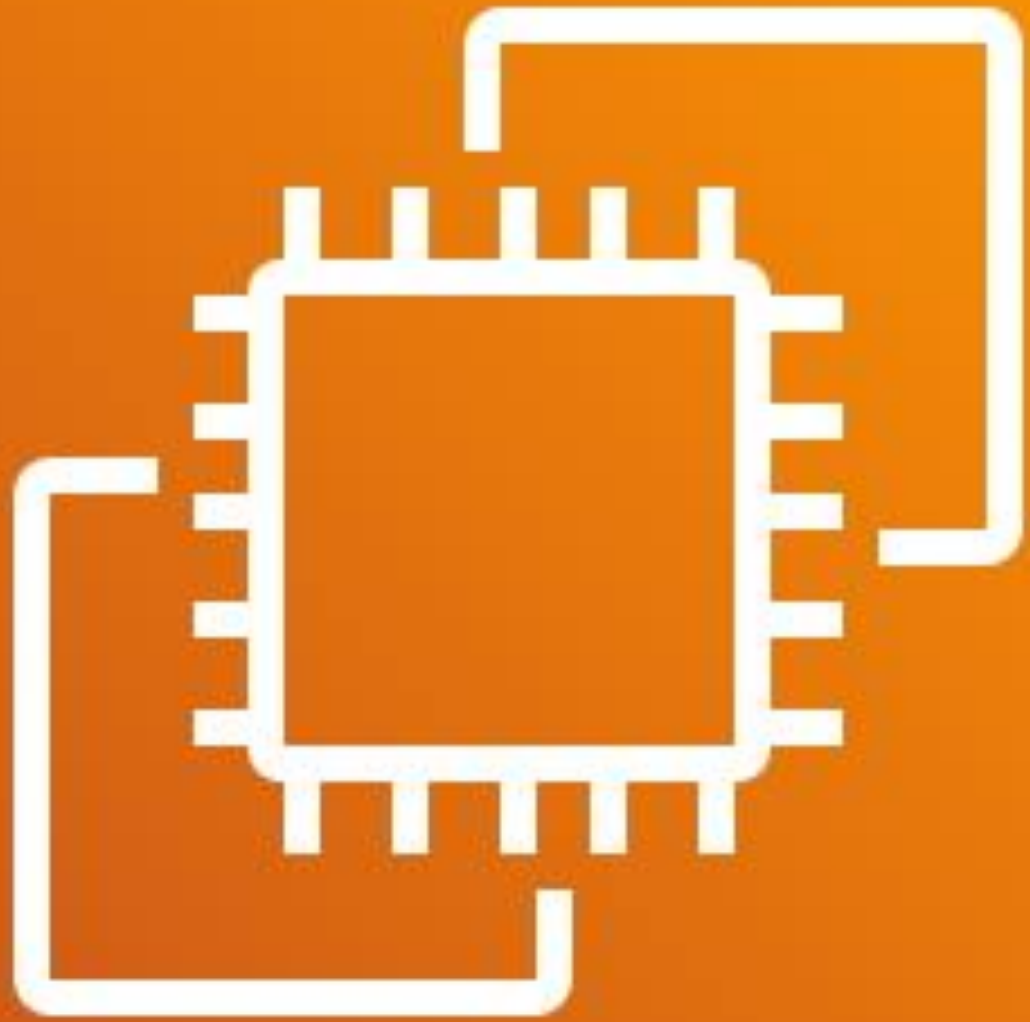
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operating EC2 Nitro

Amazon EC2 developers and operators have no access to EC2 Nitro Instance Memory

Seniority and tenure make no difference

Applies even to diagnostic and debugging operations



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

Customer data is radioactive to us

We never want to see or touch it directly

We build shielding so that we can’t see or touch it directly

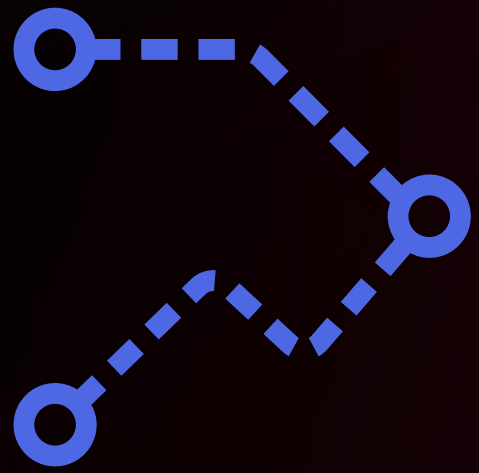
We give customers many of the same tools, for their customer data



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

Disclaimers

Compliance is a journey, the AWS compliance team can help you with yours



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

Disclaimers

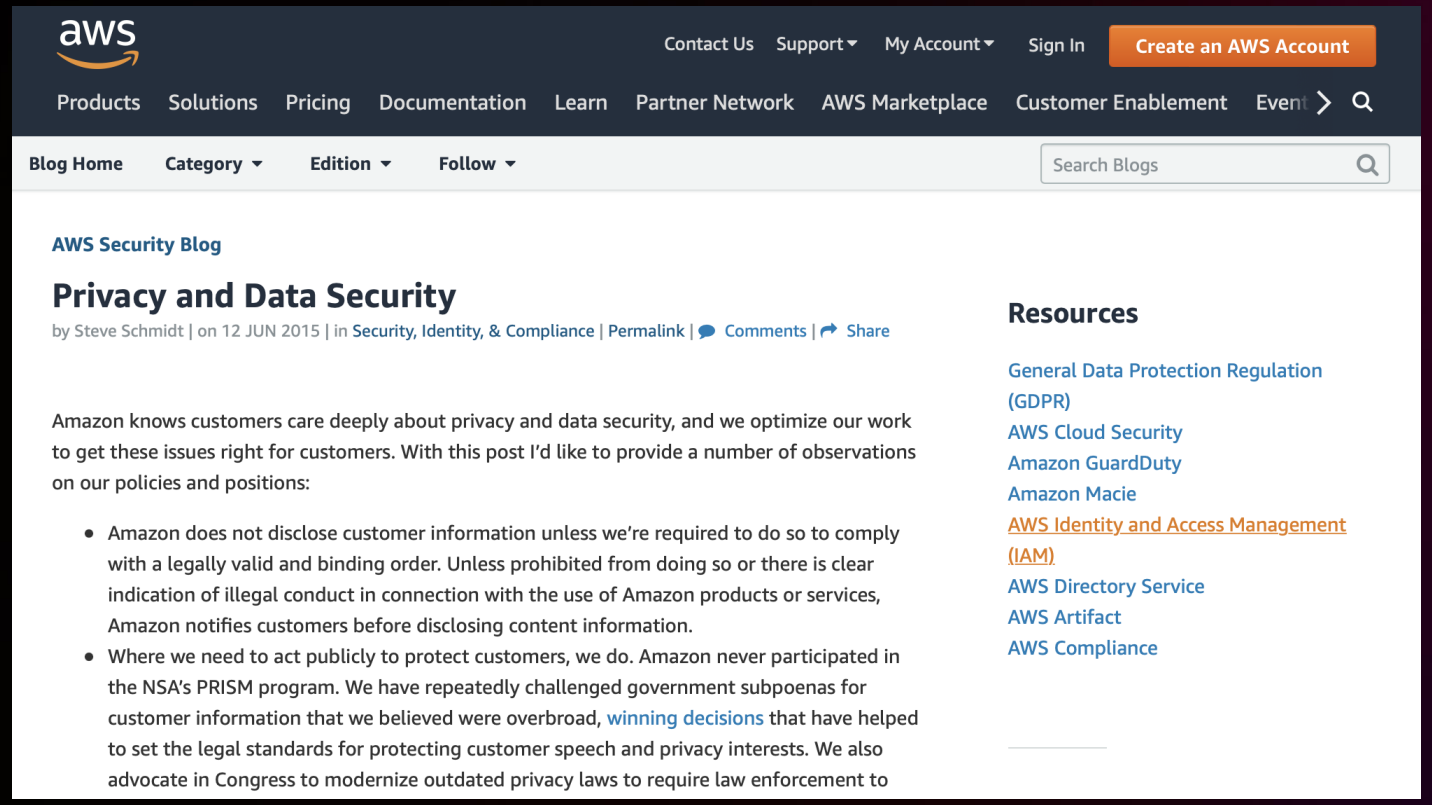
This talk includes several movie-plot threat models.



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

Disclaimers

See our CISO posts and our Data Privacy Center for more.



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

How do we host data?

Constantly raise the bar for the principle of least privilege

Integrate access auditing into our operational business practices

Integrate simple strong isolation into our systems



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

How do we host data?

Defense in depth against bugs and issues in systems

Defense in depth against operational errors and mistakes

Defense in depth against untrusted access



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

Principle of least privilege

Don’t grant access unless it is needed

Grant access only *while* it is needed

Prove that it is needed



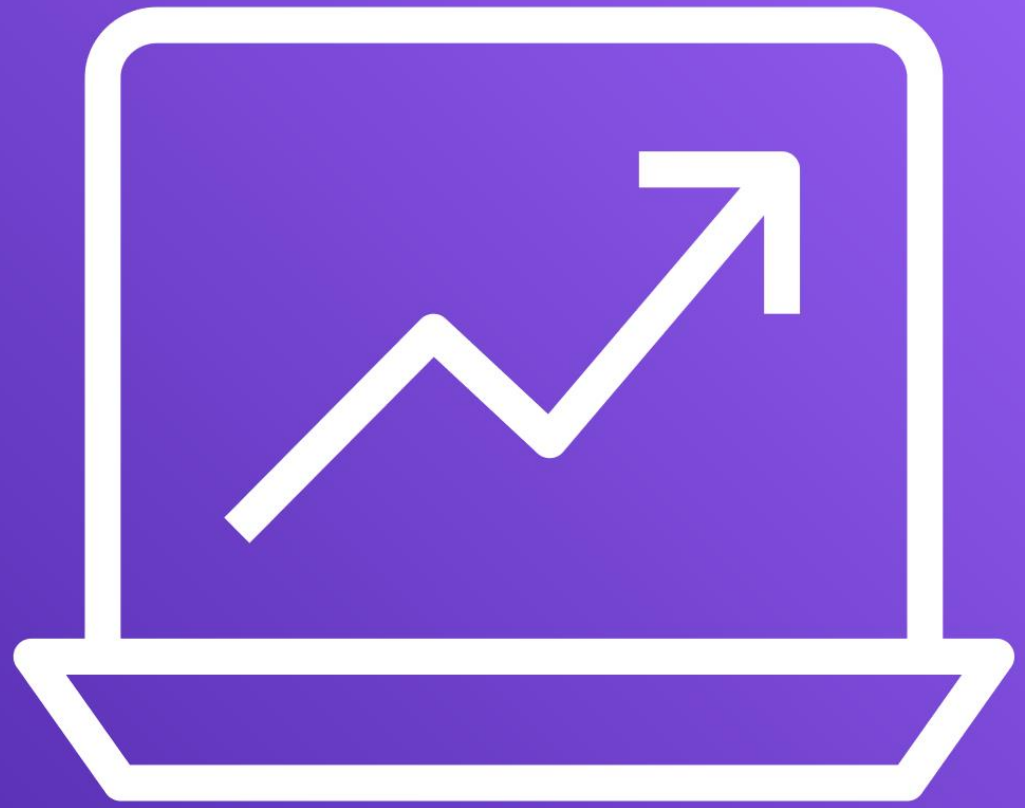
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do we get anything done?

Measure it

Drive it

Course-correct as necessary



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

Measuring progress

Not all systems and services need the same levels of protection

Integrate access auditing into our operational business practices

Integrate strong isolation into our systems



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

Zero-privilege operations

1. Foundational Principles
2. Elemental Protections
3. Always-on Accountability
4. Contingent Authorization
5. Hermetic Systems

aws

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

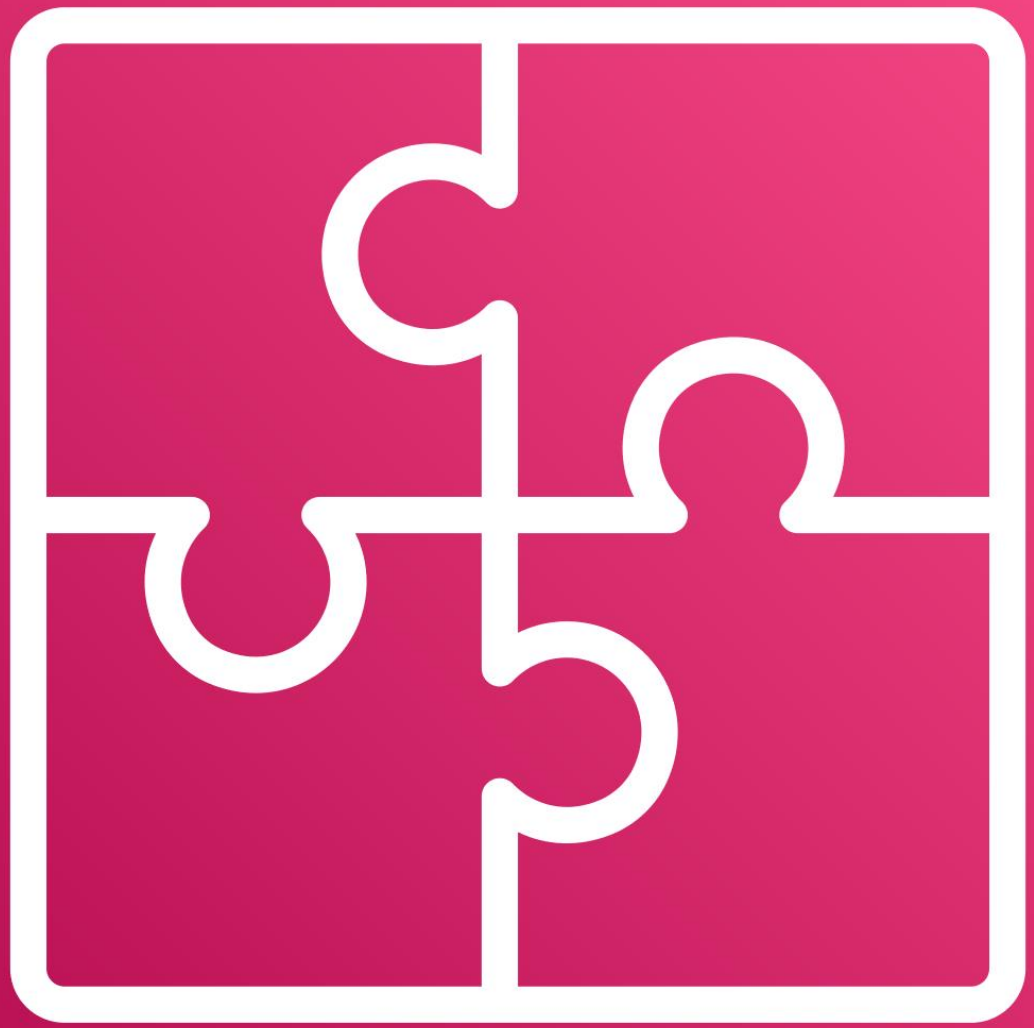
1 Foundational principles

ZERO-PRIVILEGE OPERATIONS

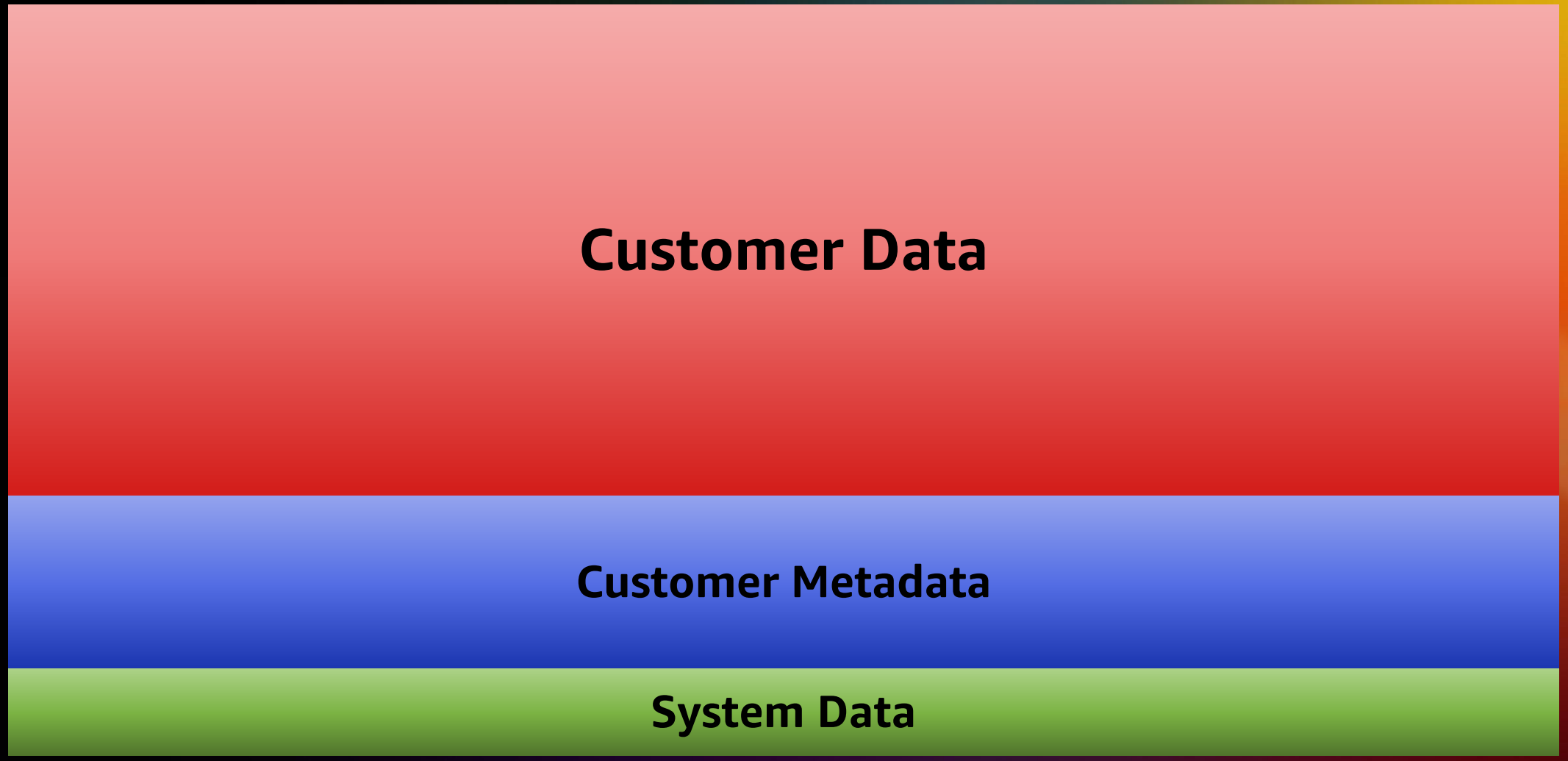
The first step is deciding to minimize access to data, even when it is inconvenient.

Always ask “What would the customer want us to do?” as the first question.

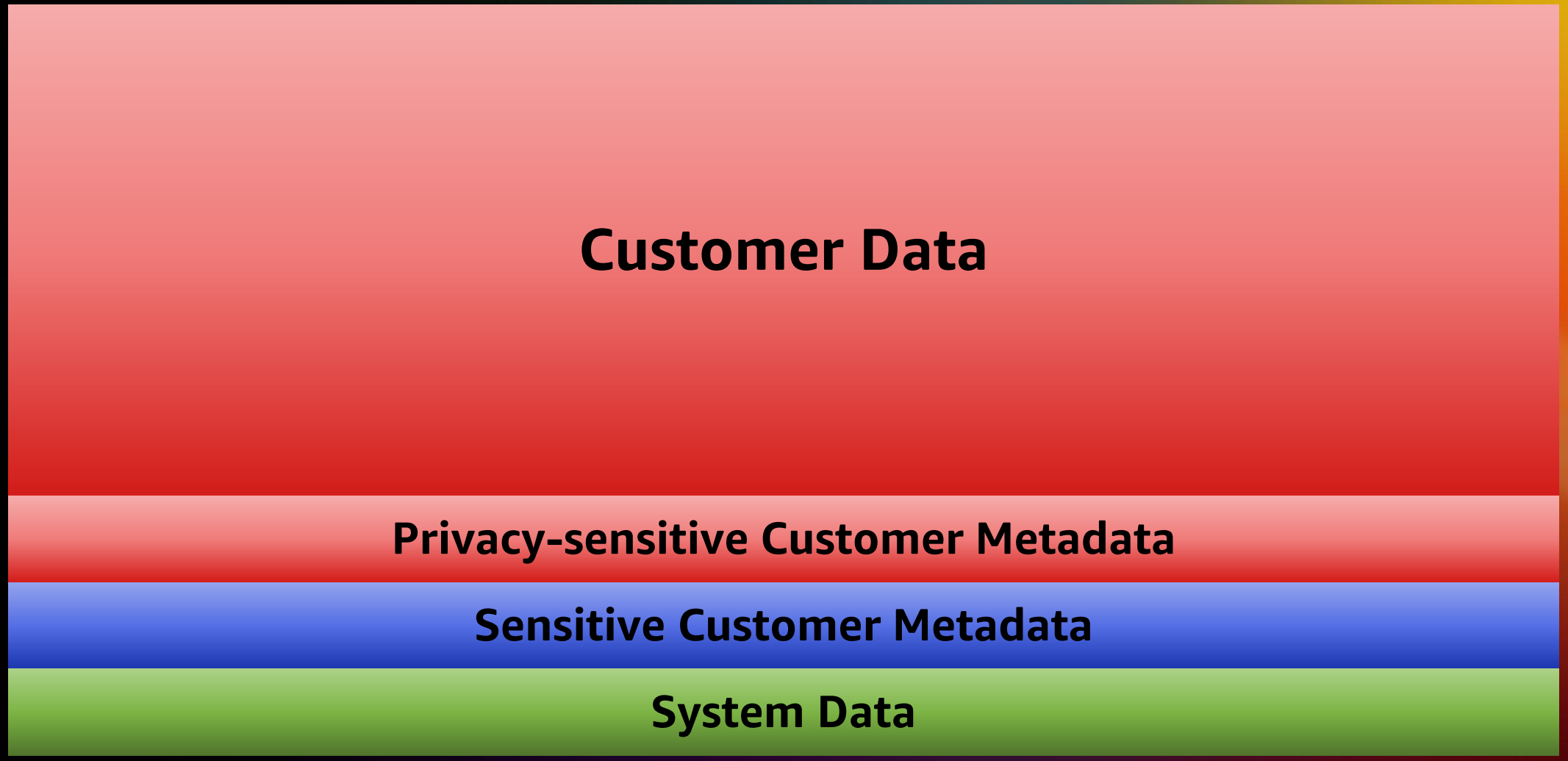
Classify data. E.g., configuration data, administrative data, PII, . . .



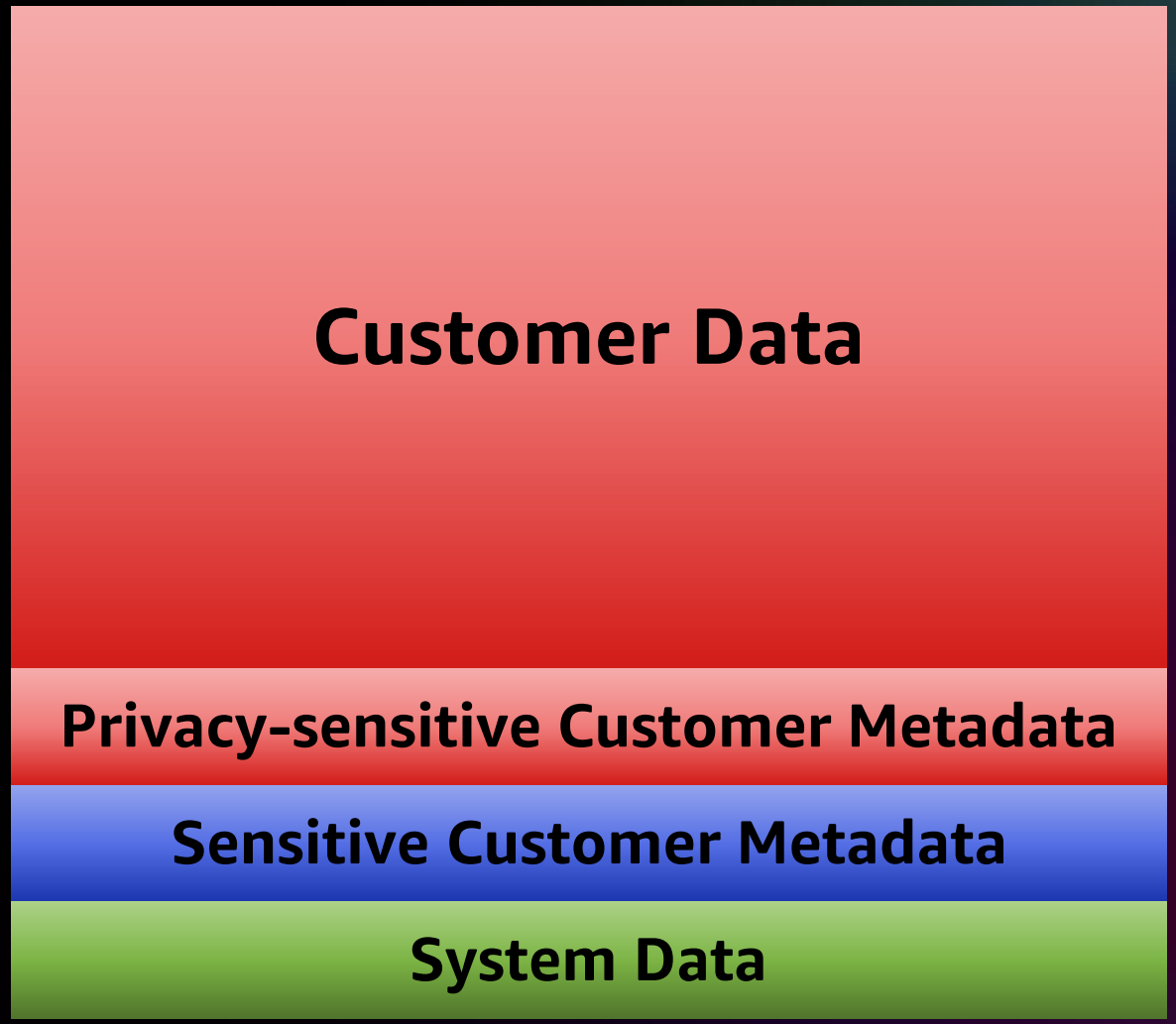
aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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



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



No one else's business

Names, addresses, etc

Configurations, Administrative Info

Software, System Configuration

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

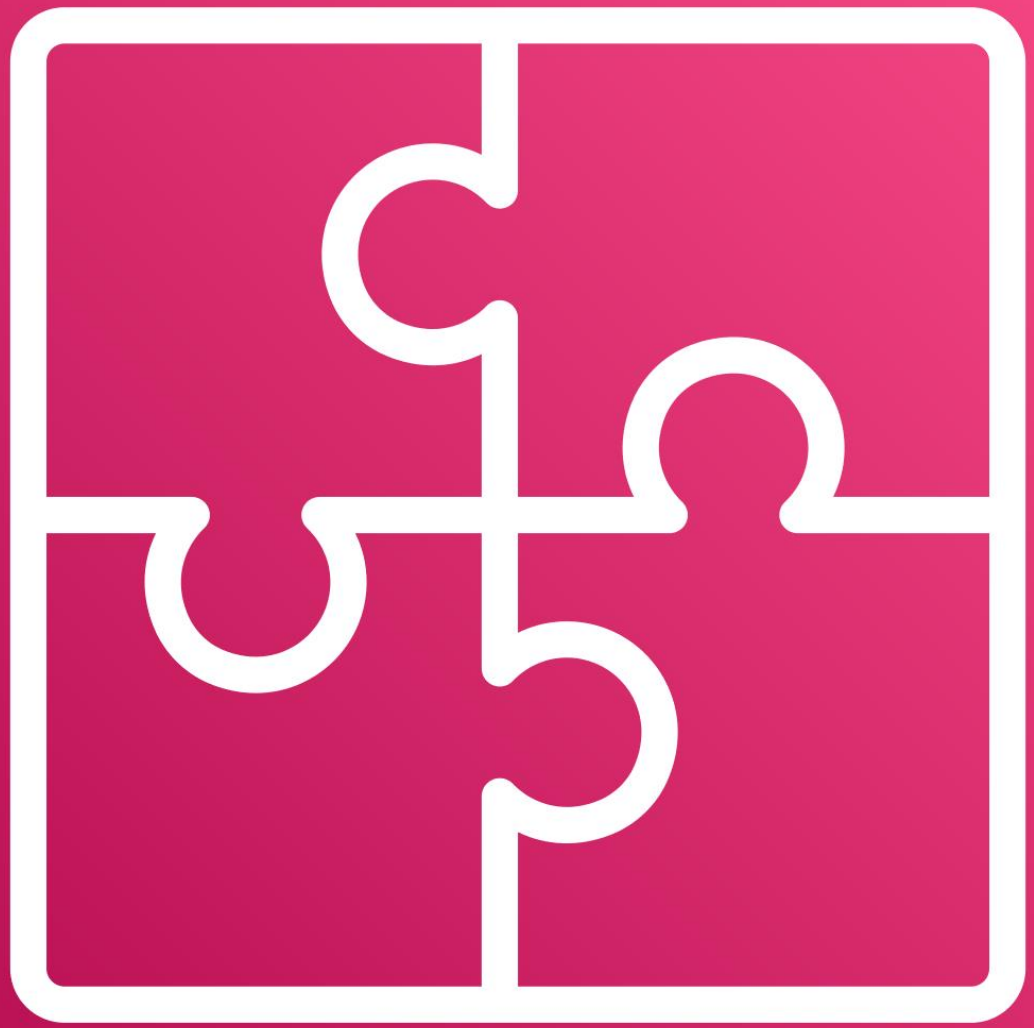
1 Foundational principles

ZERO-PRIVILEGE OPERATIONS

Build feedback mechanisms – listen to employees and operators

Lean on automation and focus on reducing the burden of operations for humans

Amazon Comprehend can identify and label PII



aws

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

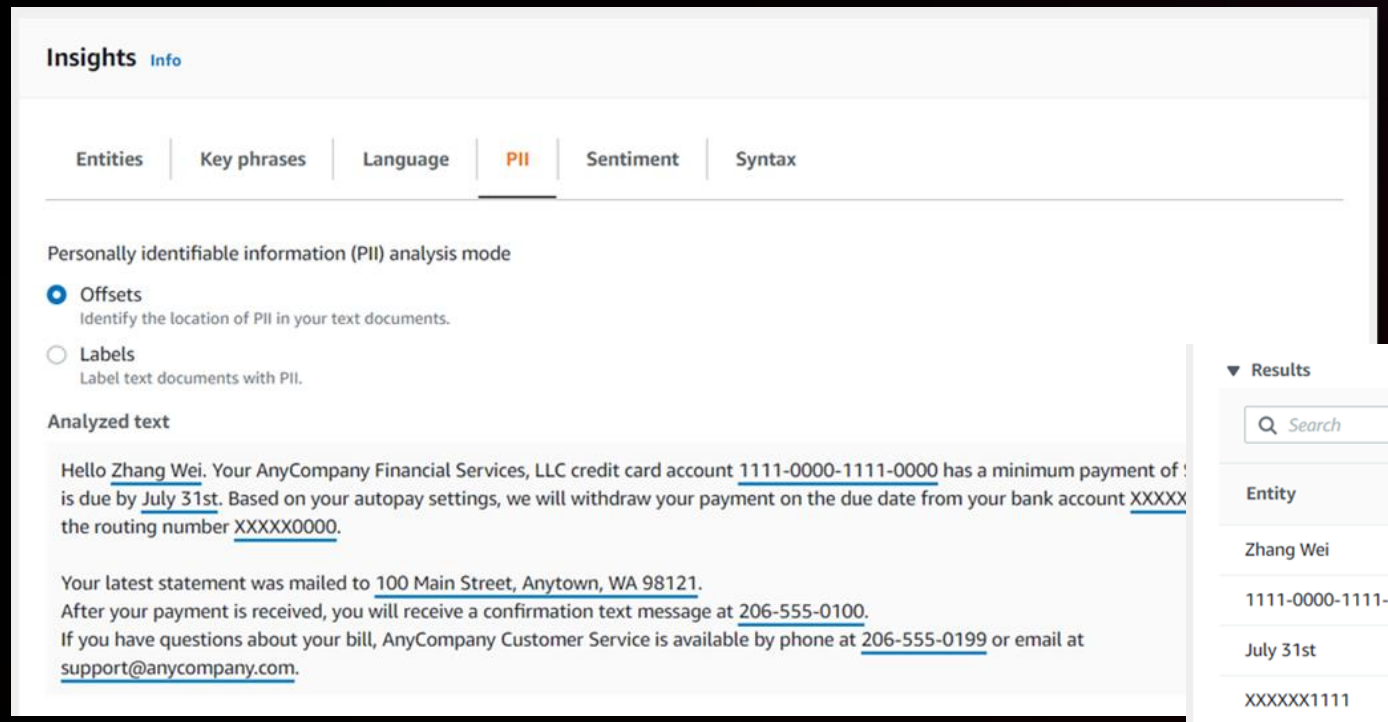
Zero-privilege operations

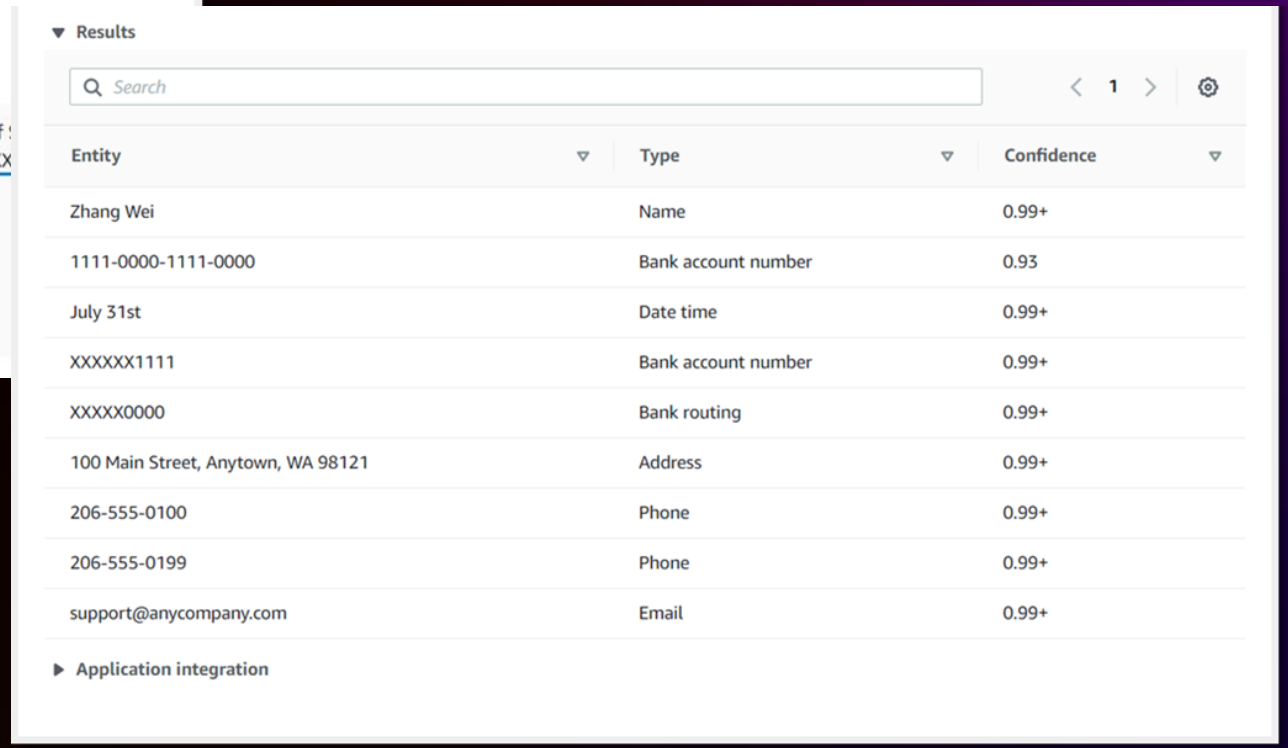
1. Foundational Principles ✓
2. Elemental Protections
3. Always-on Accountability
4. Contingent Authorization
5. Hermetic Systems

aws

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

Identifying PII with Amazon Comprehend





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

2

Elemental protections

ZERO-PRIVILEGE OPERATIONS

Make the physical storage of data secure against theft

Network encryption

Tested backup/restore processes

Secure multi-factor authentication (MFA) for operators



aws

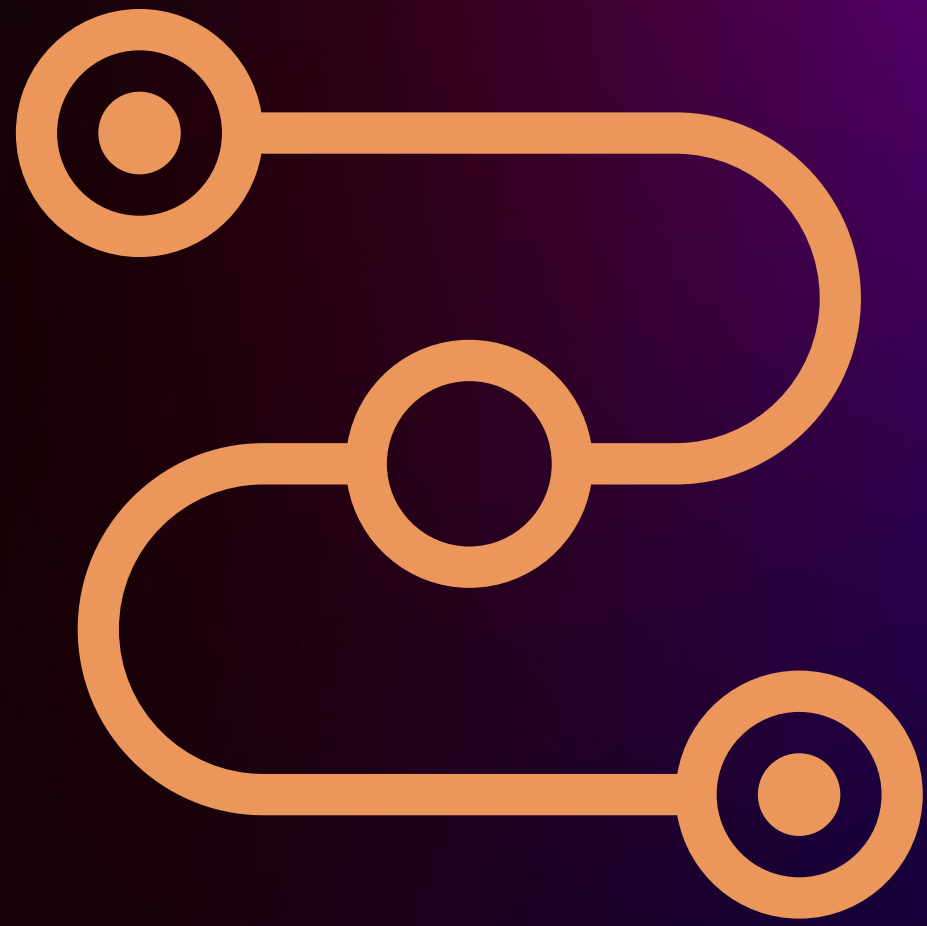
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Defense-in-depth encryption

All network traffic on links out of AWS physical control is encrypted using AES256 or optical-layer encryption

This includes all traffic between AWS data-centers, buildings, and regions

This encryption is always on



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

2 Elemental protections

ZERO-PRIVILEGE OPERATIONS

At-rest encryption

AWS VPN, AWS VPC Encryption

AWS Backup

AWS IAM, AWS IAM Identity Center, Cognito



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

Zero-privilege operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability
4. Contingent Authorization
5. Hermetic Systems

aws

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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

Regularly baseline all access

Who has access to what systems?

What do those systems have access to?

Always be reviewing



aws

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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

Eliminate anonymous shared accounts

Use roles instead

Ensure that role assumption can be traced end to end



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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

AWS Identity and Access Management

AWS Identity Center

AWS Systems Manager

EC2 Instance Connect



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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

AWS CloudTrail

AWS Config

AWS GuardDuty

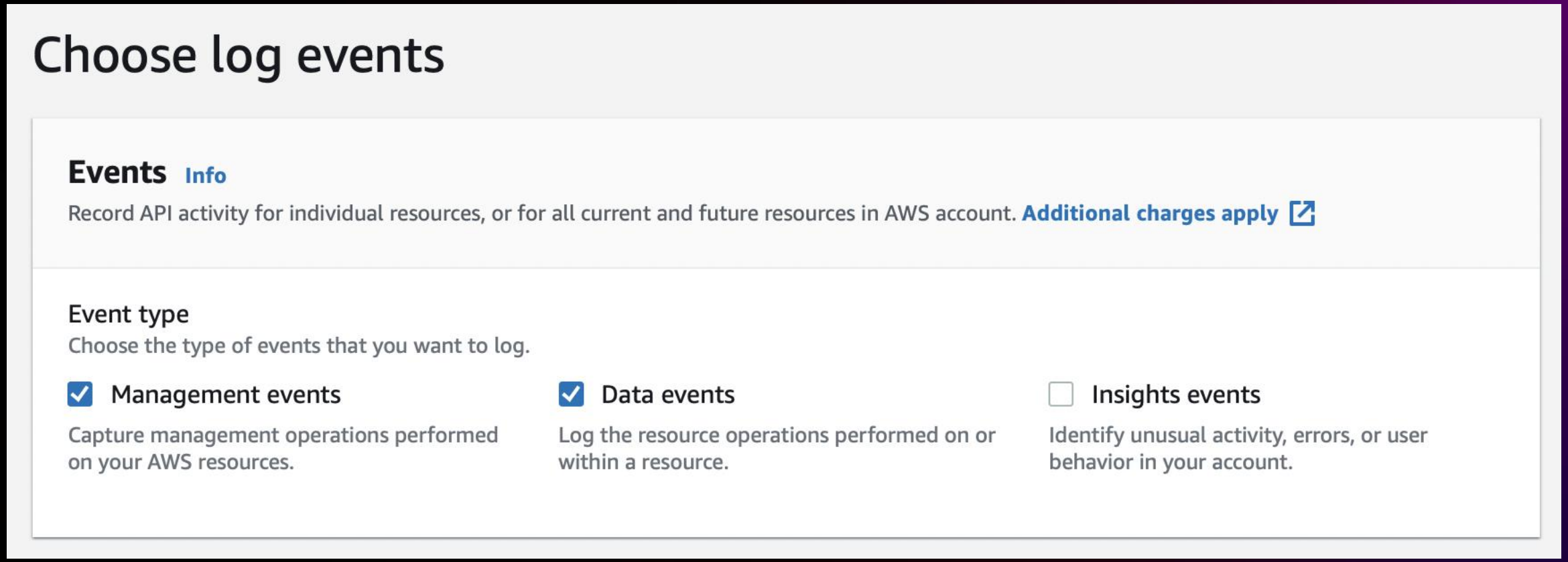
VPC Traffic Mirroring



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

3 Always-on accountability

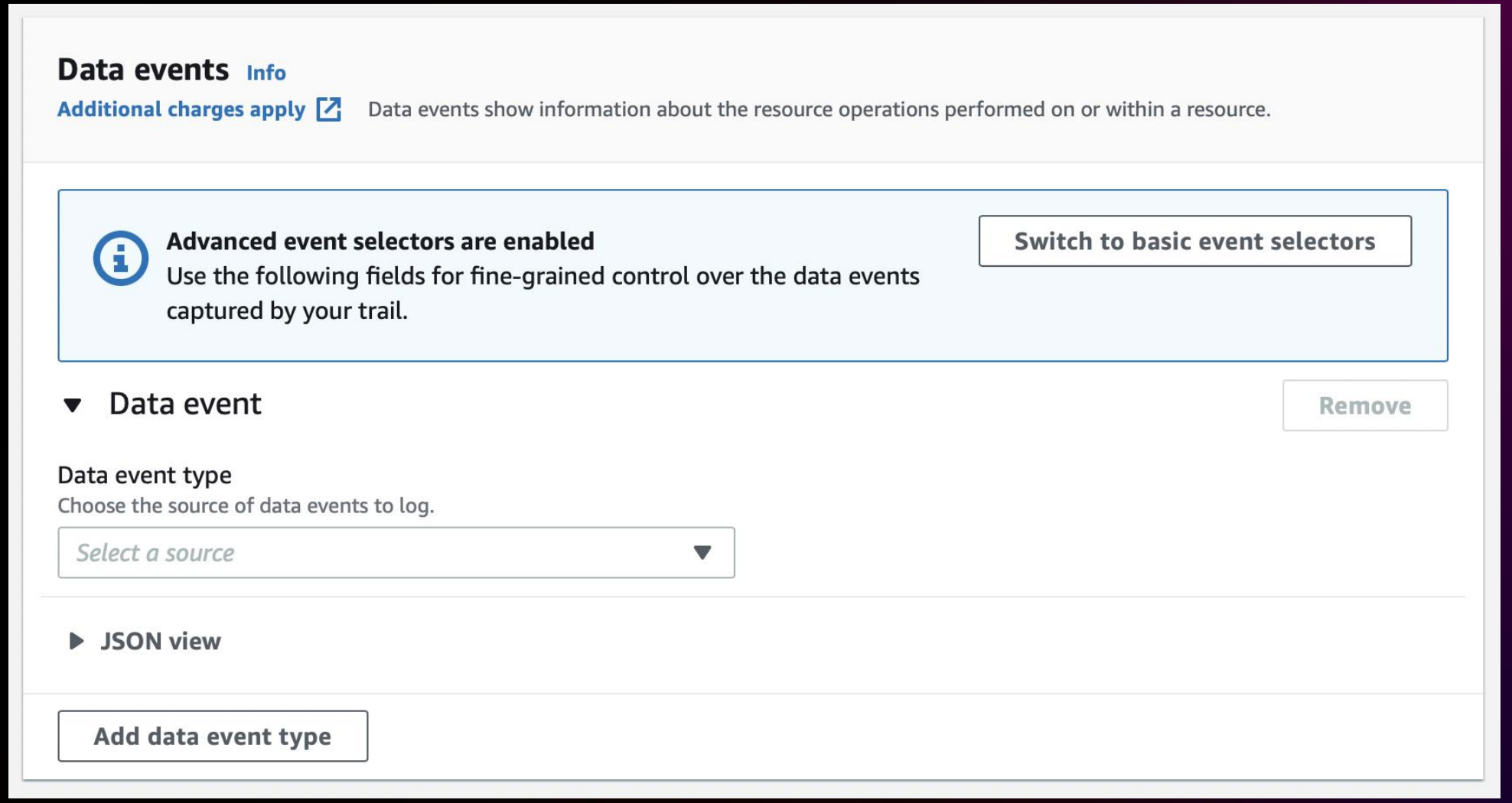
ZERO-PRIVILEGE OPERATIONS



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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS



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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

The AWS IAM service and SIGv4 protocols are widely used internally at AWS

Access between services is mediated by principals, roles, policies, . . .

The IAM service is also ring-fenced internally



aws

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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

Transparency and consent are front and center

Changes over time are not applied automatically and are published and tracked

Customers can revoke access



aws

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

AWS managed policies

Elastic Load Balancing updates to AWS managed policies

View details about updates to AWS managed policies for Elastic Load Balancing since this service began tracking these changes.

Change	Description	Date
AWS managed policy: AWSElasticLoadBalancingServiceRolePolicy - Update to an existing policy.	Elastic Load Balancing added a new action to grant permissions to use peering connections. This action was added to the service-linked role policy, for Elastic Load Balancing control plane. It is associated with the `ec2:DescribeVpcPeeringConnections` API operation.	October 11, 2021
AWS managed policy: ElasticLoadBalancingFullAccess - Update to an existing policy.	Elastic Load Balancing added a new action to grant permissions to use peering connections. This action was added to the Elastic Load Balancing full access policy. It is associated with the `ec2:DescribeVpcPeeringConnections` API operation.	October 11, 2021
AWS managed policy: AWSElasticLoadBalancingClassicServiceRolePolicy - Update to an existing policy.	Elastic Load Balancing added a service-linked role policy (for the control plane) for the Classic Load Balancer. This update is for version 2 (default).	October 7, 2019
AWS managed policy: ElasticLoadBalancingReadOnly	Provides read-only access to Elastic Load Balancing and dependent services. This is the version 1 (default).	September 20, 2018
Elastic Load Balancing started tracking changes	Elastic Load Balancing started tracking changes for its AWS managed policies.	July 23, 2021

aws

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

3 Always-on accountability

ZERO-PRIVILEGE OPERATIONS

Managed policies specify what kinds of permissions a service may have to your resources

We use AWS IAM Access Analyzer to constantly baseline the permissions that we ourselves use



aws

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

AWS IAM Access Analyzer

Access Analyzer

Monitor access to resources

How it works



1 Create an analyzer

You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.



2 Review active findings

When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

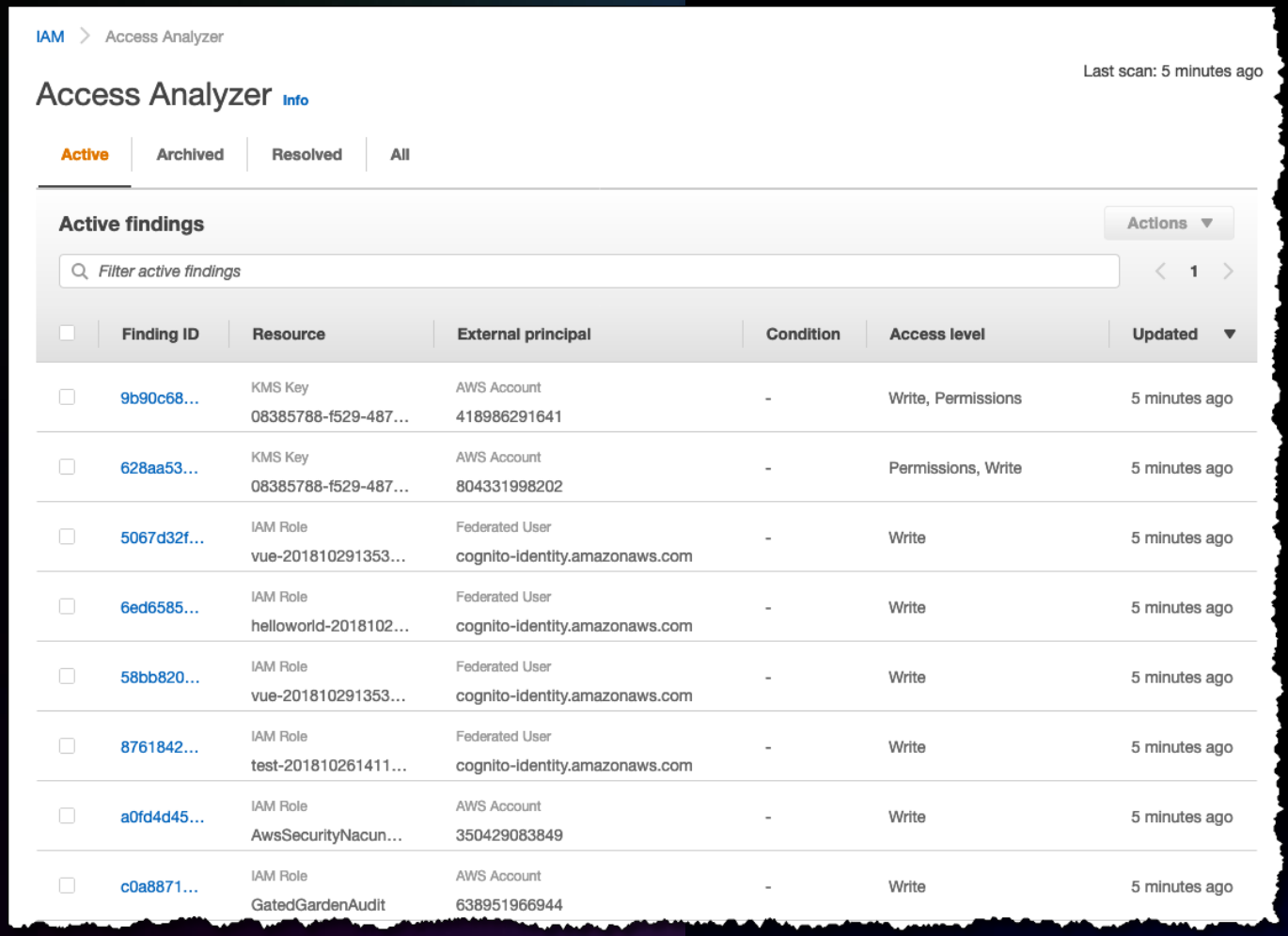


3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

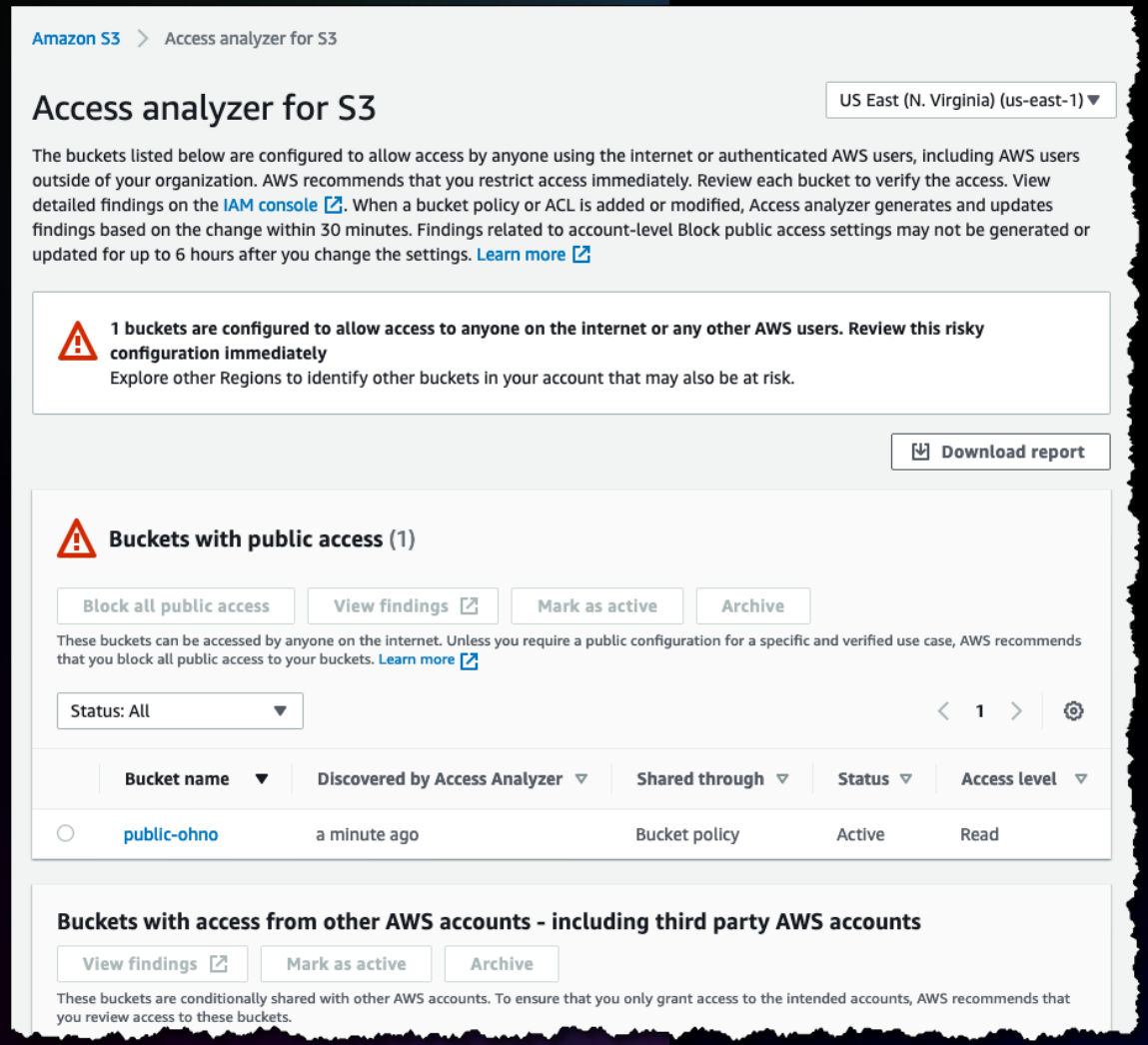
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS IAM Access Analyzer



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

AWS IAM Access Analyzer



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

Zero-privilege operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability ✓
4. Contingent Authorization
5. Hermetic Systems

aws

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

Zero-privilege operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability ✓

---

4. Contingent Authorization
5. Hermetic Systems

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

4 Contingent authorization

ZERO-PRIVILEGE OPERATIONS

Remove “Single Points of Failure”

Access should be highly specific and conditional

Access granted only *because* it is needed

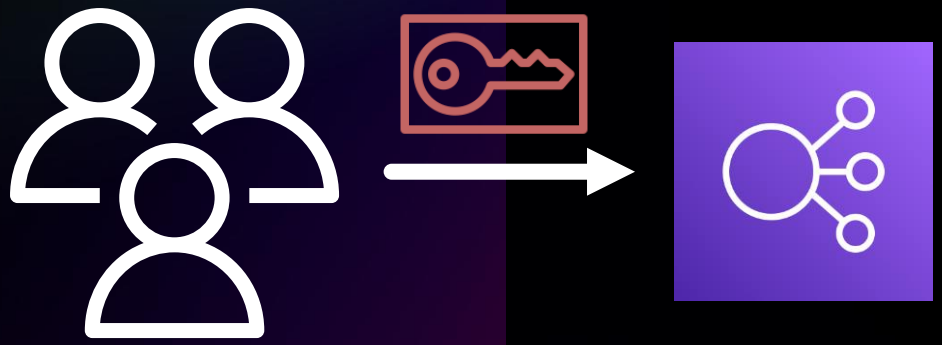
Access granted only *while* it is needed



aws

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

AWS SIGv4 requests

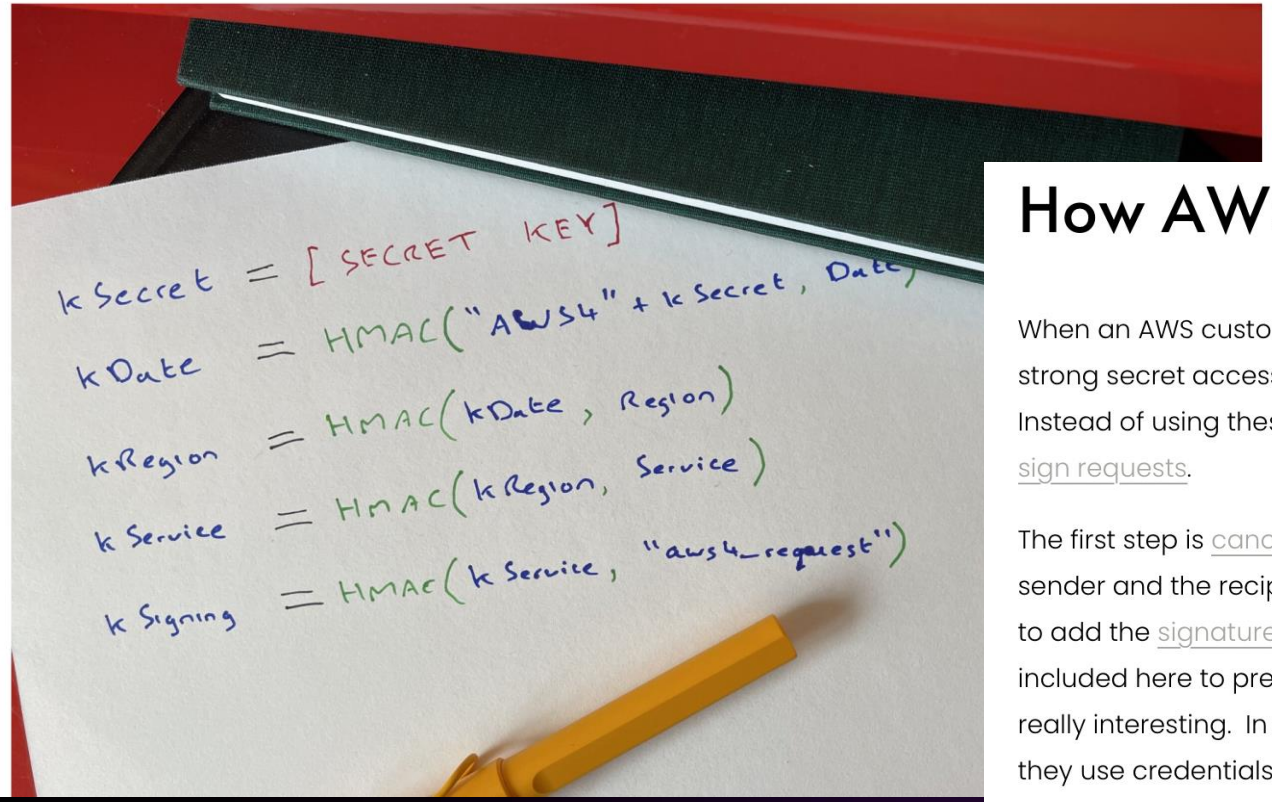


Customer signs request to Elastic Load Balancer API with their key

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

AWS SIGv4 requests

AWS SIGv4 and SIGv4A



https://shufflesharding.com/posts/aws-sigv4-and-sigv4a

How AWS SIGv4 requests are signed

When an AWS customer creates an IAM user, they get an access key ID, and a cryptographically strong secret access key from the IAM service, which together identify and authenticate that user. Instead of using these secret keys directly as bearer tokens, SIGv4 uses a simple four step process to sign requests.

The first step is canonicalize the request and any headers we want to sign into a string. That's so the sender and the recipient can all agree about what is to be signed in the first-place. The second step is to add the signature algorithm, time, and credential scope. The signature algorithm and time are included here to prevent downgrade and replay attacks, but credential scope is where things get really interesting. In SIGv4, the clients don't even use their secret keys to sign the requests, instead they use credentials that are finely scoped down in important ways. Each scoped credential is valid only for a request made using a particular version of the signature protocol, to a particular AWS service, in a particular AWS region, on a particular day.

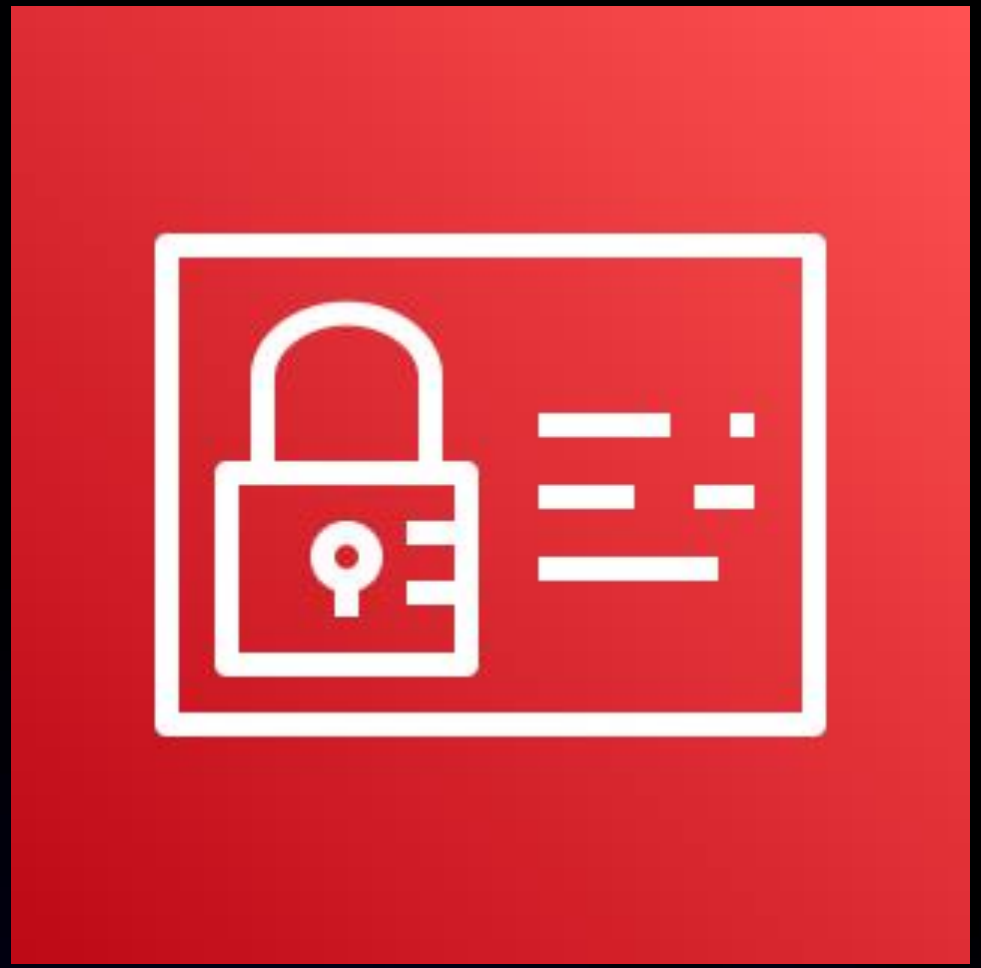
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS IAM and SIGv4

Customer’s AWS secret keys are stored only in the central IAM system and are not not on our AWS services

Signing keys are per-day, per-service, per-Region

SIGv4A uses public-private keys



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

4 Contingent authorization

ZERO-PRIVILEGE OPERATIONS

IAM also has support for time-limited “Forward Access Sessions” based on a cryptographic chain of custody

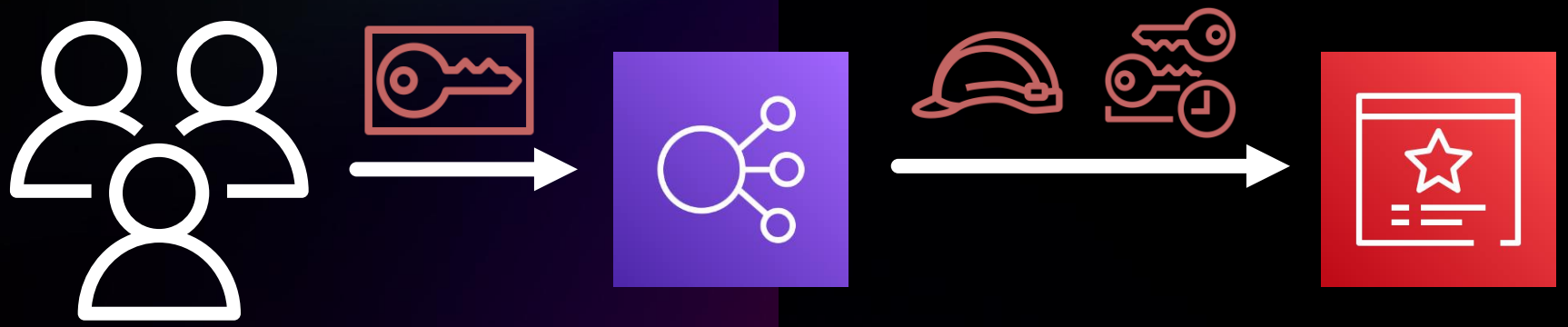
“On behalf of” access is granted to a service only if that service can prove it was recently called by the customer



aws

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

IAM Forward Access Sessions



Customer signs request to Elastic Load Balancer API with their key

ELB signs request to ACM with a temporary key derived from the customer request

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

IAM Forward Access Sessions

Granting EC2 access to an EBS encryption key

Launching VPC PrivateLink endpoints

Attaching VPC Transit Gateways



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

4 Contingent authorization

ZERO-PRIVILEGE OPERATIONS

Used for pre-approved automation and scripts that are vetted and do not access/disclose data

Enforce multi-person review/approval for anything non-standard

“Break glass” procedures that provide strong accountability even during the unpredictable

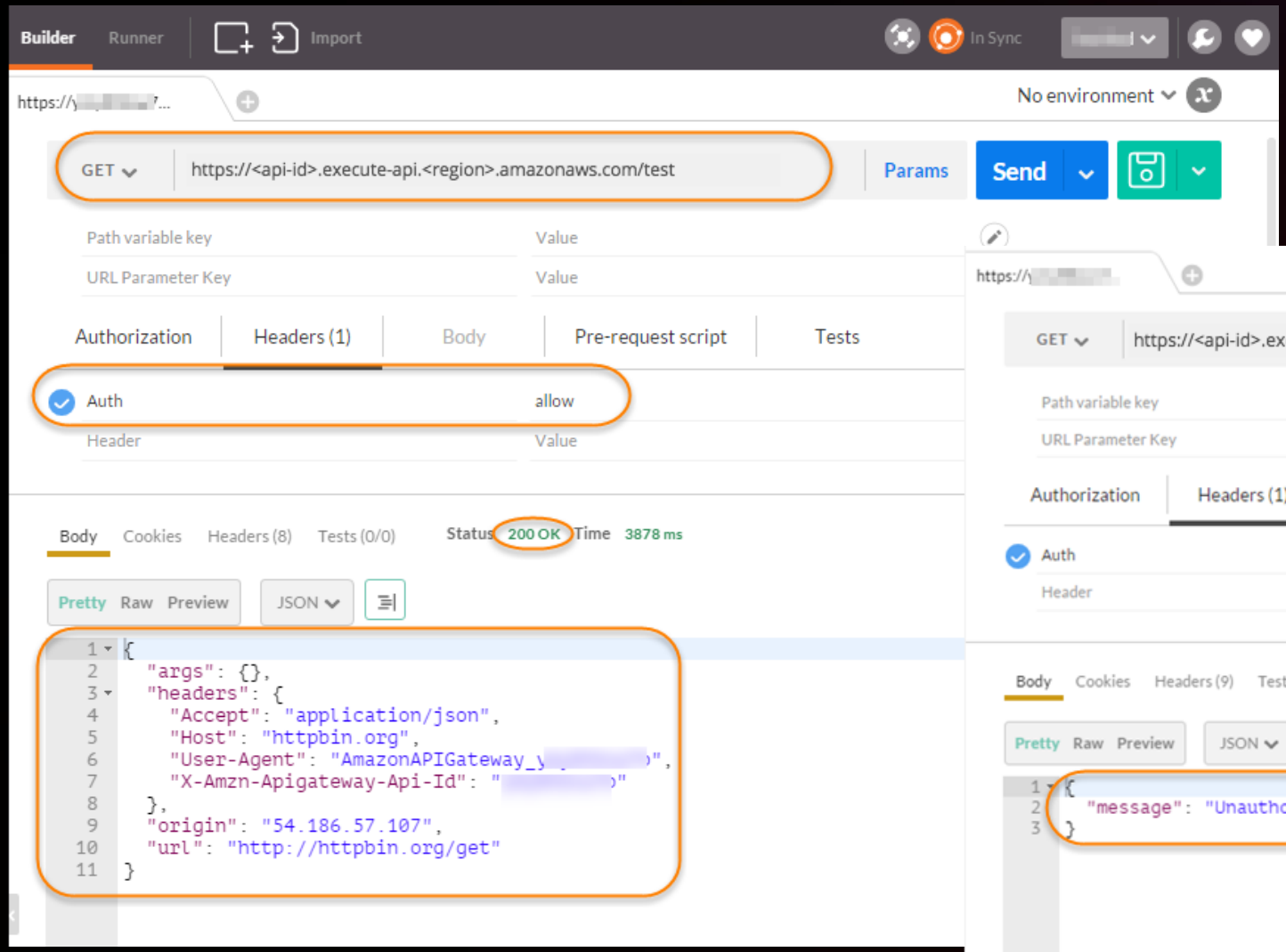


aws

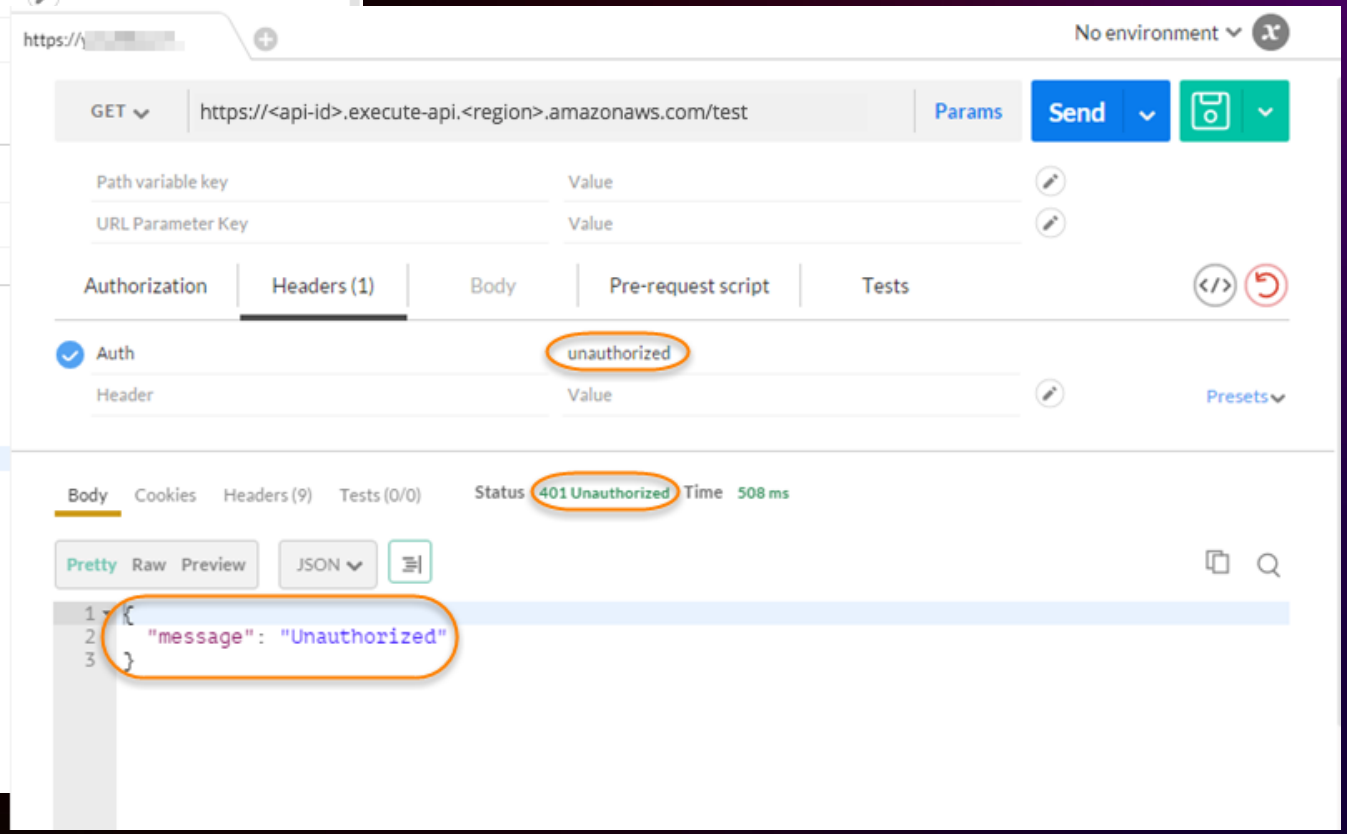
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

4 Contingent authorization

ZERO-PRIVILEGE OPERATIONS



API Gateway Lambda Authorizers



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

Zero-privilege operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability ✓
4. Contingent Authorization ✓
5. Hermetic Systems

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

5 Hermetic systems

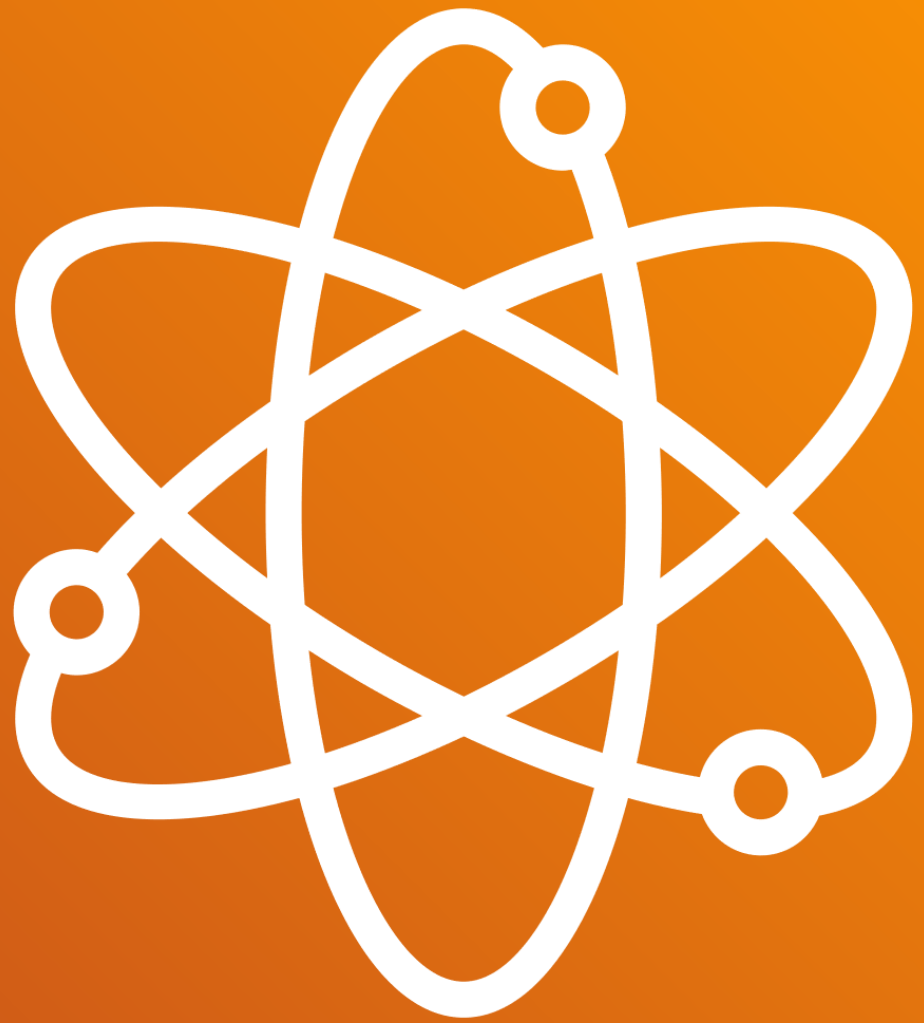
ZERO-PRIVILEGE OPERATIONS

Systems that have **no** general-purpose or operator access

Incorporate a secure root of trust

AWS Nitro System

AWS Key Management Service (KMS)



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

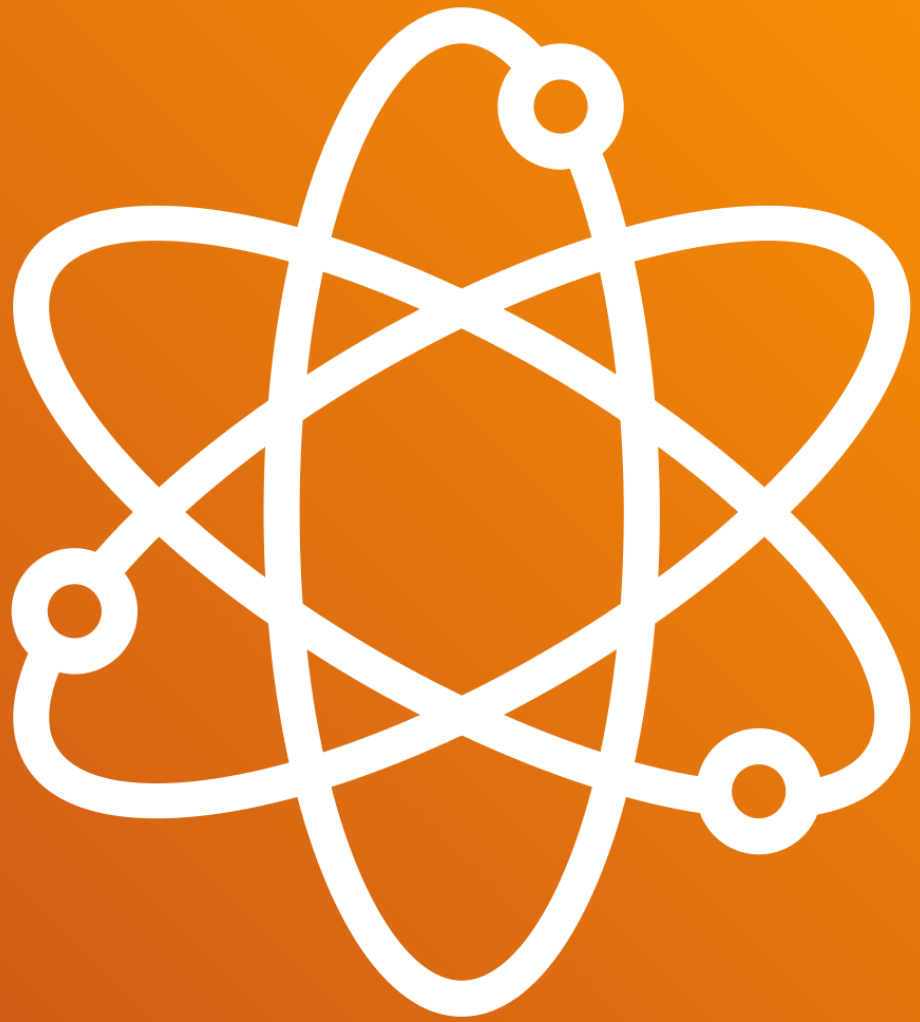
5 Hermetic systems

ZERO-PRIVILEGE OPERATIONS

AWS Nitro system built with physical isolation between the Nitro Cards and the hardware that is running customer instances

Offers Bare Metal and Virtualized EC2 Instance types

All modern EC2 Instances are powered by Nitro



aws

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

Homomorphic encryption

Cryptographic Computing

Enabling computation on cryptographically protected data

AWS Cryptography tools and services utilize a wide range of encryption and storage technologies that can help customers protect their data at rest and in transit. In some instances, customers also require protection of their data even while it is in use. To address this need, AWS is developing new techniques for cryptographic computing, an emerging technology that allows computations to be performed on encrypted data, so that sensitive data is never exposed. It is the foundation used to help protect the privacy and intellectual property of data owners, data users, and other parties involved in machine learning activities.

Our team of experts is innovating in Privacy Preserving Machine Learning with techniques such as Homomorphic Encryption and Secure Multi-Party Computation to help AWS and its customers meet their security and compliance goals, while allowing them to take advantage of the flexibility, scalability, performance and ease of use that AWS offers.

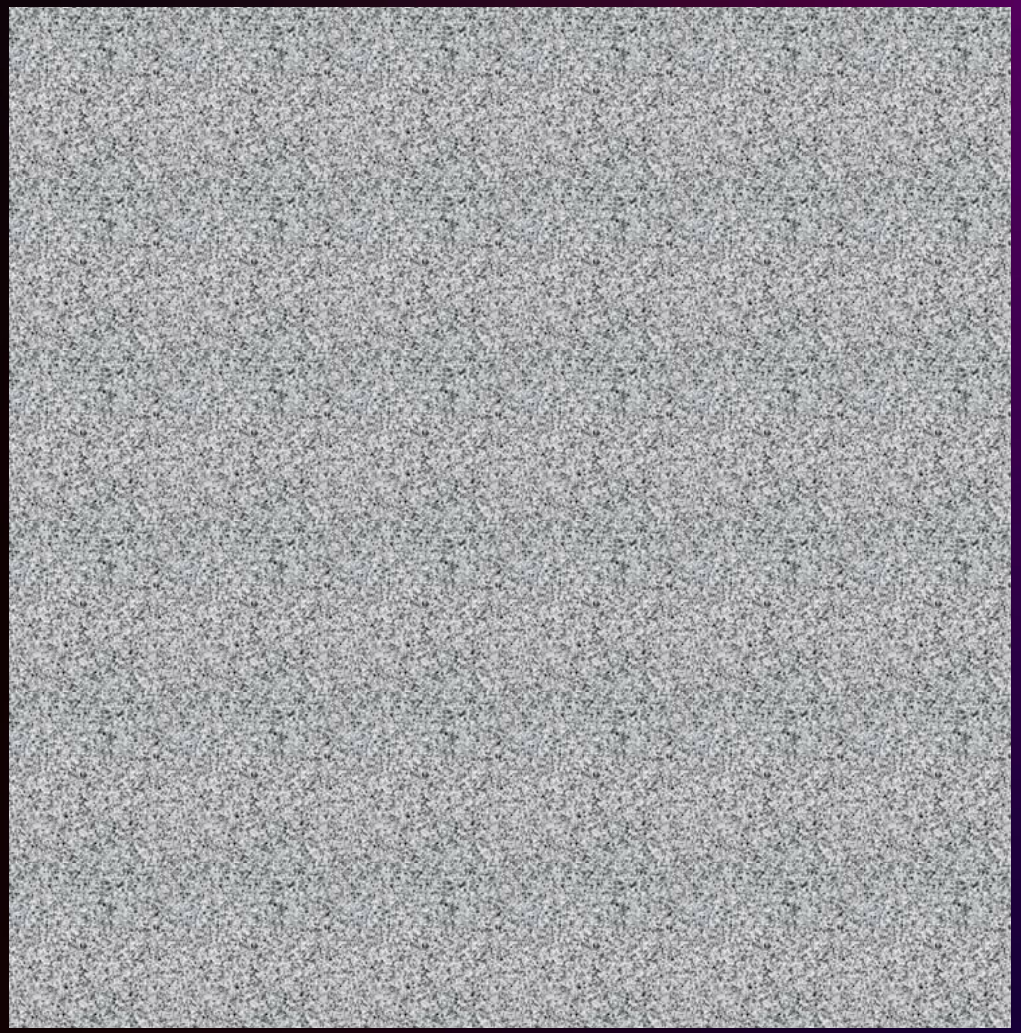


Privacy-Preserving Machine Learning

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

Encryption and side channels

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Lorem ipsum dolor sit amet, consectetur adipiscing elit, Lorem ipsum dol

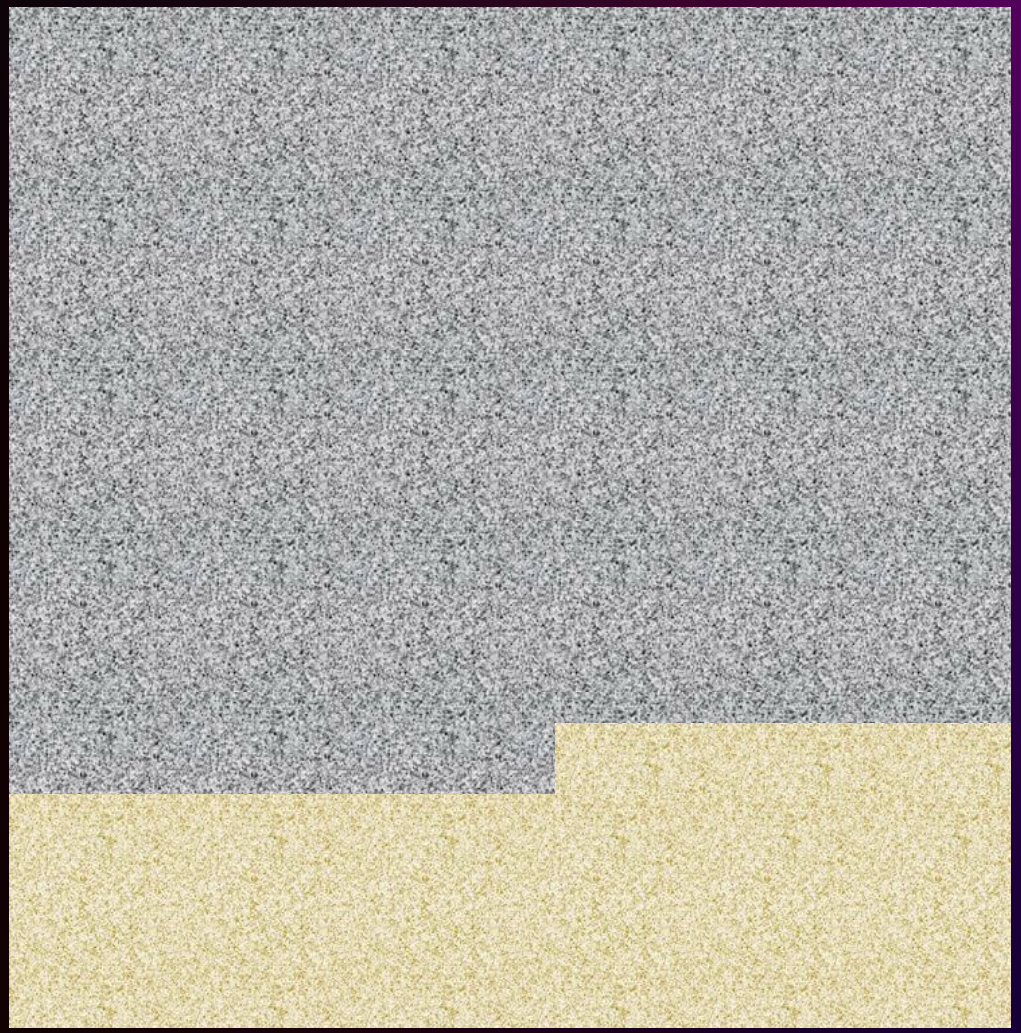


aws

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

Encryption and side channels

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. **Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat duis aute irure**



aws

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

Encryption and side channels

Encryption for data “in-use” still exposes patterns of changes in the data

Encryption for data “in-use” is usually unauthenticated and malleable

With encryption for data ”in-use,” the data is not encrypted in the CPU when it is used and is still exposed to microarchitectural side-channels

The AWS Nitro system does use memory encryption, but only as a secondary control

aws

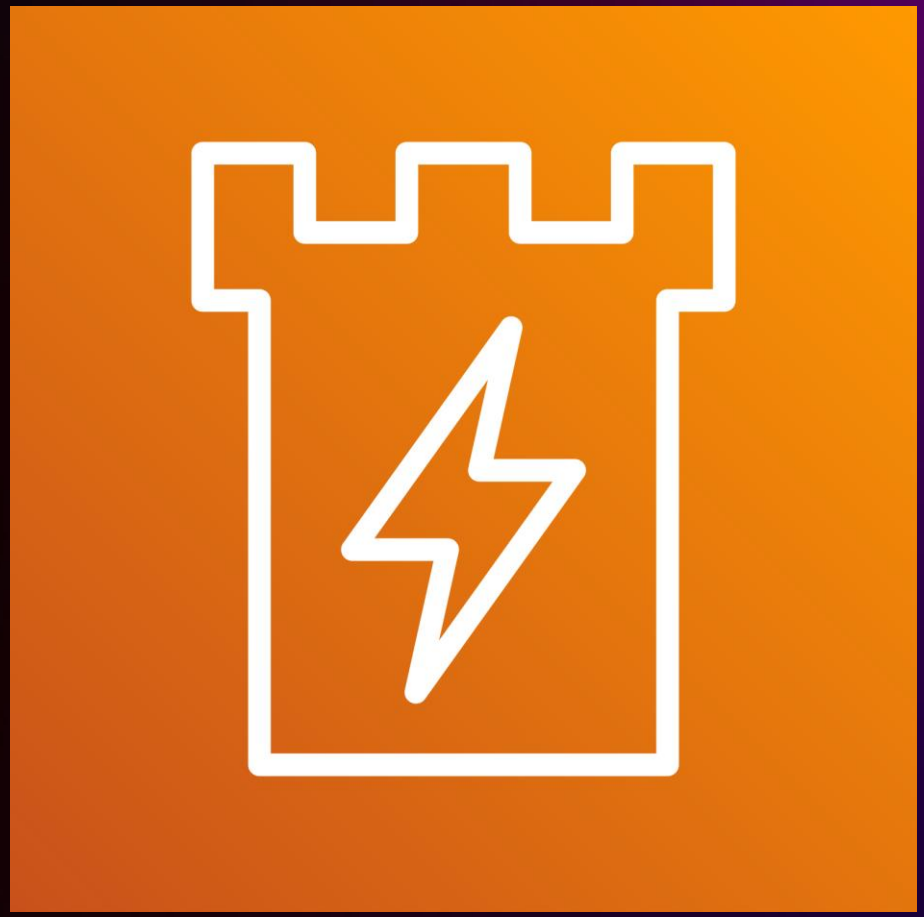
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro System

Designed from day one to provide strong isolation between AWS and the customer

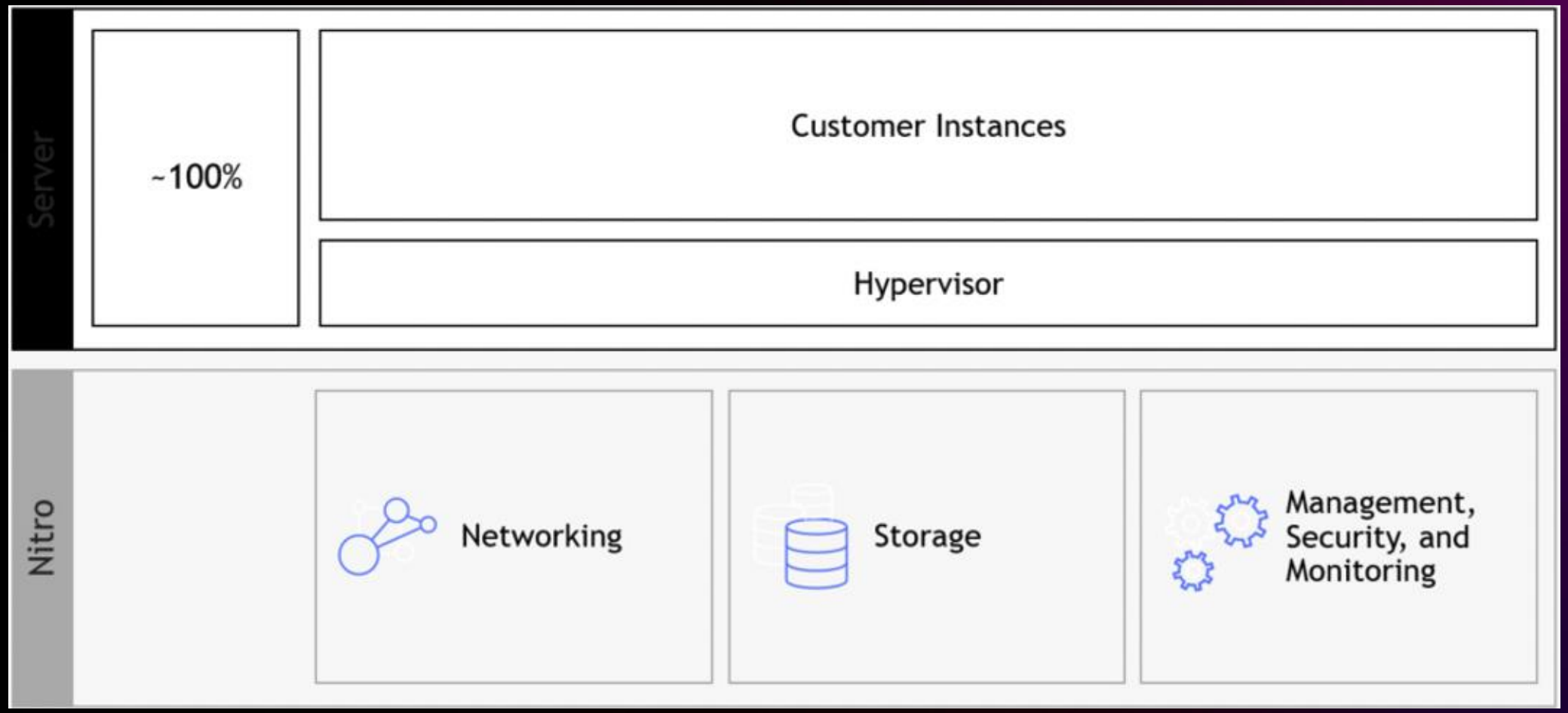
AWS Nitro cards are physically separate from the hardware running customer instances

Dedicated CPU, Memory, and hardware security chip



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

AWS Nitro System



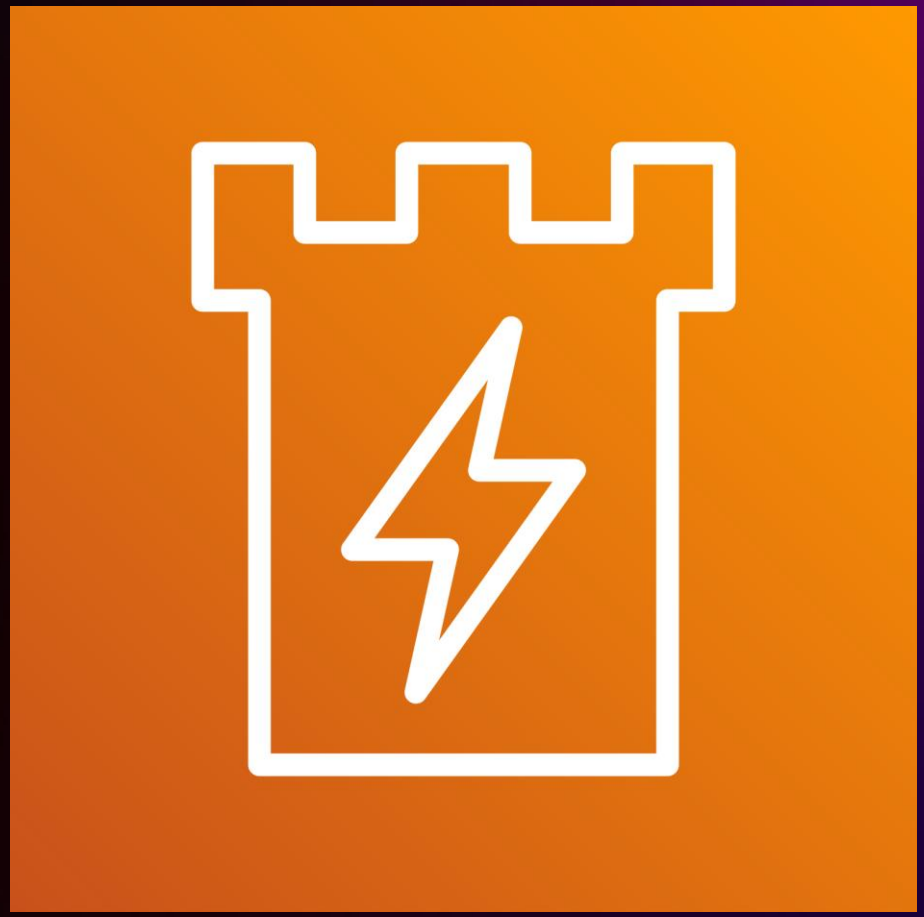
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro System

There is no operational access to the AWS Nitro system

No ssh, no general purpose access of any kind

All Nitro operations are done via secure, authenticated APIs and microservices



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

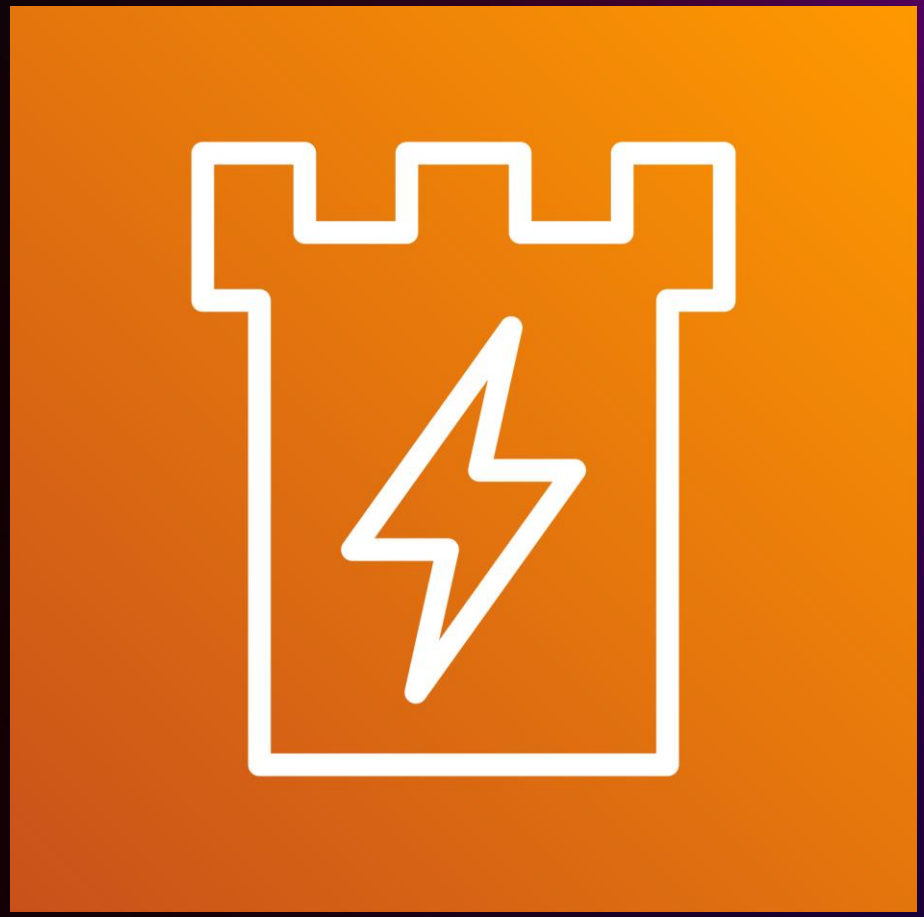
AWS Nitro System

Every build is signed and every operation is pre-vetted for safety

Nitro systems run in an isolated network

Debugging features don’t disclose customer data

We’ve been extending this model to other systems



aws

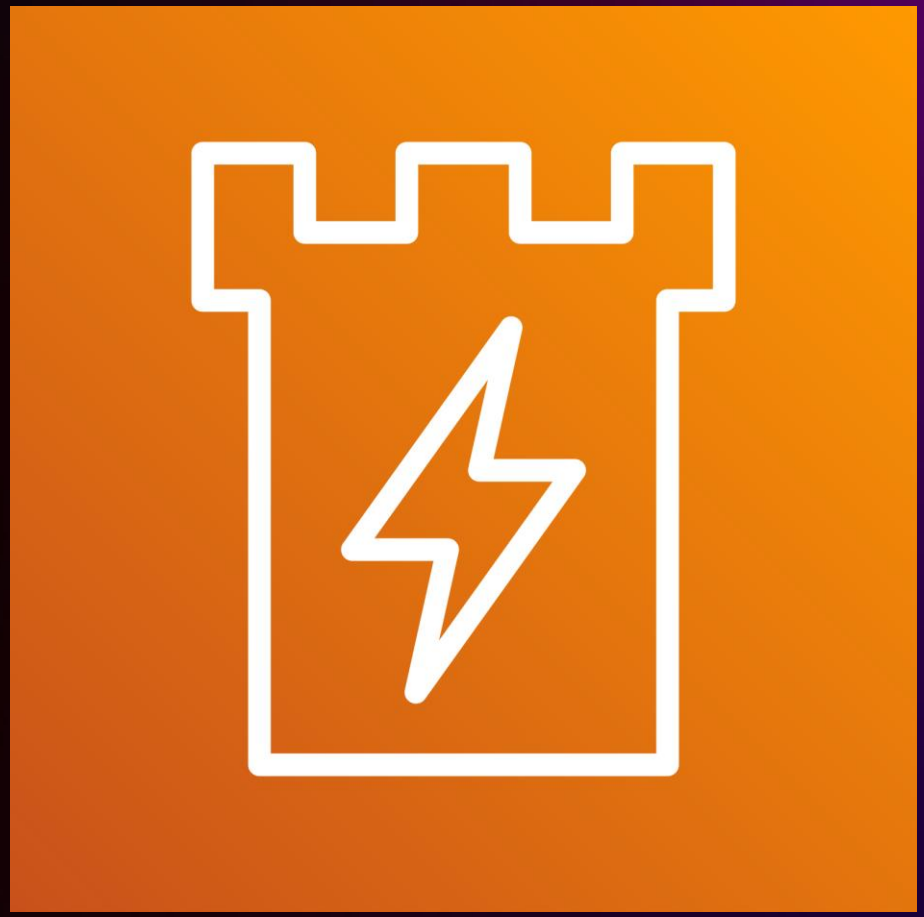
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro System

With metal instances, customers get the dedicated hardware

Virtual instances are fully isolated from one another and from the Nitro Hypervisor

Instances don’t share CPU cores or L1/L2 cache lines



aws

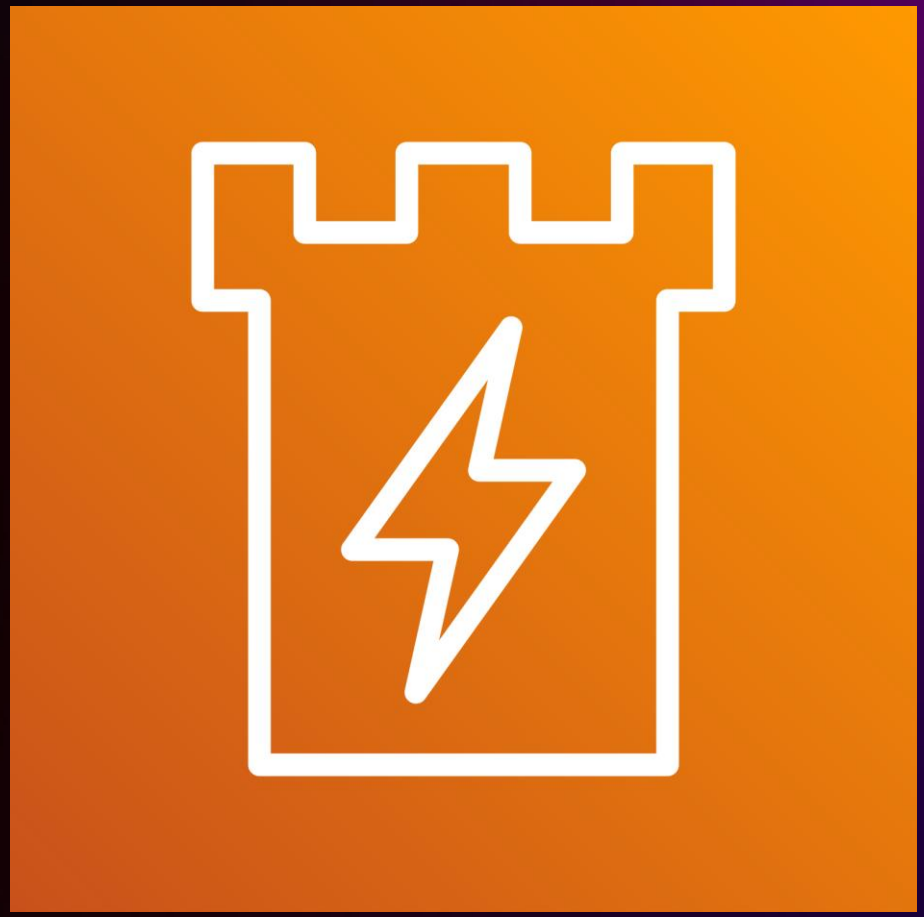
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro System

Nitro provides confidential computing based on hard isolation that complements encryption

Graviton2 includes memory encryption

Launch and run your application as normal, no modifications needed



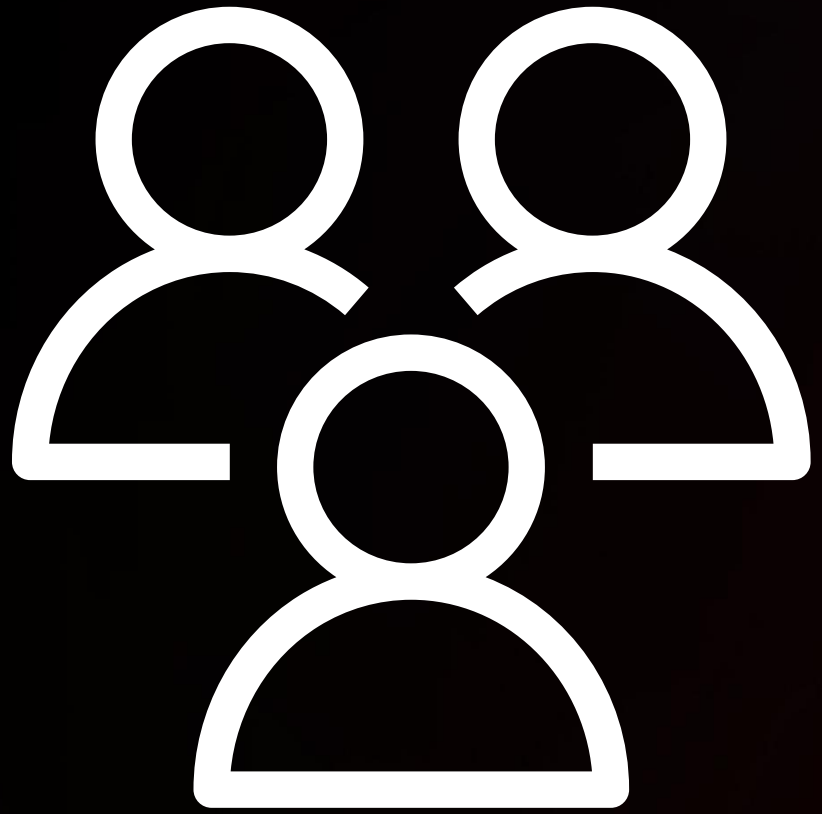
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

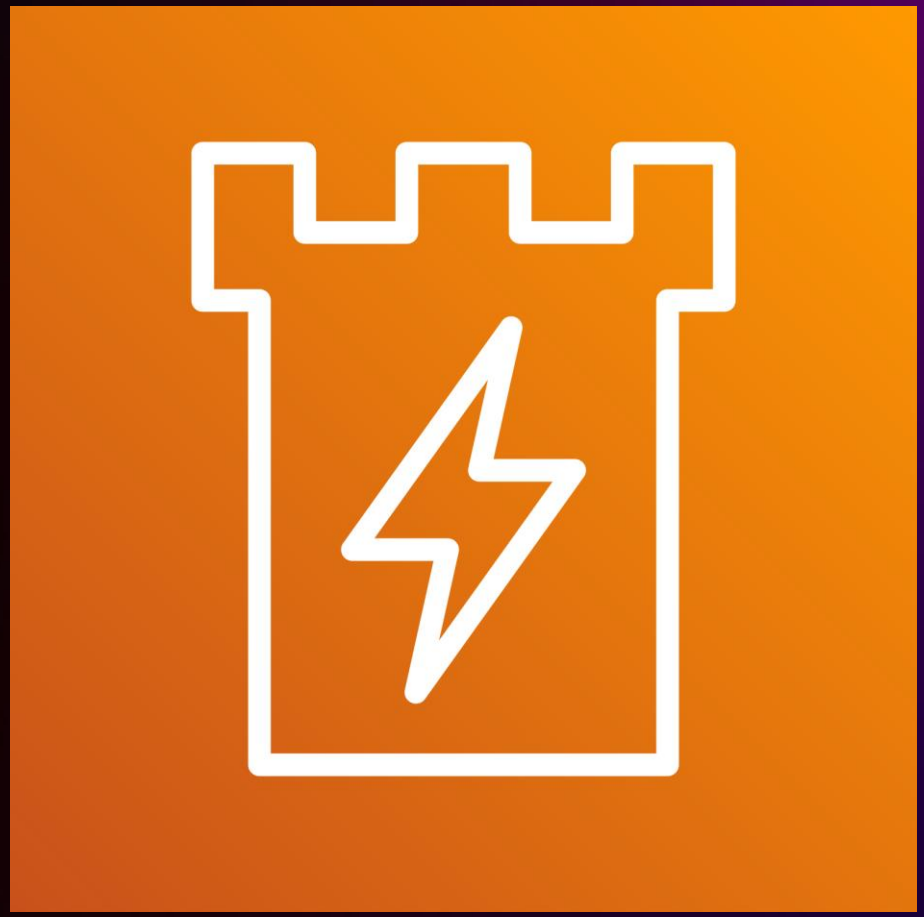
Zero-privileges operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability ✓
4. Contingent Authorization ✓
5. Hermetic Systems ✓

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

AWS Nitro Enclaves





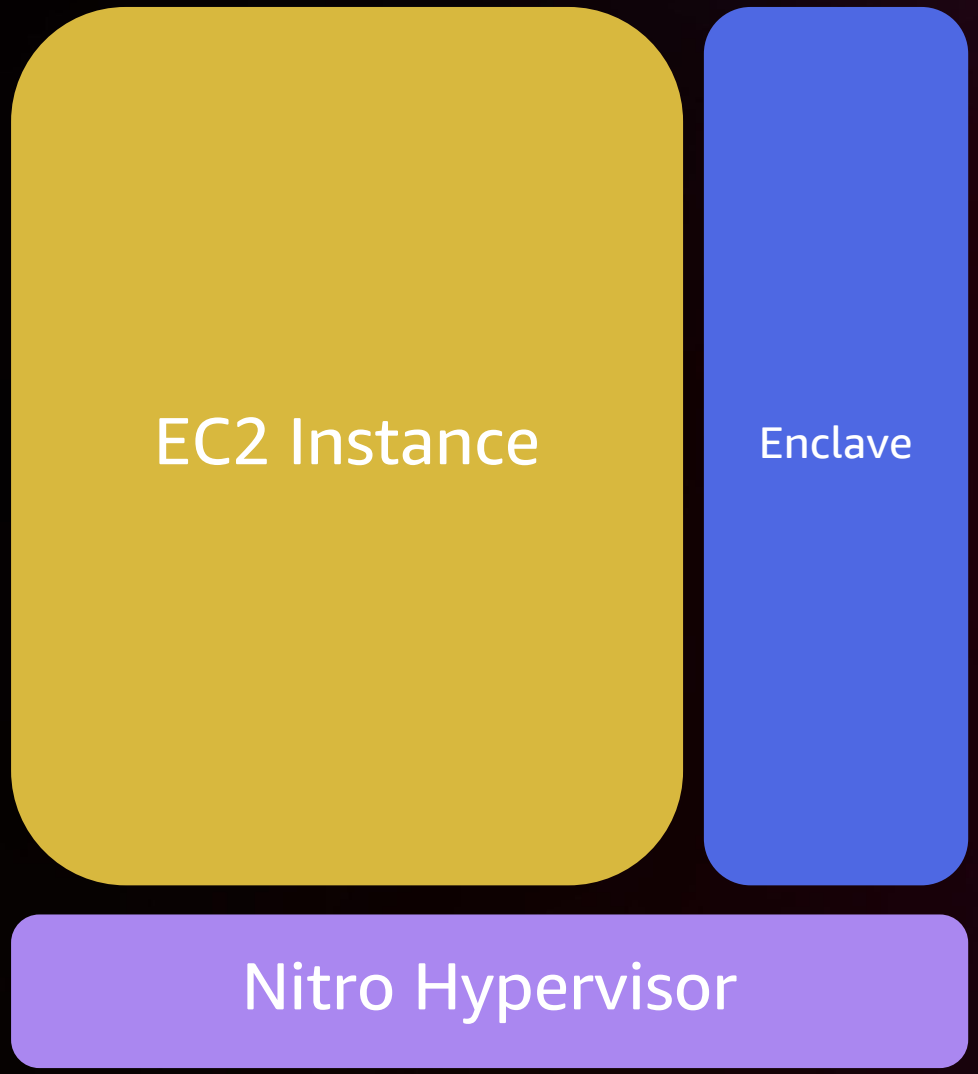
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro Enclaves



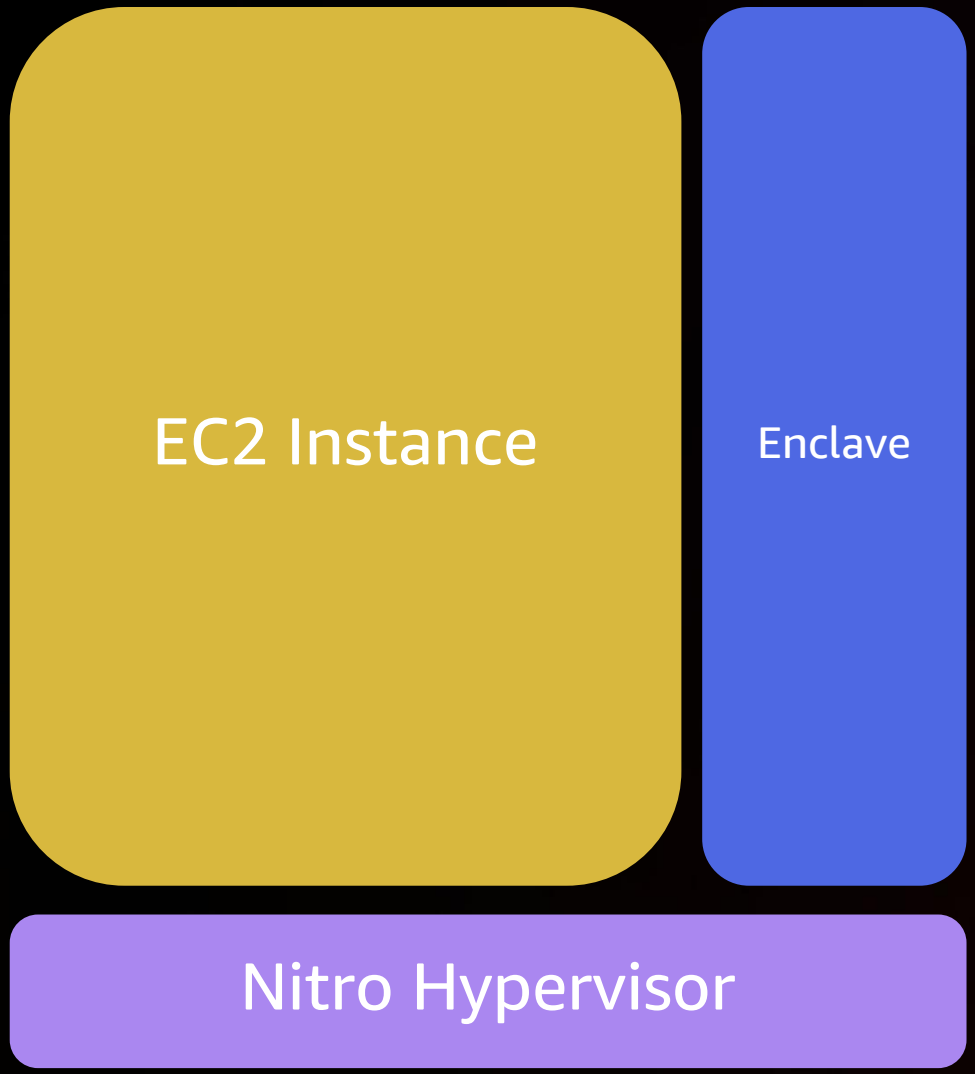
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro Enclaves



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

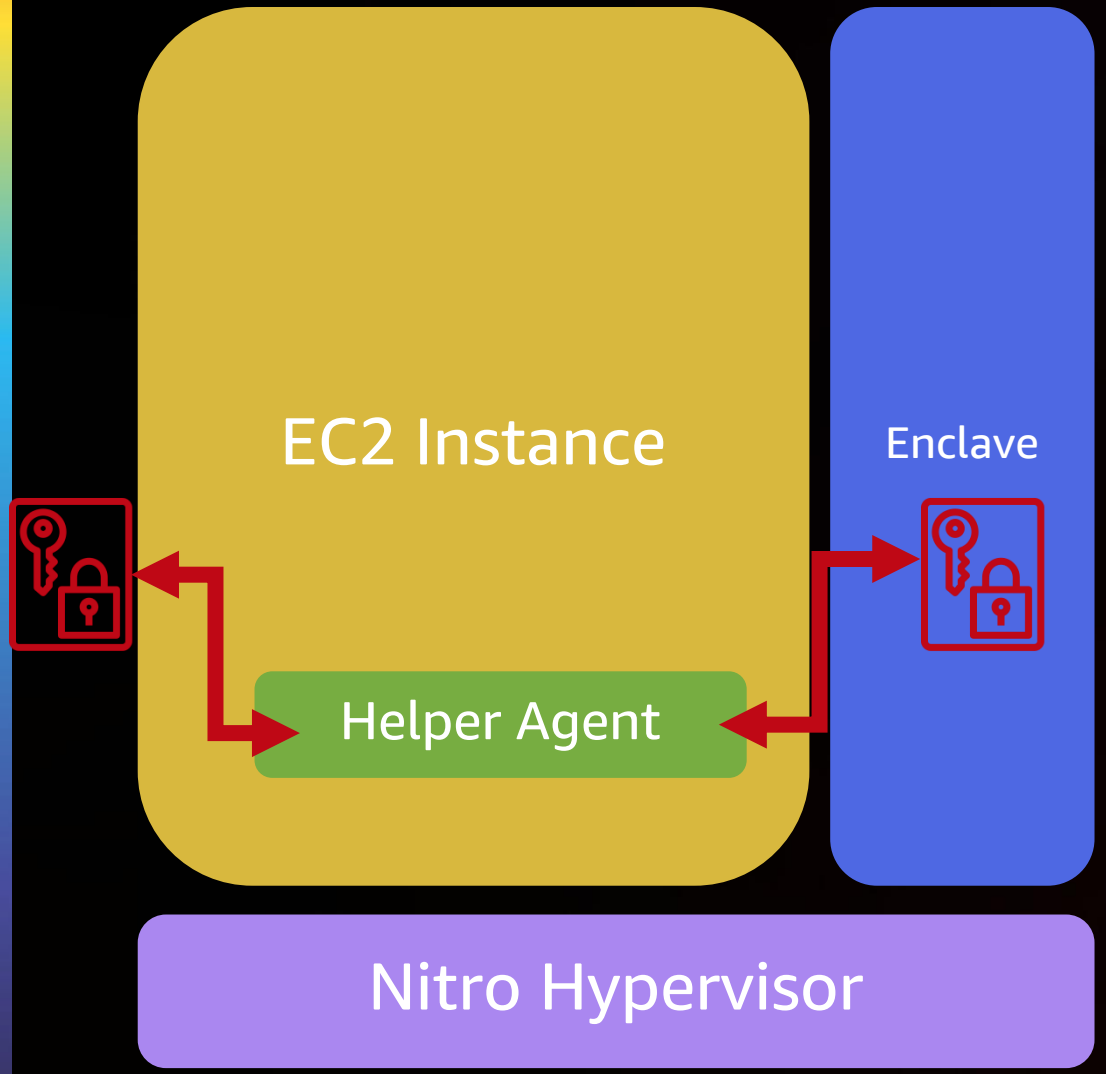
AWS Nitro Enclaves



- Nitro Enclaves are highly isolated
- No durable storage
- No network access
- No interactive access
- No metadata service, DNS, NTP

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

AWS Nitro Enclaves



- Helper agent forwards end-to-end encrypted communications between the enclave and select services
- Communications can be SSL/TLS or message-level encryption
- The agent has no visibility of the plaintext

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

AWS Nitro Enclaves attestation

- Cryptographic attestation is perfect precision biometrics for code
- Authenticates what the software ***is***
- Can be used contemporaneously or retroactively to verify what software handled data

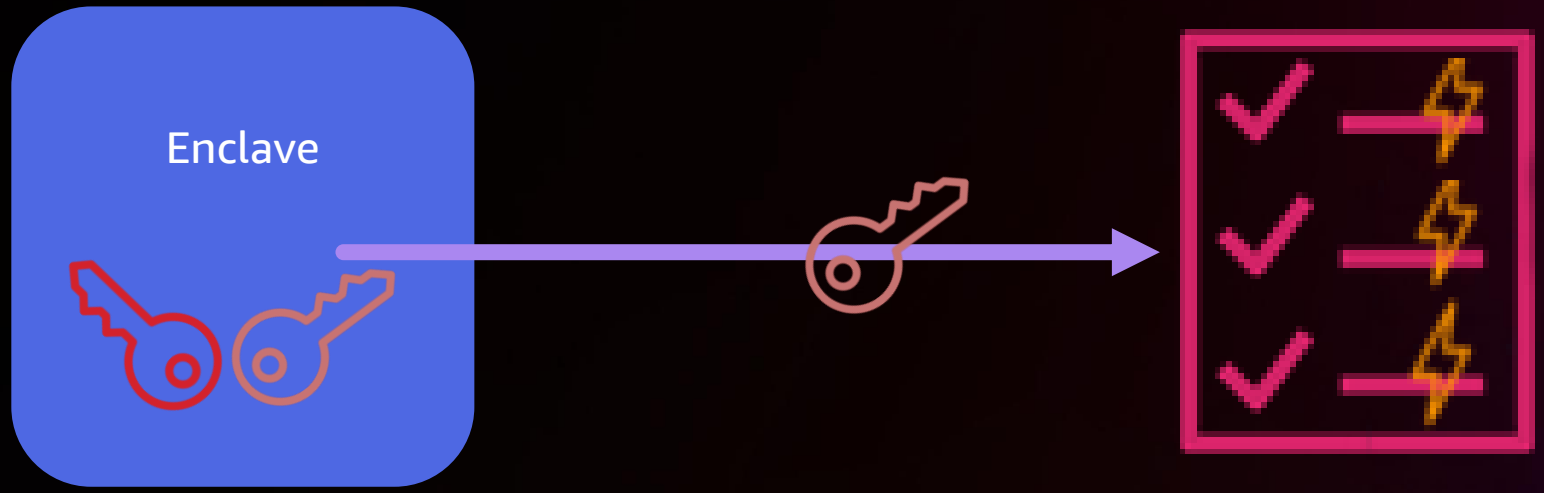


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Nitro Enclaves attestation

- Enclave generates a local public-private key pair

- Enclave supplies the public key, and an optional nonce, to the Nitro attestation service



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

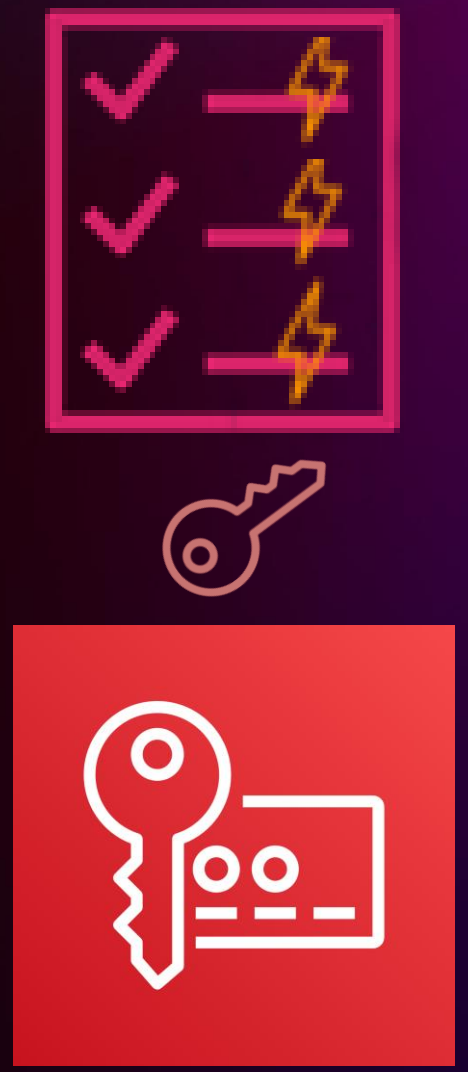
AWS Nitro Enclaves attestation

Nitro attestation service produces an attestation document that covers:

- Nonce, public key, enclave image checksum, kernel checksum, application checksum, enclave signing key, attached instance, instance role, launch time, current time

Attestation document is signed by the AWS Nitro Attestation PKI

Attestation document can be used with AWS KMS or third-party services



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

Introducing: *The Security Overview of the AWS Nitro System* whitepaper

- Detailed review of the security design the three primary components of the AWS Nitro System:
  - Nitro Cards,
  - Nitro Security Chip
  - Nitro Hypervisor
- Deep dive on the AWS Nitro System integrity protections, tenant isolation model, and no operator access design





https://a.co/hYWhsH9

aws

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

Zero-privilege operations

1. Foundational Principles ✓
2. Elemental Protections ✓
3. Always-on Accountability ✓
4. Contingent Authorization ✓
5. Hermetic Systems ✓

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

Zero-privilege operations takeaways

Ratcheting down permissions and access is the new normal. Go hand-in-hand with automation and operational improvements. Everybody wins!

Enable CloudTrail and MFA

Focus on at least achieving ZPO3 and ensuring that all access is accountable

Hermetic systems are more practical than ever

aws

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

Thank you!



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

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