ACM Symposium on Access Control Models and Technologies (SACMAT) 2023

Qualitative Intention-Aware Attribute-Based Access Control Policy Refinement

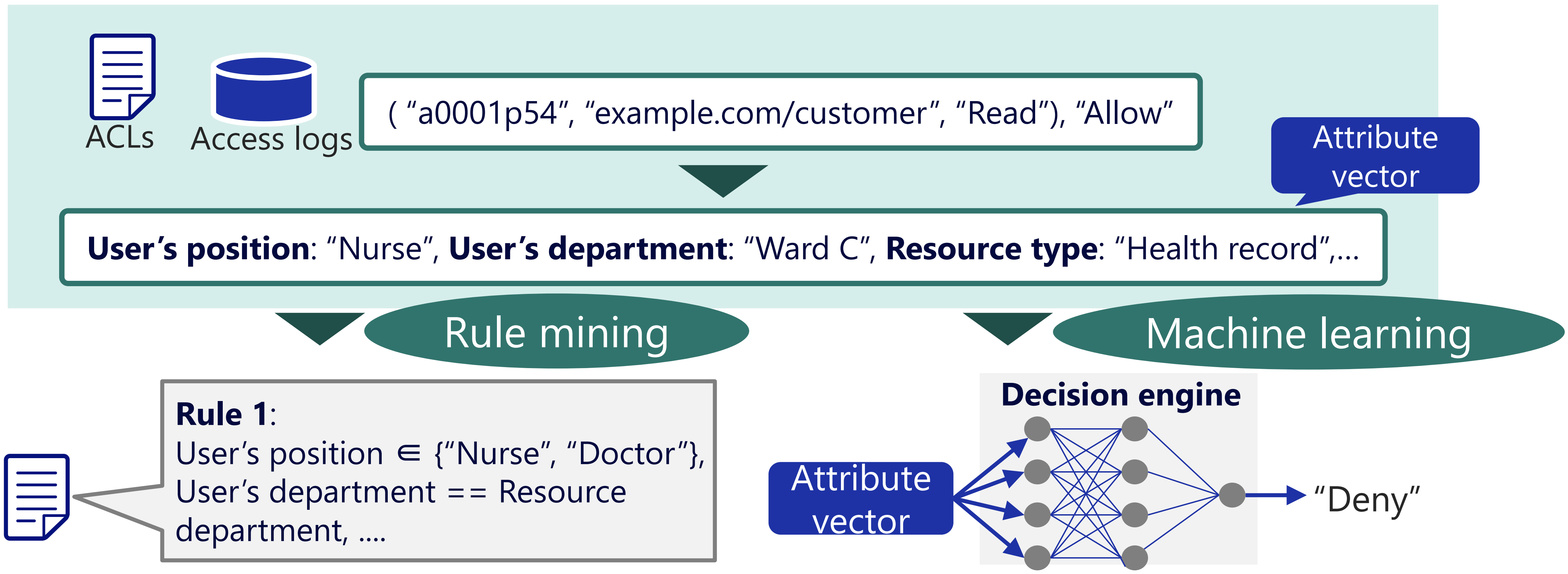
Shohei Mitani[1], Jonghoon Kwon[2], Nakul Ghate[1], Taniya Singh[1], Hirofumi Ueda[1], Adrian Perrig[2]

[1]NEC Corporation, Japan
[2]ETH Zürich, Switzerland

Background

Attribute-based Access Control (ABAC) policy generation.

✓ Rule mining vs. Machine learning (ML).



ACLs

Access logs

("a0001p54", "example.com/customer", "Read"), "Allow"

Attribute vector

User's position: "Nurse", **User's department**: "Ward C", **Resource type**: "Health record",...

Rule mining

Machine learning

Rule 1:
User's position ∈ {"Nurse", "Doctor"},
User's department == Resource department, ...

Decision engine

Attribute vector

"Deny"

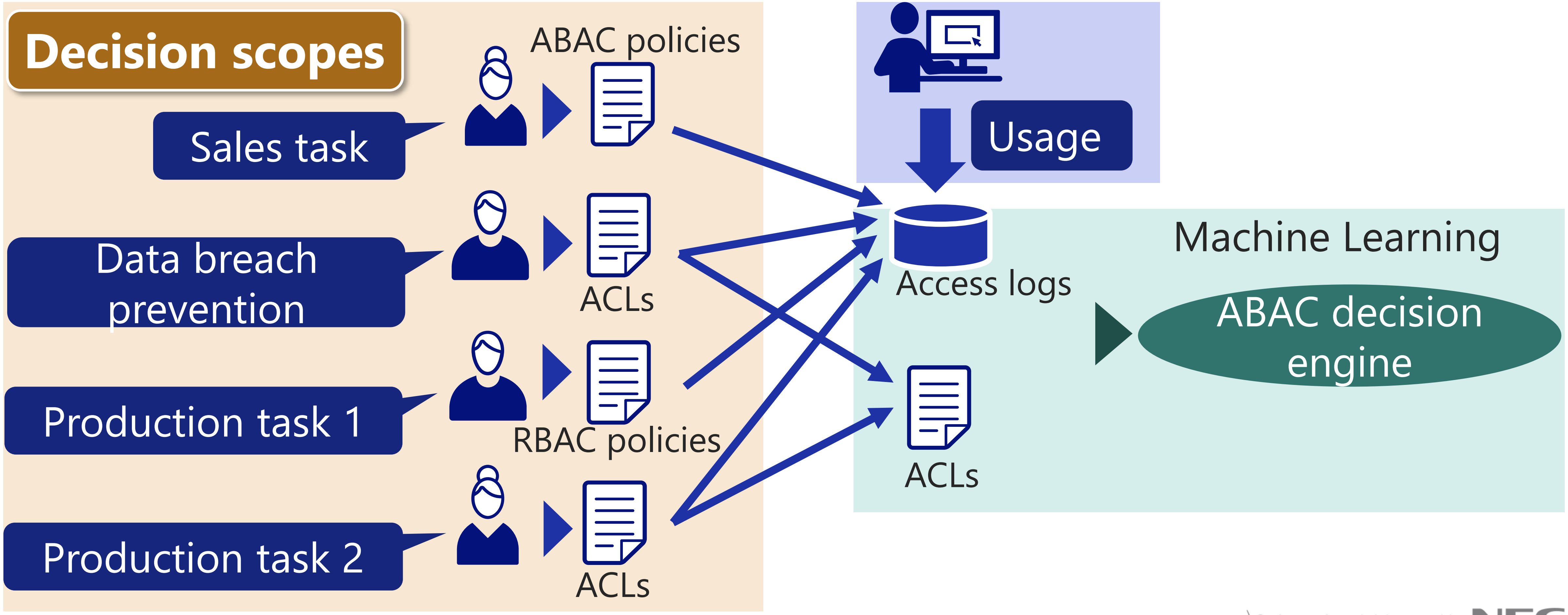
[22] Zhongyuan Xu and Scott D Stoller. 2014.
[13] Leila Karimi and James Joshi. 2018.

[4] Luca Cappelletti, Stefano Valtolina, Giorgio Valentini, Marco Mesiti, and Elisa Bertino. 2019.

Problem Definition

Pre-designed policies are assumed.

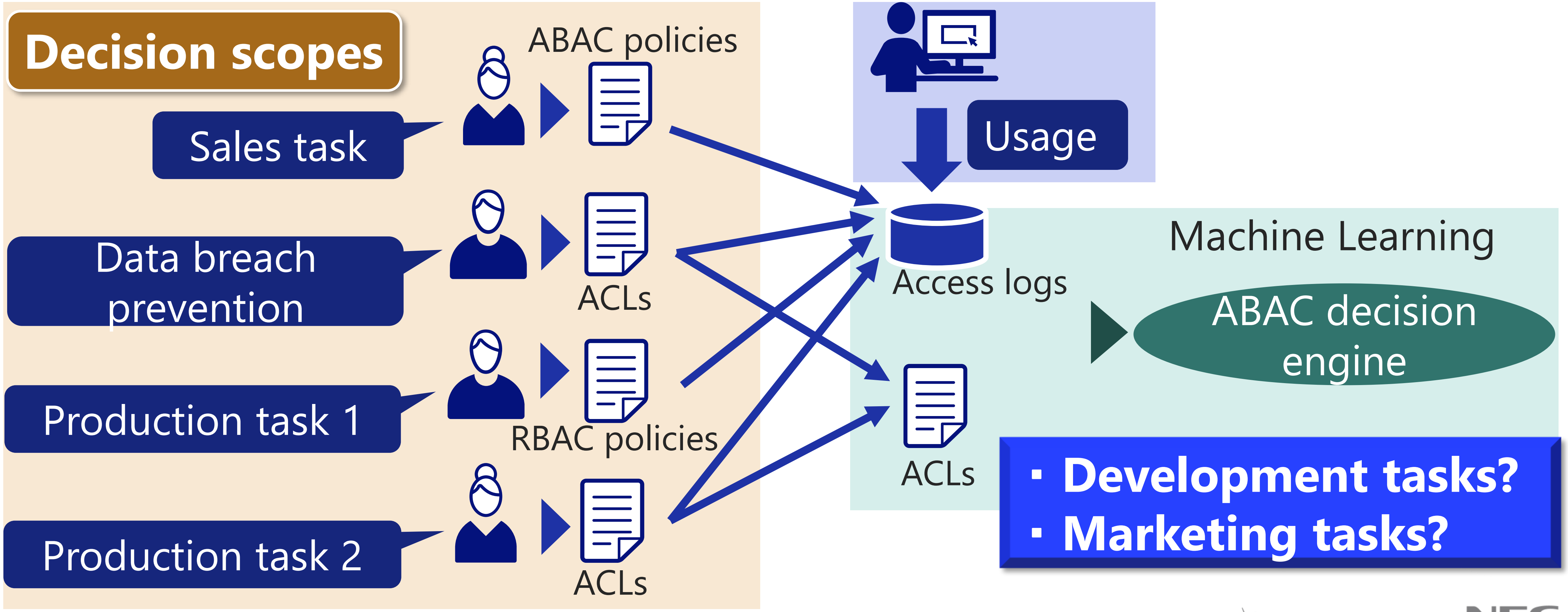
✓ Poor decisions arise outside the policy designers' scopes (i.e., not envisioned).



Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).

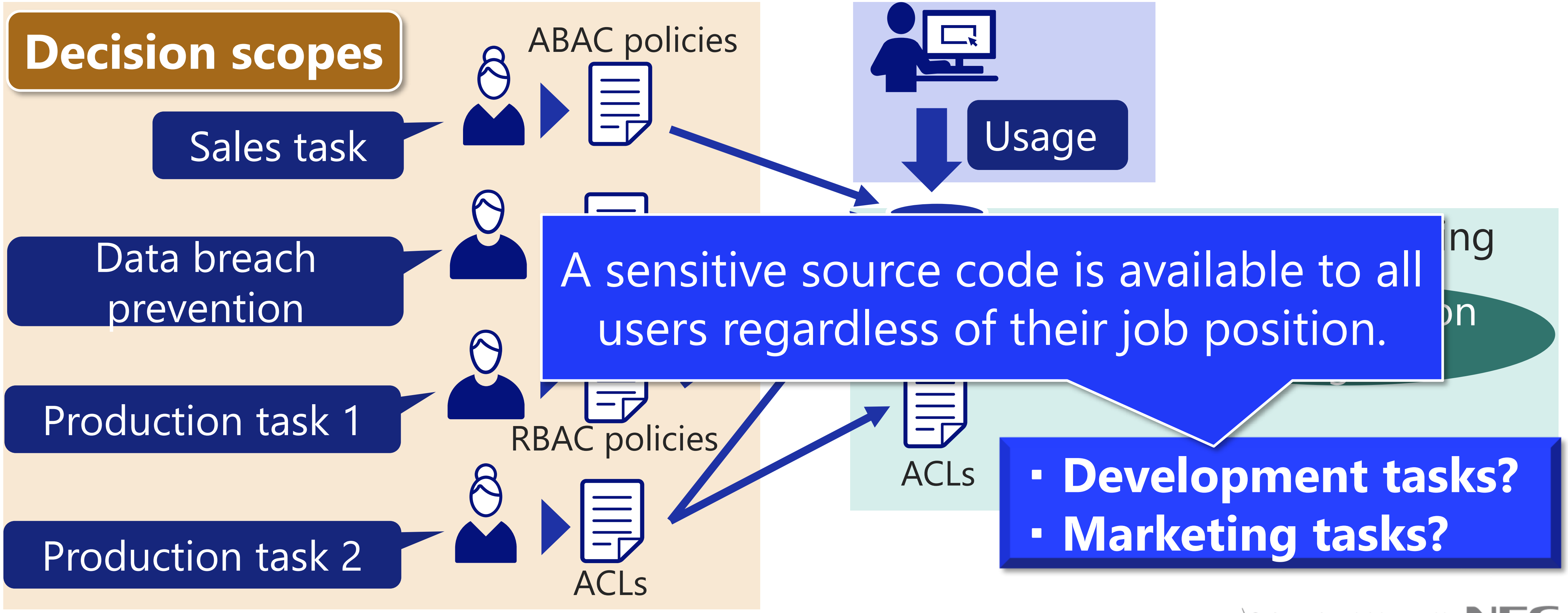


- Development tasks?
- Marketing tasks?

Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers’ scopes (i.e., not envisioned).



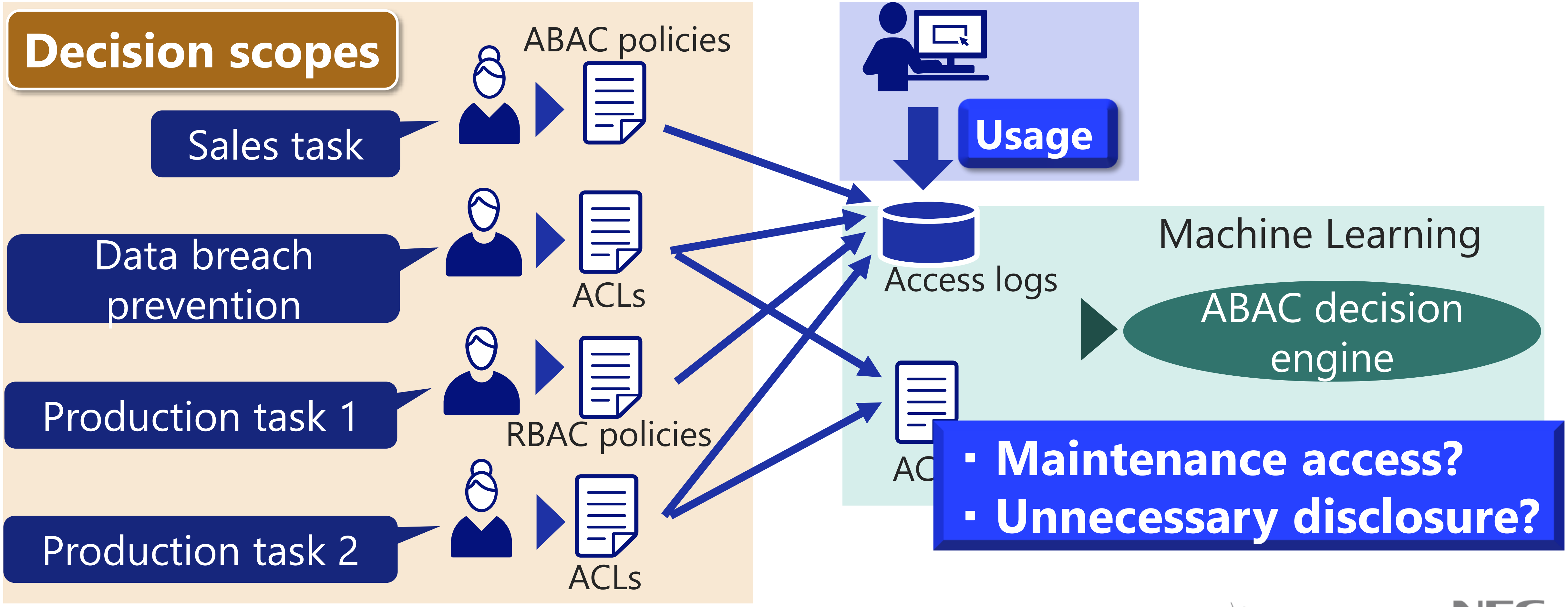
A sensitive source code is available to all users regardless of their job position.

- Development tasks?
- Marketing tasks?

Problem Definition

Pre-designed policies are assumed.

✓ Poor decisions arise outside the policy designers' scopes (i.e., not envisioned).

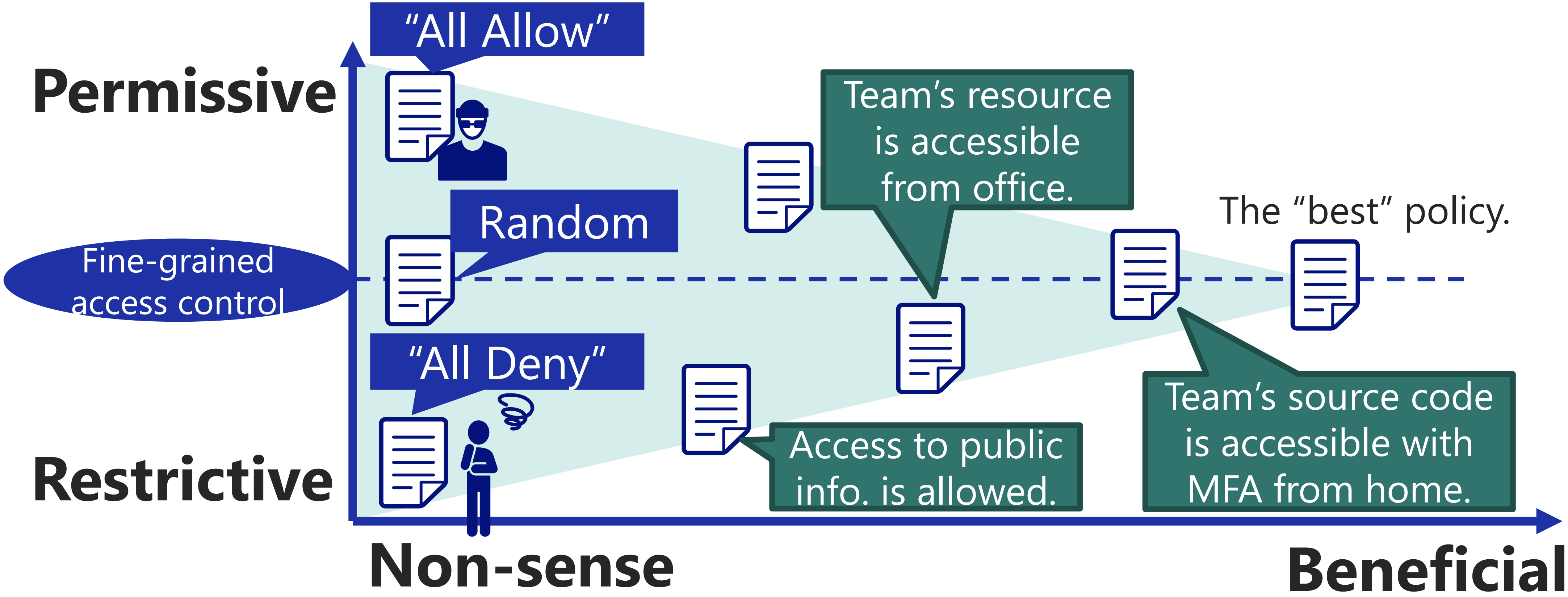


- Maintenance access?
- Unnecessary disclosure?

Motivation

Better balances of security and usability,

✓ By refining access control policies (or access logs.)

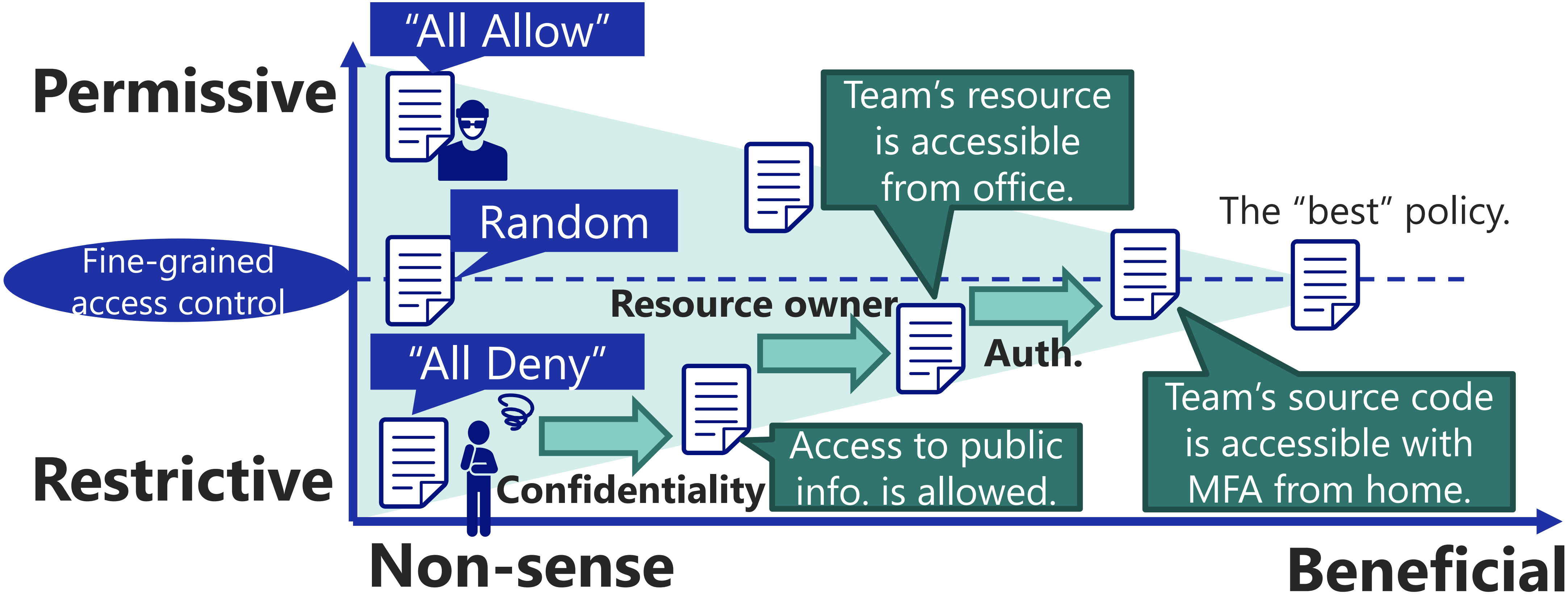


"All Allow"
Permissive
Team's resource is accessible from office.
Random
The "best" policy.
Fine-grained access control
"All Deny"
Team's source code is accessible with MFA from home.
Access to public info. is allowed.
Restrictive
Non-sense
Beneficial

Motivation

Policy designers underlying intentions are assumed.

✓ Explicitly reflect the **intentions from various aspects** to policy refinement.

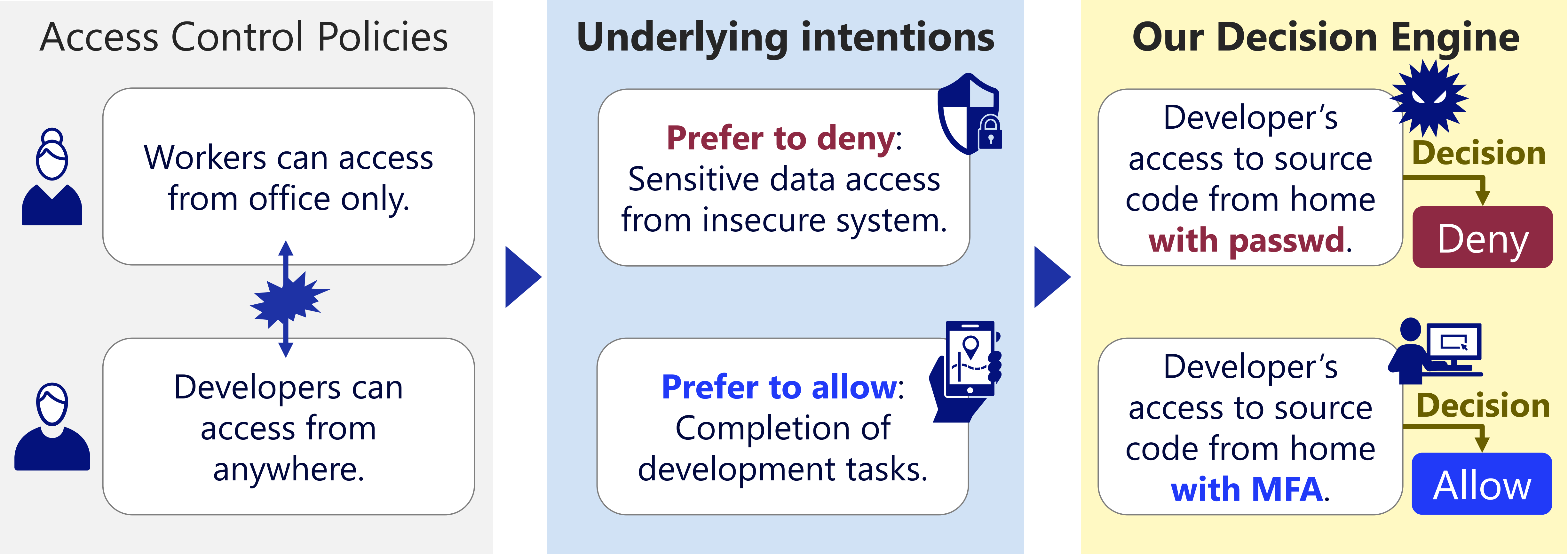


"All Allow"
Permissive
Random
Fine-grained access control
"All Deny"
Restrictive
Confidentiality
Resource owner
Auth.
Team's resource is accessible from office.
The "best" policy.
Access to public info. is allowed.
Team's source code is accessible with MFA from home.
Non-sense
Beneficial

Goal

A decision engine is created by refining access control policies.

✓ Intentions lead to enhancing security without compromising usability.



Access Control Policies

Workers can access from office only.

Developers can access from anywhere.

Underlying intentions

Prefer to deny: Sensitive data access from insecure system.

Prefer to allow: Completion of development tasks.

Our Decision Engine

Developer’s access to source code from home **with passwd**.

Decision

Deny

Developer’s access to source code from home **with MFA**.

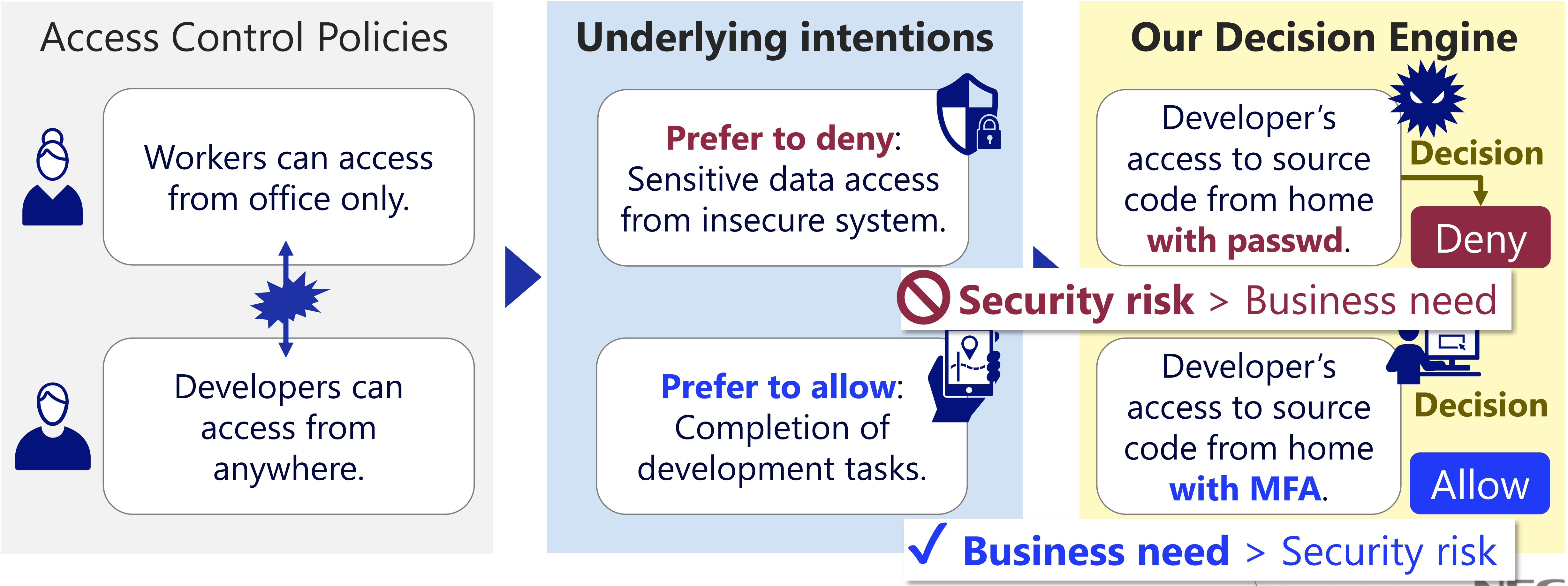
Decision

Allow

Goal

A decision engine is created by refining access control policies.

✓ Intentions lead to enhancing security without compromising usability.



Access Control Policies

Workers can access from office only.

Developers can access from anywhere.

Underlying intentions

Prefer to deny: Sensitive data access from insecure system.

Prefer to allow: Completion of development tasks.

Our Decision Engine

Developer's access to source code from home **with passwd.**

Decision

Deny

🚫 **Security risk** > Business need

Developer's access to source code from home **with MFA.**

Decision

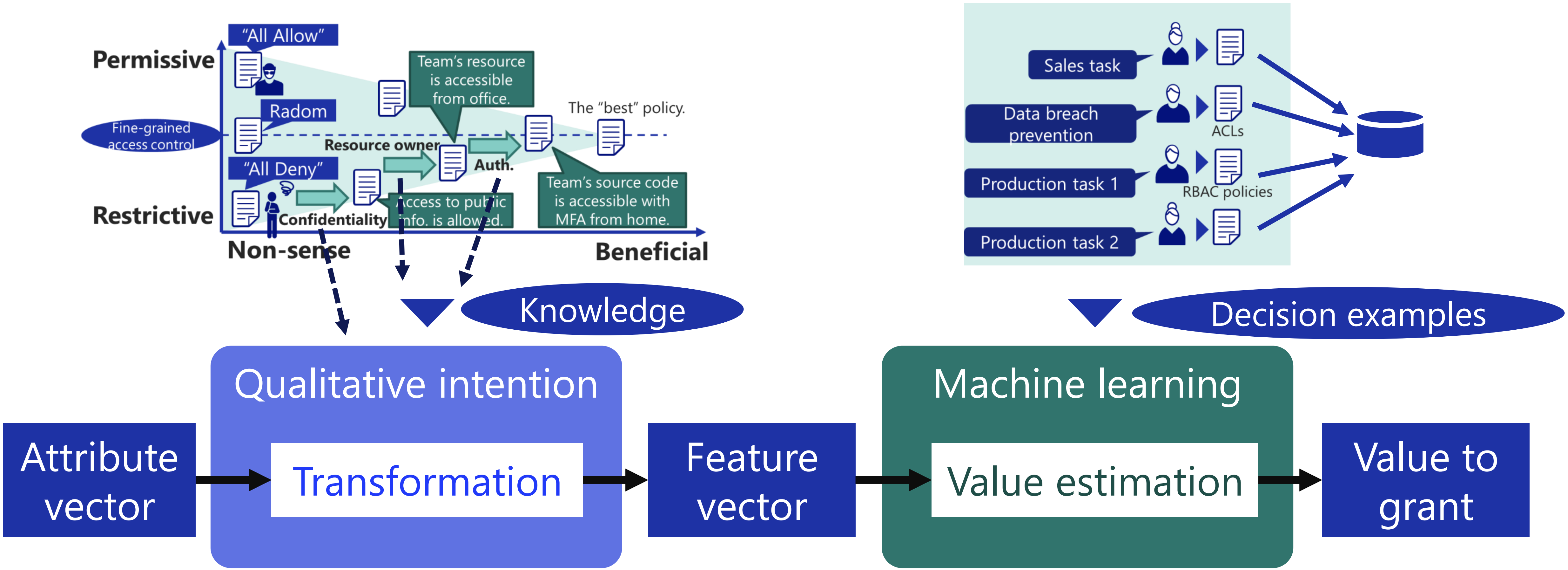
Allow

✓ **Business need** > Security risk

Methodology

A knowledge-informed ML which learns decision examples that follow initial policies.

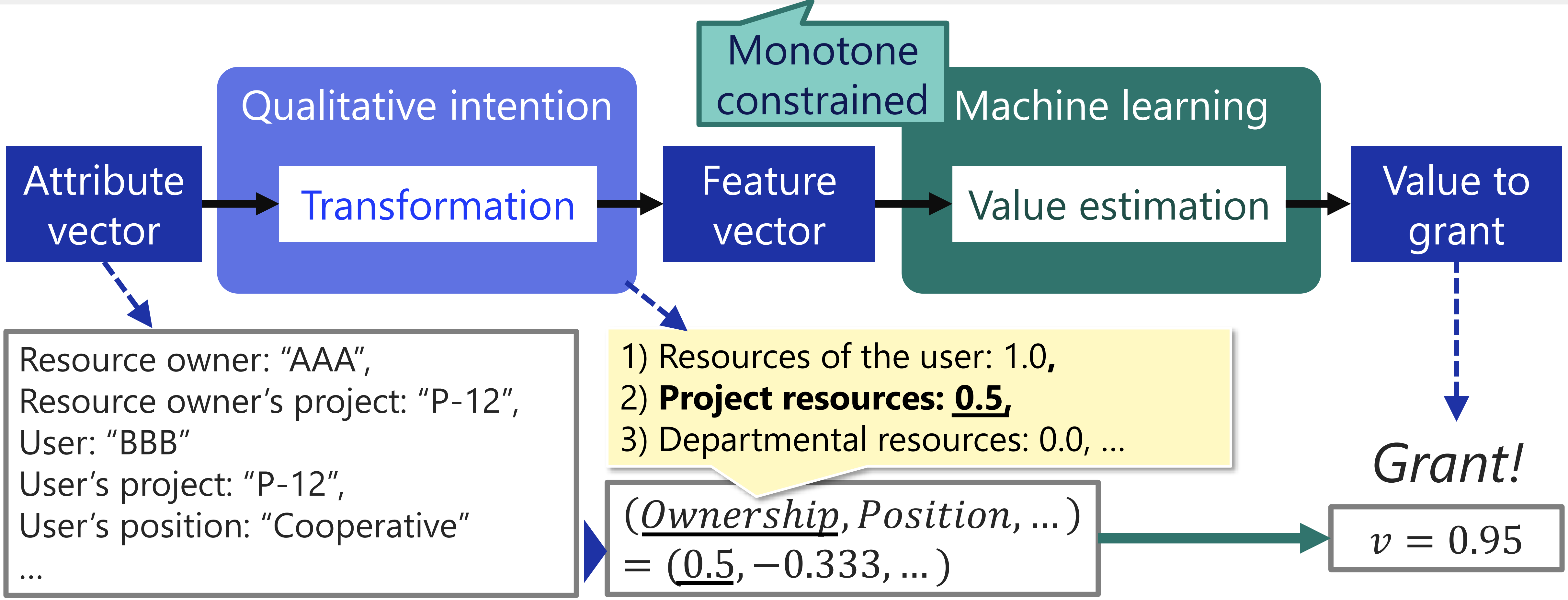
✓ The feature vector is created by extra knowledge “Qualitative Intention.”



Methodology

A "Qualitative Intentions" is a preference to grant access from an aspect.

✓ *Access that is preferable to grant in all aspect is, overall, more valuable to grant.*



Resource owner: "AAA",
Resource owner's project: "P-12",
User: "BBB"
User's project: "P-12",
User's position: "Cooperative"
…

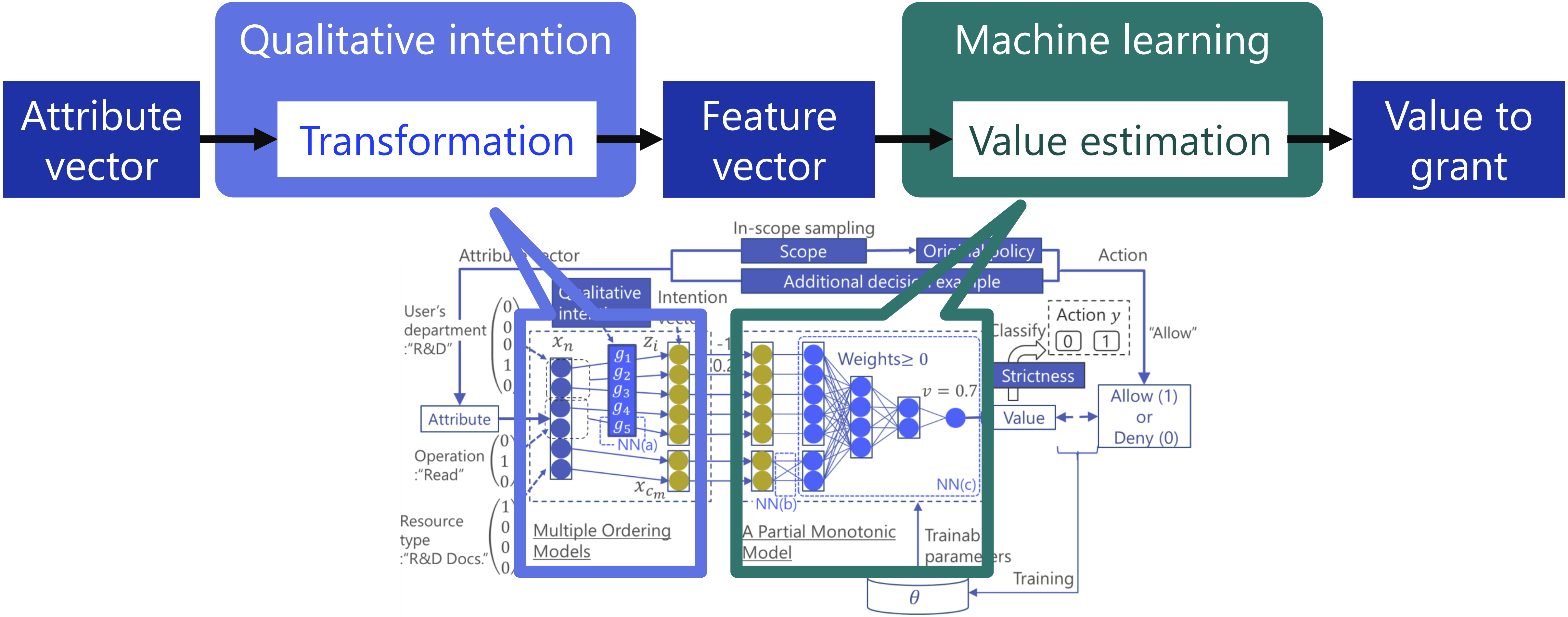
1) Resources of the user: 1.0,
2) **Project resources: 0.5,**
3) Departmental resources: 0.0, …

$(\underline{Ownership}, Position, \ldots) = (\underline{0.5}, -0.333, \ldots)$

$v = 0.95$

Methodology

In the paper, we present a two-stages computational model. The two stages correspond to the transformation and the value estimation model, respectively.

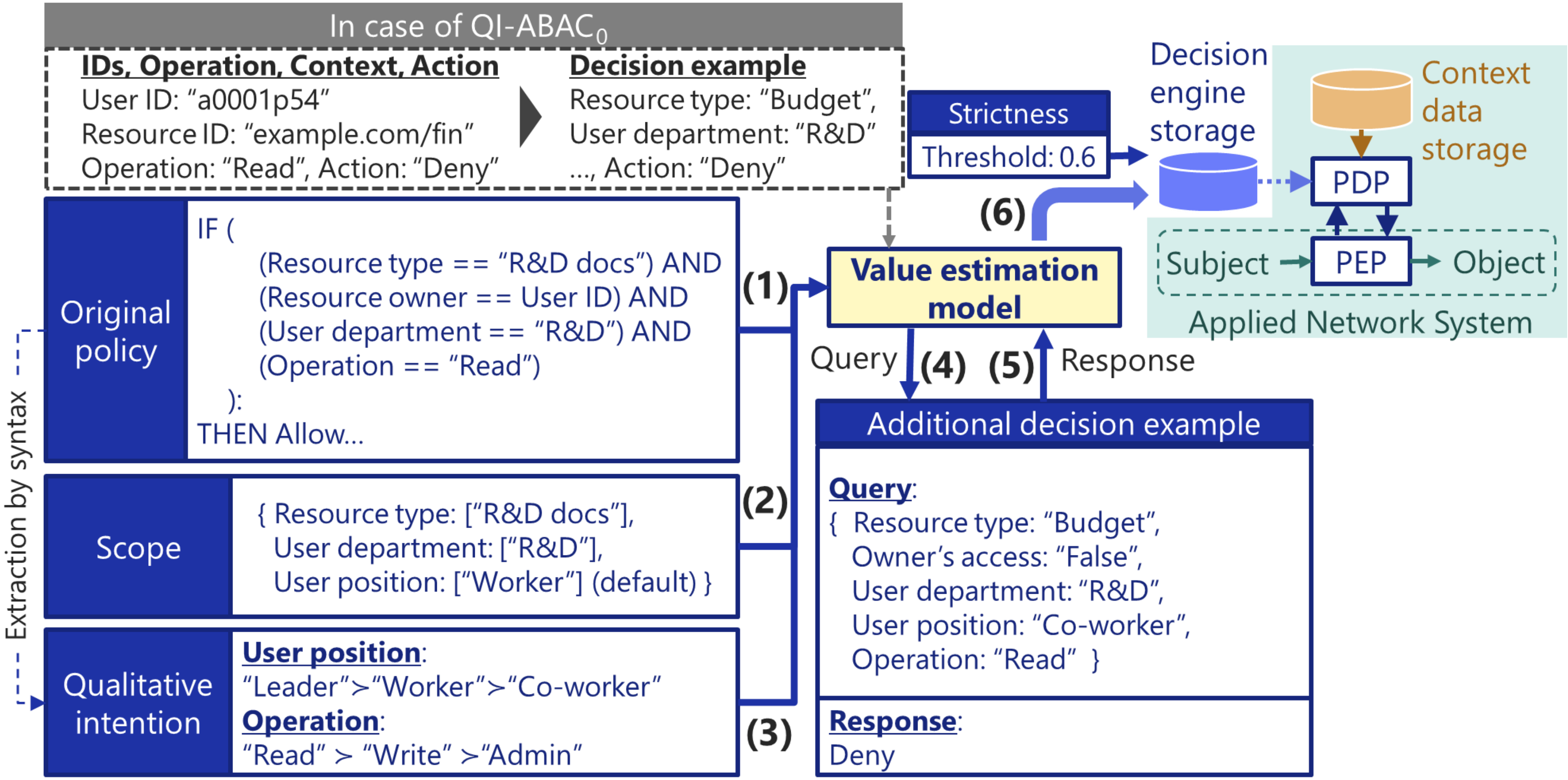


Attribute vector → Qualitative intention: Transformation → Feature vector → Machine learning: Value estimation → Value to grant

Methodology

Three applications to create ABAC decision engines from...

✓ (a) ACL/logs, (b) ABAC policy, (c) plus Q&A with policy managers.



In case of QI-ABAC$_0$

IDs, Operation, Context, Action
User ID: “a0001p54”
Resource ID: “example.com/fin”
Operation: “Read”, Action: “Deny”

Decision example
Resource type: “Budget”,
User department: “R&D”
..., Action: “Deny”

Original policy

```
IF (
        (Resource type == “R&D docs”) AND
        (Resource owner == User ID) AND
        (User department == “R&D”) AND
        (Operation == “Read”)
    ):
THEN Allow...
```

Scope

{ Resource type: [“R&D docs”],
User department: [“R&D”],
User position: [“Worker”] (default) }

Qualitative intention

User position:
“Leader”>“Worker”>“Co-worker”
Operation:
“Read” ≻ “Write” ≻“Admin”

Additional decision example

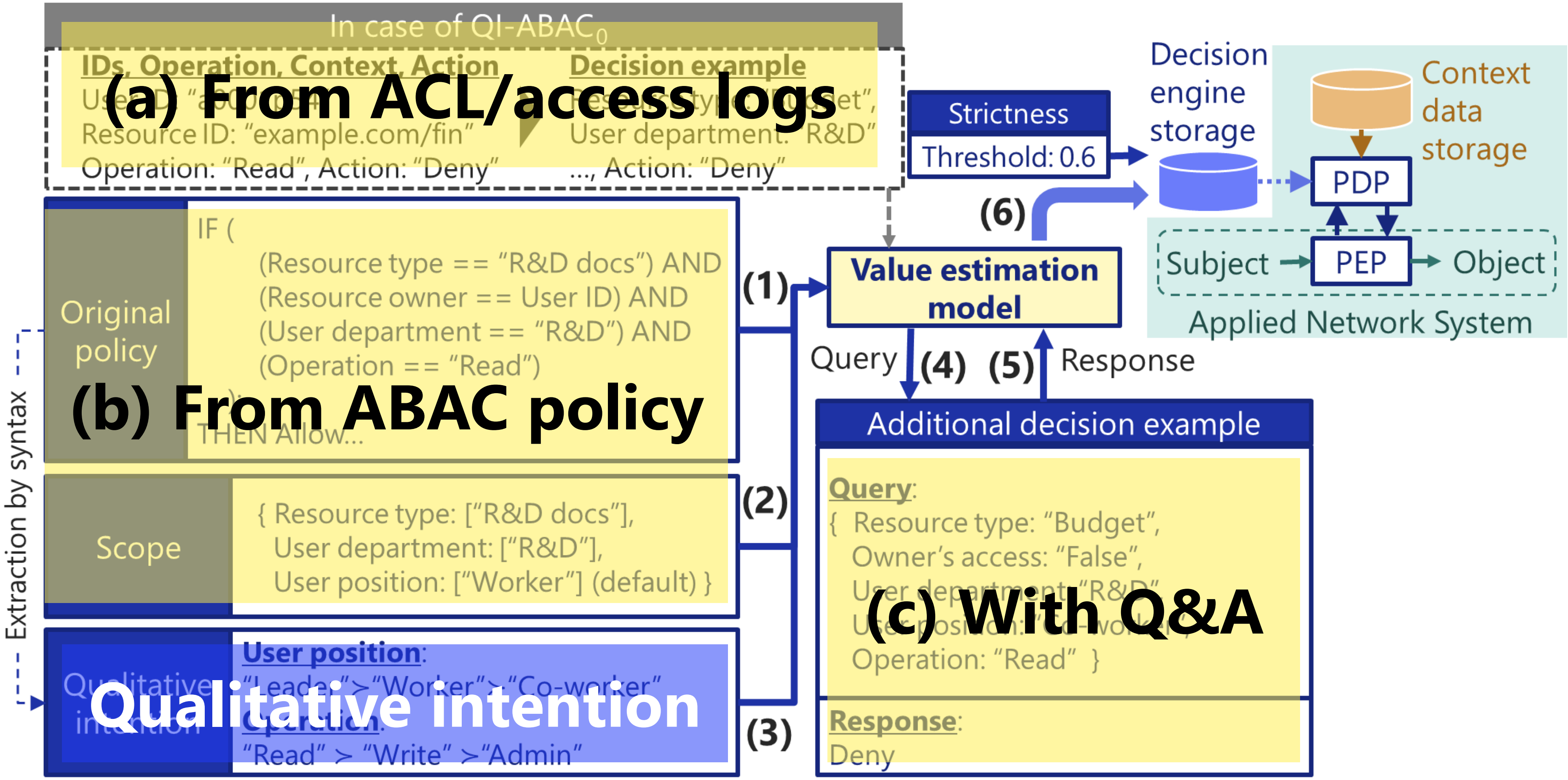
Query:
{ Resource type: “Budget”,
Owner’s access: “False”,
User department: “R&D”,
User position: “Co-worker”,
Operation: “Read” }

Response:
Deny

Methodology

Three applications to create ABAC decision engines from…

✓ (a) ACL/logs, (b) ABAC policy, (c) plus Q&A.



In case of QI-ABAC$_0$

(a) From ACL/access logs

IDs, Operation, Context, Action
User ID: "a00[illegible]"
Resource ID: "example.com/fin"
Operation: "Read", Action: "Deny"

Decision example
Resource type: "Budget",
User department: "R&D"
…, Action: "Deny"

(b) From ABAC policy

Original policy

IF (
(Resource type == "R&D docs") AND
(Resource owner == User ID) AND
(User department == "R&D") AND
(Operation == "Read")
)
THEN Allow…

Scope

{ Resource type: ["R&D docs"],
User department: ["R&D"],
User position: ["Worker"] (default) }

Qualitative intention

Qualitative intention

User position:
"Leader">"Worker">"Co-worker"
Operation:
"Read" > "Write" >"Admin"

Additional decision example

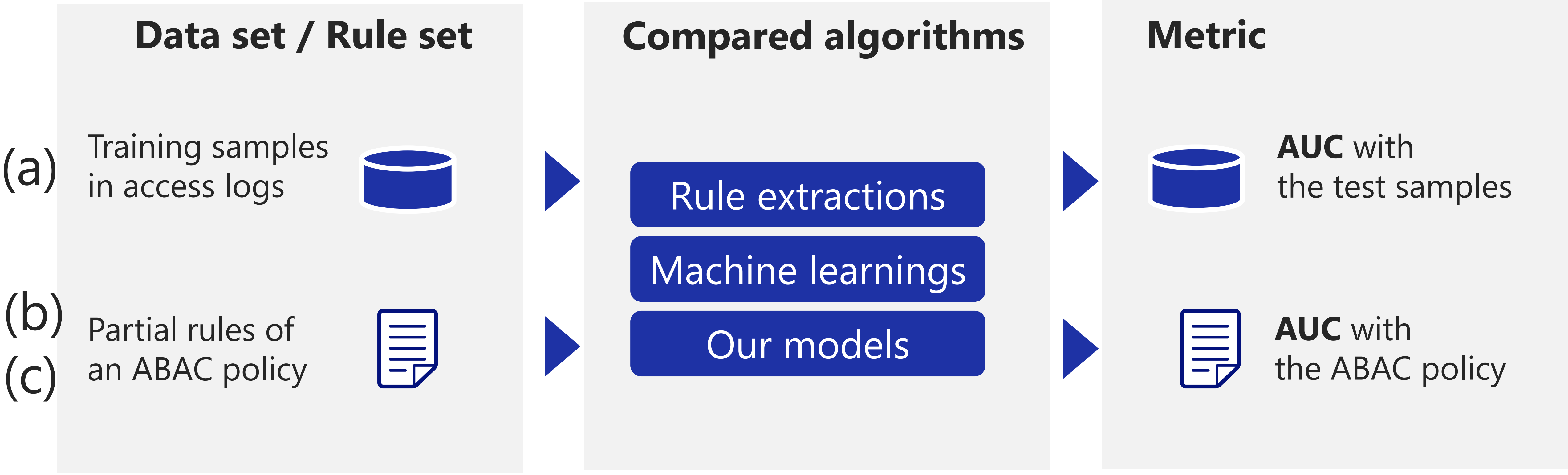
(c) With Q&A

Query:
{ Resource type: "Budget",
Owner's access: "False",
User department: "R&D",
User position: "Co-worker",
Operation: "Read" }

Response:
Deny

Evaluation Method

We have evaluated the **AUC** using access log dataset for the application for access logs. We used synthetic ABAC policies to evaluate other applications.



Data set / Rule set

(a) Training samples in access logs

(b) (c) Partial rules of an ABAC policy

Compared algorithms

Rule extractions

Machine learnings

Our models

Metric

AUC with the test samples

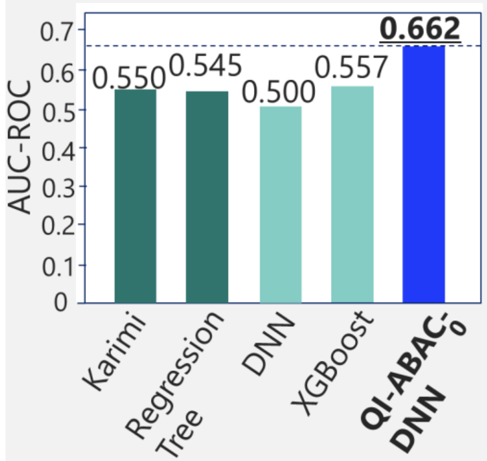
AUC with the ABAC policy

Evaluation Results

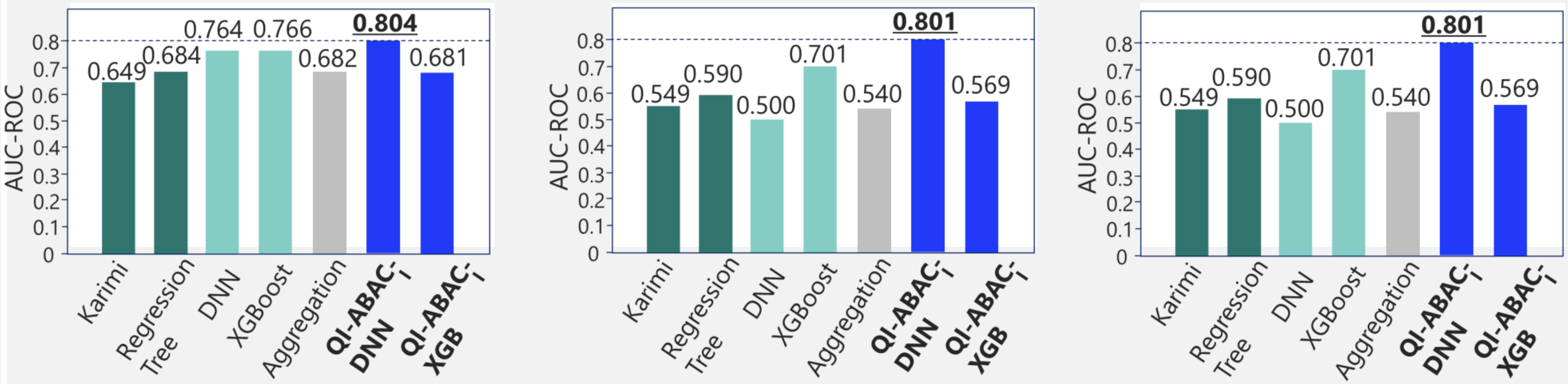
Two applications :Logs to decision engine and ABAC policy to decision engine.

- Our methods (especially DNN-based one) outperformed existing methods.

(a) Logs to ABAC decision engine



(b) ABAC policies to ABAC decision engine

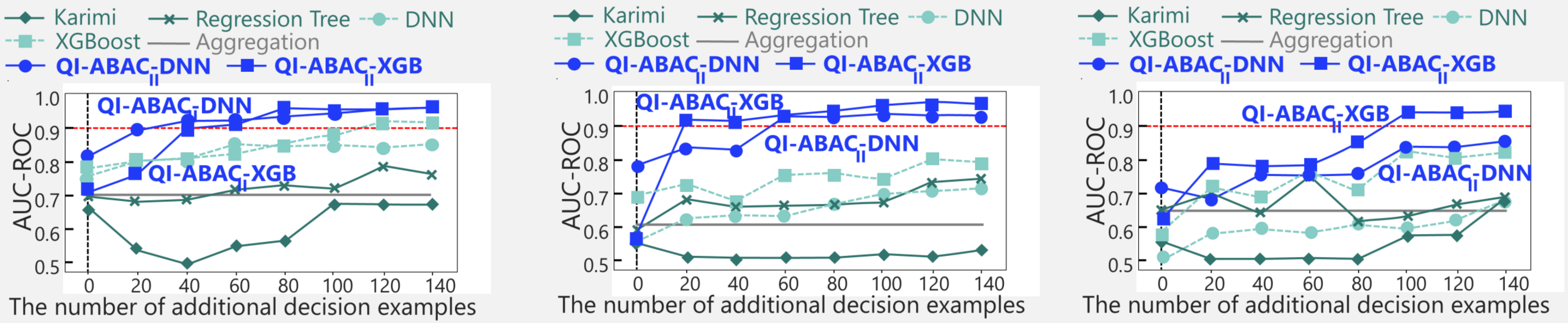


Evaluation Results

Application of ABAC policies to a decision engine with additional examples.

➢ Our methods performed the best with the least examples.

(c) ABAC policies to ABAC decision engine
with additional decision examples (simulated Q&A).



Conclusion

- **Proposal**

  A framework to refine access control policies (ACL policy, access logs, and ABAC policies) to an improved ABAC decision engine.

- **Challenge**

  Appropriate decisions in business tasks and situations not envision.

- **Solution**

  “Qualitative Intentions” to guide better access decisions defined as a minimal knowledge.

- **Evaluation**

  The best performance in real access logs and synthetic sample policies.

\Orchestrating a brighter world

NEC

Qualitative intentions for University sample policy

1. {User.ID ==Resource.StudentID} > {User.ID !=Resource.StudentID}
2. {User.course.taken ∈ Resource.course} > {User.course.taken ∉ Resource.course}
3. {User.course.taught∈ Resource.course} > {User.course.taught ∉ Resource.course}
4. {User.department ==Resource.department} > {User.department !=Resource.department}
5. {User.ischair == True} > {User.ischair == False}