



Agentic AI Foundation

AGNTCon + MCPCon

North America

Authorization After OAuth: Controlling Tools on Hosted MCP Servers You Don't Own

Nick Taylor

Developer Advocate, Pomerium

Where the agentic stack is being built.



Where the agentic stack is being built.

'Ran through me' & 'good value in pub' - ex-NFL star Kelce tries rugby

"At the very start, he sort of went round the back of a ruck and picked the ball up, which he obviously was then penalised for."

Dave Lewis, Hackney RFC, to BBC Sport

Durrans, T. (2026, October 9).
'Ran through me' & 'good value in pub' -
ex-NFL star Kelce tries rugby. BBC Sport.

<https://www.bbc.com/sport/articles/cm79pdw50y7wo>



Agentic AI Foundation

AGNTCon + MCPCon

North America

Governance

Where the agentic stack is being built.

Governance

Some servers ship read-only

- GitHub: an HTTP header, or /readonly in the URL path.
- Linear: /mcp/readonly in the URL path, or the read OAuth scope.
- Atlassian: a query parameter on the URL.

Governance

All of these are deploy-time controls.

- Read-only, scopes, or a fixed list of tools.
- Set when deployed. Can't change until the next deploy.
- Same tools for every caller, on every call.



Where the agentic stack is being built.

Governance

A lot of MCP servers still skip OAuth

Of 7,973 live remote servers:

- 30% use OAuth
- 29% use a static token or API key
- 41% have no authentication

Zhou, H., Zhang, X., Zhang, H., Zhang, H.,
Zhang, M., & Yang, M. (2026, May).

A first measurement study on authentication security
in real-world remote MCP servers. arXiv.

<https://arxiv.org/abs/2605.22333>

Governance

A static token is often one person's key.

- Share it, and the log can't name the teammate.
- A key per person fixes that, but doesn't scale and is a maintenance burden.



Where the agentic stack is being built.

Governance

OAuth scopes are coarse and static

- A scope grants broad access, not per-tool control
- You can't remove one action from a scope
- Still set when the client is configured



Where the agentic stack is being built.



Agentic AI Foundation

AGNTCon + MCPCon

North America

MCP Gateways

Where the agentic stack is being built.

MCP Gateways

- MCP gateways are proliferating
- An MCP server's own controls aren't enough



Where the agentic stack is being built.

MCP Gateways

- A gateway can enforce policy between the client and the server
- A central point for managing security posture
- One kind of gateway is an identity-aware proxy



Where the agentic stack is being built.



Agentic AI Foundation

AGNTCon + MCPCon

North America

Identity Aware Proxy

Where the agentic stack is being built.

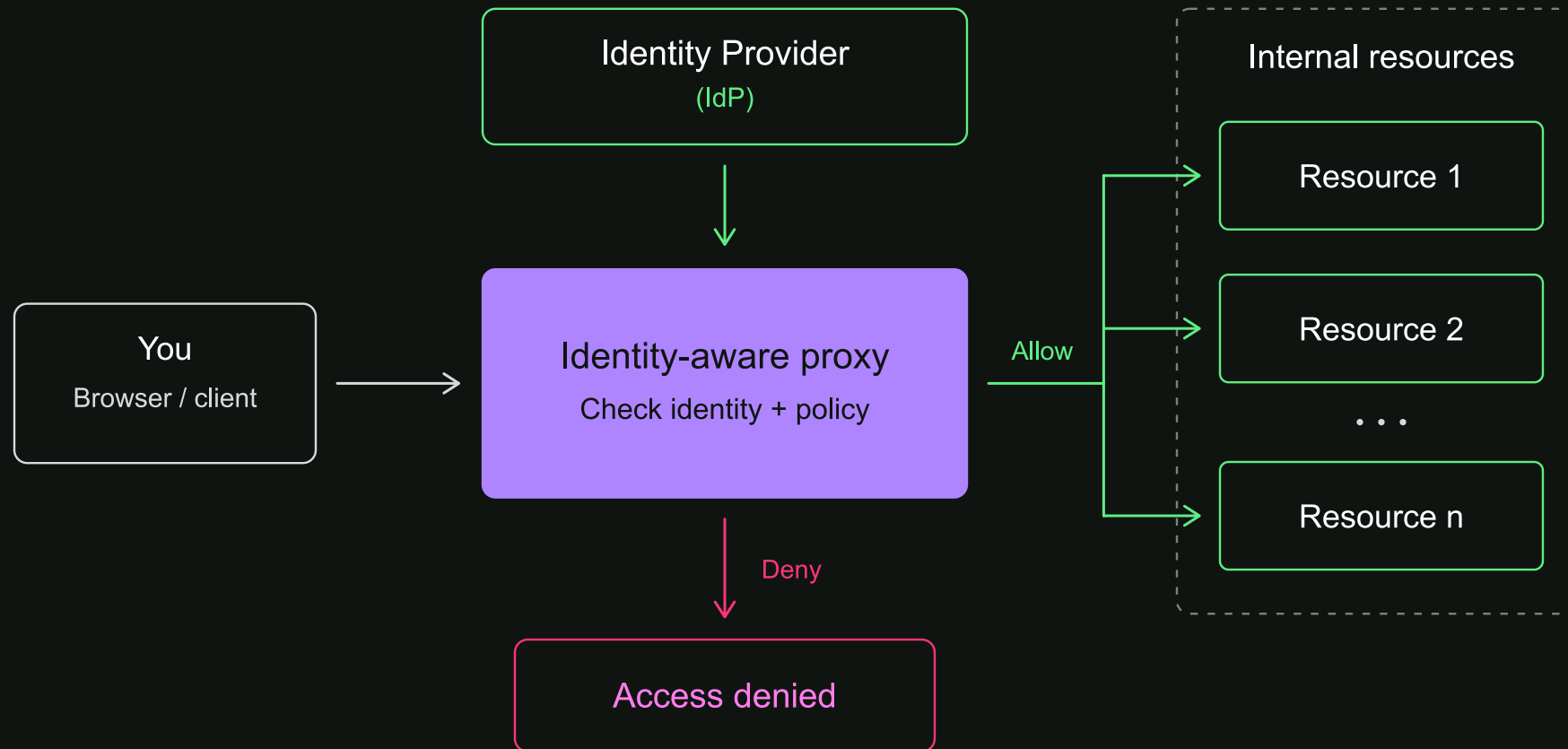
What is an Identity Aware Proxy?

- Checks identity and policy on every request, not just at login
- No VPN, identity over network location
- Policy enforced at the proxy, not in each app
- Audit logs out of the box



Where the agentic stack is being built.

What is an Identity Aware Proxy (IAP)?





Agentic AI Foundation

AGNTCon + MCPCon

North America

Pomerium

Where the agentic stack is being built.

Pomerium

- An identity-aware proxy
- Open core
- Installs at your network's edge



Where the agentic stack is being built.

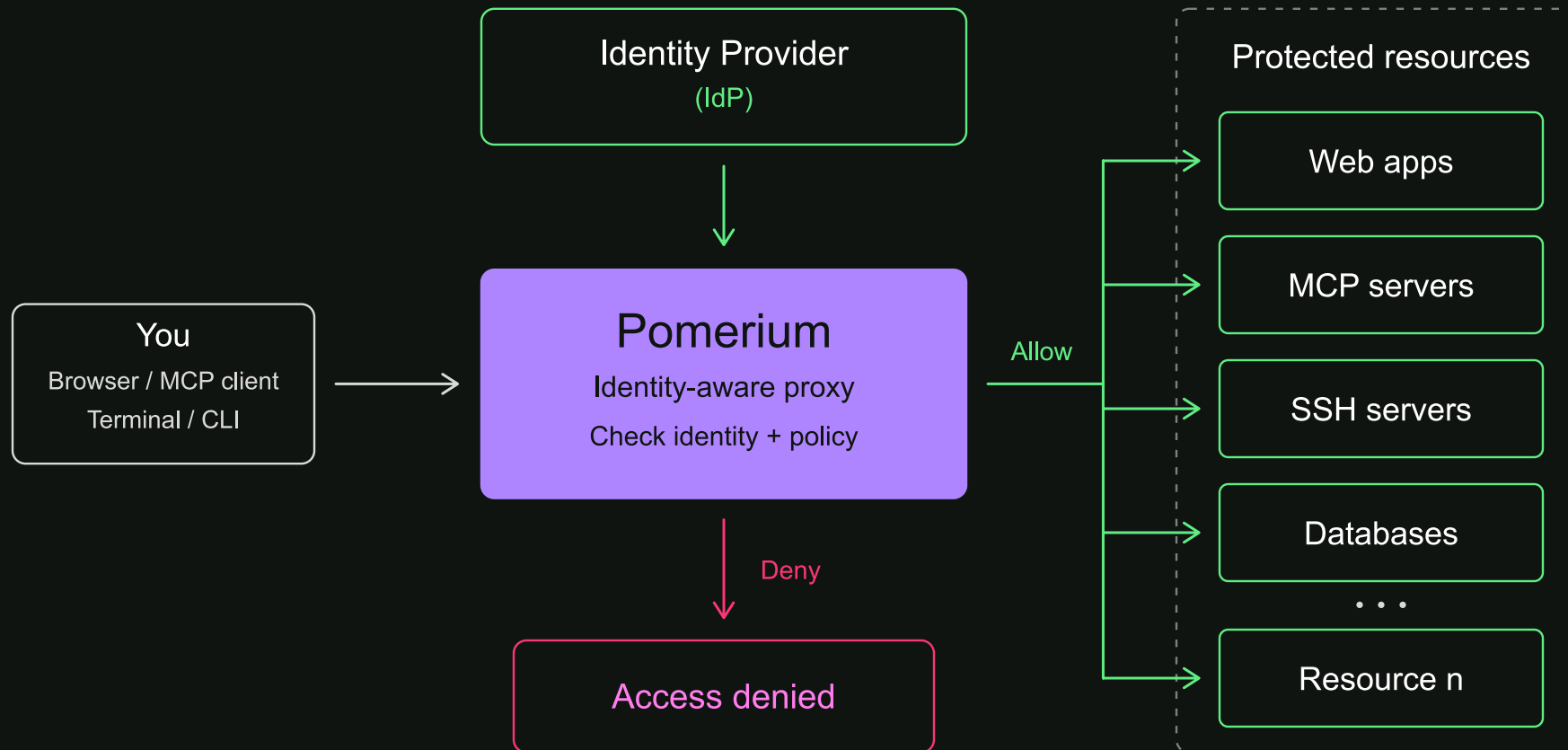
Pomerium

- Always self-hosted
- All your data flows through your own infrastructure
- Handles OAuth for you, including upstream flows
- Tokens stay in the gateway, whether or not you own the server



Where the agentic stack is being built.

Pomerium is an IAP



Fine-grained authorization

Who gets in

Control who can access the MCP server.

Fine-grained Tool Authorization

Allow the server, but deny one or more tools.

Servers you own

- Policy lives at the proxy, not in your app
- No OAuth code in the server
- Allow or deny per caller, per tool



Where the agentic stack is being built.

Servers you don't own

- Policy lives at the proxy, not in your app
- Allow or deny per caller, per tool
- You don't need to control the server to govern access



Where the agentic stack is being built.

Pomerium bridges it

- Your identity provider signs the person in
- Pomerium runs the upstream OAuth flow
- The upstream token is injected into each request — the client never sees it



Where the agentic stack is being built.

Route configuration



Agentic AI Foundation

AGNTCon + MCPCon
North America

```
from: https://github.maisonlab.dev
to: https://api.githubcopilot.com
name: GitHub
mcp:
  server:
    upstream_oauth2:
      client_id: xxxxxxxxxxxx
      client_secret: xxxxxxxxxxxx
      scopes: ["read:user", "user:email", "read:org", "repo"]
      endpoint:
        auth_url: https://github.com/login/oauth/authorize
        token_url: https://github.com/login/oauth/access_token
```

Policy for a Route

```
policy:
  - allow:
    and:
      - email:
        in:
          - nick@nickyt.co
          - ntaylor@pomerium.com
```

Policy for a Route that Denies a Tool Call



Agentic AI Foundation

AGNTCon + MCPCon
North America

```
policy:
  - allow:
    and:
      - email:
        in:
          - nick@nickyt.co
          - ntaylor@pomerium.com
  - deny:
    and:
      - mcp_tool:
        is: merge_pull_request
```

Where the agentic stack is being built.



Agentic AI Foundation

AGNTCon + MCPCon

North America

Demo Time!

Where the agentic stack is being built.

Resources

- [Pomerium MCP capabilities](#)
- [Bridge a third-party MCP server](#)
- [Pomerium open source](#)
- [A First Measurement Study on Authentication Security in Real-World Remote MCP Servers](#)

Homework

Everything demoed today, you can do yourself in this free interactive lesson.

go.pomerium.com/agntcon26-lesson



Full free course

You can also do the full free course to learn about leveraging Pomerium as an MCP gateway.

go.pomerium.com/agntcon26-mcp-course



Let's connect!

I'm always looking to connect with people in the community. Don't be shy!

nickyt.co/socials



Thank you!

Slide deck

agentcon.netlify.app



Where the agentic stack is being built.