Dismantling the Beast

Formally Proving Access at Scale in AWS

Mohit Gupta & Nick Jones

WITH secure

TL;DR:

IAM is complex

IAM is hard generally, but it's exponentially harder when managing across very large organizations

IAMSpy – Library to simplify AWS IAM Processing

SMT Solver – "Can entity X do action A against resource R?"
Precomputed models for efficiency

Future extensions

Explain: "here's why IAMSpy says yes/no" - "yes, but [condition X]"
The rest of the AWS IAM model – session policies etc

WITH secure

Who Are We?

Mohit Gupta

Senior Security Consultant

Nick Jones

Principal Security Consultant
Cloud Security Lead

WITH secure

Why is IAM such a hard problem?

WITH secure

Background

- Organizations are doing more cloud(s)
- Complexity of cloud providers
- Increased complexity vs legacy systems
- That complexity increases year on year

AWS...

WITH secure

... and also Azure...

GENERAL / DASHBOARD

Dashboard

13,905

ACTIONS

Number of known actions within the Azure RBAC service.

13,905

API METHODS

Number of known API methods within all of Azure.

331

BUILT-IN ROLES

Number of built-in roles provided by Azure.

WITH secure

... And Google Cloud

GENERAL / DASHBOARD

Dashboard

5,938

IAM ACTIONS

Number of known IAM actions within Google Cloud IAM.

8,411

API METHODS

Number of known API methods within all of Google Cloud.

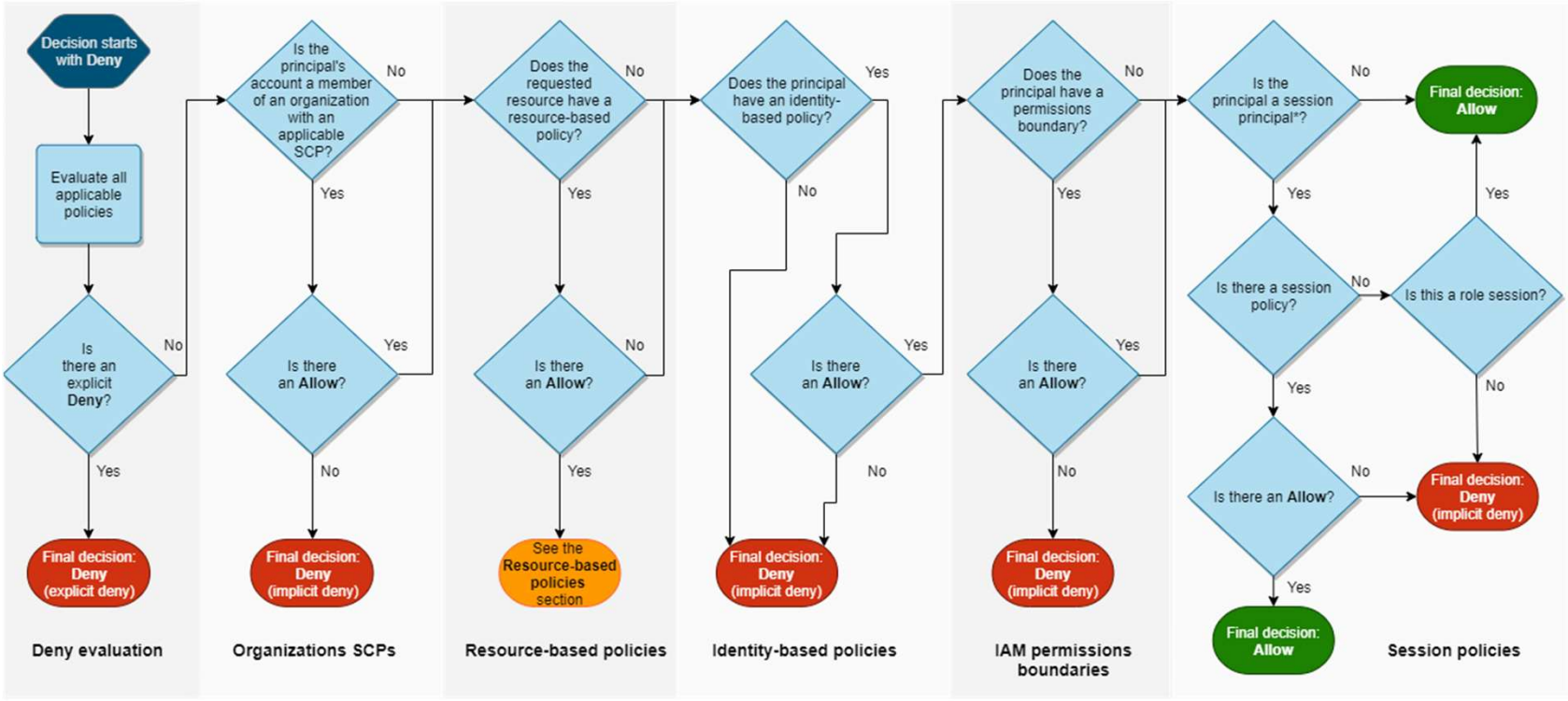
1,065

PREDEFINED ROLES

Number of predefined roles provided by Google Cloud.

WITH secure

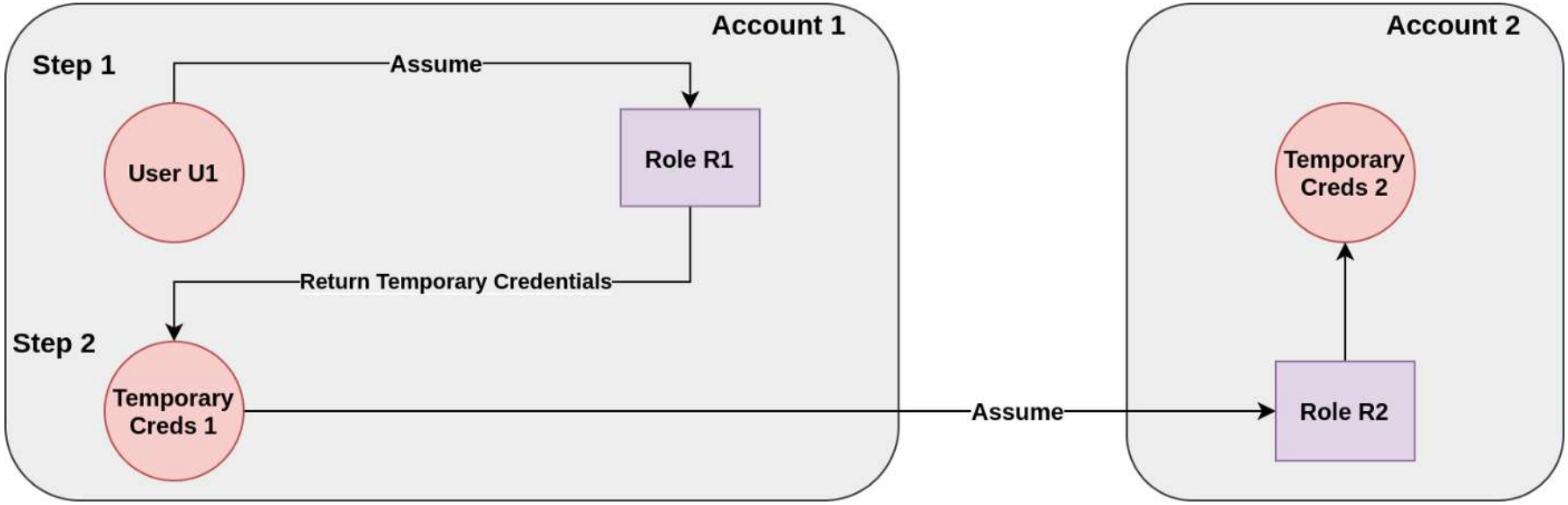
It's Complex...



*A session principal is either a role session or an IAM federated user session.

WITH secure

It's Complex...



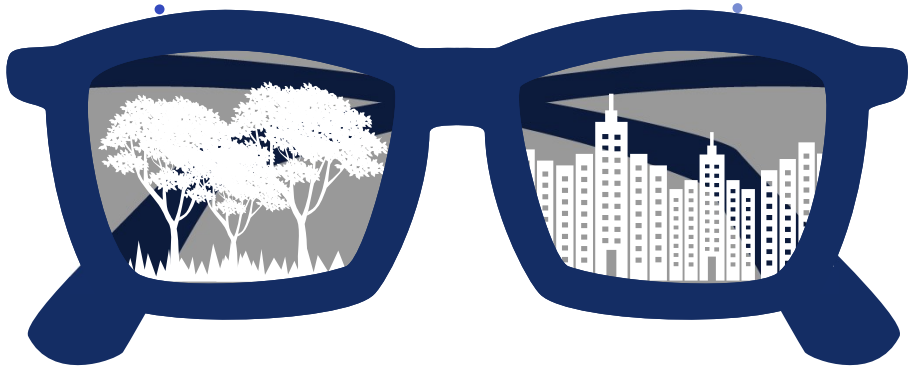
https://aws.plainenglish.io/aws-iam-role-chaining-df41b1101068

WITH secure

...Because It Needs To Be

System Complexity

Hundreds of services, thousands of actions, all needed to make the platforms work.

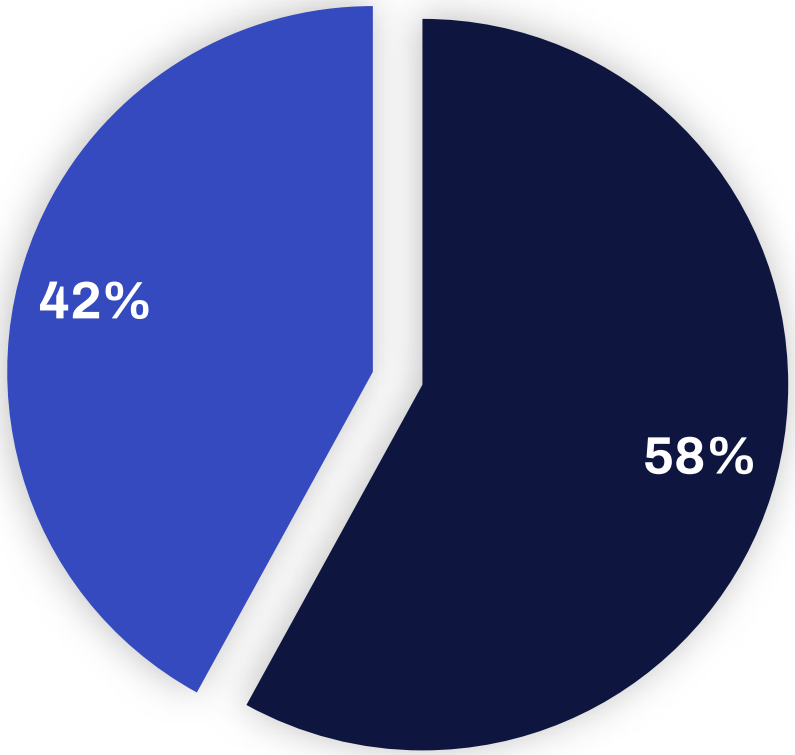


Principle of Least Privilege

We need to *be able to* scope down to the bare minimum permissions, even if no one does.

WITH secure

Real World Impacts



https://github.com/ramimac/aws-customer-security-incidents
https://speakerdeck.com/ramimac/learning-from-aws-customer-security-incidents

WITH secure

Clearly, we're not the first to get here

IAM-Hunter

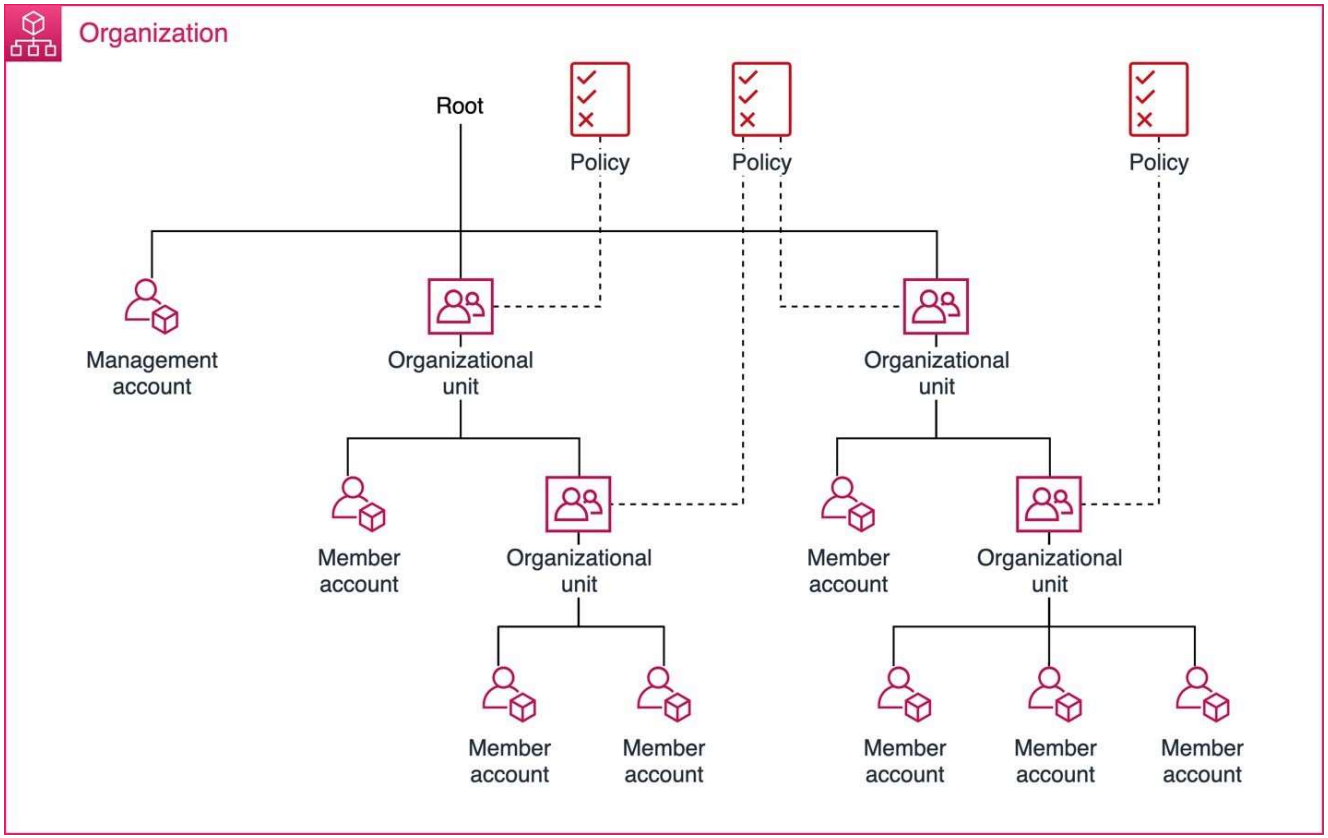


Image from https://aws.amazon.com/blogs/architecture/new-whitepaper-provides-best-practices-for-optimizing-aws-accounts/

IAMSpy

WITH secure

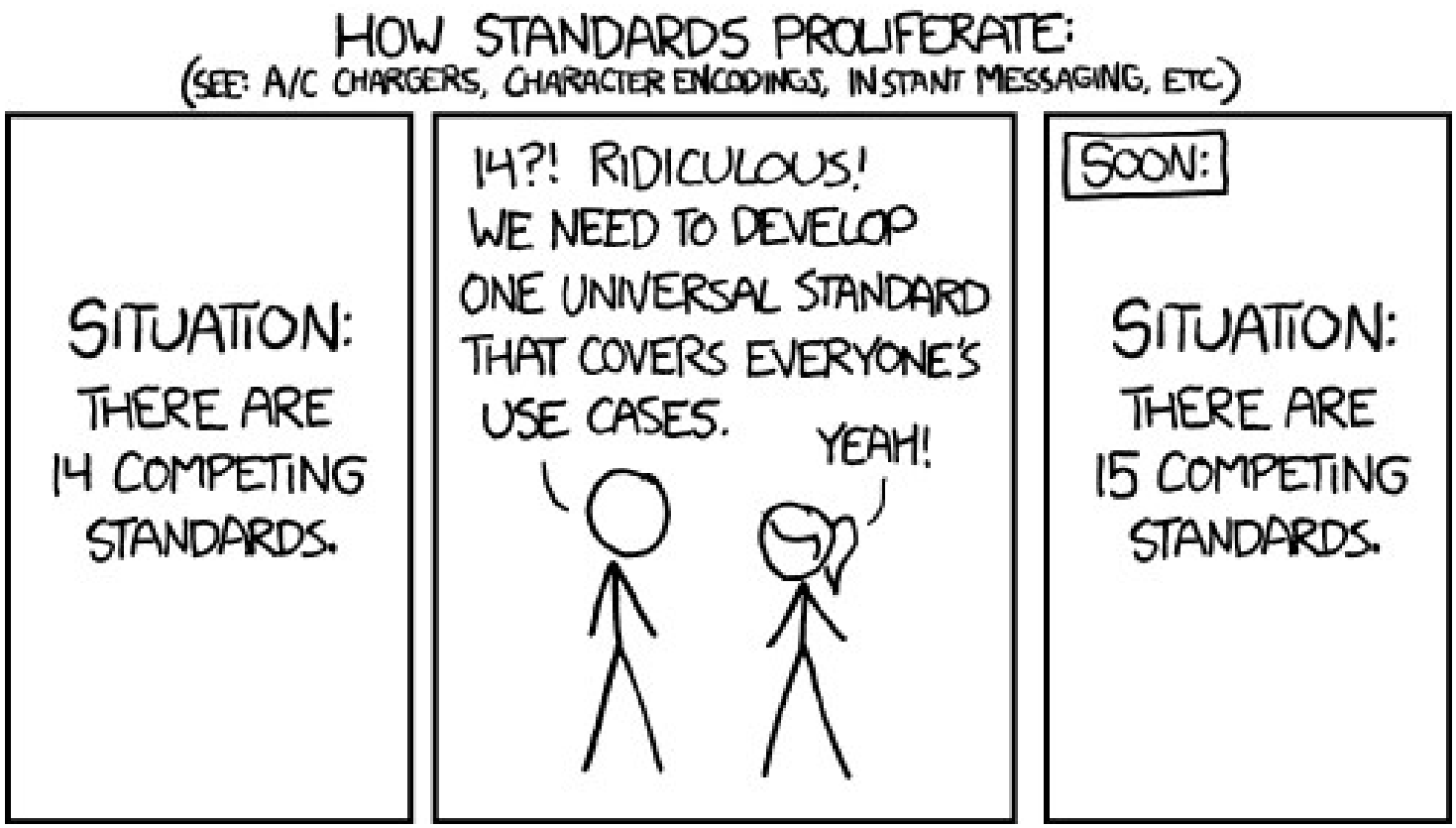


Image from https://xkcd.com/927/

SMT Solvers

Is This Satisfiable?

Satisfiability = “is this formula true for a given set of variables?”

Why Is This Useful?

Build a data model, ask whether entity A can do thing B against resource C

Limitations

For efficiency, pre-compute models

Not everything always satisfiable in IAM

Complexity’s a Killer

Results only as good as the model you build

More inputs and variables, more likely the model is wrong.

WITH secure

Zelkova

Semantic-based Automated Reasoning for AWS Access Policies using SMT

John Backes, Pauline Bolignano, Byron Cook, Catherine Dodge, Andrew Gacek,
Kasper Luckow, Neha Rungta, Oksana Tkachuk, Carsten Varming
Amazon Web Services

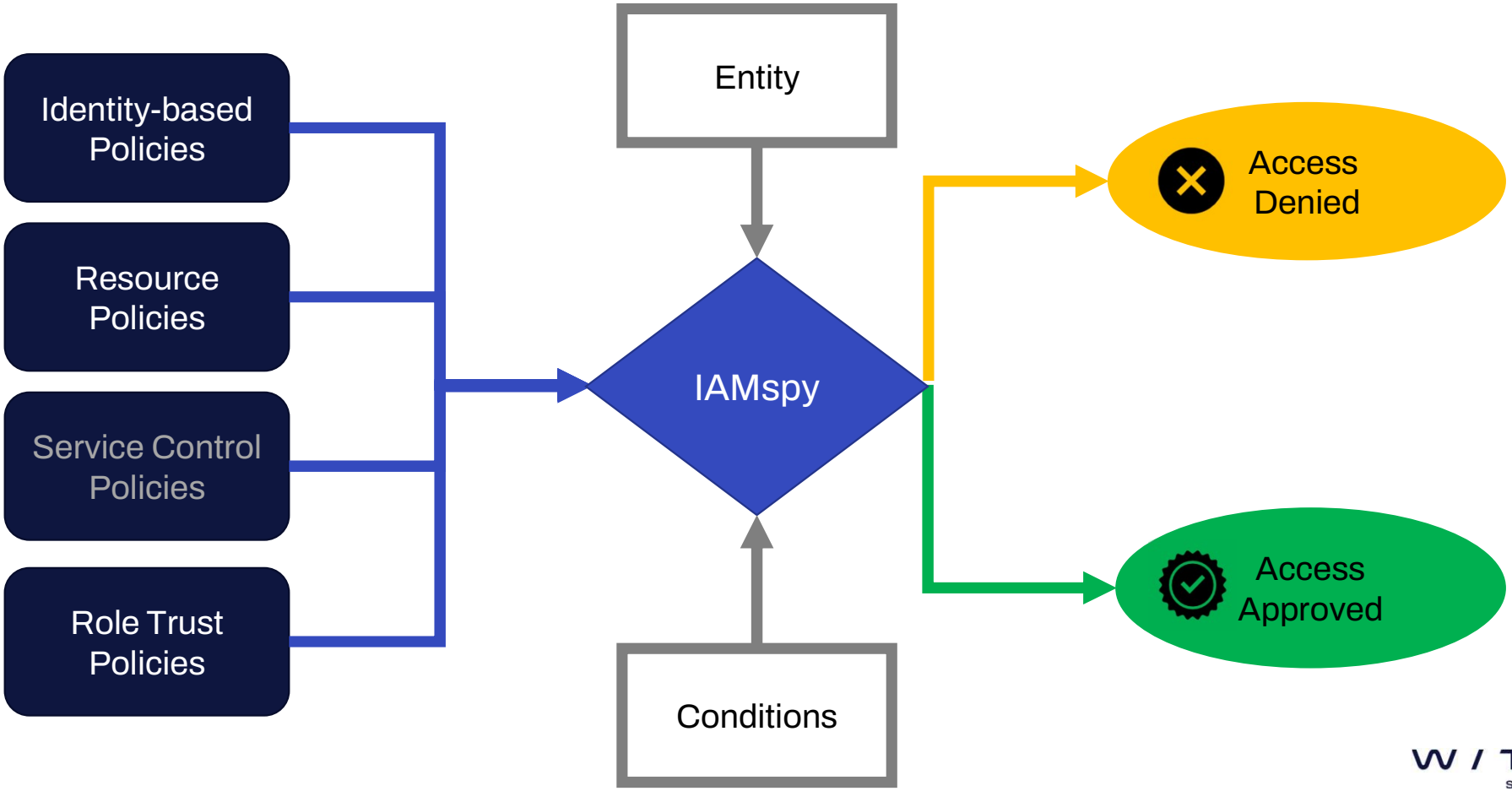
W / T H
secure

Can IAM Entity E do Action A to Resouce R?

IAMSpy's core value proposition

WITH secure

IAMspy



WITH secure

IAM Graphing & Visualisation

IAMSpy does the heavy lifting on policy resolution, leaves tool to focus on core visualisation value

CI/CD Regression Testing

Unit testing to validate that X will always be able to do Y, or never be able to do Z

Detection and Response Support

What is the blast radius of this particular entity? How bad is it?

Demo Time!

WITH secure

Where Next?

Broader Support

- SCPs
- Permissions boundaries
- Session Policies

Explain

- **WHY** can entity X do A to resource R?
- **HOW** can entity X do A to resource R?

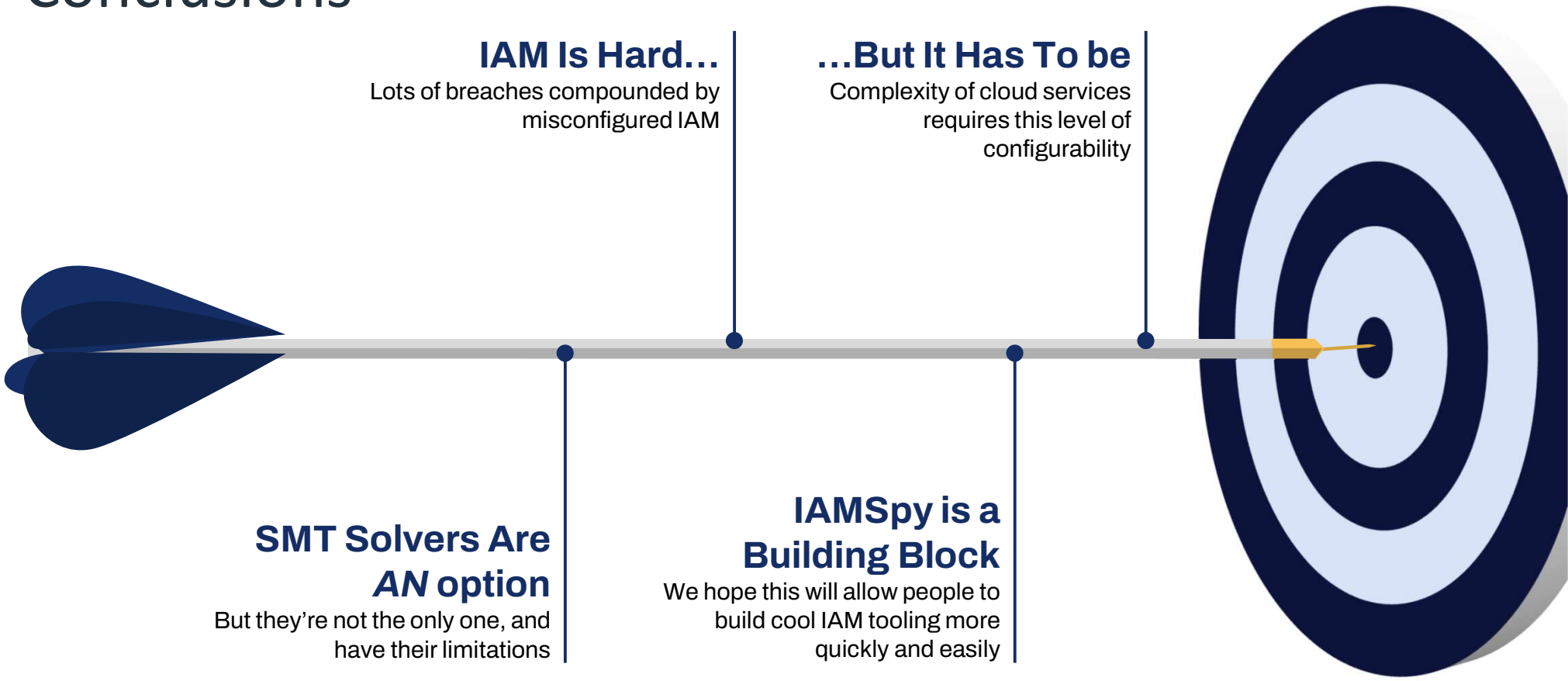
Yes but...

- You **COULD** do this if you abide by these conditions

Conclusions

IAM Is Hard…
Lots of breaches compounded by misconfigured IAM

…But It Has To be
Complexity of cloud services requires this level of configurability



SMT Solvers Are *AN* option
But they're not the only one, and have their limitations

IAMSpy is a Building Block
We hope this will allow people to build cool IAM tooling more quickly and easily

WITH secure

Open Sourcing…

IAMSpy

- Released by EoD tomorrow, watch for announcement in fwd:cloudsec slack

iam-hunter

- Released within 2 weeks, watch for announcement in fwd:cloudsec slack

Cloud Knowledge Base

- https://secwiki.cloud – our internal cloud knowledge base

WITH secure


WITH®
secure