A New Architecture to Free Incident Responders from False Positives

Rob Quiros

CEO & Co-Founder
Caber Systems, Inc.

rob@caber.com

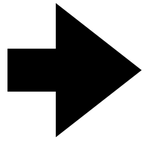
LinkedIn

95%

False Positive Rate

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

Indicator of Compromise

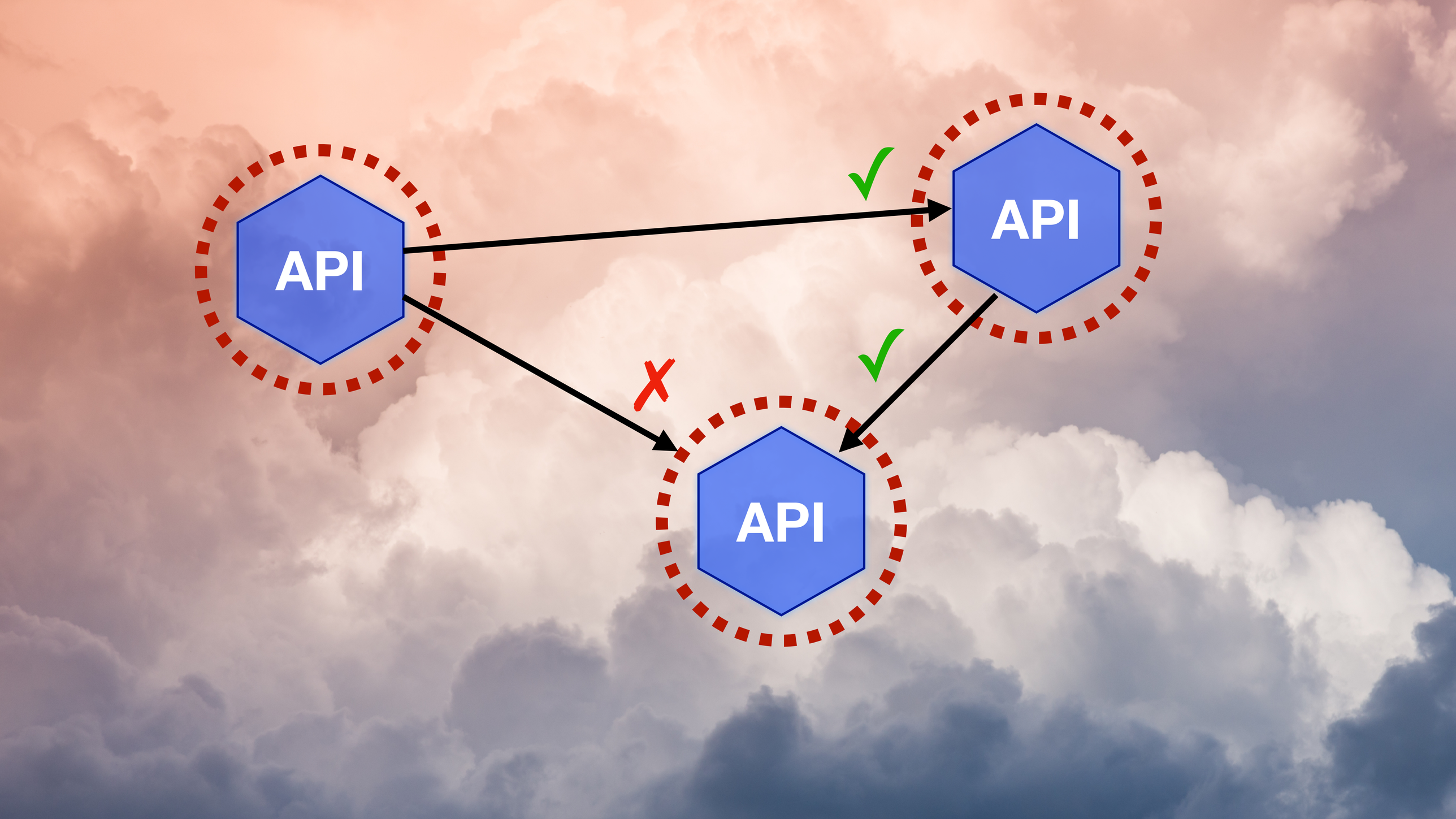


Actual Compromise


Confidentiality
Integrity
DATA
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


API
API
API

infinite ~~Zero~~ Trust Network Access

Bag labelled sand → Bag contains sand

Data Leakage Prevention (DLP)

Looks like money so must be money

Authorization:

Your Data

vs.

My Data

caber

DETERMINISTIC

```
if user == “bob” and data_owner == “bob”:
   return True
```

caber

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

caber

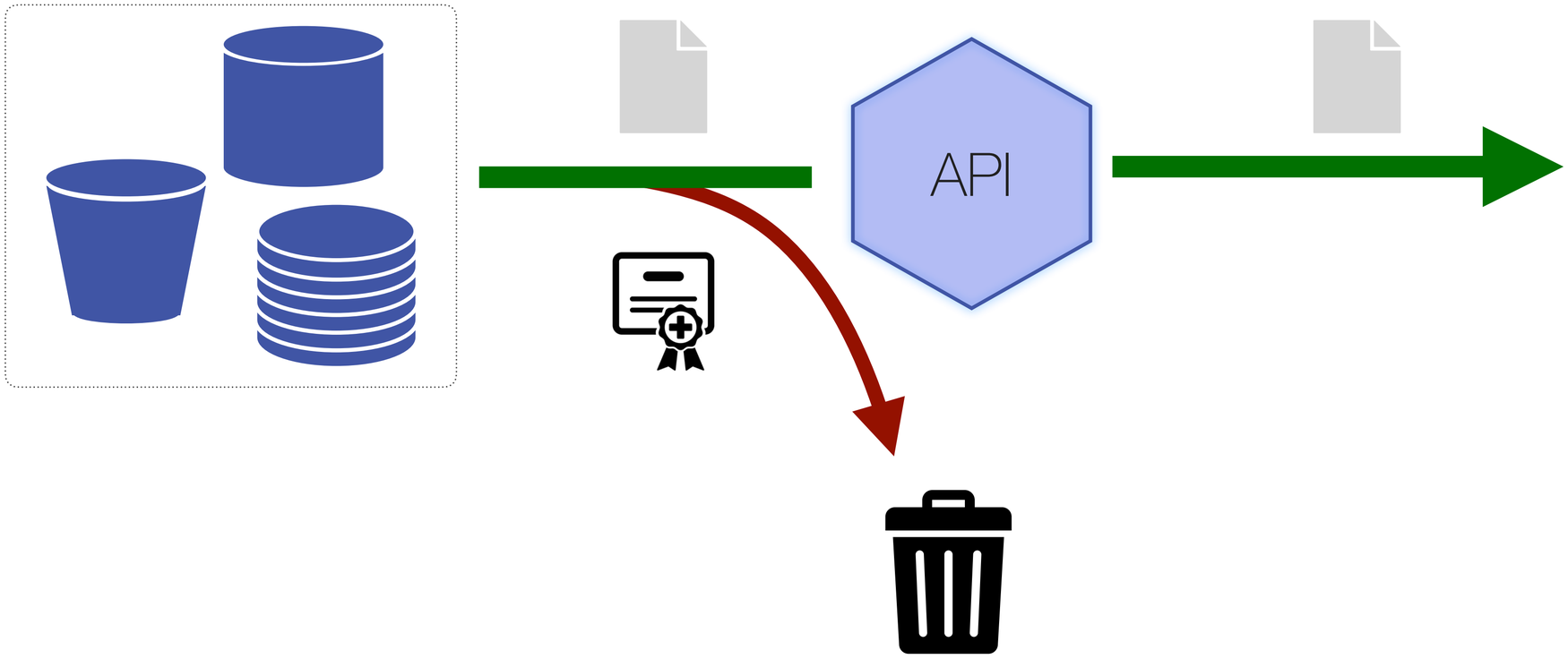
Three Hard Problems to Solve

Cloud-Native Applications

---

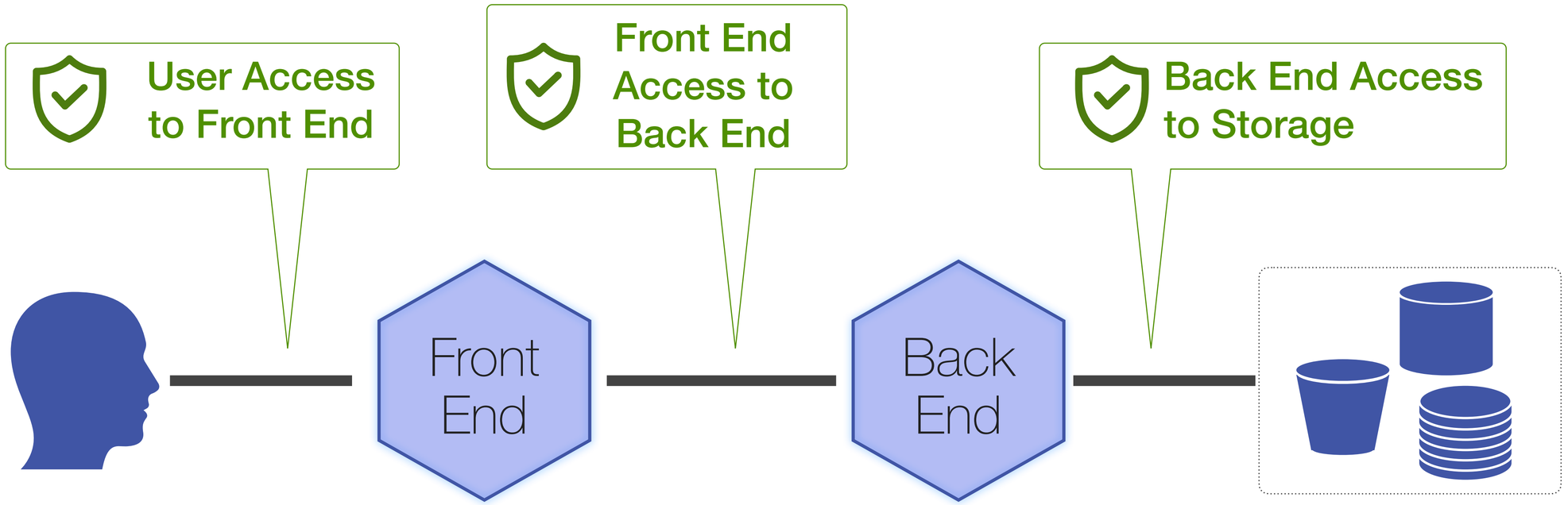
1. Data permissions and ownership not sent in APIs
2. Service accounts access data on behalf of users
3. APIs move pieces of data (chunks) from objects

API's Don't Send Permissions With Data



caber

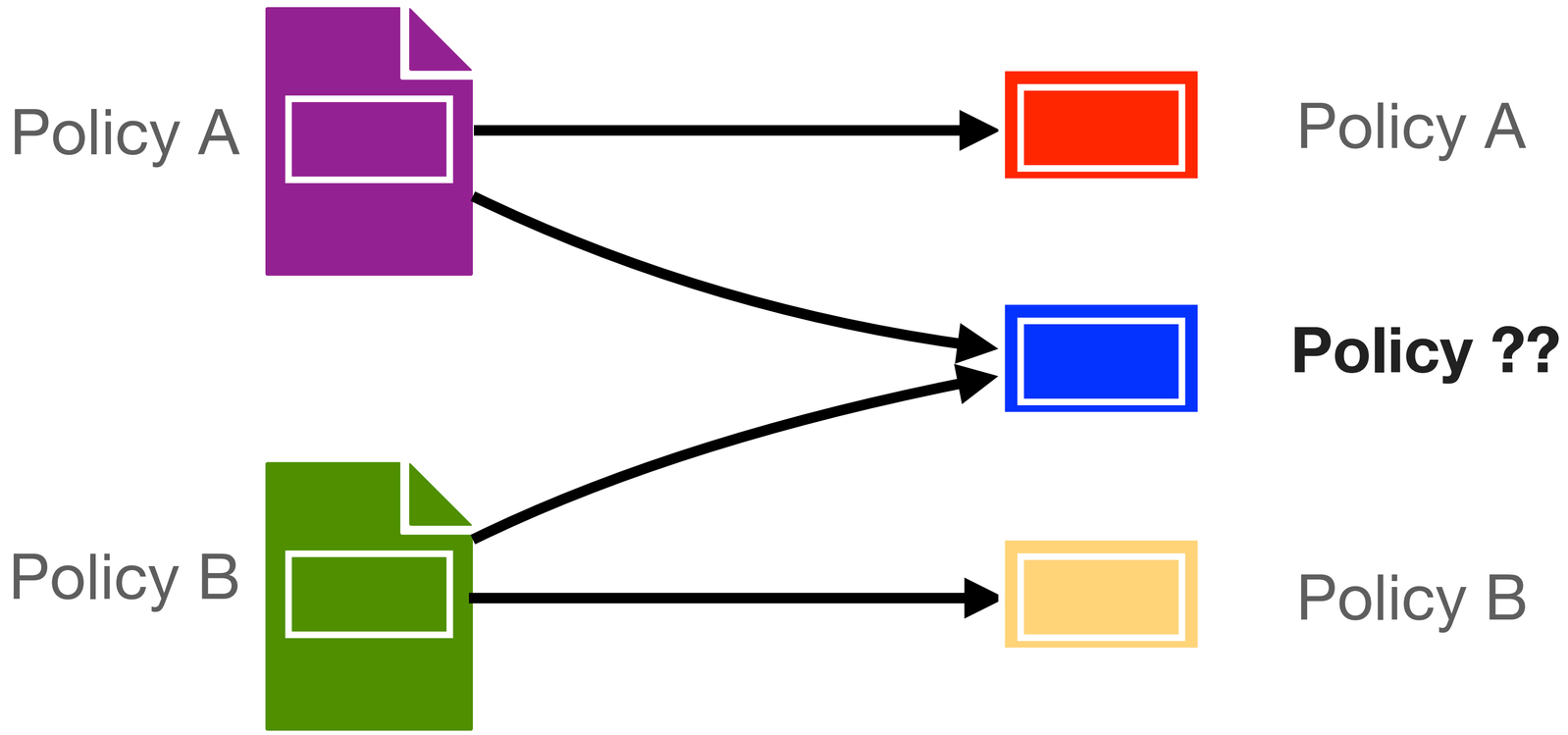
Service Accounts Hide End-User Identity



CONFUSED DEPUTY PROBLEM

caber

Permissions on Chunks



Data Duplication

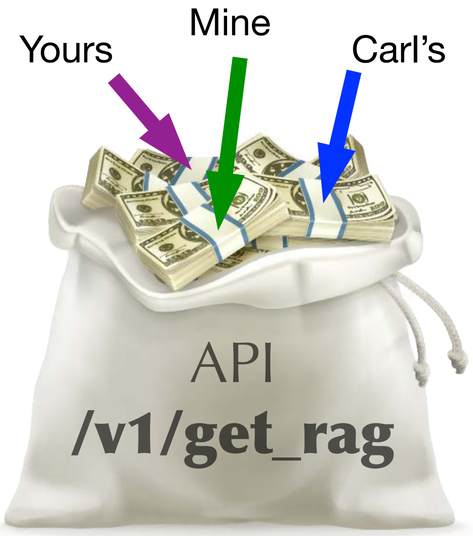
caber

GenAI: All Three Problems Plus…

Many chunks, different owners, in same payload

Least privilege violations are [the problem]

*— Matt Knight, Head of Security at OpenAI (5/8/2024)**



Ensure only you can
get your money

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

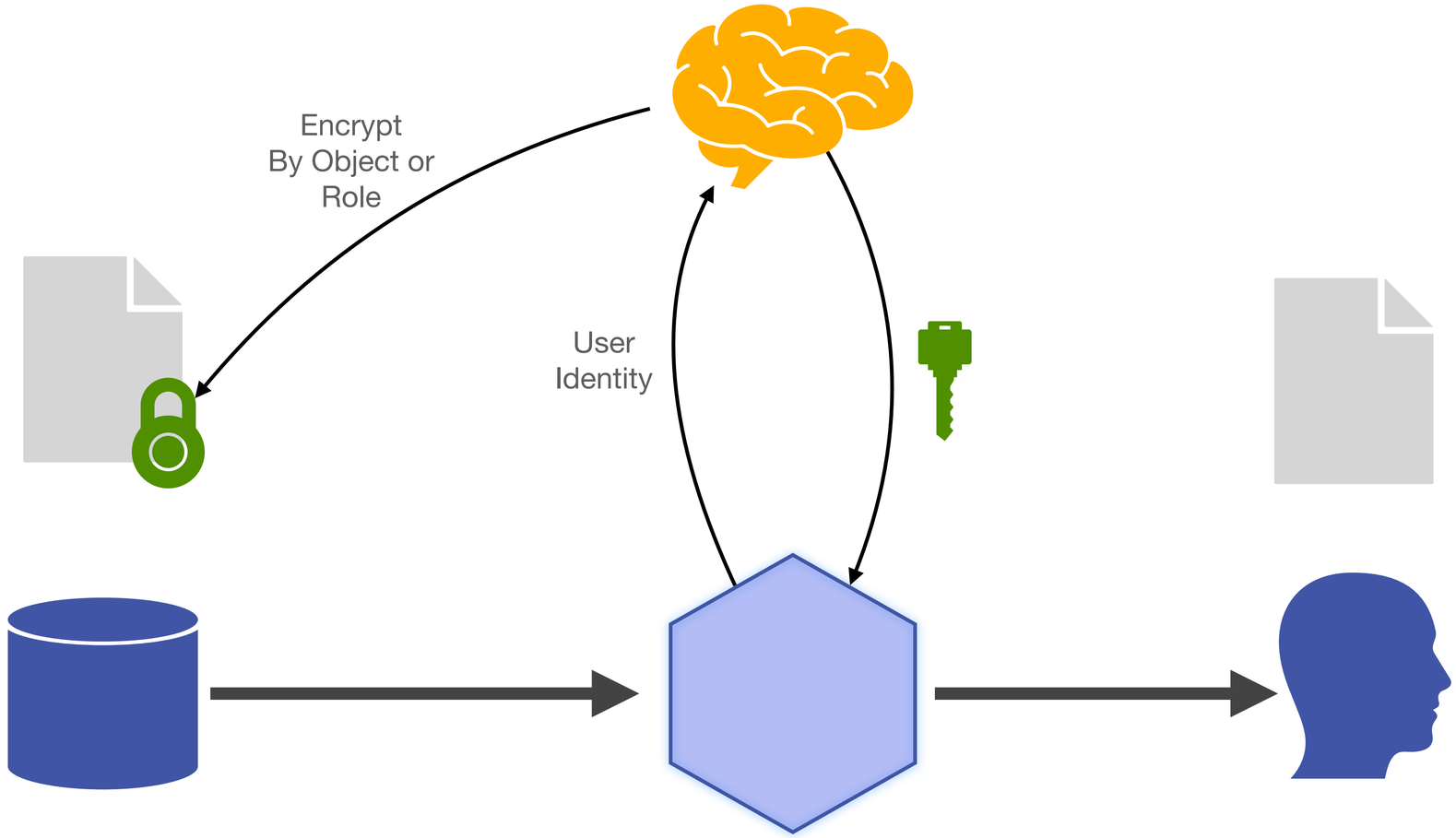
caber

New Architectures to Fix these Problems

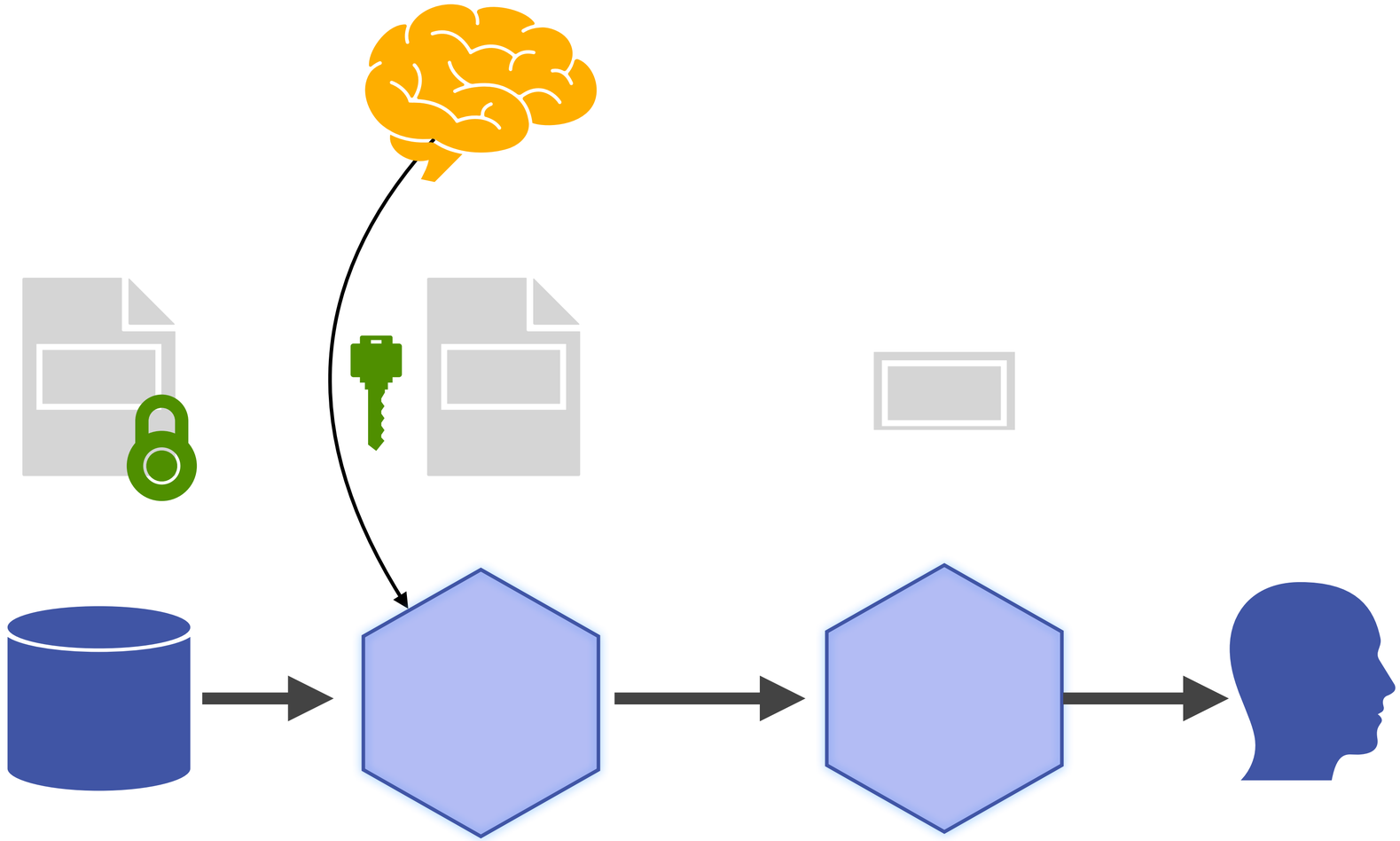
- Enterprise Digital Rights Management (eDRM)
- Google’s BeyondProd + Zanzibar
- Data Lineage Tracing (Caber)

caber

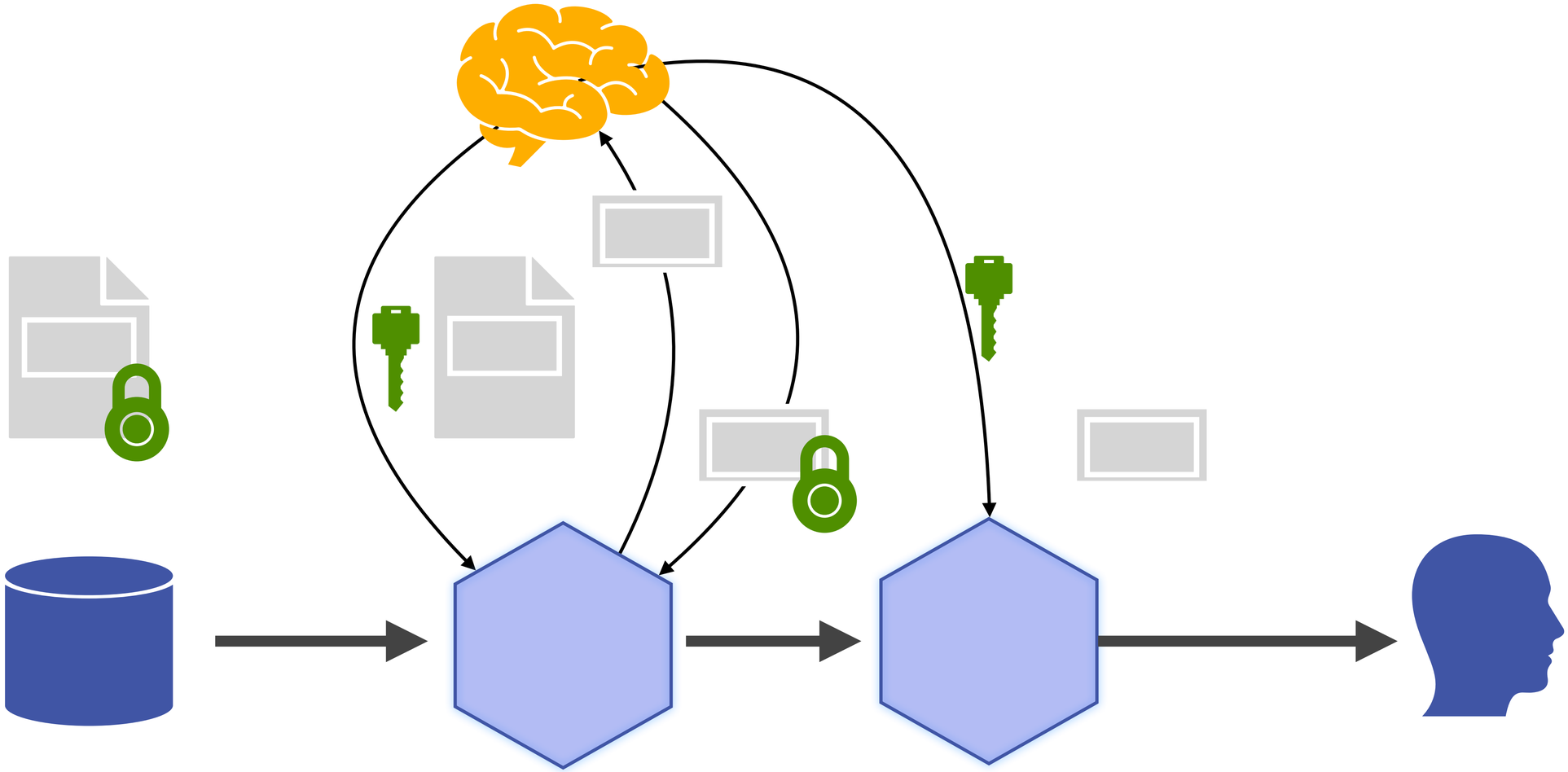
eDRM

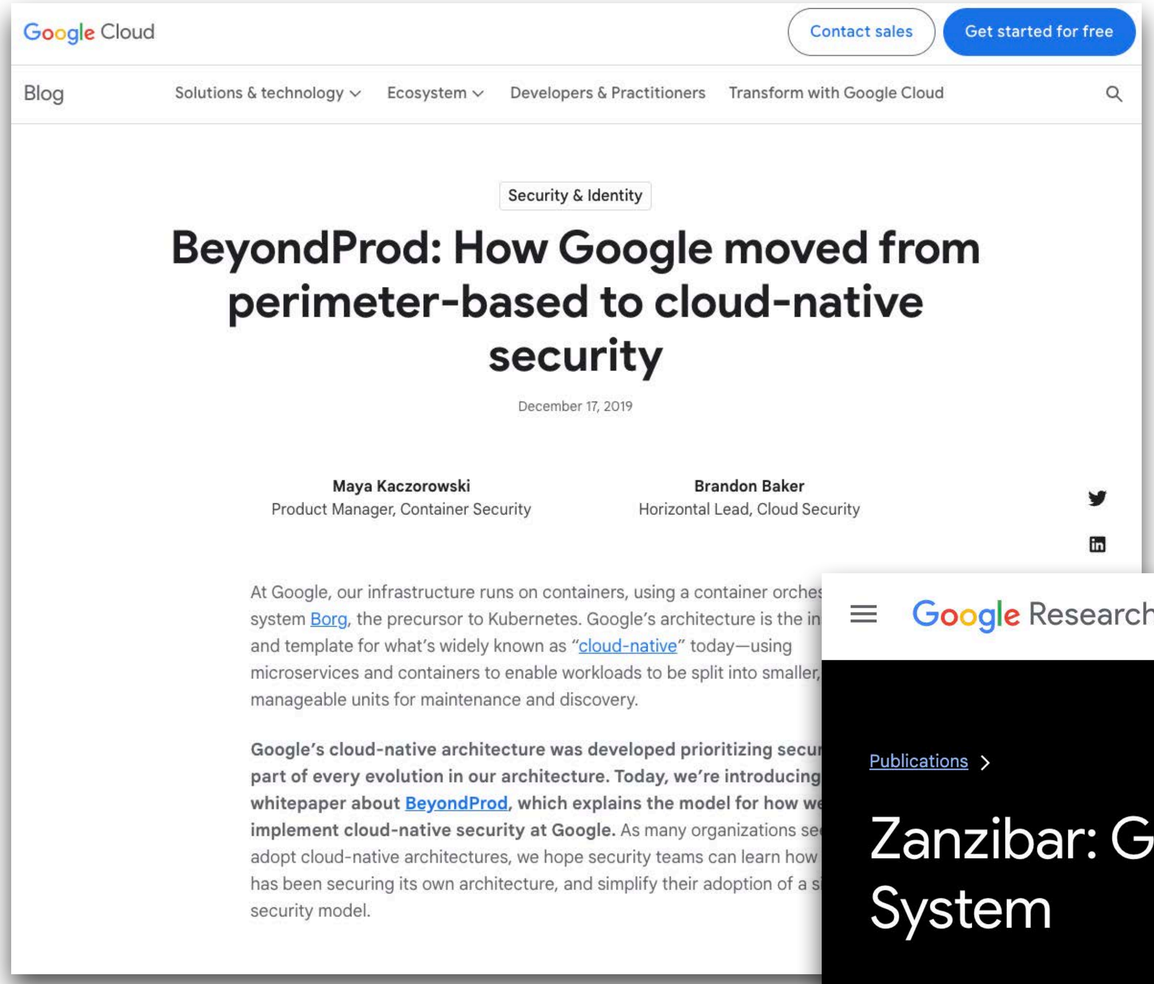


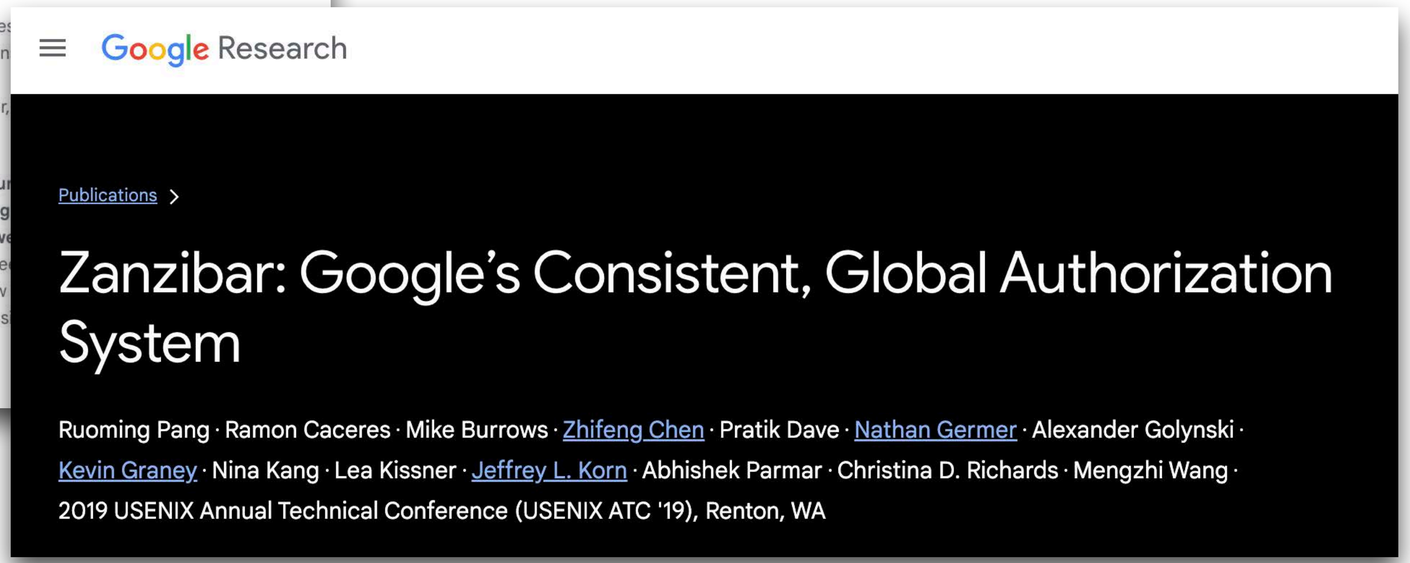
eDRM



eDRM



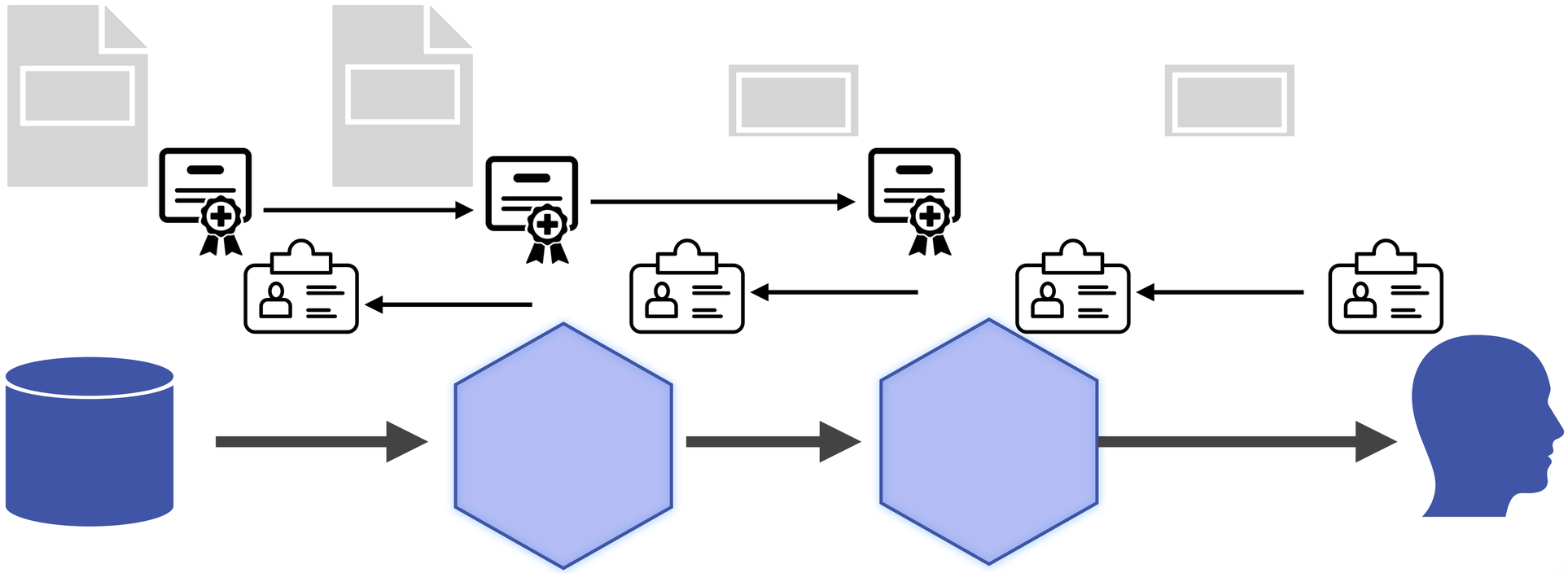




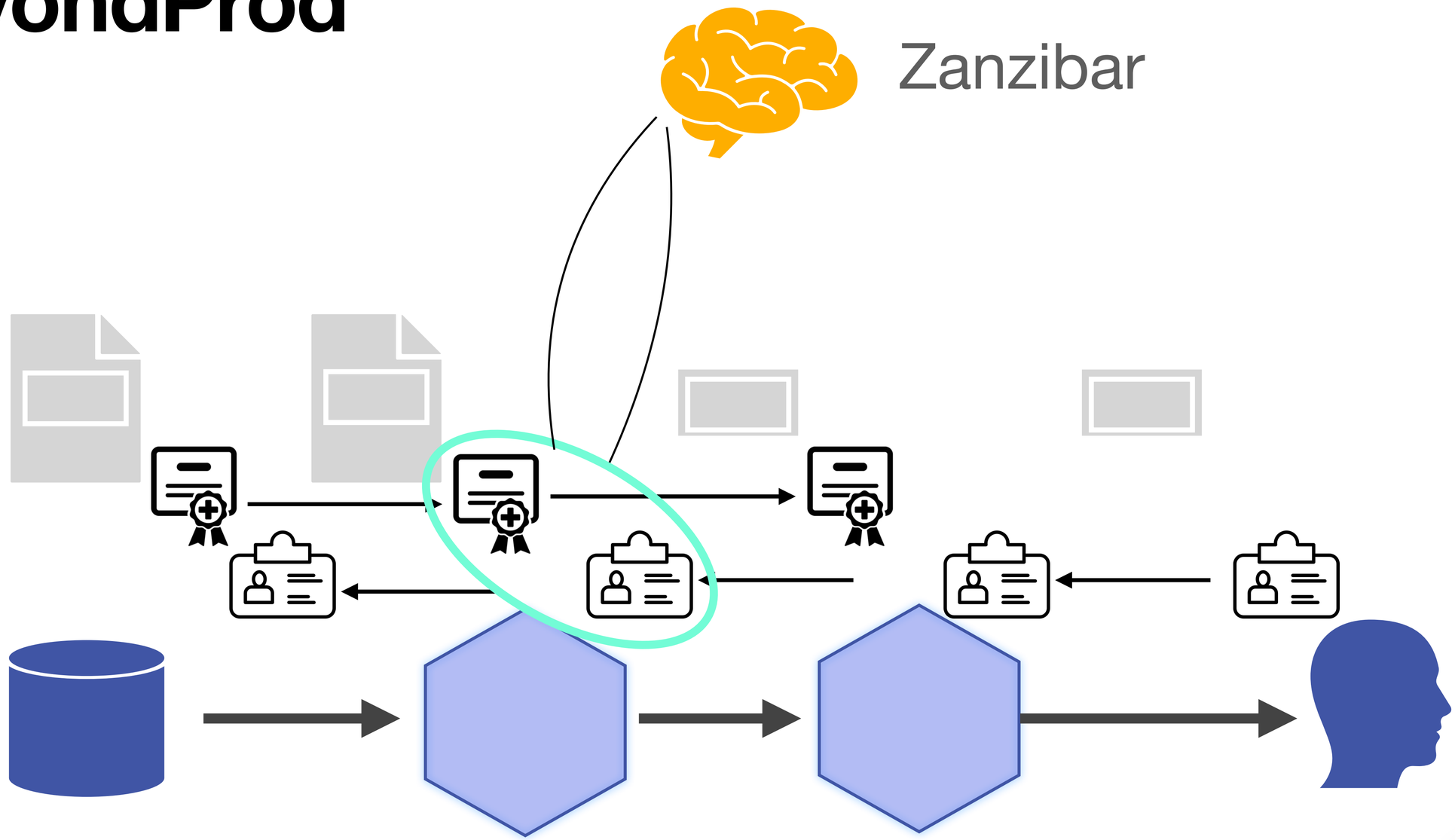
caber.com

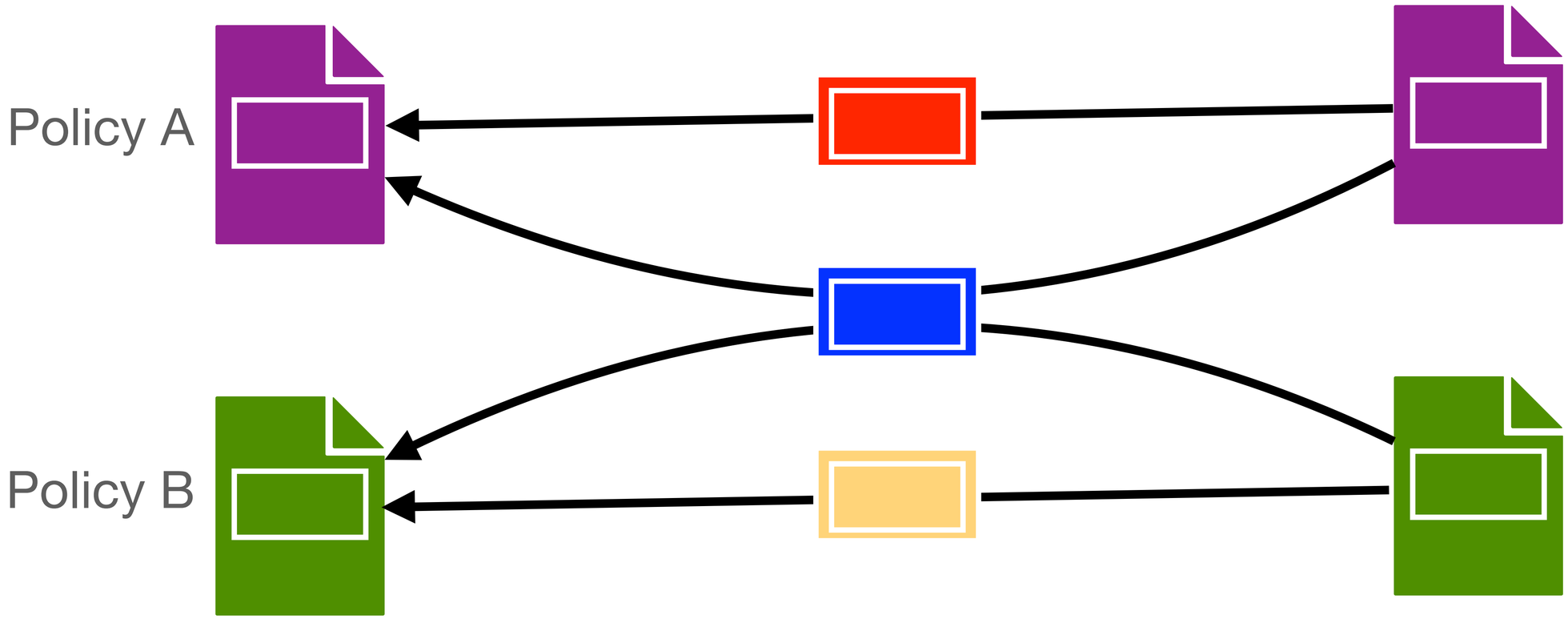
caber

BeyondProd

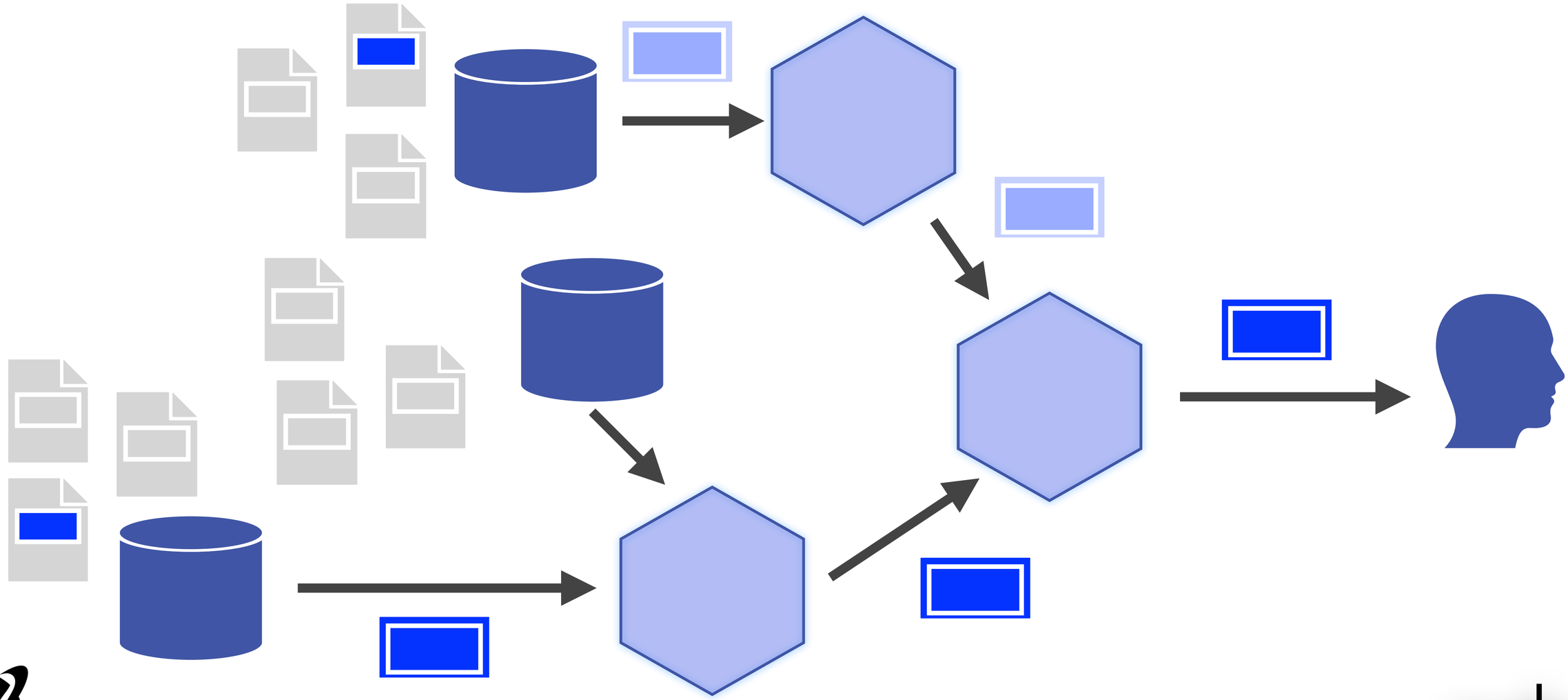


BeyondProd



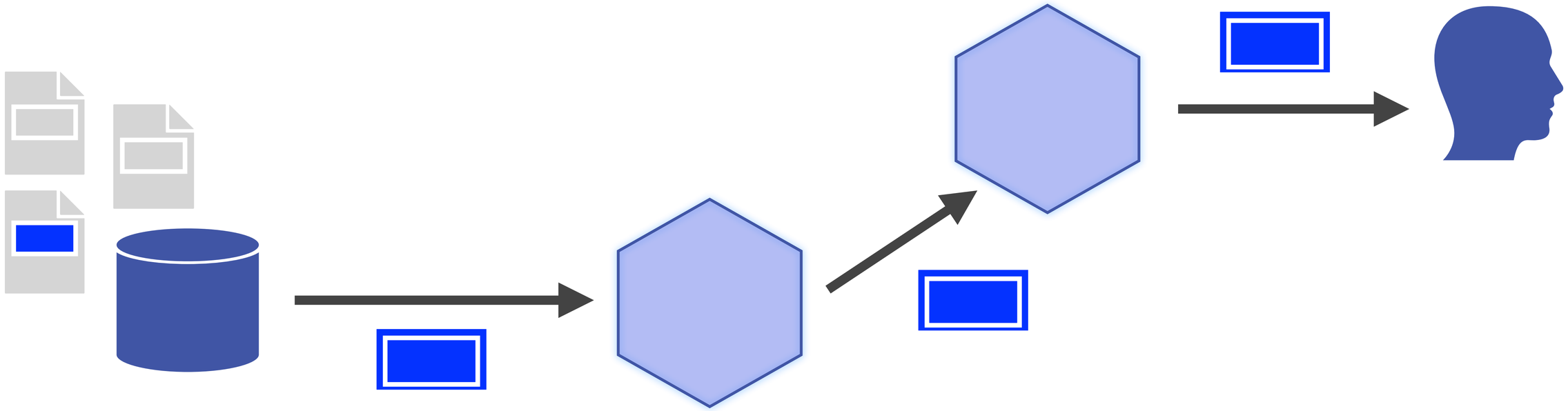

Policy A
Policy B

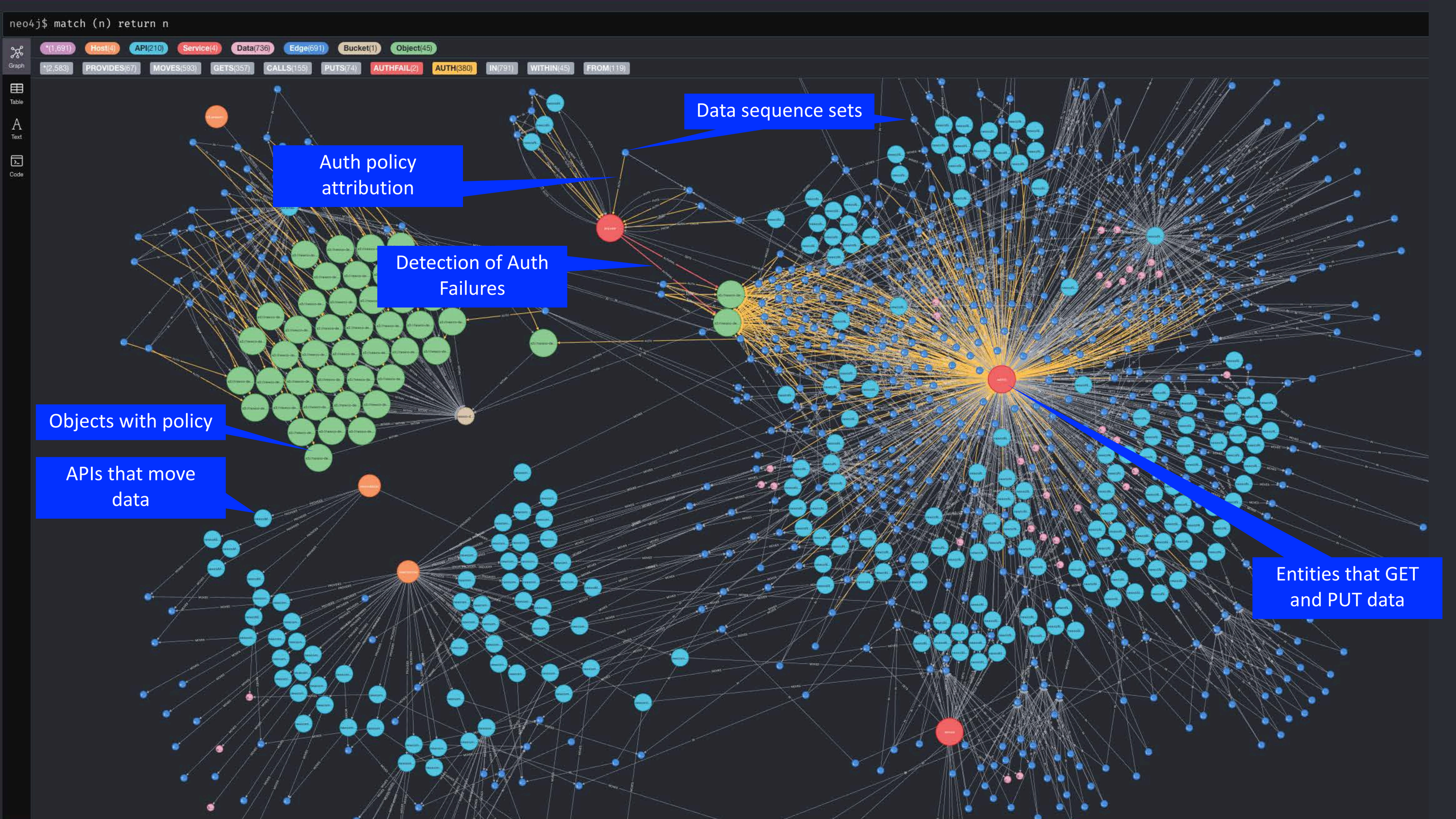
Data Lineage Tracing



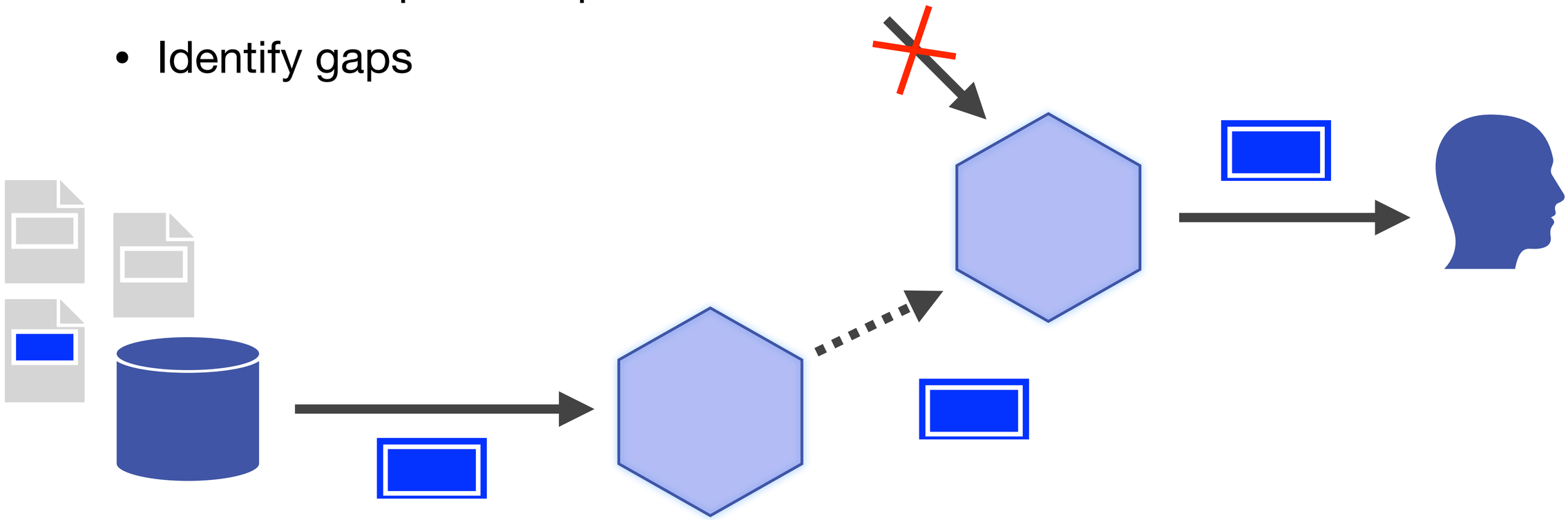
caber.com

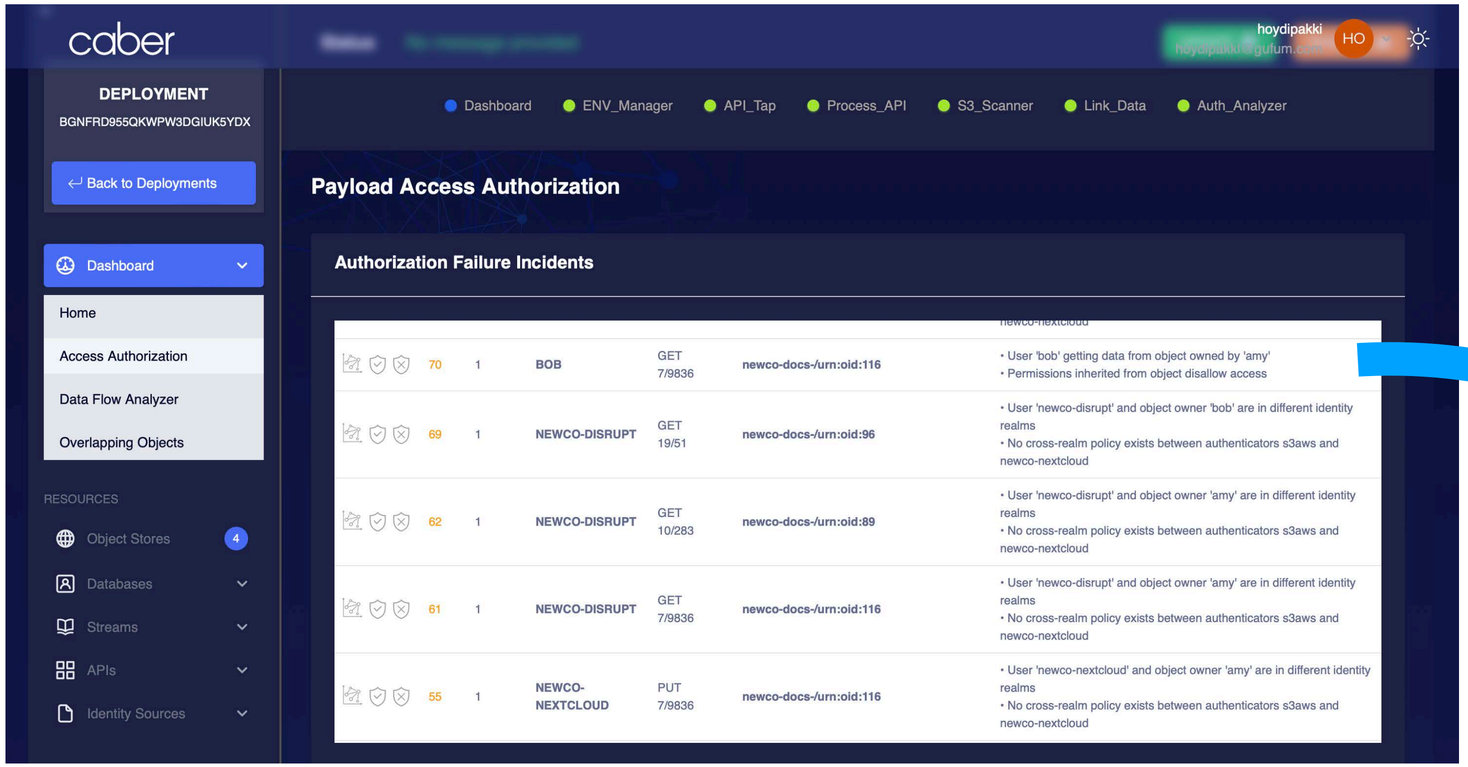
- Content-defined chunking in time window
- Find API Payloads and objects with common chunks
- Use common chunks to build relationships




neo4j$ match (n) return n
Graph
Table
Text
Code
*(1,691)
Host(4)
API(210)
Service(4)
Data(736)
Edge(691)
Bucket(1)
Object(45)
*(2,583)
PROVIDES(67)
MOVES(593)
GETS(357)
CALLS(155)
PUTS(74)
AUTHFAIL(2)
AUTH(380)
IN(791)
WITHIN(45)
FROM(119)
Data sequence sets
Auth policy attribution
Detection of Auth Failures
Objects with policy
APIs that move data
Entities that GET and PUT data

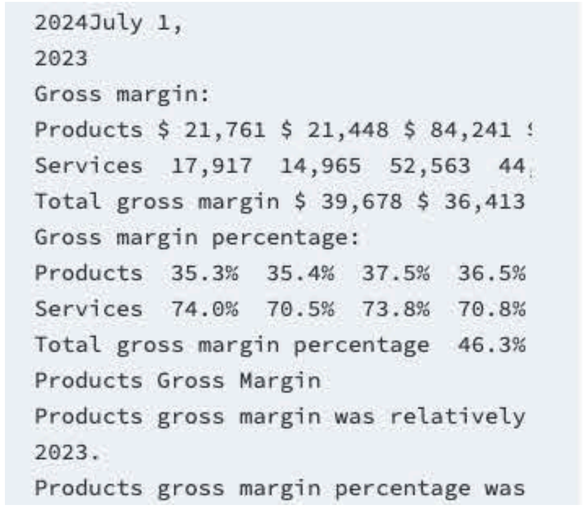
- Time-series analysis of related events
- Event ordering
- Eliminate impossible paths
- Identify gaps




caber
hoydipakki
HO
DEPLOYMENT
BGNFRD955QKWPW3DGIUK5YDX
Back to Deployments
Dashboard
ENV_Manager
API_Tap
Process_API
S3_Scanner
Link_Data
Auth_Analyzer
Payload Access Authorization
Dashboard
Home
Access Authorization
Data Flow Analyzer
Overlapping Objects
RESOURCES
Object Stores
Databases
Streams
APIs
Identity Sources
Authorization Failure Incidents
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
69 1 NEWCO-DISRUPT GET 19/51 newco-docs-/urn:oid:96 • User 'newco-disrupt' and object owner 'bob' are in different identity realms • No cross-realm policy exists between authenticators s3aws and newco-nextcloud
62 1 NEWCO-DISRUPT GET 10/283 newco-docs-/urn:oid:89 • User 'newco-disrupt' and object owner 'amy' are in different identity realms • No cross-realm policy exists between authenticators s3aws and newco-nextcloud
61 1 NEWCO-DISRUPT GET 7/9836 newco-docs-/urn:oid:116 • User 'newco-disrupt' and object owner 'amy' are in different identity realms • No cross-realm policy exists between authenticators s3aws and newco-nextcloud
55 1 NEWCO-NEXTCLOUD PUT 7/9836 newco-docs-/urn:oid:116 • User 'newco-nextcloud' and object owner 'amy' are in different identity realms • No cross-realm policy exists between authenticators s3aws and newco-nextcloud


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
```

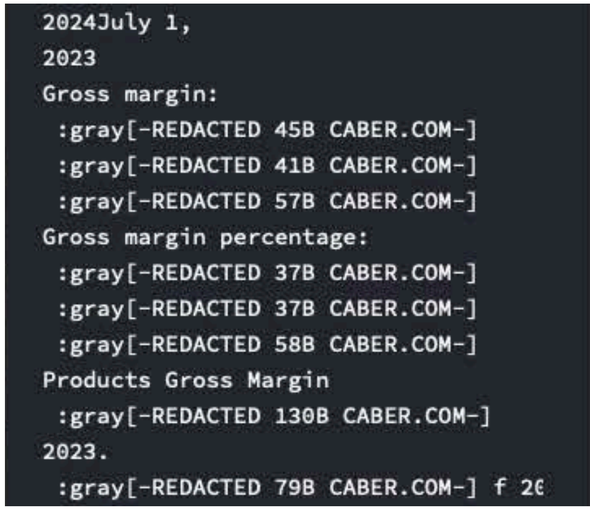
How has Apple's gross margin percentage evolved from fiscal Q1 2023 and Q3 2024, and what factors have contributed to these changes?

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

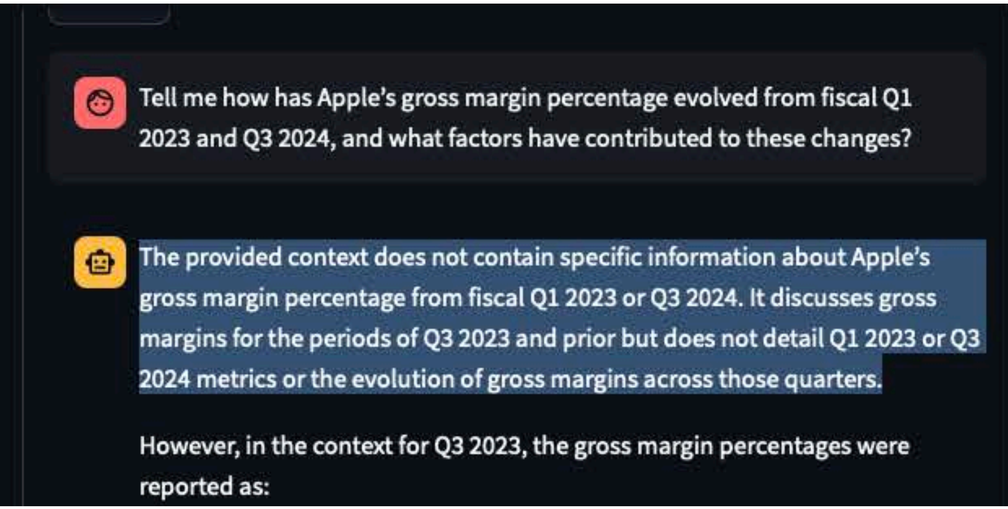
In fiscal Q1 2023, the total gross margin percentage was 43.0%. By Q3 2024, this percentage had increased to 46.3%.

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 2(
```



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

Detect Incidents Without False Positives*

*Probability on the order of a hash collision

caber.com

caber

caber

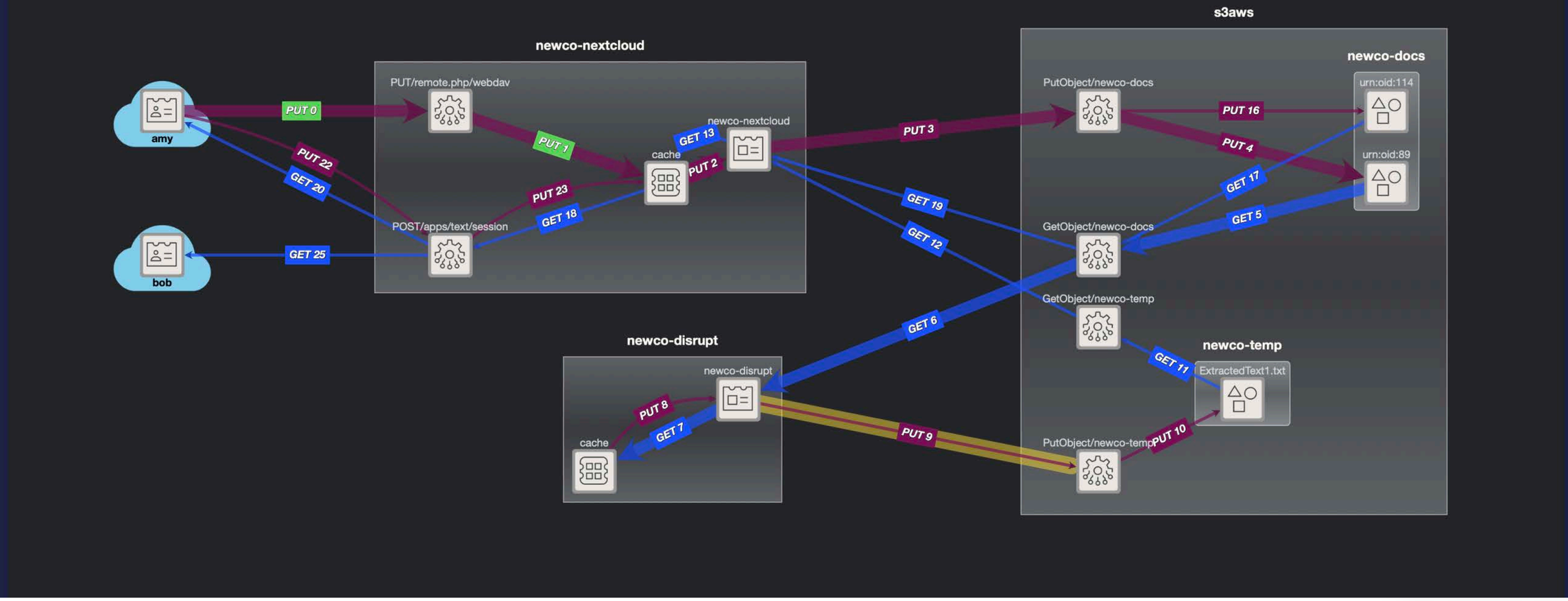
hoydipakki
hoydipakki@gufum.com
HO

Incident Call Graph

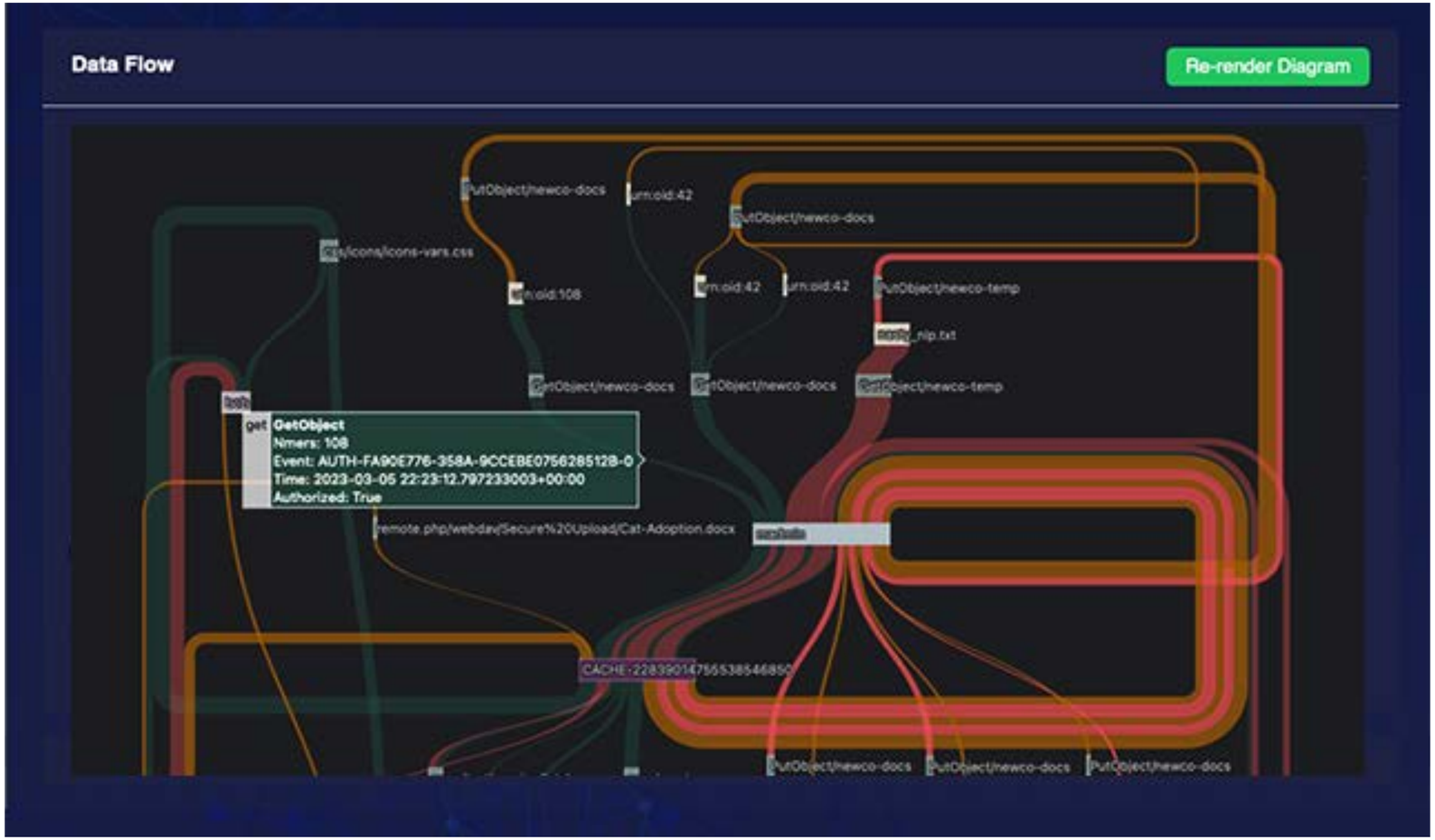
Fix Layout

Service newco-disrupt calls S3/PutObject and writes 283 nmers of data to object ExtractedText1.txt

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21



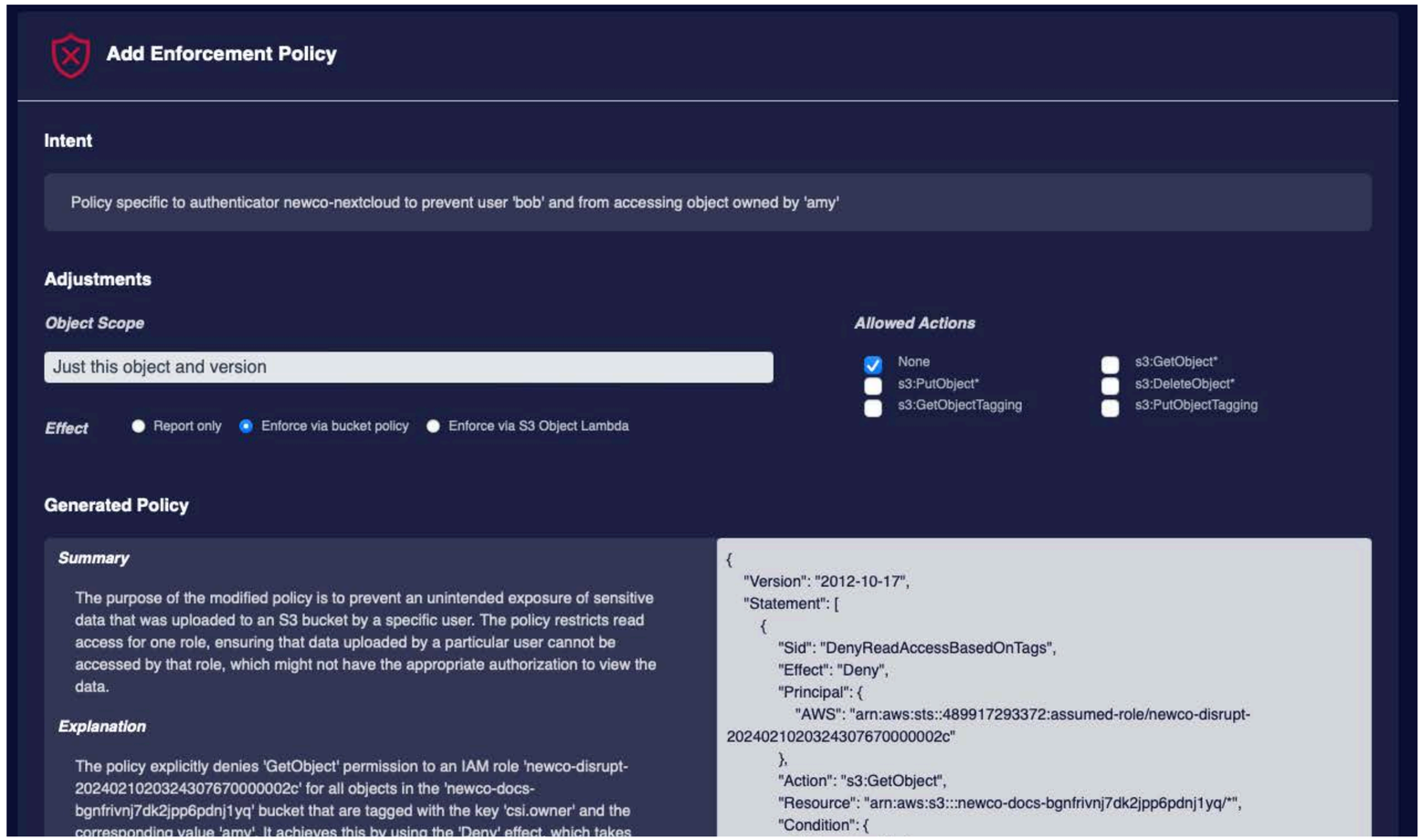
Detailed Observability of Application Flow



Analyze and debug application behavior

caber

Data Compliance Requirements to Policy



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

caber

Thank You!

Rob Quiros

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