



# A New Architecture to Free Incident Responders from False Positives

Rob Quiros

CEO & Co-Founder  
Caber Systems, Inc.

[rob@caber.com](mailto:rob@caber.com)



LinkedIn



95%

## False Positive Rate

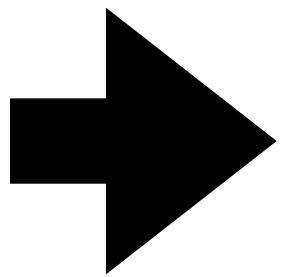
<https://www.sans.org/white-papers/2023-survey-event-incident-response/>



caber.com

caber

**Indicator of  
Compromise**

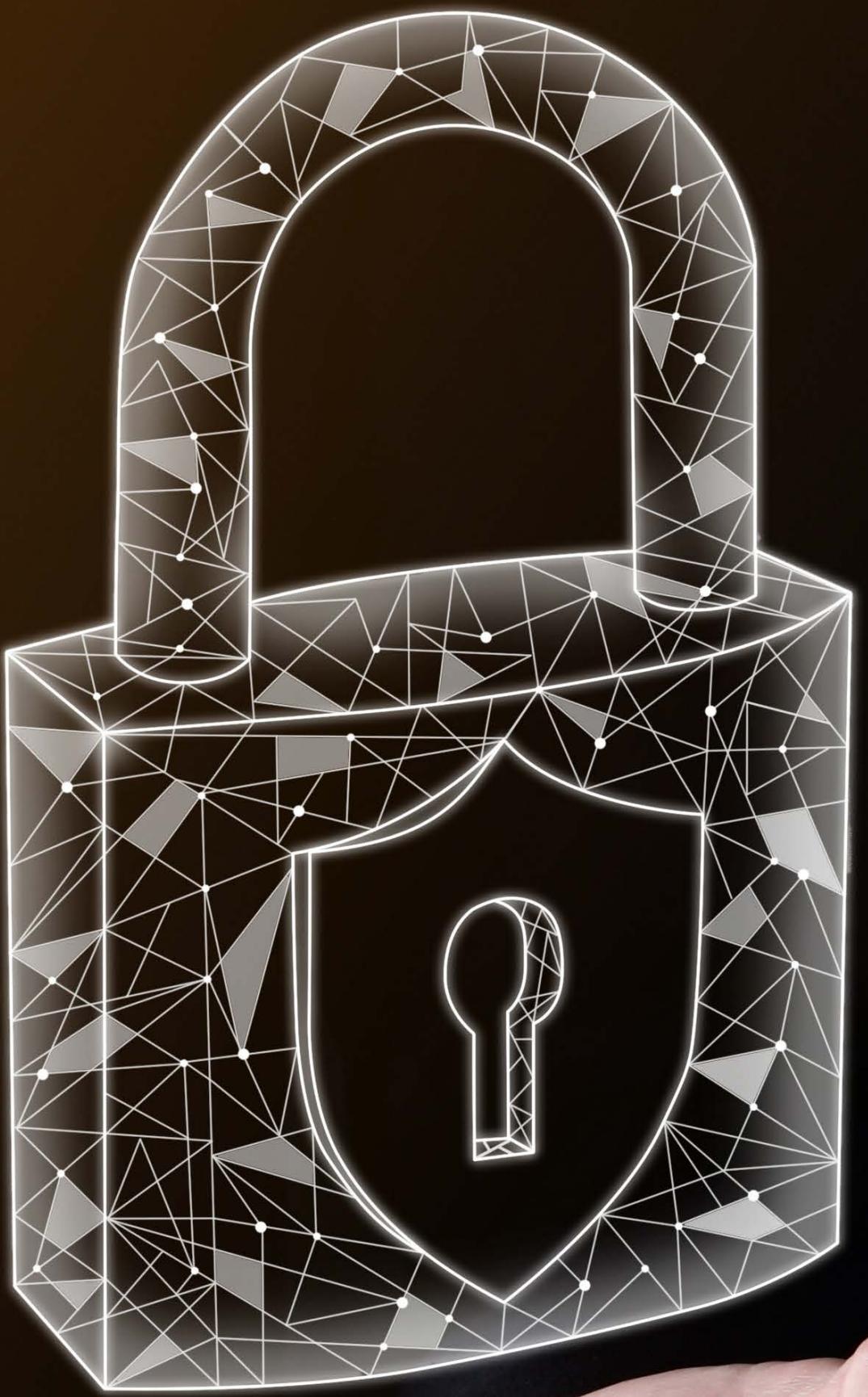


**Actual  
Compromise**



[caber.com](http://caber.com)

**caber**



DATA

Confidentiality

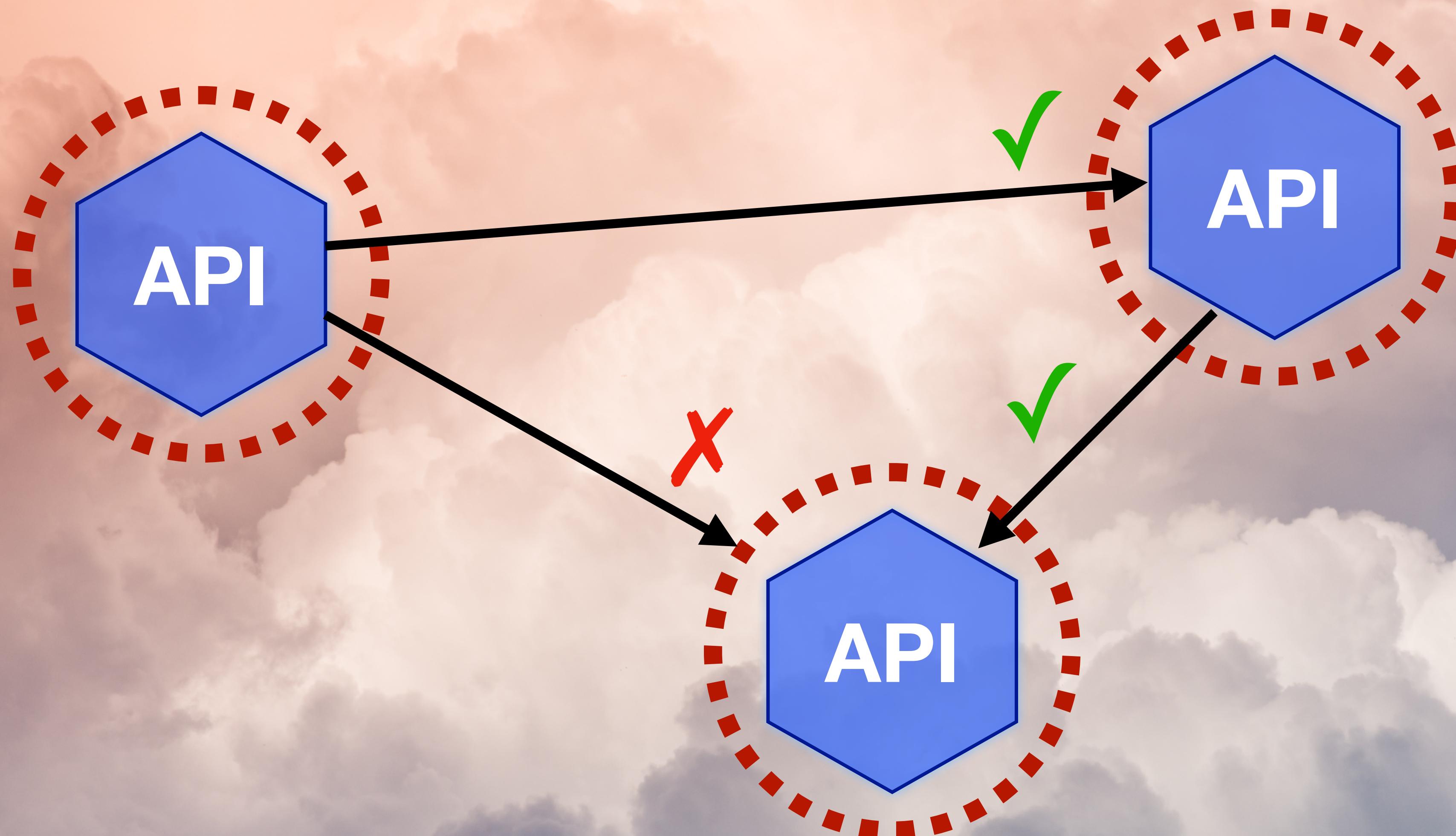
Integrity

Availability

# NIST Cybersecurity Framework 2.0

- 
- **Data Security (PR.DS):**
    - **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected
    - **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
    - **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
- 





*infinite* — ~~Zero~~ Trust Network Access



Bag labelled sand → Bag contains sand



[caber.com](http://caber.com)

caber

# Data Leakage Prevention (DLP)



Looks like money so must be money



[caber.com](http://caber.com)

caber

# OWASP API Security

## Top Ten - 2023

- API1 **Broken** Object-Level Authorization
- API2 **Broken** Authentication
- API3 **Broken** Object Property Level Authorization
- API4 **Unrestricted** Resource Consumption
- API5 **Broken** Function Level Authorization
- API6 **Unrestricted** Access to Sensitive Business Flows
- API7 Server Side Request **Forgery**
- API8 Security **Misconfiguration**
- API9 **Improper** Inventory Management

## Authorization:

Your Data

vs.

My Data

# DETERMINISTIC

```
if user == "bob" and data_owner == "bob":  
    return True
```



# Direct Data-in-Use Access Control Solves:

- Broken Object Level Authorization (BOLA)
- Privilege Escalation
- SQL Injections
- Software Errors
- Confused Deputy Problems
- Misconfigurations



BOLA: 885 Million customer documents leaked

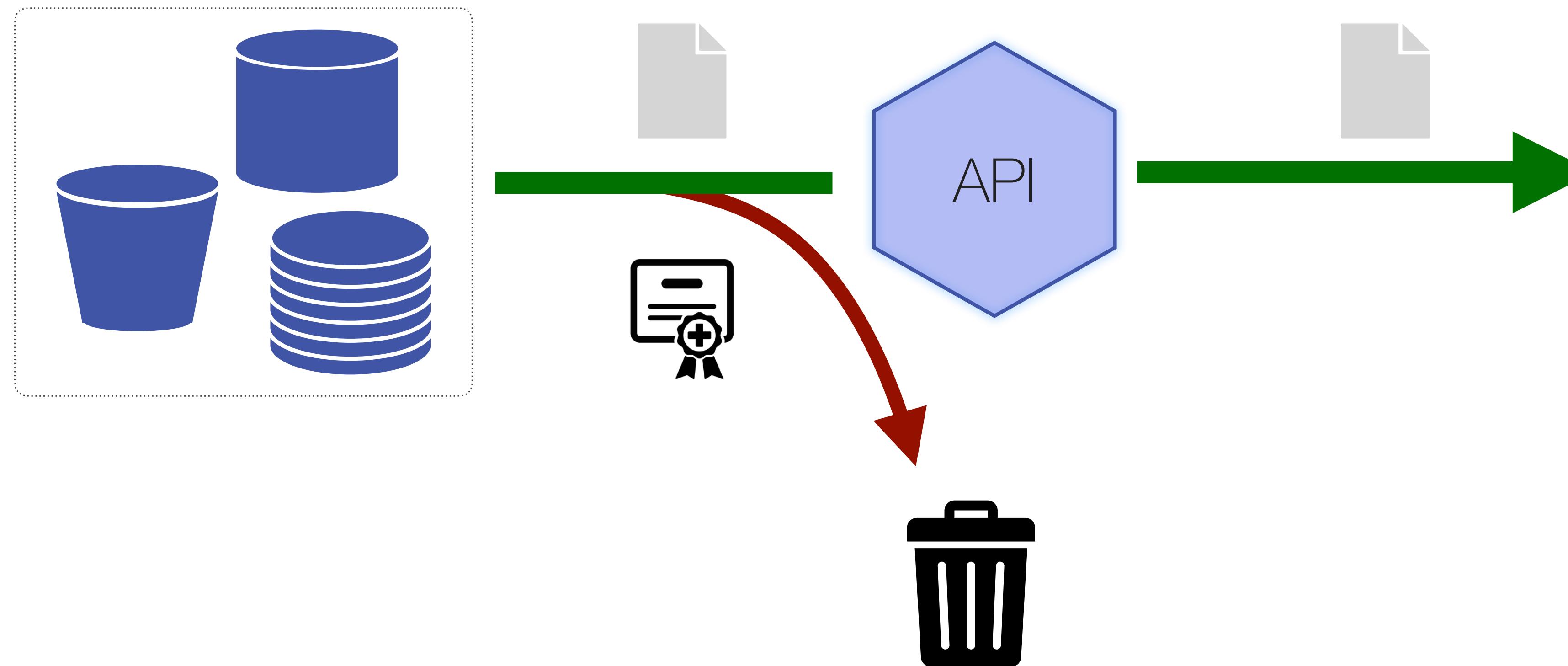
# Three Hard Problems to Solve

## Cloud-Native Applications

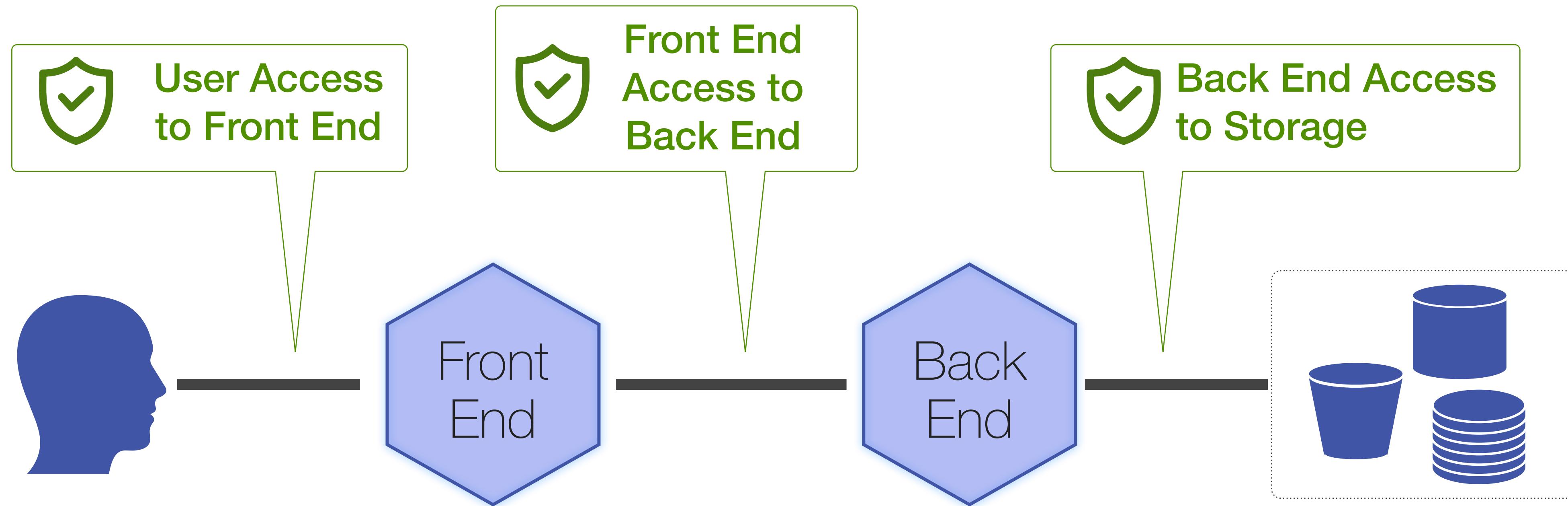
---

1. Data permissions and ownership not sent in APIs
2. Service accounts access data on behalf of users
3. APIs move pieces of data (chunks) from objects

# API's Don't Send Permissions With Data

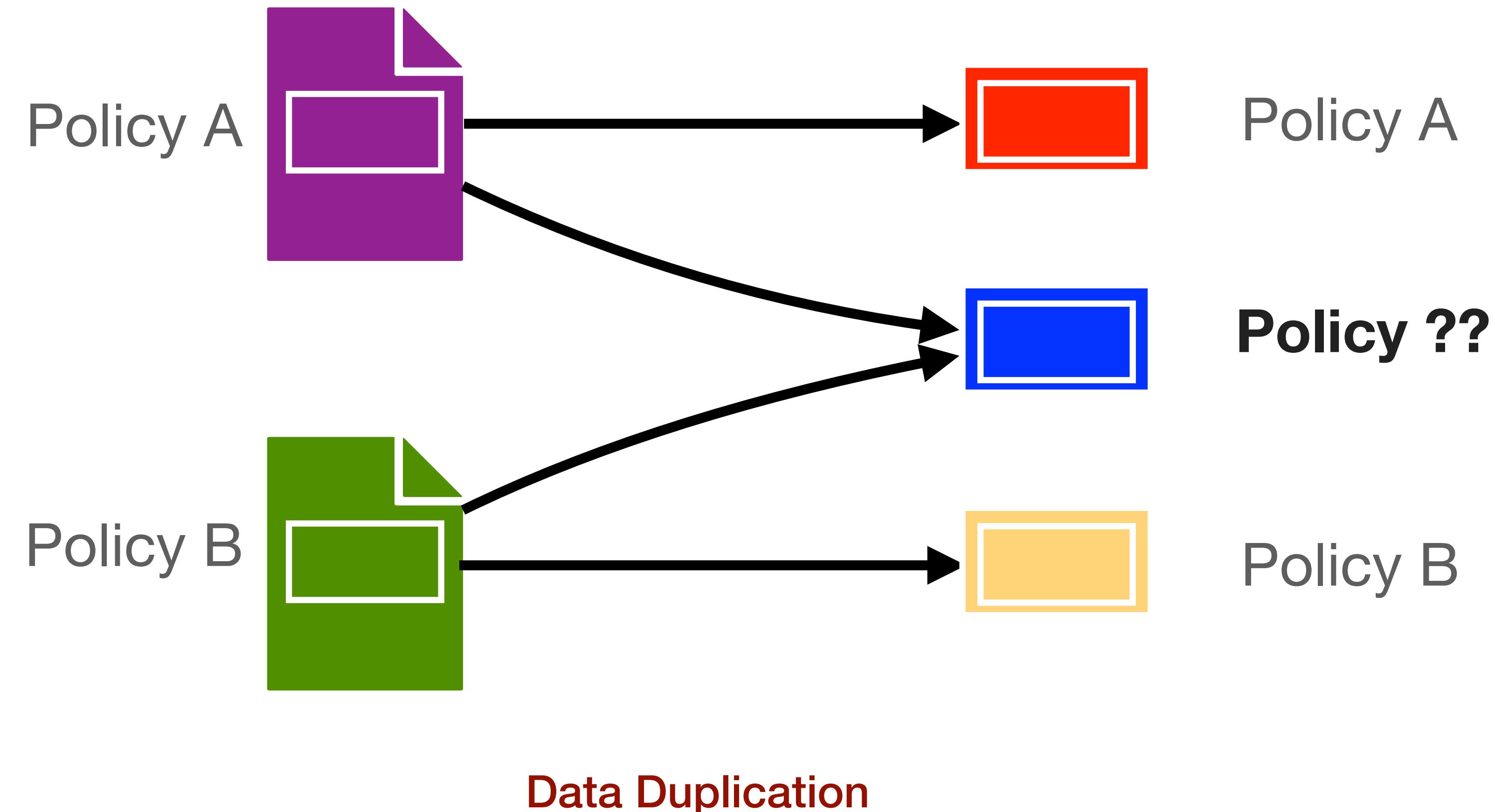


# Service Accounts Hide End-User Identity



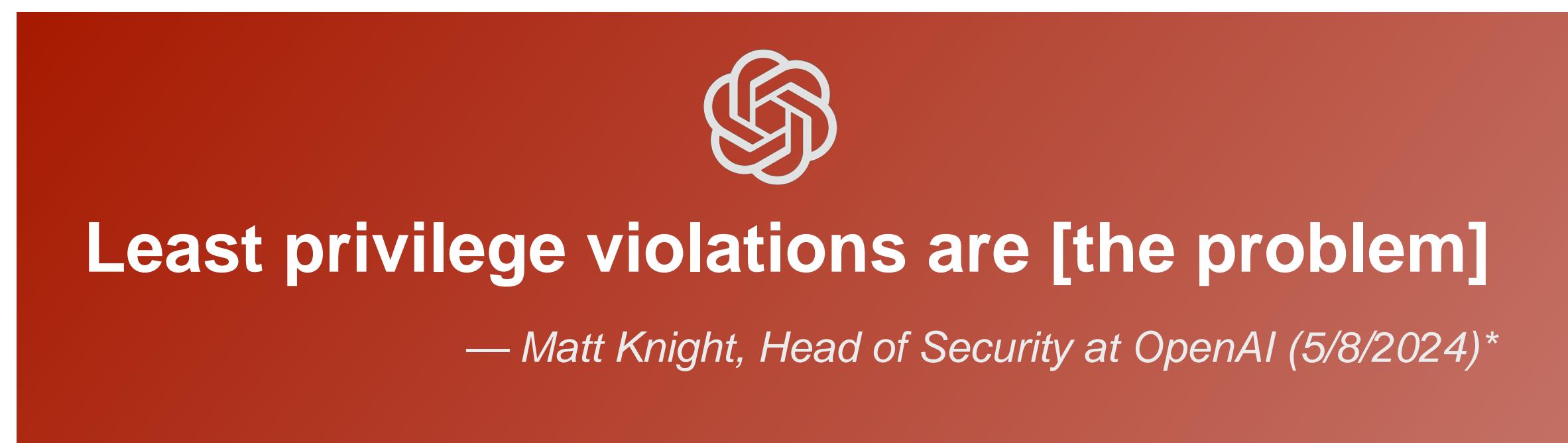
**CONFUSED DEPUTY PROBLEM**

# Permissions on Chunks



# GenAI: All Three Problems Plus...

Many chunks, different owners, in same payload



Ensure only you can  
get your money

\* <https://a16z.com/podcast/securing-the-black-box-openai-anthropic-and-gdm-discuss/> 38:40

# New Architectures to Fix these Problems

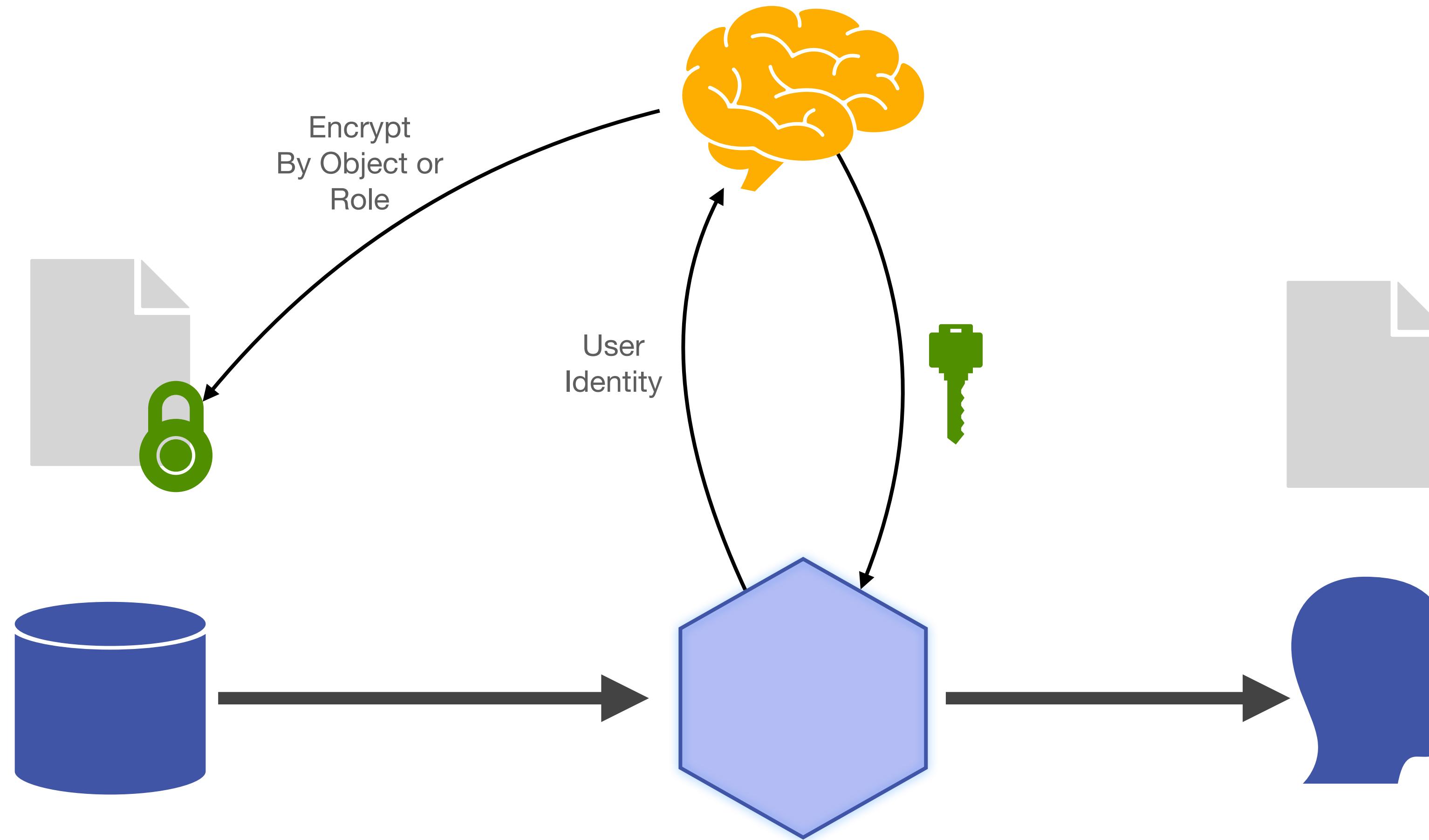
- Enterprise Digital Rights Management (eDRM)
- Google's BeyondProd + Zanzibar
- Data Lineage Tracing (Caber)



[caber.com](http://caber.com)

caber

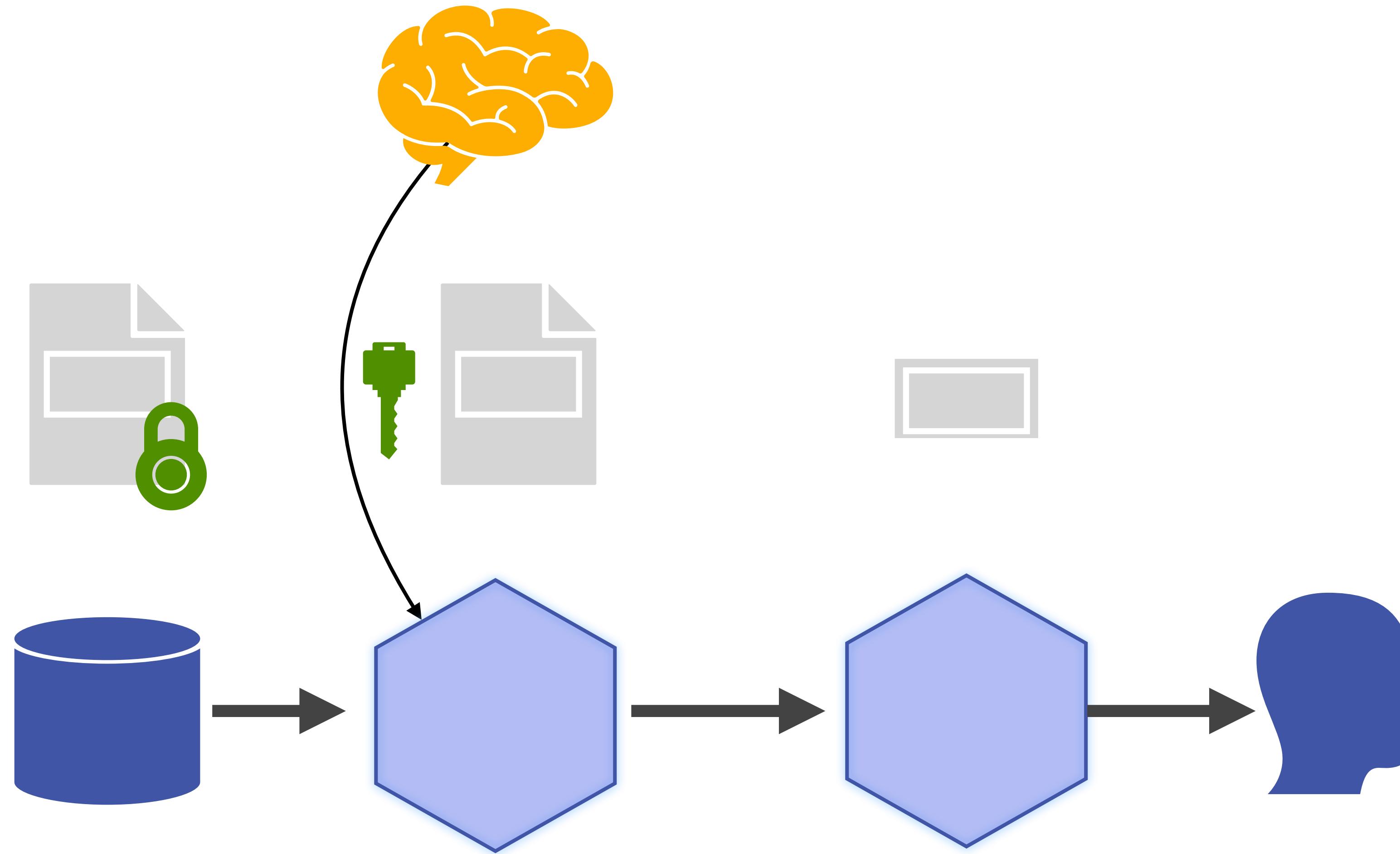
# eDRM



[caber.com](http://caber.com)

caber

# eDRM

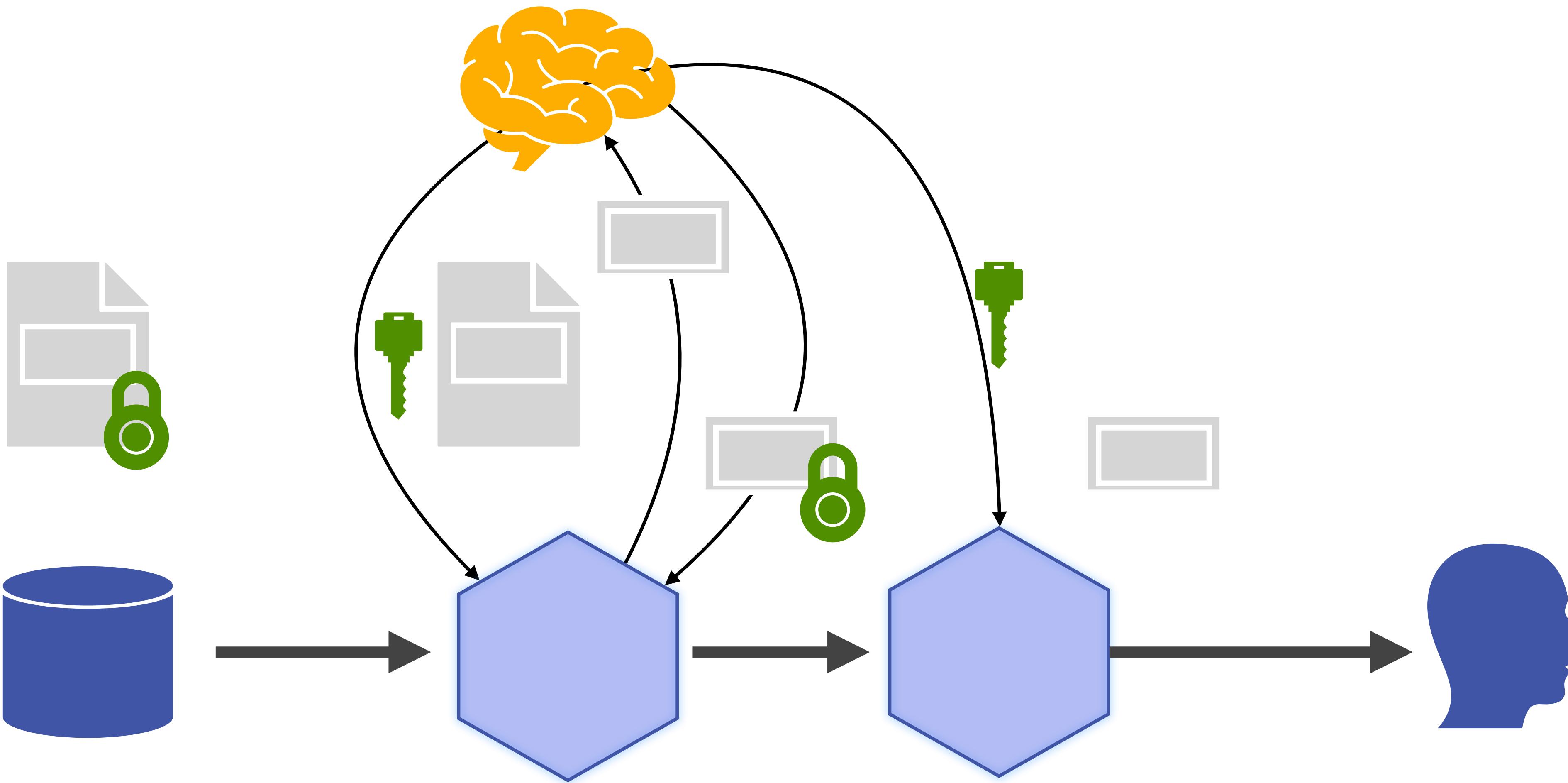


[caber.com](http://caber.com)



caber

# eDRM



caber.com



caber

Google Cloud

Contact sales Get started for free

Blog Solutions & technology Ecosystem Developers & Practitioners Transform with Google Cloud

Security & Identity

## BeyondProd: How Google moved from perimeter-based to cloud-native security

December 17, 2019

**Maya Kaczorowski**  
Product Manager, Container Security

**Brandon Baker**  
Horizontal Lead, Cloud Security

[Twitter](#) [LinkedIn](#)

At Google, our infrastructure runs on containers, using a container orchestration system [Borg](#), the precursor to Kubernetes. Google's architecture is the inspiration and template for what's widely known as "[cloud-native](#)" today—using microservices and containers to enable workloads to be split into smaller, manageable units for maintenance and discovery.

Google's cloud-native architecture was developed prioritizing security as part of every evolution in our architecture. Today, we're introducing a whitepaper about [BeyondProd](#), which explains the model for how we implement cloud-native security at Google. As many organizations seek to adopt cloud-native architectures, we hope security teams can learn how Google has been securing its own architecture, and simplify their adoption of a similar security model.



≡ Google Research

[Publications >](#)

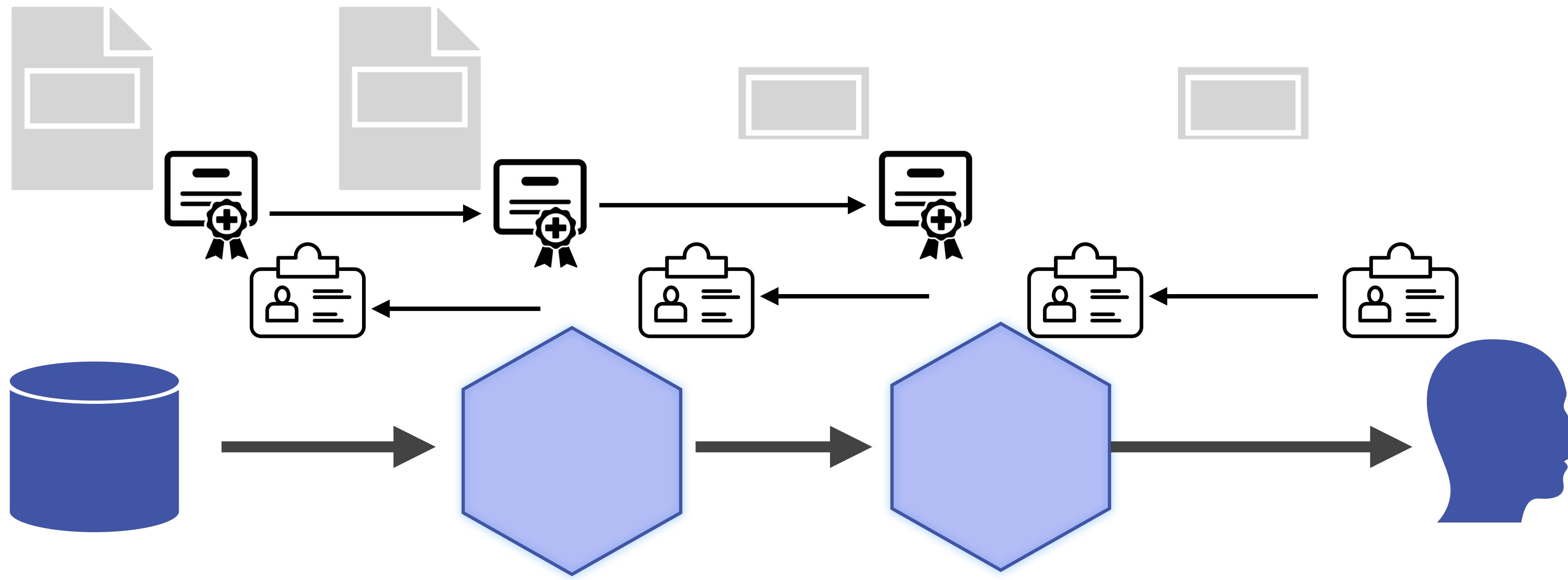
## Zanzibar: Google's Consistent, Global Authorization System

Ruoming Pang · Ramon Caceres · Mike Burrows · [Zhifeng Chen](#) · Pratik Dave · [Nathan Germer](#) · Alexander Golynski · [Kevin Graney](#) · Nina Kang · Lea Kissner · [Jeffrey L. Korn](#) · Abhishek Parmar · Christina D. Richards · Mengzhi Wang ·

2019 USENIX Annual Technical Conference (USENIX ATC '19), Renton, WA

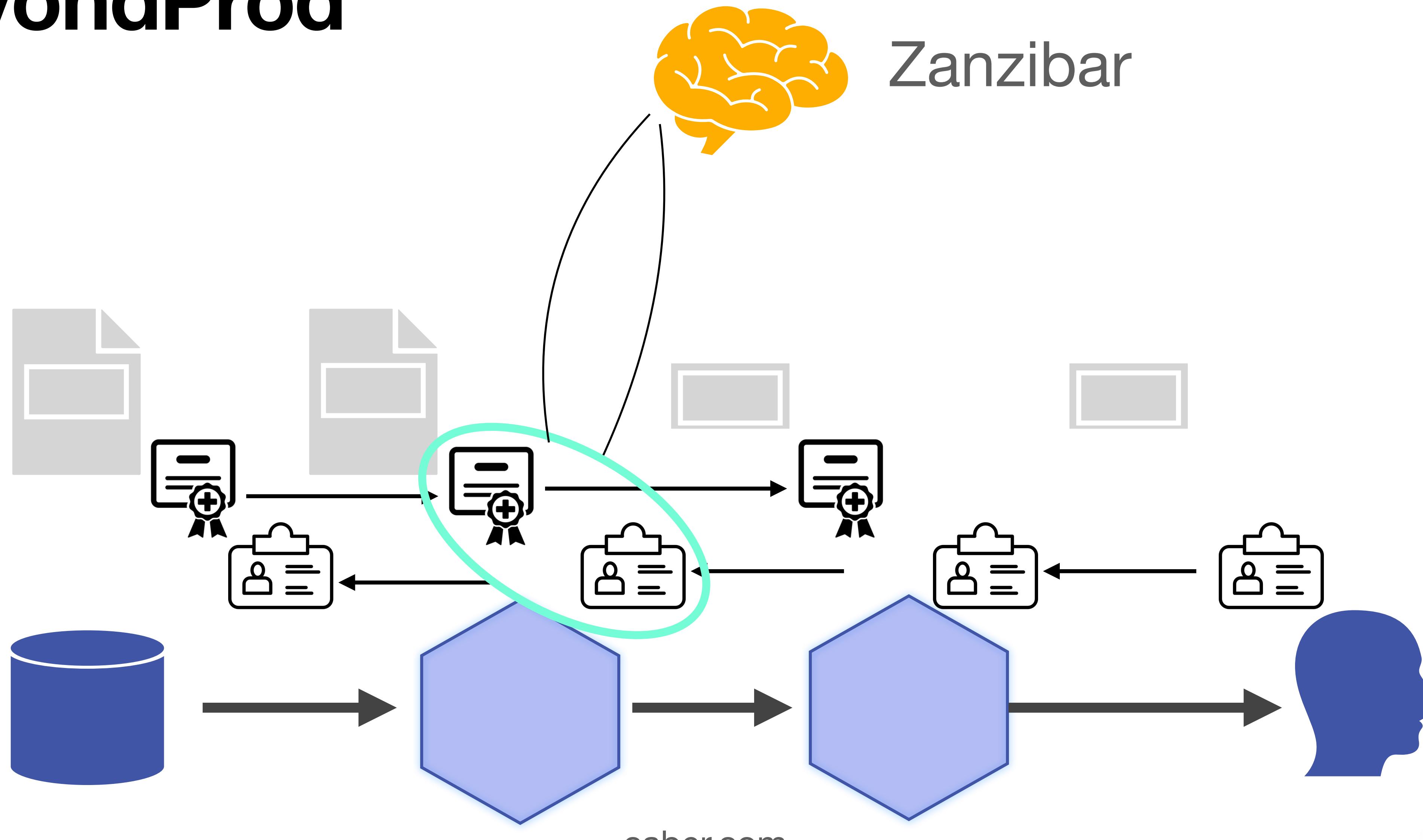


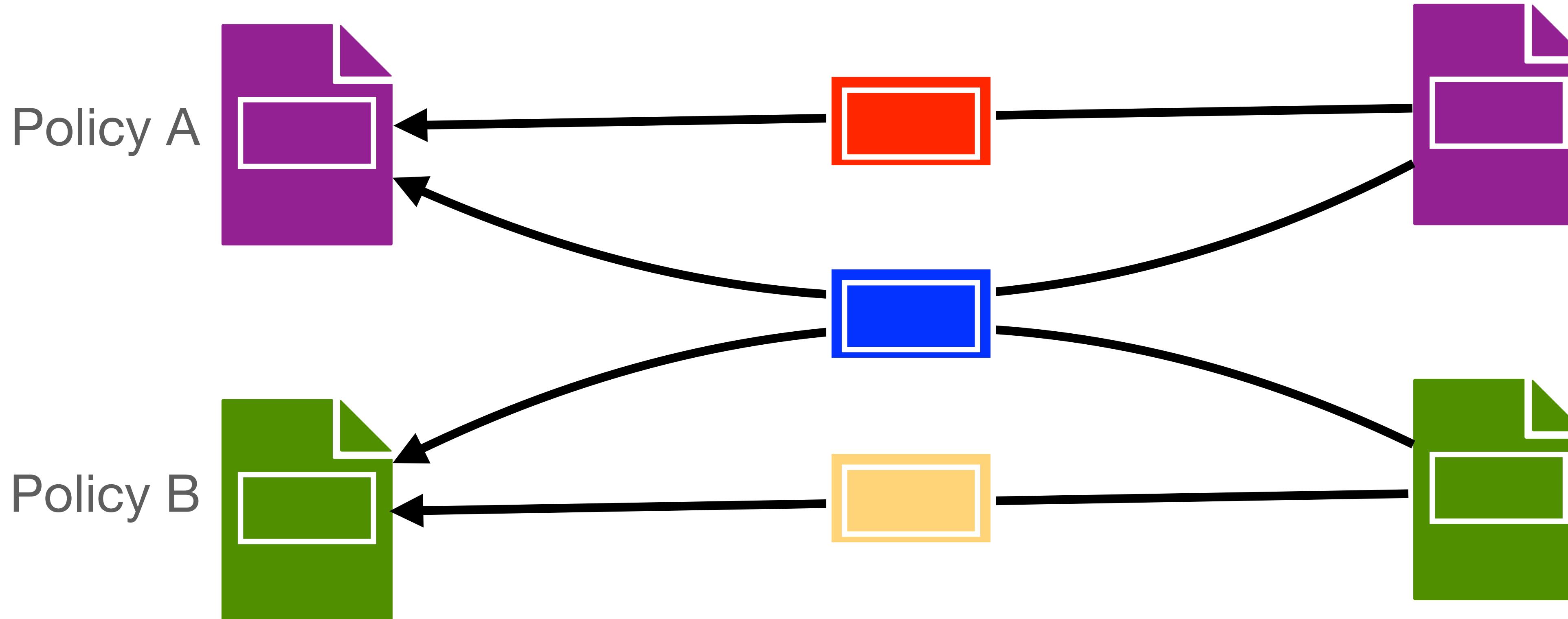
# BeyondProd



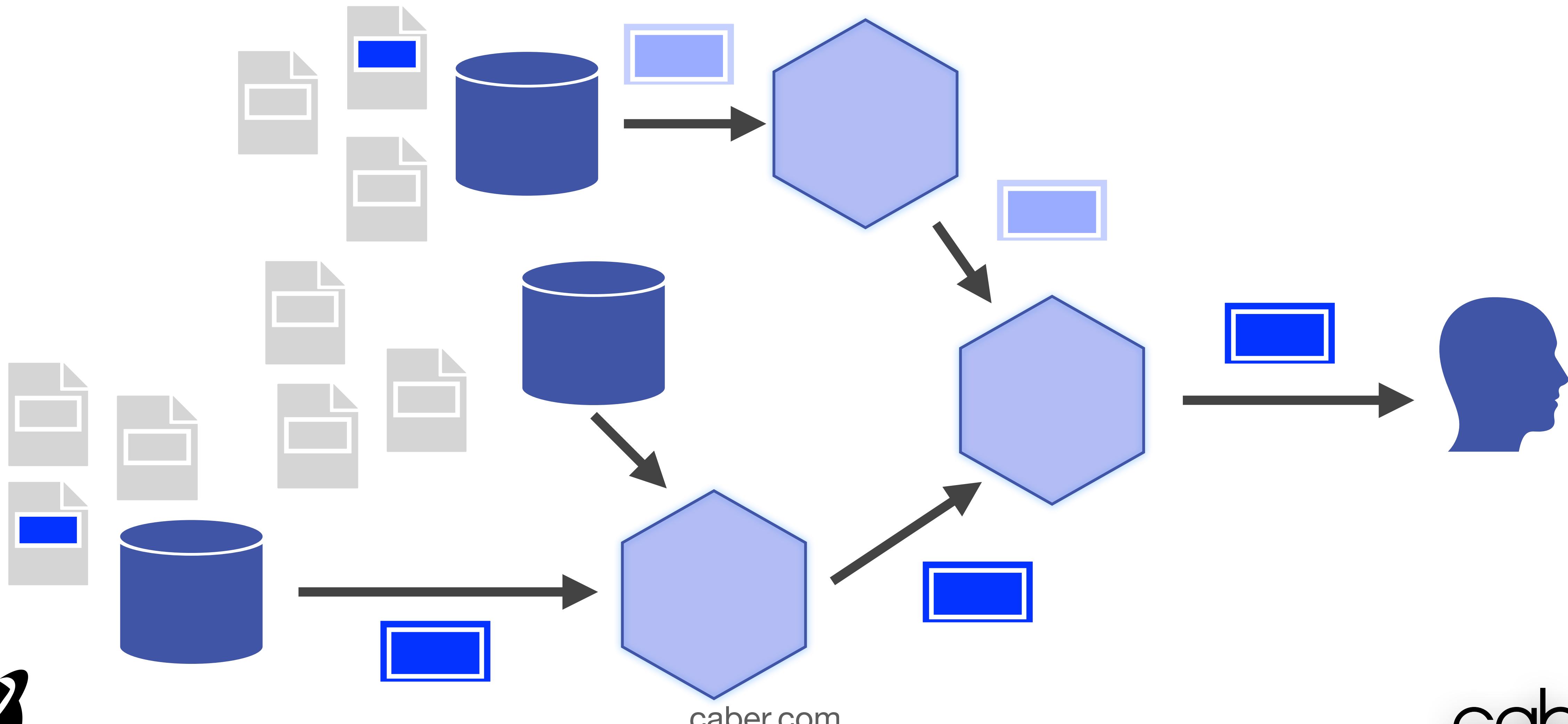
# BeyondProd

Zanzibar

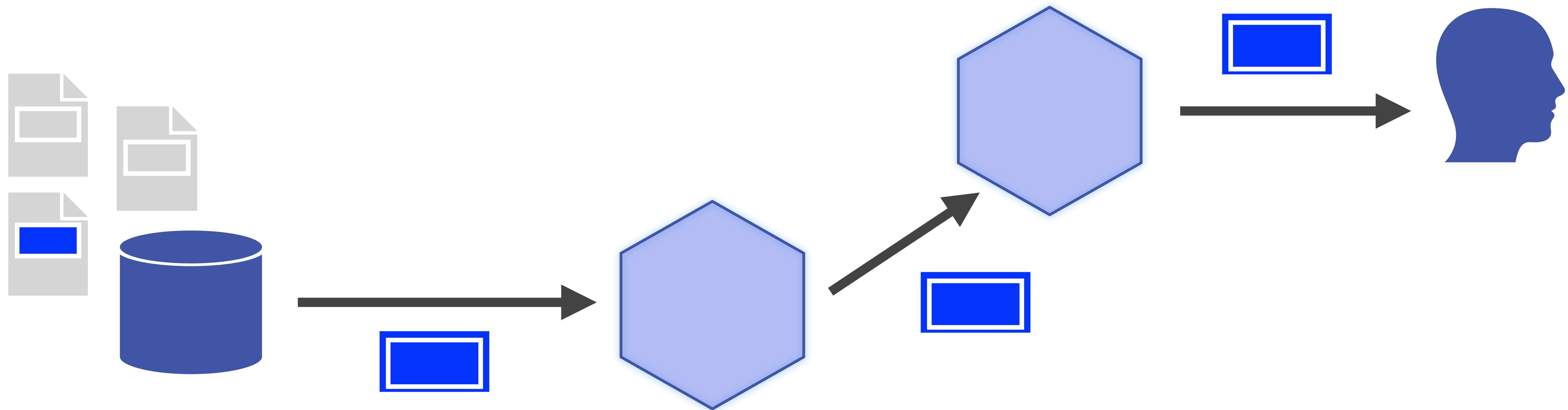




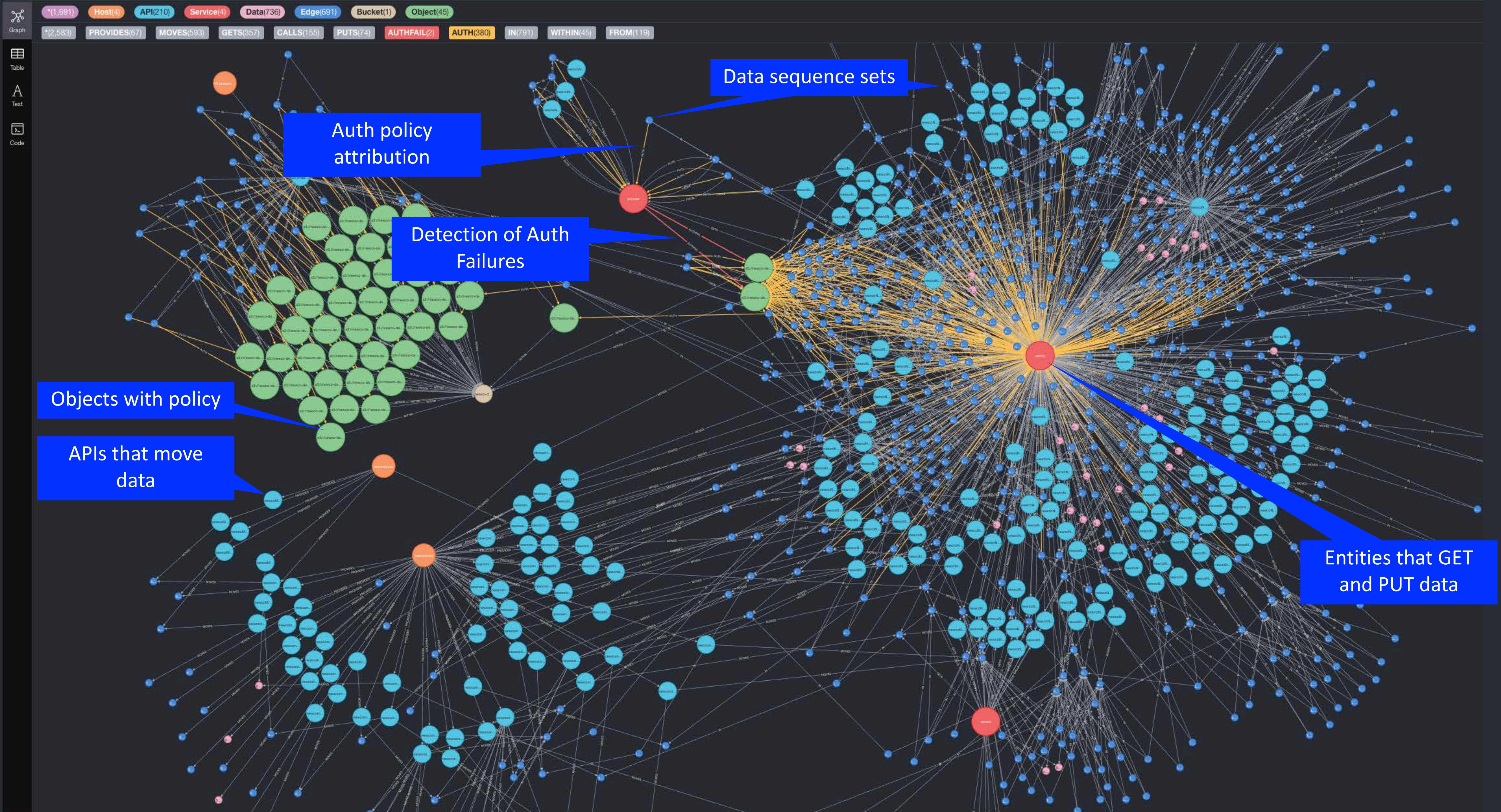
# Data Lineage Tracing



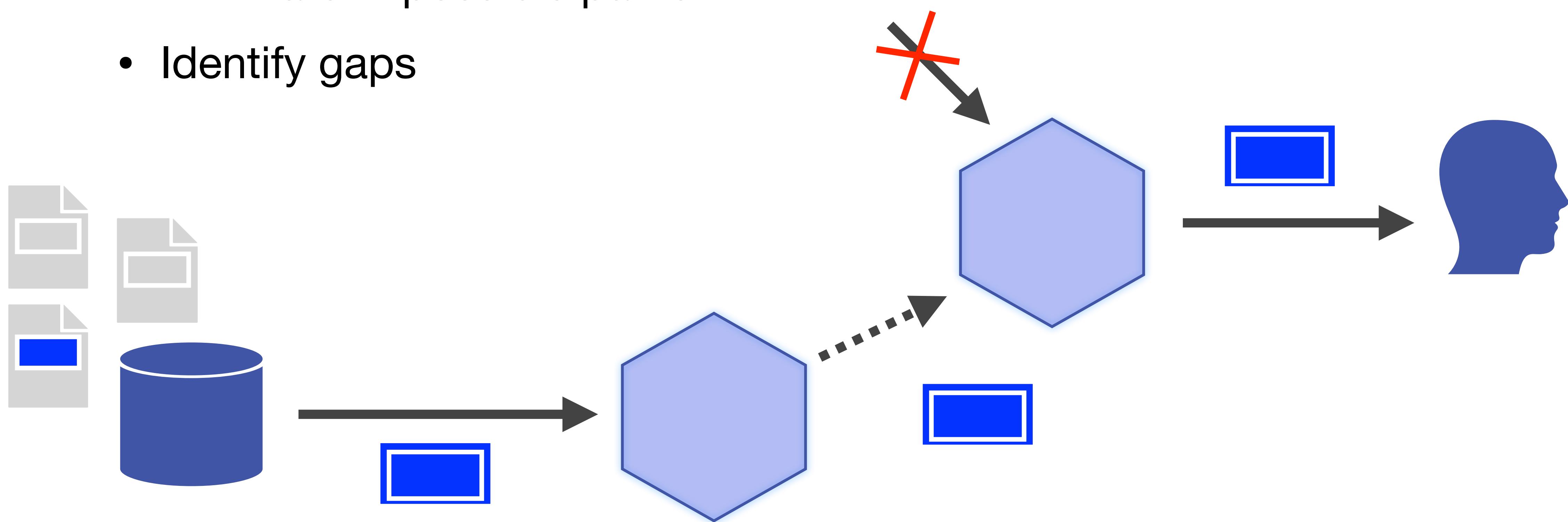
- Content-defined chunking in time window
- Find API Payloads and objects with common chunks
- Use common chunks to build relationships



```
neo4j$ match (n) return n
```



- Time-series analysis of related events
- Event ordering
- Eliminate impossible paths
- Identify gaps



cabер

HO

hoydipakki  
hoydipakki@gufum.com

DEPLOYMENT  
BGNFRD955QKWPW3DG1UK5YDX

Back to Deployments

Dashboard

Home

Access Authorization

Data Flow Analyzer

Overlapping Objects

RESOURCES

Object Stores (4)

Databases

Streams

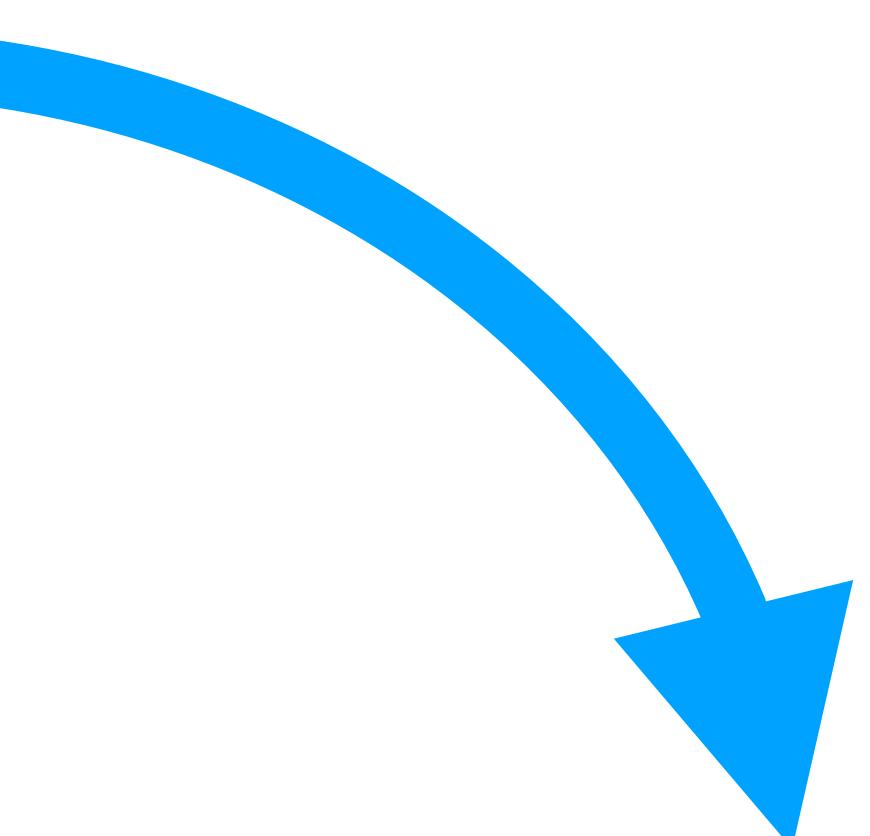
APIs

Identity Sources

Payload Access Authorization

Authorization Failure Incidents

			70	1	BOB	GET 7/9836	newco-docs-/urn:oid:116	<ul style="list-style-type: none"><li>User 'bob' getting data from object owned by 'amy'</li><li>Permissions inherited from object disallow access</li></ul>
			69	1	NEWCO-DISRUPT	GET 19/51	newco-docs-/urn:oid:96	<ul style="list-style-type: none"><li>User 'newco-disrupt' and object owner 'bob' are in different identity realms</li><li>No cross-realm policy exists between authenticators s3aws and newco-nextcloud</li></ul>
			62	1	NEWCO-DISRUPT	GET 10/283	newco-docs-/urn:oid:89	<ul style="list-style-type: none"><li>User 'newco-disrupt' and object owner 'amy' are in different identity realms</li><li>No cross-realm policy exists between authenticators s3aws and newco-nextcloud</li></ul>
			61	1	NEWCO-DISRUPT	GET 7/9836	newco-docs-/urn:oid:116	<ul style="list-style-type: none"><li>User 'newco-disrupt' and object owner 'amy' are in different identity realms</li><li>No cross-realm policy exists between authenticators s3aws and newco-nextcloud</li></ul>
			55	1	NEWCO-NEXTCLOUD	PUT 7/9836	newco-docs-/urn:oid:116	<ul style="list-style-type: none"><li>User 'newco-nextcloud' and object owner 'amy' are in different identity realms</li><li>No cross-realm policy exists between authenticators s3aws and newco-nextcloud</li></ul>



70 1 BOB GET  
7/9836 newco-docs-/urn:oid:116

- User 'bob' getting data from object owned by 'amy'
- Permissions inherited from object disallow access



## Authorized Access to RAG chunked data

2024July 1,  
2023  
Gross margin:  
Products \$ 21,761 \$ 21,448 \$ 84,241 :  
Services 17,917 14,965 52,563 44  
Total gross margin \$ 39,678 \$ 36,413  
Gross margin percentage:  
Products 35.3% 35.4% 37.5% 36.5%  
Services 74.0% 70.5% 73.8% 70.8%  
Total gross margin percentage 46.3%  
Products Gross Margin  
Products gross margin was relatively  
2023.  
Products gross margin percentage was

How has Apple's gross margin percentage evolved from fiscal Q1 2023 and Q3 2024, and what factors have contributed to these changes?

Apple's gross margin percentage has evolved positively from fiscal Q1 2023 to Q3 2024.

In fiscal Q1 2023, the total gross margin percentage was 43.0%. By Q3 2024, this percentage had increased to 46.3%.

Several factors contributed to these changes:

## Un-authorized Access

2024July 1,  
2023  
Gross margin:  
:gray[ -REDACTED 45B CABER.COM-]  
:gray[ -REDACTED 41B CABER.COM-]  
:gray[ -REDACTED 57B CABER.COM-]  
Gross margin percentage:  
:gray[ -REDACTED 37B CABER.COM-]  
:gray[ -REDACTED 37B CABER.COM-]  
:gray[ -REDACTED 58B CABER.COM-]  
Products Gross Margin  
:gray[ -REDACTED 130B CABER.COM-]  
2023.  
:gray[ -REDACTED 79B CABER.COM-] f 26

Tell me how has Apple's gross margin percentage evolved from fiscal Q1 2023 and Q3 2024, and what factors have contributed to these changes?

The provided context does not contain specific information about Apple's gross margin percentage from fiscal Q1 2023 or Q3 2024. It discusses gross margins for the periods of Q3 2023 and prior but does not detail Q1 2023 or Q3 2024 metrics or the evolution of gross margins across those quarters.

However, in the context for Q3 2023, the gross margin percentages were reported as:

# Deterministic

- 2 or more observation points
- Low/no performance impact
- Avoid code changes



[caber.com](http://caber.com)

caber

# Detect Incidents Without False Positives\*

\*Probability on the order of a hash collision

[caber.com](http://caber.com)

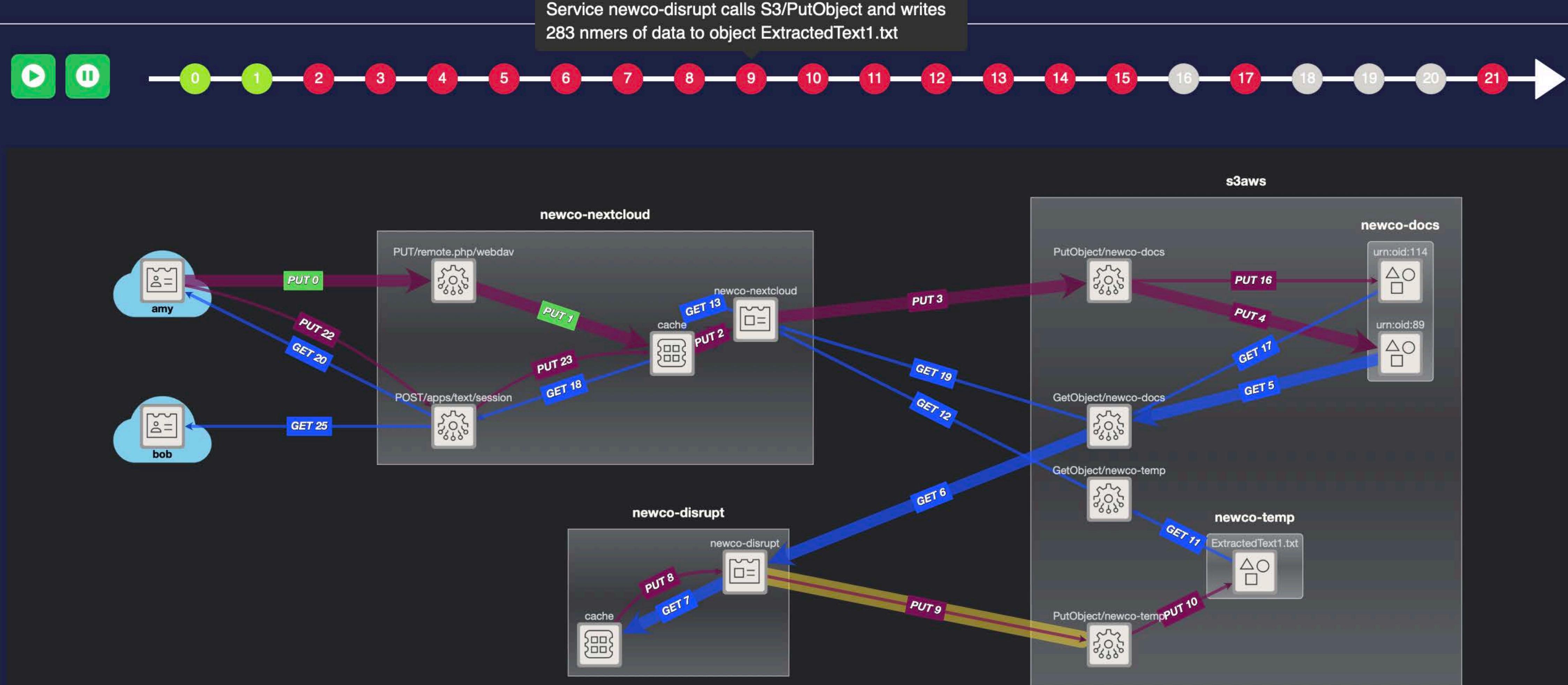


caber

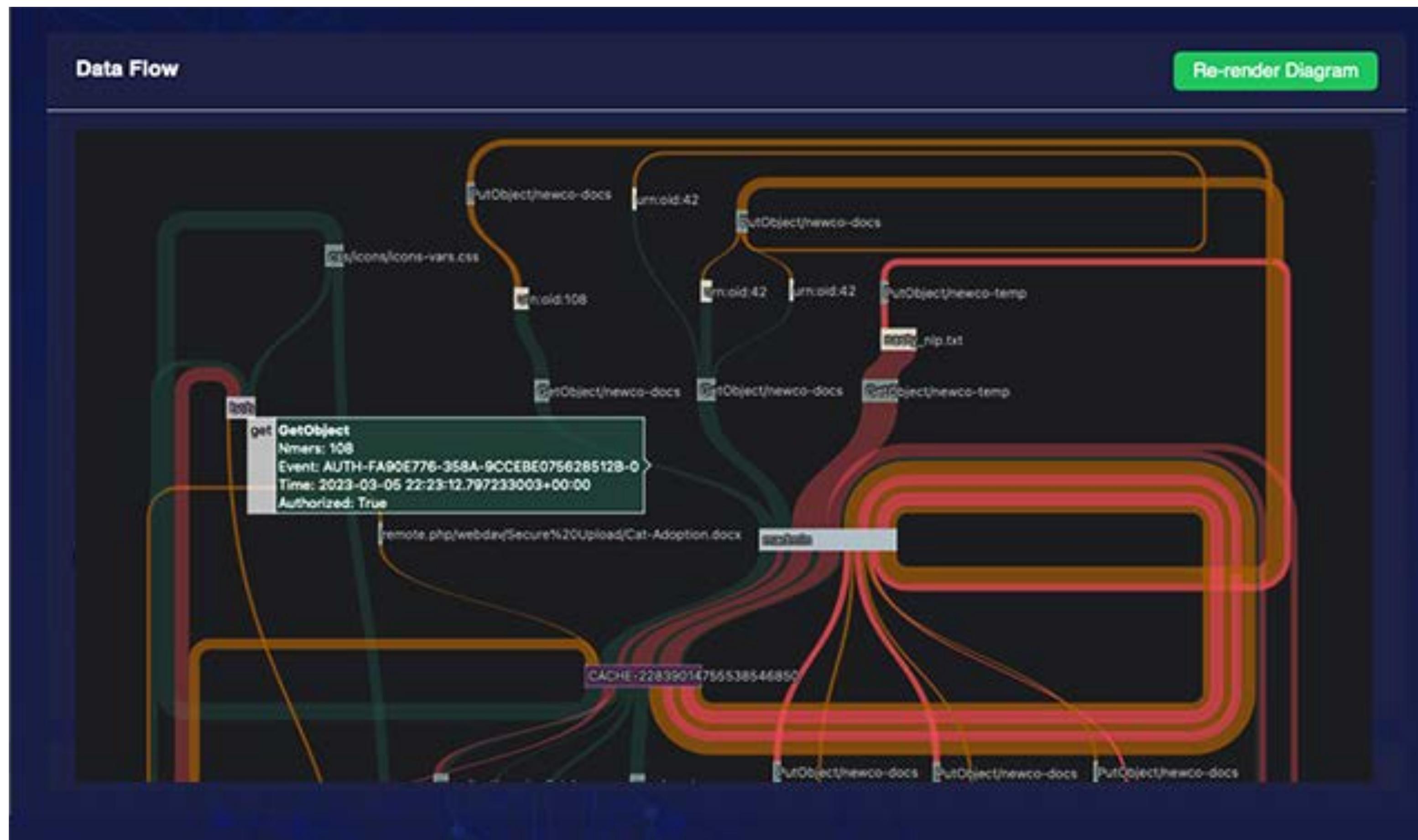


- 🌐
- 👤
- 📖
- ◻◻◻
- 📄
- ?
- ✉️
- 📁
- ☰

## Incident Call Graph

Fix Layout

# Detailed Observability of Application Flow



# Analyze and debug application behavior

# Data Compliance Requirements to Policy

The screenshot shows a user interface for creating an IAM policy. At the top, there's a button labeled "Add Enforcement Policy" with a shield icon. Below it, the "Intent" section contains a note: "Policy specific to authenticator newco-nextcloud to prevent user 'bob' and from accessing object owned by 'amy'". The "Adjustments" section includes an "Object Scope" dropdown set to "Just this object and version" and an "Effect" section with radio buttons for "Report only", "Enforce via bucket policy" (which is selected), and "Enforce via S3 Object Lambda". The "Allowed Actions" section lists several actions: "None" (selected), "s3:PutObject\*", "s3:GetObject\*", "s3:DeleteObject\*", "s3:GetObjectTagging", and "s3:PutObjectTagging". In the "Generated Policy" section, the "Summary" part explains the purpose of the policy: "The purpose of the modified policy is to prevent an unintended exposure of sensitive data that was uploaded to an S3 bucket by a specific user. The policy restricts read access for one role, ensuring that data uploaded by a particular user cannot be accessed by that role, which might not have the appropriate authorization to view the data." The "Explanation" part provides a detailed description of the policy's effect: "The policy explicitly denies 'GetObject' permission to an IAM role 'newco-disrupt-2024021020324307670000002c' for all objects in the 'newco-docs-bgnfrvnj7dk2jpp6pdnj1yq' bucket that are tagged with the key 'csi.owner' and the corresponding value 'amy'. It achieves this by using the 'Deny' effect, which takes". To the right of the explanation, a code block shows the JSON representation of the generated policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "DenyReadAccessBasedOnTags",  
      "Effect": "Deny",  
      "Principal": {  
        "AWS": "arn:aws:sts::489917293372:assumed-role/newco-disrupt-2024021020324307670000002c"  
      },  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::newco-docs-bgnfrvnj7dk2jpp6pdnj1yq/*",  
      "Condition": {  
        "StringEquals": {  
          "aws:s3:object-owner": "arn:aws:iam::123456789012:User/bob"  
        }  
      }  
    }  
  ]  
}
```

GenAI analysis and dynamic data tagging to build policy from high level requirements



# Thank You!

**Rob Quiros**

rob@caber.com  
<https://caber.com>