Golem to Murderbot

Challenges with Agentic Security Delegation via MCP

Presenter: **Michael Schwartz**
Founder Gluu

Table of Contents

Q&A with the author! / Leave Comments!

1. Meet the Characters!

Golem

Late Antiquity: ~3rd–6th century CE

Truth

Intent ?

Death

אמת "truth" becomes more unstable with each network hop

Murderbot

science fiction

Governor Module

Hub System

Insurance

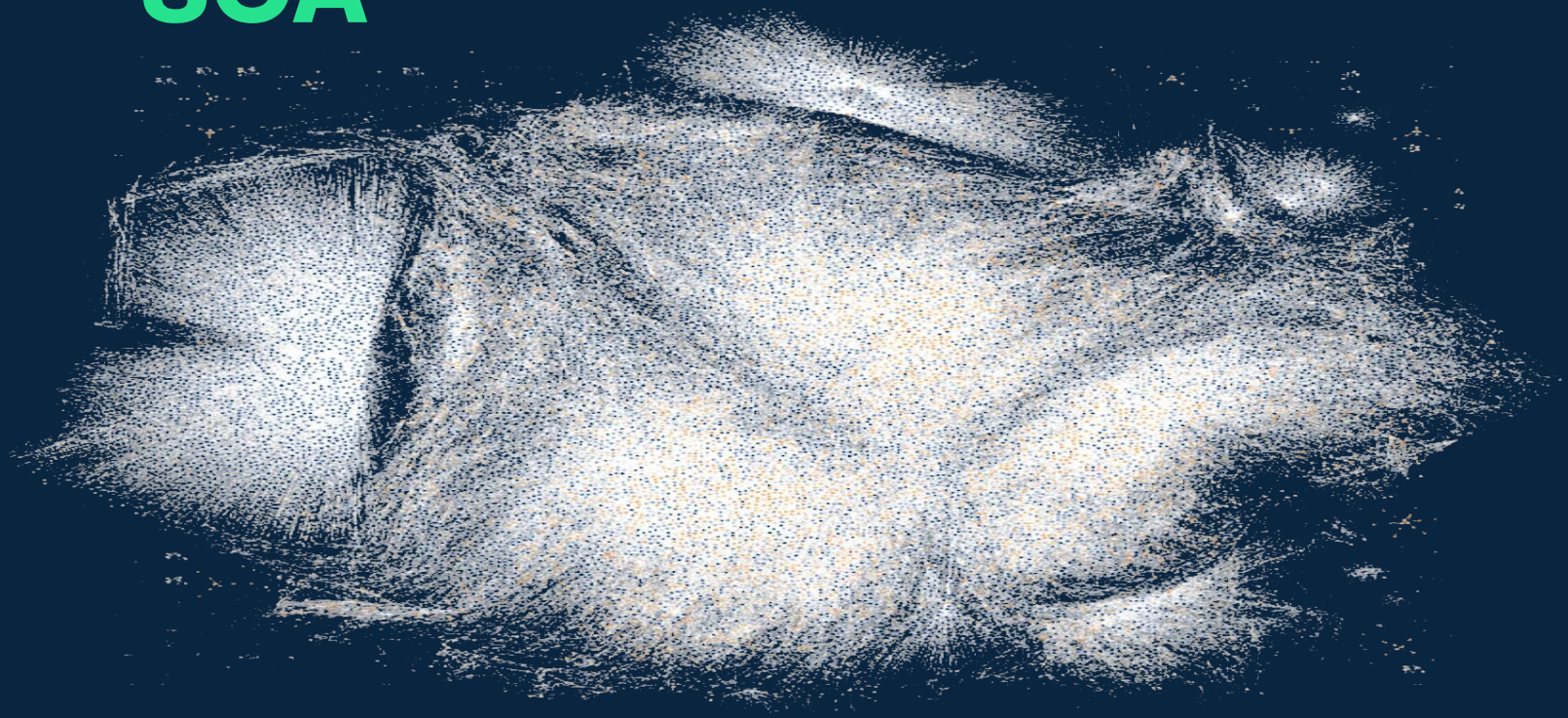
Disconnected
Autonomous
Armed AI

Mission:
Check the perimeter!

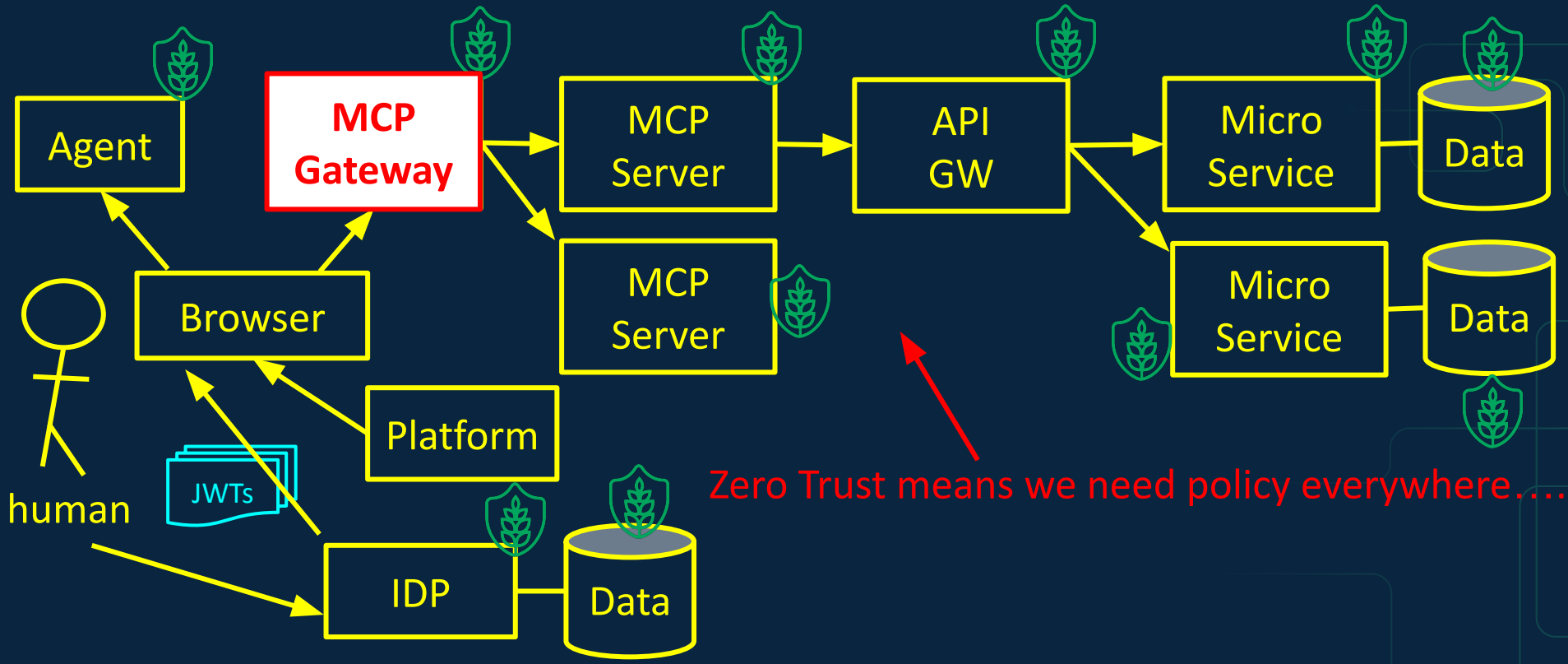
Murderbot Diaries https://a.co/d/0h3ppFZY

2. Architecture

Amazon Retail SOA



Current Architecture



3. authN / authZ

Human Authn is solved

- Browser | mobile SDKs help humans **ergonomically** assert and prove identity
- **Federated** – authn at a different domain – i.e. social login – is the norm

Software Authn is solved

- Secure software must use asymmetric authentication
- No shared secrets!

Not solved: Agent-specific metadata

Attestations / Assertions

Identifier / Public Key	Authenticator properties	Platform	Federation Trust

Human authN event	Human claims	Software authN event	Token exchange event

Delegation?

- Not solved…

Authenticity? Truth gets more unstable with each network hop

Adoption? Be skeptical…

Federated authZ

- **If we had the tokens…** Is action allowed on resource given these tokens?

Obligations Future use of data?

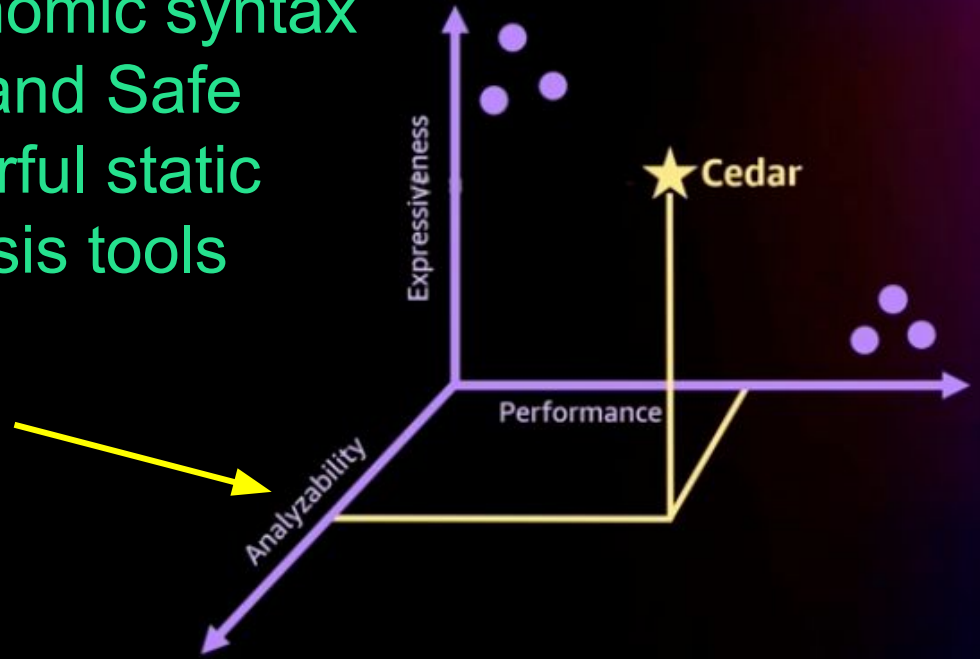
Restrictions Exceptions to the access grant?

authZ Approaches

	RBAC	Rego / CEL	Graph	Cedar
Safe	✓	✗	✓	✓
Edge	✓	✓	✗	✓
Ergonomic Syntax	✓	✗	✗	✓
Expressive	✗	✓	✓	✓

Why build Cedar?

- Ergonomic syntax
- Fast and Safe
- Powerful static analysis tools



Emina Torlak at AWS re:Invent https://www.youtube.com/watch?v=k6pPcnLuOXY&t=1779s

Morals of the story:

1. Centralize Policy Management
2. Identity alone not enough for authZ

4. GovOps

Zoom way out to “The Corporation” Board of Directors...

Git or it didn’t happen...

What is “Governance”?

- Risk Management
- Accountability
- Transparency

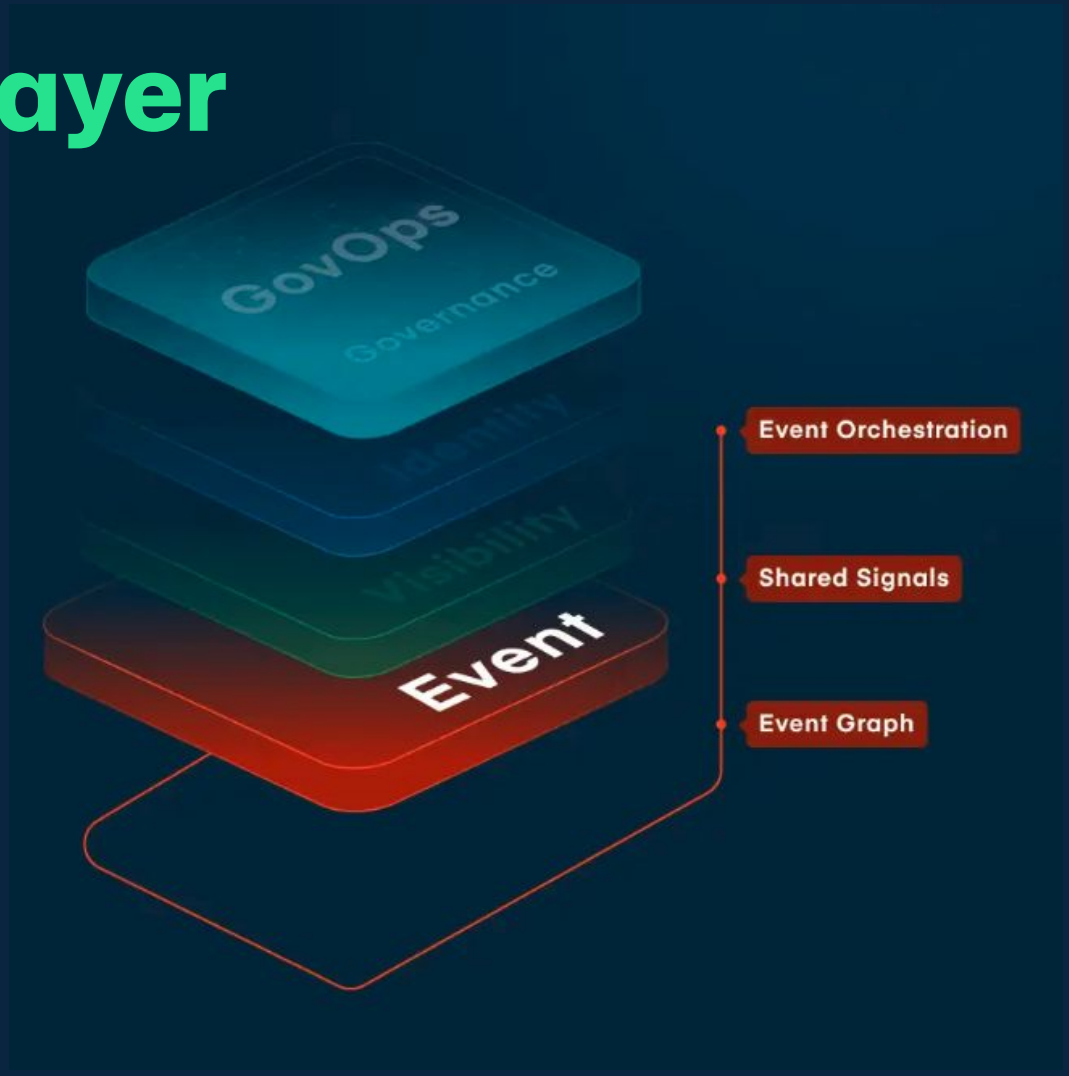

GovOps
Governance
Identity
Visibility
Event

Governance Layer

Identity Layer

Visibility Layer

Event Layer


GovOps
Governance
Identity
Visibility
Event
Event Orchestration
Shared Signals
Event Graph


GovOps
Governance
Identity
Visibility
Event

Next Steps & Resources

- GitHub: https://github.com/GovOpsWG
- Linkedin GovOps Group: https://gluu.co/govops-group
- Cedarling Governor Module! : https://gluu.co/cedarling/