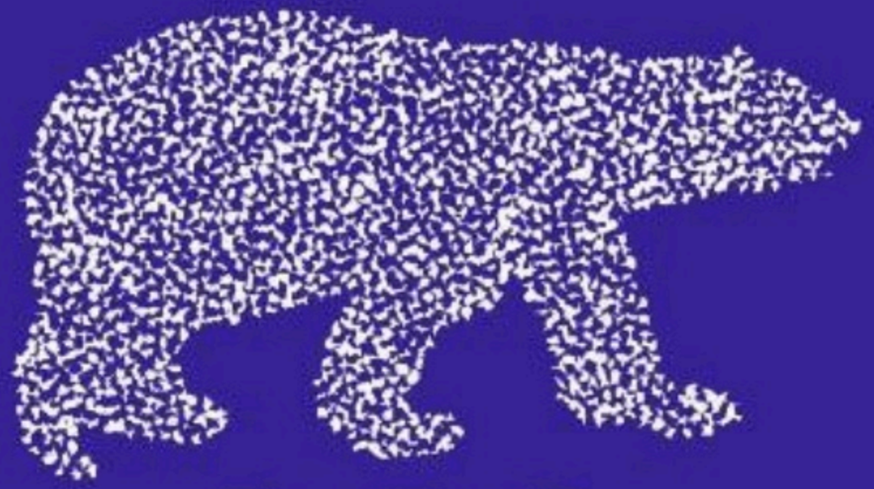


OSO

Meetup

Thursday, May 28, 2020

Why Developers Don't Care about Security

Hosted by
Bill S. and Constance M.

Details

Clearly this is a mess, but we are making the best of it. We are meeting virtually on Google Meet.

https://meet.google.com/cvo-orfp-cva

Security conversations with application teams don't have to be an uphill battle. In this compelling session, we will discover the underlying challenges app teams face that cause them to seemingly dismiss security concerns, and we will collaboratively find solutions to those problems.

To us as Information Security professionals, it can certainly feel like app teams don't care about security. That seems clear in those moments when they proceed with a production deployment despite poor static code analysis results or when they hesitate to add a high priority security remediation to the

stripe twilio

aws

Low Friction

oso

Security products were not built for developers

oso

We put security in the hands of the makers


Charity Majors
@mipsytipsy
Replying to @mipsytipsy
"Consumer-quality developer tools" is how I think of it.
3
8
63
Tweet your reply
oso

Authorization

Authorization is a mess

```
export class UserMetadataComponent implements OnInit {
  metadata = {};

  // Inject both AuthService and HttpClient
  constructor(public auth: AuthService, private http: HttpClient) {}

  ngOnInit(): void {
    this.auth.user$
    .pipe(
```

```
@app.route('/articles/<int:ident>', methods=['GET', 'PUT'])
@login.logged_in
def single_article(ident):
    article = db.session.query(Article).filter_by(id=ident).first()
    if not article:
        raise NotFound
    if request.method == 'GET':
        if not authorize.read(article):
            raise Unauthorized
        return jsonify(id=article.id, name=article.name), 200
```

```
# We check
self._cr.e
```

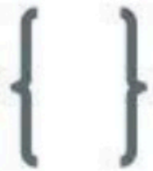
```
post('/create',requireAdmin, function (req, res) {
/.....


tion requireAdmin(request, response, next) {
if (request.decoded.role != 'admin') {
    response.json({message: 'Permission denied.' });
```

Database

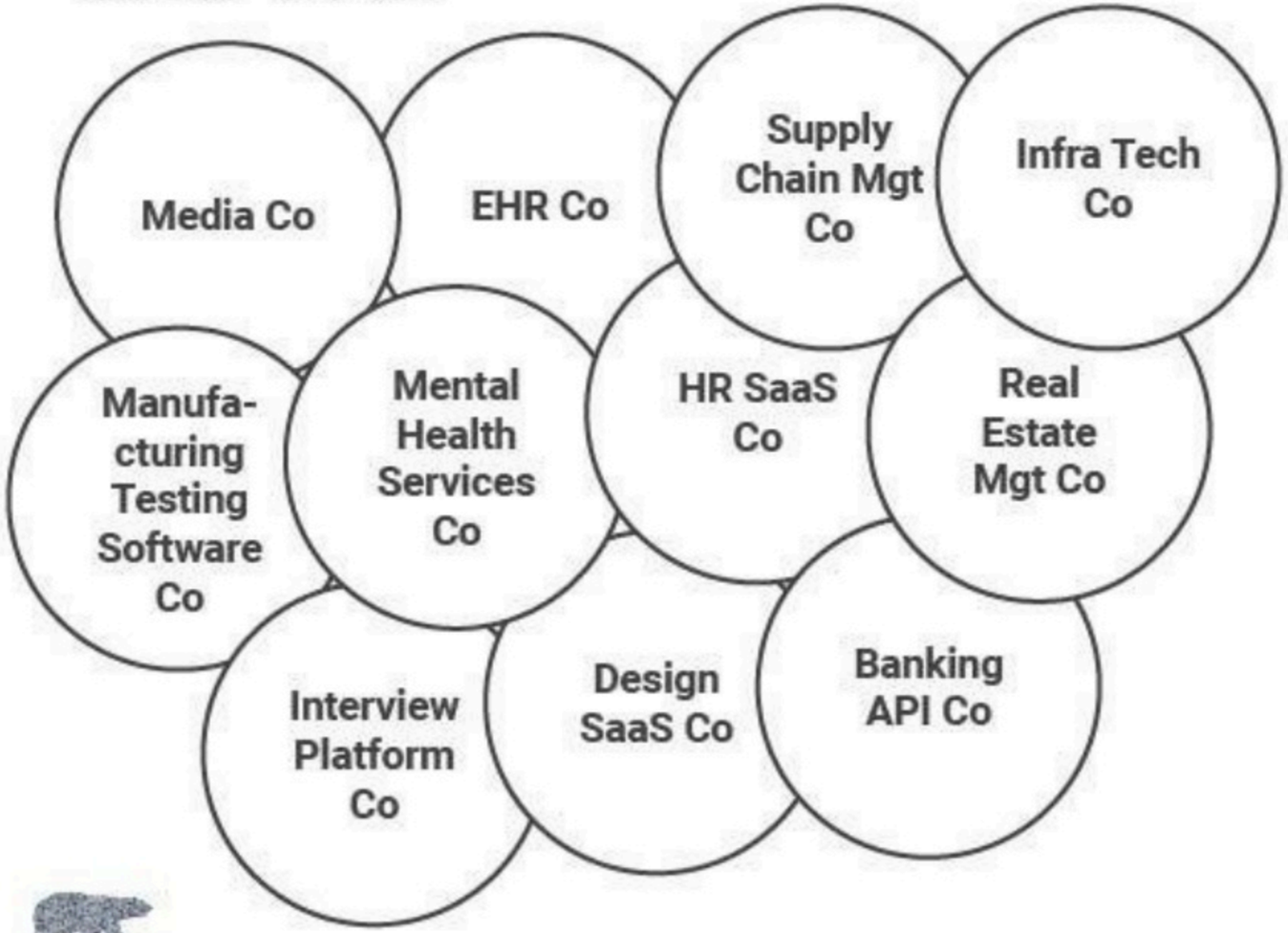
Active Directory

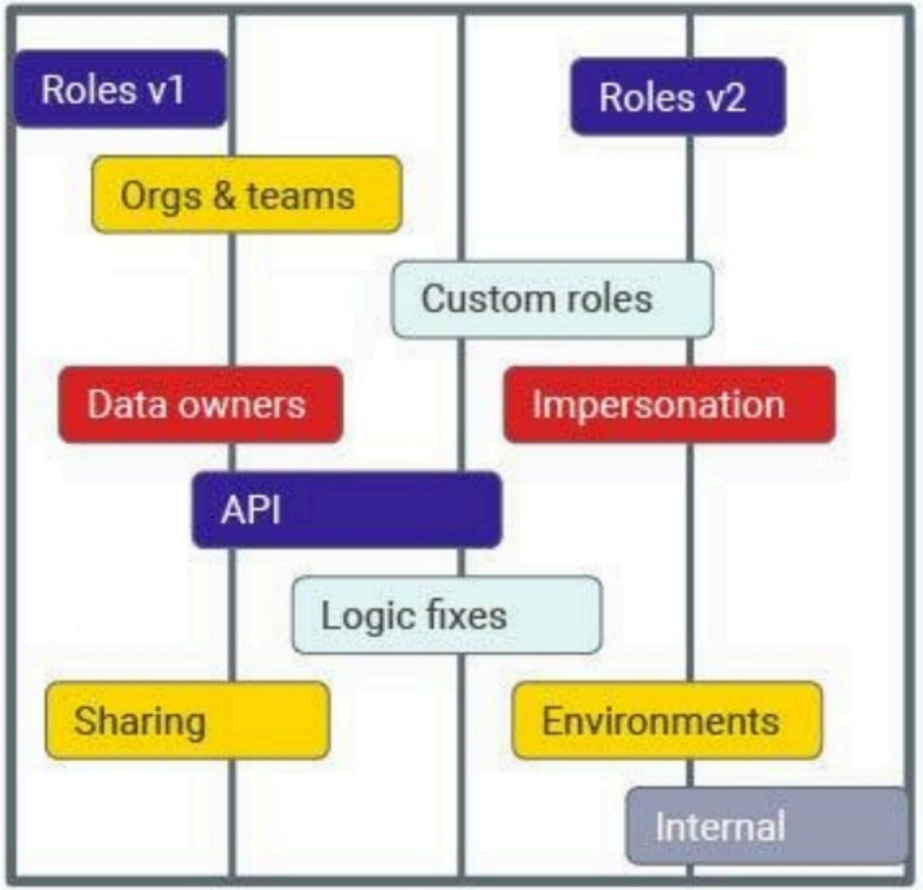
Auth0, Okta, et al



Open Source
(e.g., Pundit)

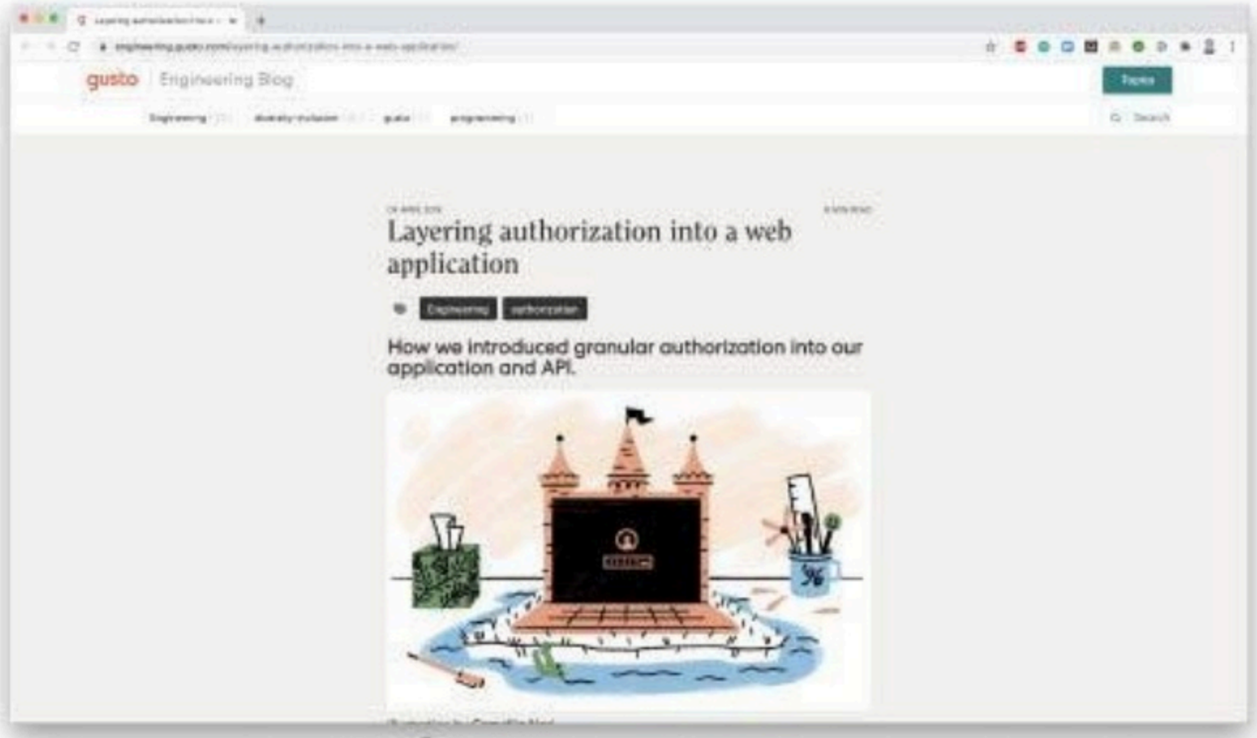
Dev teams repeat this undifferentiated work over and over





oso

Then hit a wall and do a big refactor



gusto

"This is a journey that I expect **many software engineering teams** embark on. My team worked on this project for about **10 months**"

oso

Oso fastracks authorization for developers

What is Oso?

Why anything?

- Delegate to experts
- Write less authZ code
- Focus on core product

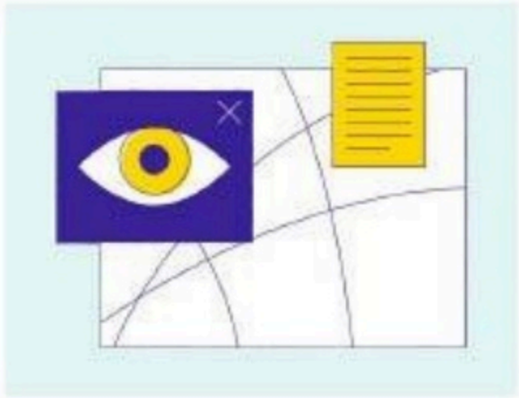
```
# Example VC policy
allow(you: VC, "catch_up", oso: Company) if
      "developer tools" in you.interests and
       you.desired_outcome >= $1,000,000,000;
```

Why Oso?

- Single place for authorization
- Like writing natural language
- Deploy library in seconds

The security company that prioritizes developer experience

Single place for authorization



Embedded policy engine that can reach into application

Like writing natural language

Best of prolog and web 100+ iterations

Deploy library in seconds

Cross-platform, cross-language built on Rust core

oso

Ability to address both greenfield and brownfield

Greenfield

- <Redacted>
  - 1st use case: core authorization engine
- <Redacted>
  - 1st use case: basic RBAC
  - Next use case: GraphQL

Brownfield

- <Redacted>
  - 1st use case: export control
  - Next use cases: RBAC migration, IoT, GraphQL
- <Redacted>
  - 1st use case: invoice authorization
  - Next use cases: core RBAC migration, per-customer policies
- <Redacted>
  - 1st use case: v3 RBAC, internal CSM app
  - Next use cases: v1 & v2 migration

Strong signs of engagement after 14 weeks and ~no marketing investment

"We love Oso because it lets us manage the chaos of access across our models, endpoints and users. We got up to speed and into production with **1 engineer in 3 weeks**, and we're planning to expand to **more use cases** already."

- Karan Talati, CEO at First Resonance

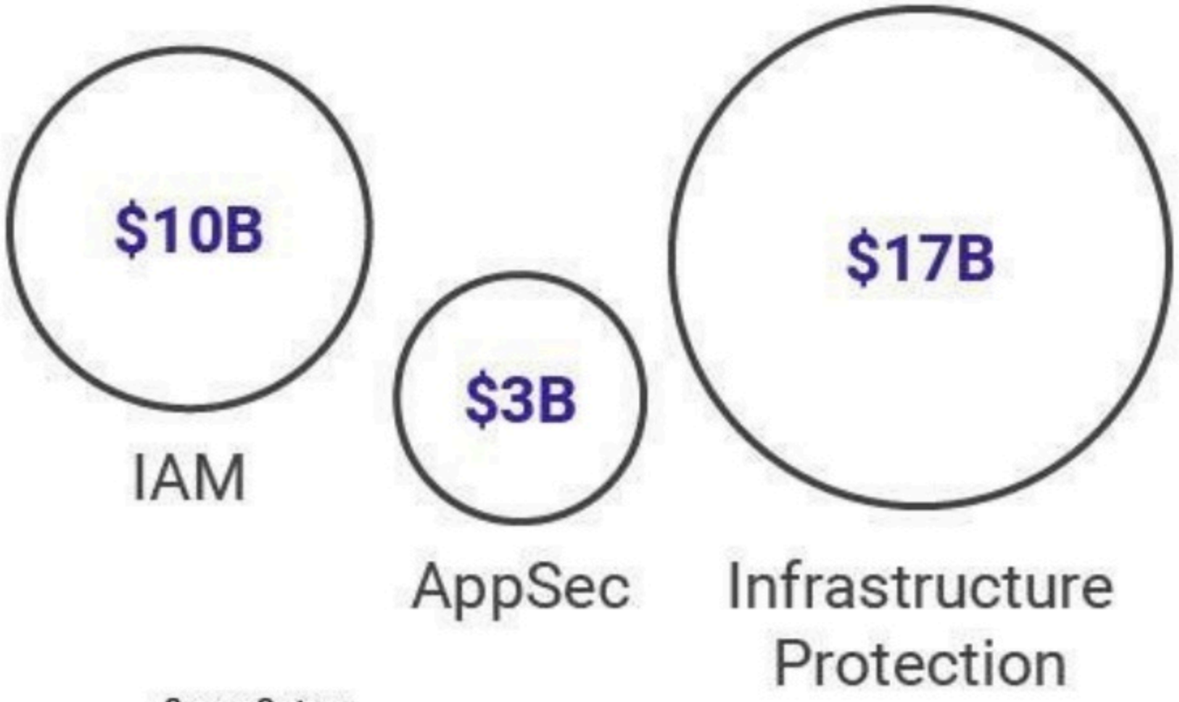
"Oso is awesome. It has made it much easier for us to represent crazy logic in our EHR application and to add new features. It **sped up our authZ roadmap 4x.**"

- Gaurub Pandey, CTO Dhi

Multi-billion dollar opportunity

Related Markets

6% growth/yr



Source: Gartner

App Authorization - 1 Project Spend

gusto $1M

$1.2M
Financial Planning SaaS Co

$1.8M
Endpoint Security Co

$1.8M
Infra Tech Co

oso