The REST Ascendancy

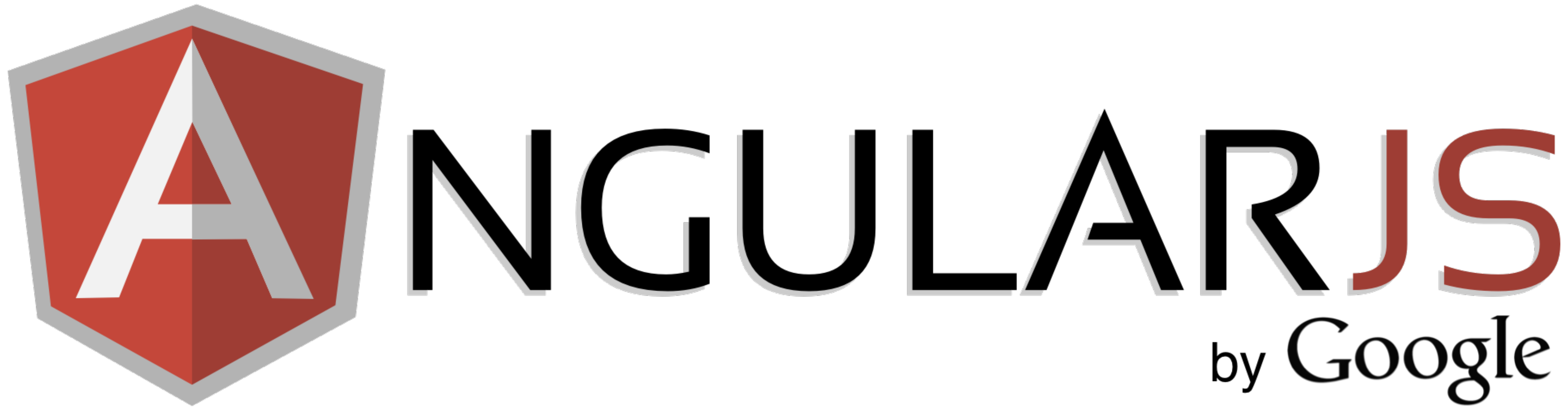
OUTLINE

1. WHY REST
2. BEST OF THE REST
3. PAIN POINTS
4. THE FUTURE

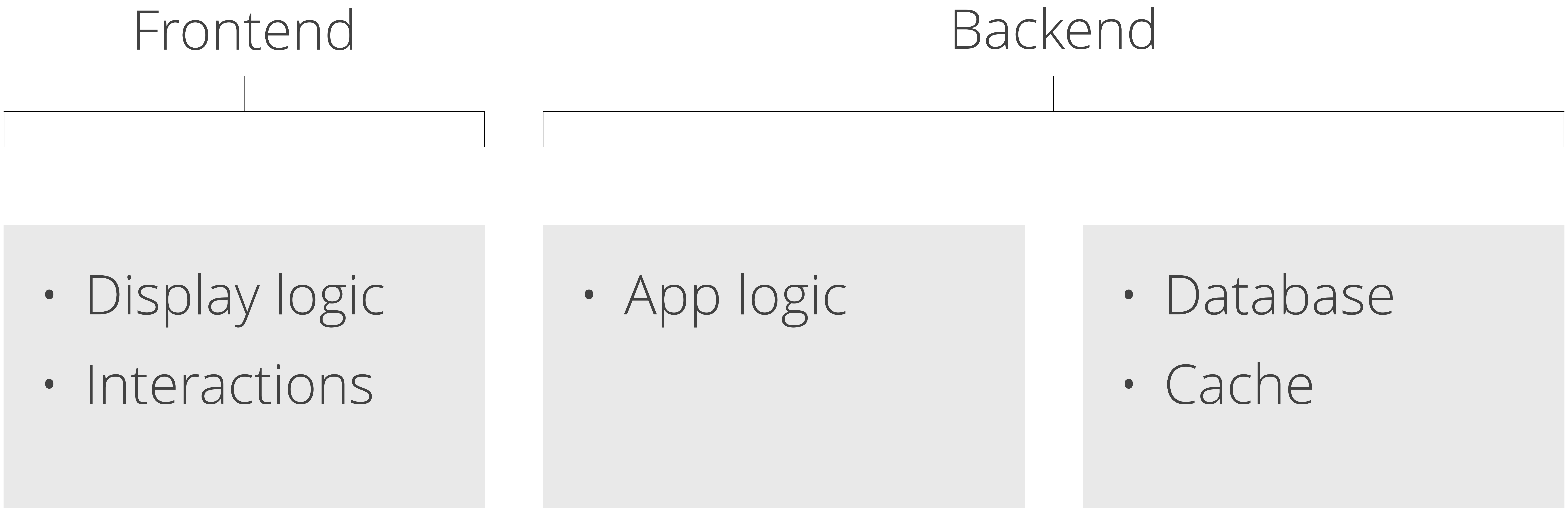
1. WHY REST

2. STATE OF REST
3. PAIN POINTS
4. THE FUTURE

The REST Ascendancy



BACKBONE.JS



Frontend

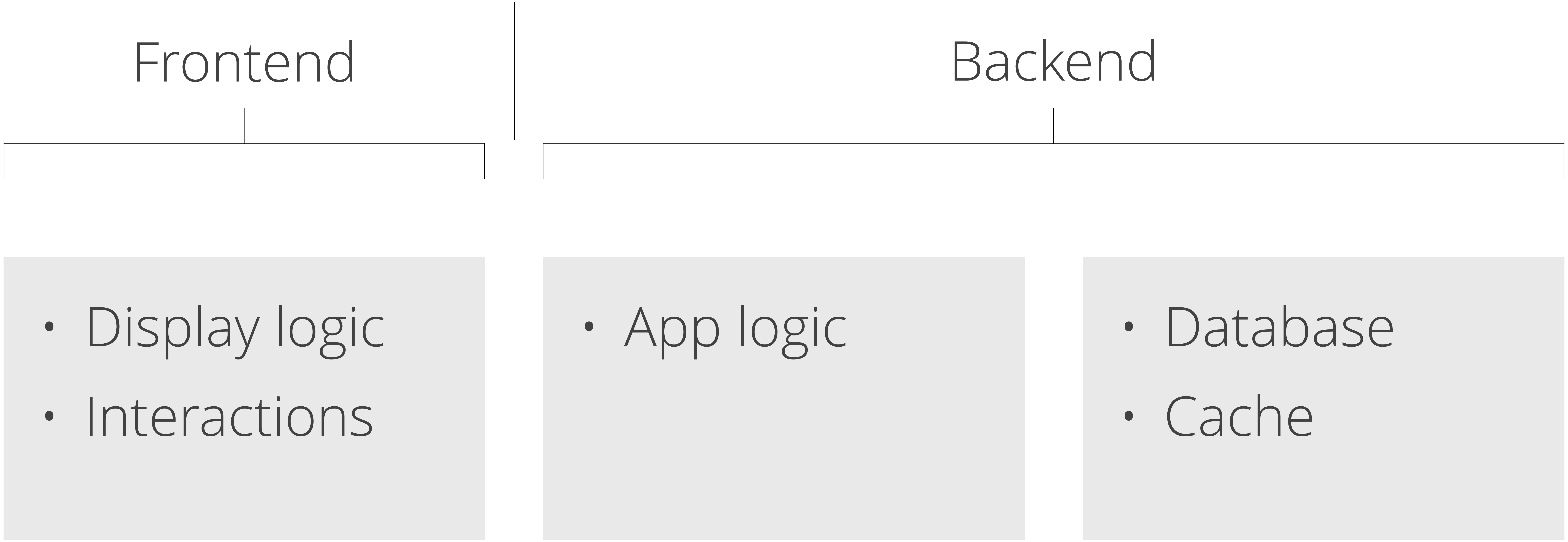
Backend

- Display logic
- Interactions

- App logic

- Database
- Cache

HTML!



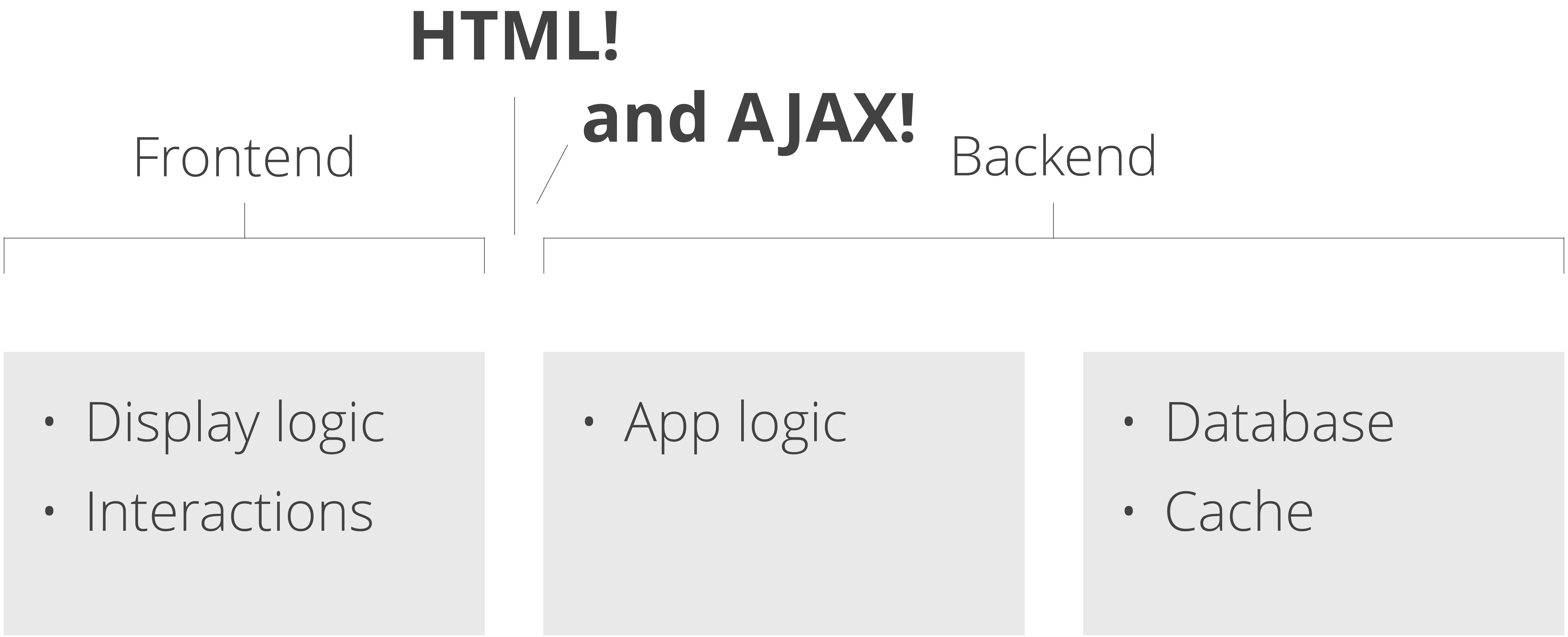
Frontend

- Display logic
- Interactions

Backend

- App logic

- Database
- Cache



HTML!

and AJAX!

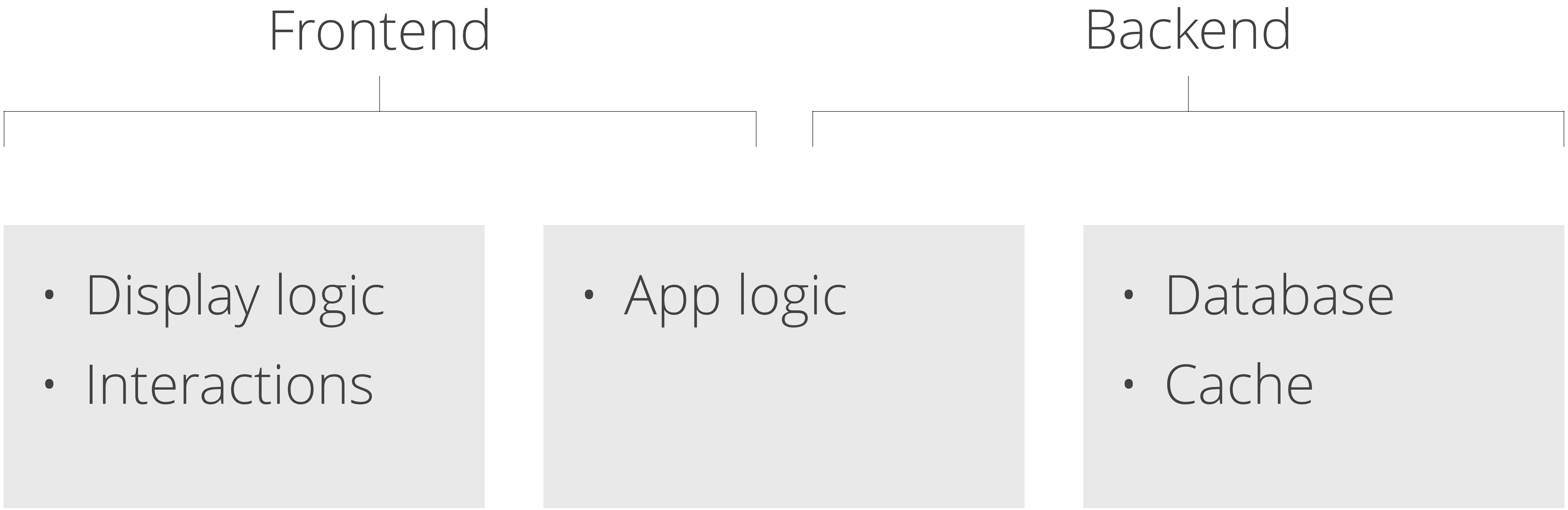
Frontend

Backend

- Display logic
- Interactions

- App logic

- Database
- Cache



Frontend

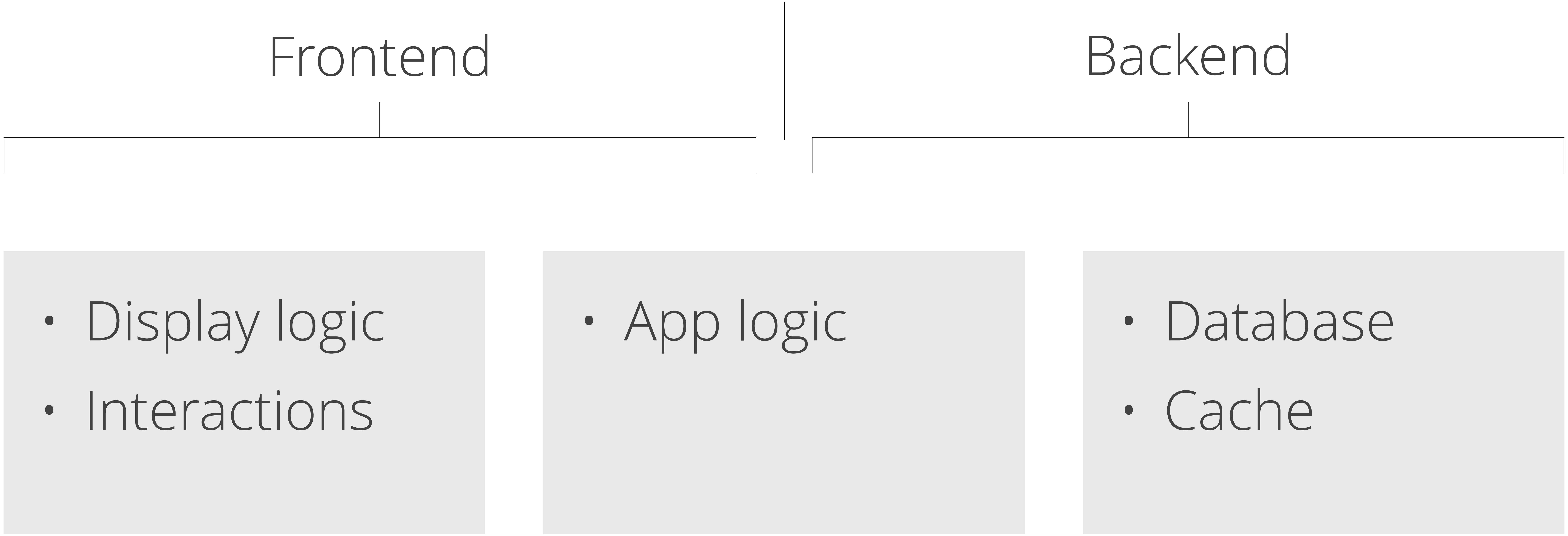
Backend

- Display logic
- Interactions

- App logic

- Database
- Cache

Representational State Transfer!



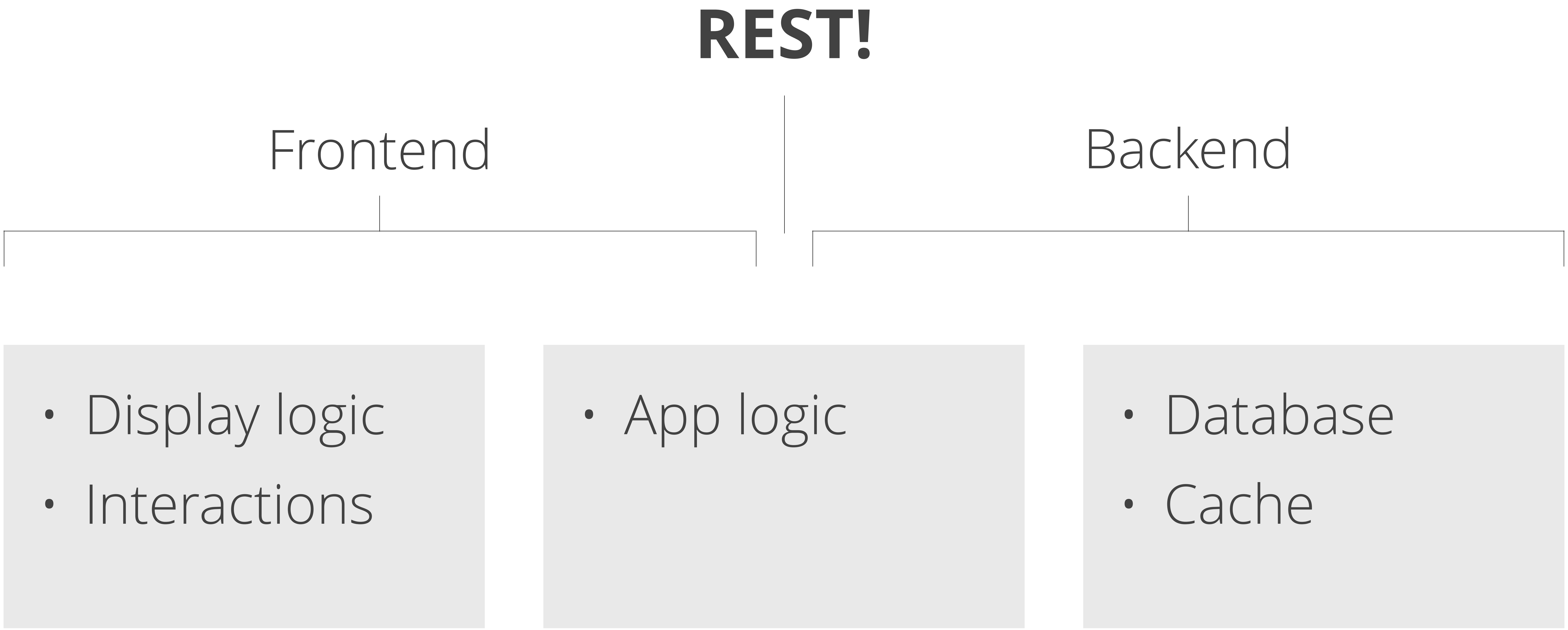
Frontend

Backend

- Display logic
- Interactions

- App logic

- Database
- Cache



REST!

Frontend

Backend

- Display logic
- Interactions

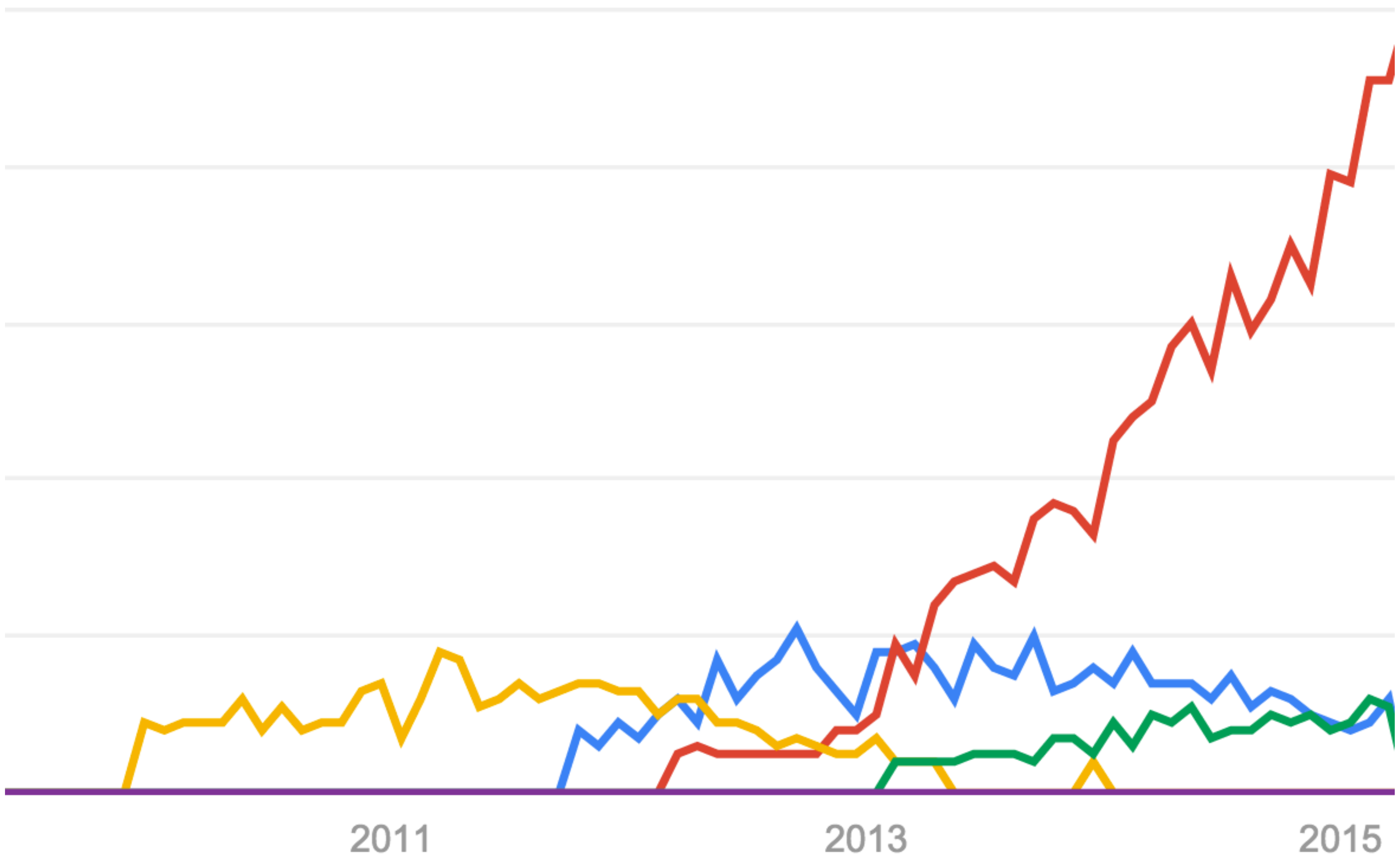
- App logic

- Database
- Cache

1. WHY REST

2. STATE OF REST

3. PAIN POINTS
4. THE FUTURE



Django REST Framework
172,000 downloads

Flask RESTful
60,000 downloads

Django Tastypie
37,000 downloads

Pyramid Cornice
12,000 downloads

Django Piston
4,000 downloads

SERIALIZERS

```
class CatSerializer(serializers.ModelSerializer):

    class Meta:
        model = Cat
        fields = ['id', 'age', 'hair', 'grumpiness',]
```

VIEWS

```
class CatViewSet(viewsets.ModelViewSet):

    queryset = Cat.objects.all()
    serializer_class = CatSerializer
```

PERMISSIONS

```
class OwnerOrReadOnlyPermission(permissions.BasePermission):

   def has_object_permission(self, request, view, obj):
        if request.method in permissions.SAFE_METHODS:
            return True
        return obj.owner == request.user
```

1. WHY REST
2. STATE OF REST

3. PAIN POINTS

4. THE FUTURE

WHO’S THE CONSUMER?

Your API

WHO’S THE CONSUMER?

Developers

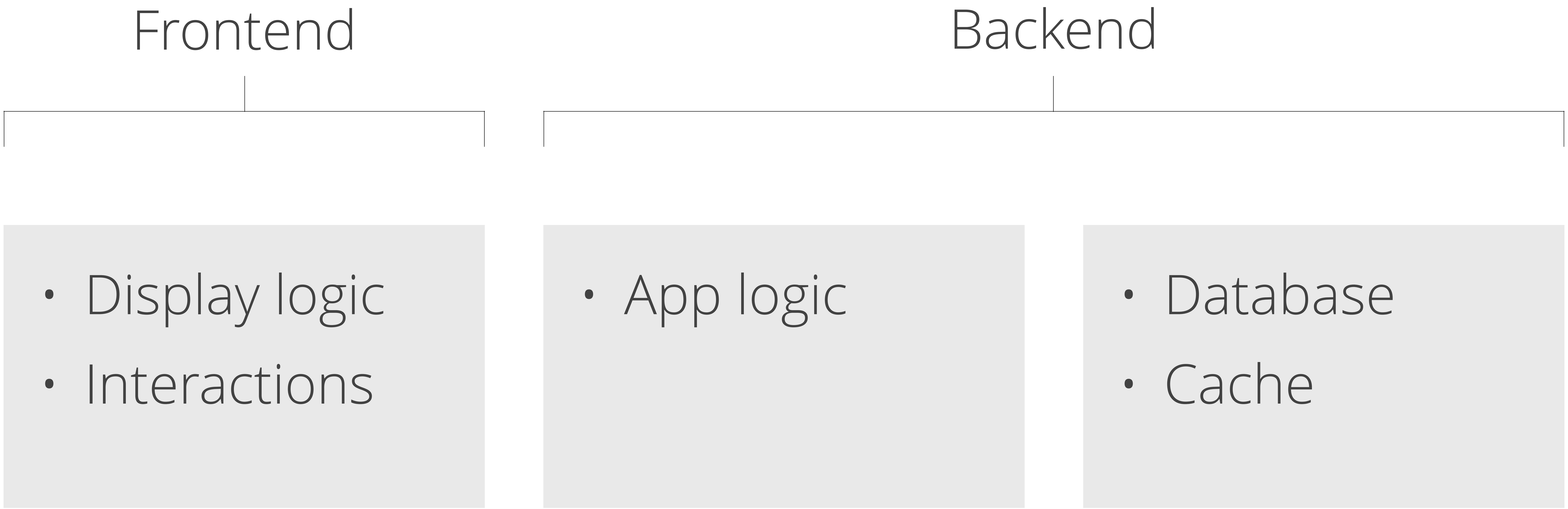
Your API

WHO’S THE CONSUMER?

Developers

Your App

Your API



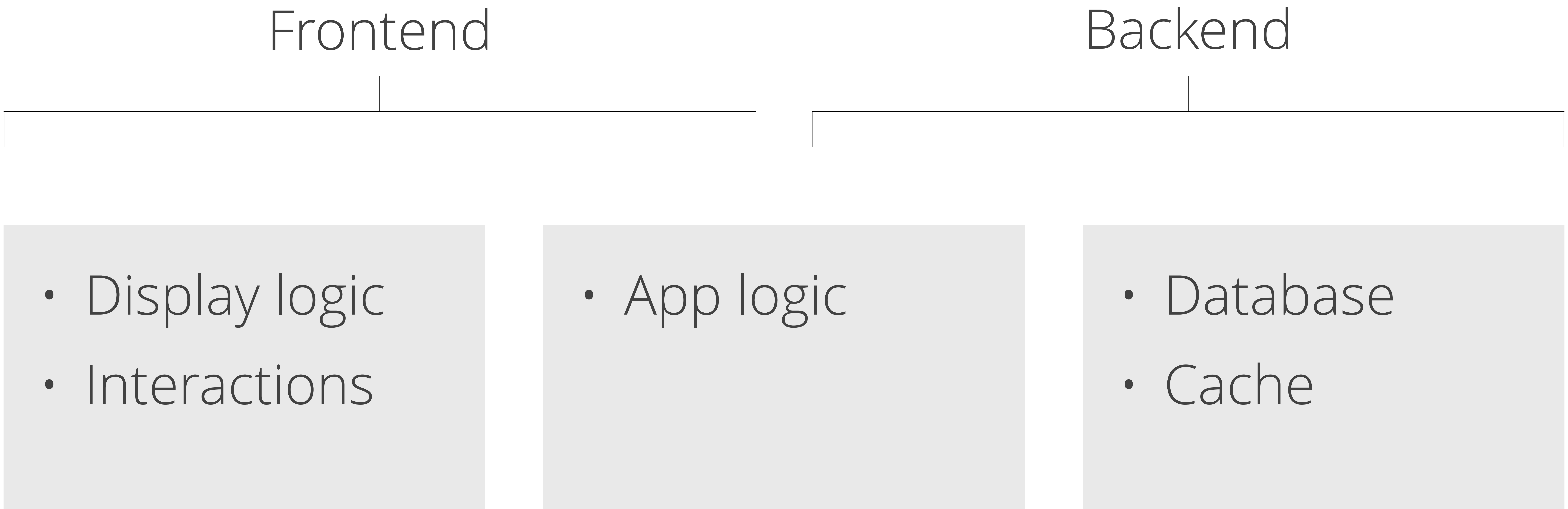
Frontend

Backend

- Display logic
- Interactions

- App logic

- Database
- Cache



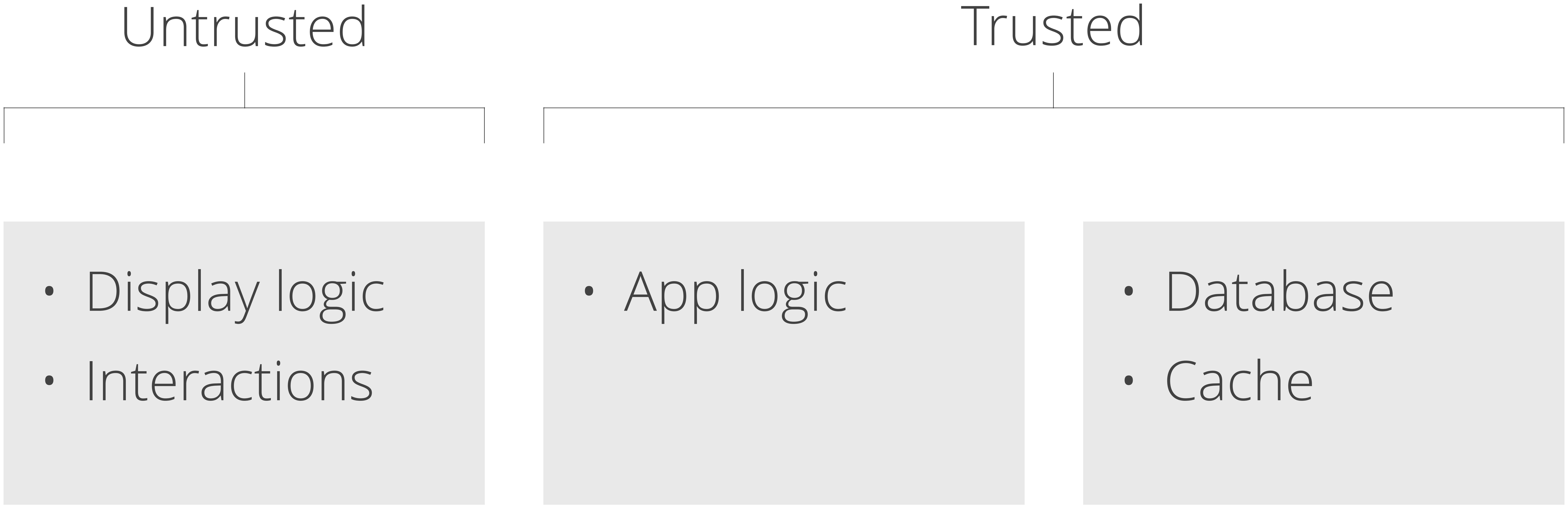
Frontend

Backend

- Display logic
- Interactions

- App logic

- Database
- Cache



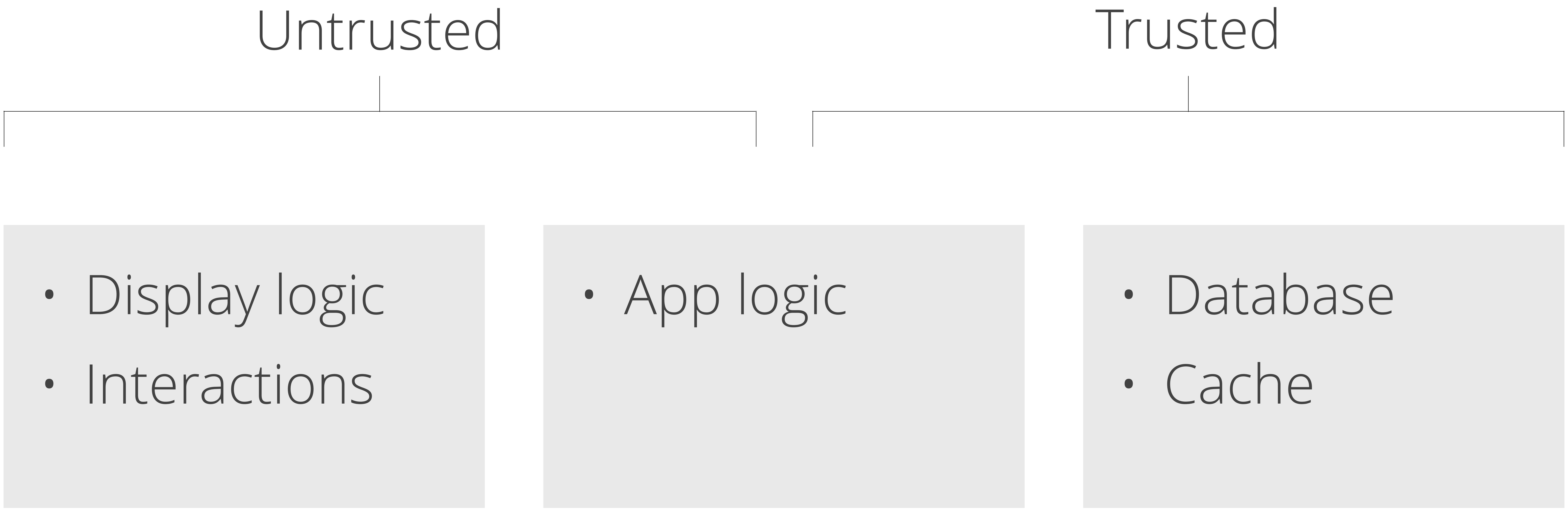
Untrusted

- Display logic
- Interactions

Trusted

- App logic

- Database
- Cache



Untrusted

Trusted

- Display logic
- Interactions

- App logic

- Database
- Cache

AUTHENTICATION

AUTHENTICATION

```
'rest_framework.authentication.SessionAuthentication'
```

- Session auth

AUTHENTICATION

```
example.com/api/products/?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIDIiLCJhZG1pbiI6dHJ1ZX0.wUJs5ArG9bewMeW3mZONhhAGs877ZWJWZlMHlROTyKU
```

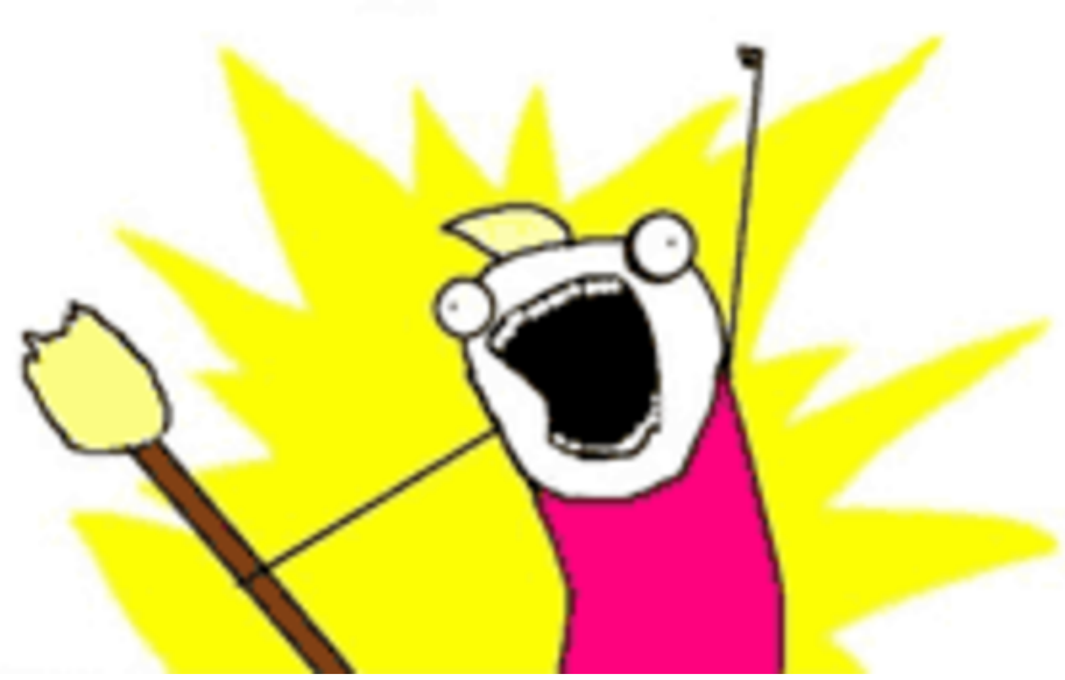
- Session auth
- Token auth

AUTHENTICATION

```
example.com/api/products/?
sign=svf668fe0d-a2ab-4855-bb65-baf210b1e64c:bZyPId_-Qmi5B-
YUkifs5FLEqqI
```

- Session auth
- Token auth
- Signed auth

AUTHENTICATION



- Session auth
- Token auth
- Signed auth
- All the things!

PERMISSIONS

PERMISSIONS

- Table-level permissions

PERMISSIONS

- Table-level permissions
- Column-level permissions

PERMISSIONS

- Table-level permissions
- Column-level permissions
- Row-level permissions

PERMISSIONS

- Table-level permissions
- Column-level permissions
- Row-level permissions
- Read vs write permissions

PERMISSIONS

- Table-level permissions
- Column-level permissions
- Row-level permissions
- Read vs write permissions
- Multiple simultaneous auth methods

PERMISSIONS

- Table-level permissions
- Column-level permissions
- Row-level permissions
- Read vs write permissions
- Multiple simultaneous auth methods
- All the things!

REAL EXAMPLE

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    queryset = Order.objects.all()
    permission_classes = [
        Or(
            And(IsOrganizationMember, IsReadOnly),
            And(IsOrganizationAdmin, patch_fields_factory()),
            IsVendorAdmin,
            And(SignedObjectActionPermission, IsReadOnly),
            IsAdminUser,
        )
    ]
    ...
```

REAL EXAMPLE

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    ...
    def get_queryset(self):
        queryset = super(OrderViewSet, self).get_queryset()
        if self.request.user.is_authenticated():
            if self.request.user.is_staff:
                return self.queryset
            return self.queryset.filter(
                Q(organization__accounts=self.request.user) |
                Q(vendor__accounts=self.request.user),
                is_visible=True,
            ).distinct()
       return queryset.none()
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    ...
    def get_queryset(self):
        queryset = super(OrderViewSet, self).get_queryset()
        if self.request.user.is_authenticated():
            if self.request.user.is_staff:
                return self.queryset
            return self.queryset.filter(
                Q(organization__accounts=self.request.user) |
                Q(vendor__accounts=self.request.user),
                is_visible=True,
            ).distinct()
       return queryset.none()
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    ...
    def get_queryset(self):
        queryset = super(OrderViewSet, self).get_queryset()
        if self.request.user.is_authenticated():
            if self.request.user.is_staff:
                return self.queryset
            return self.queryset.filter(
                Q(organization__accounts=self.request.user) |
                Q(vendor__accounts=self.request.user),
                is_visible=True,
            ).distinct()
       return queryset.none()
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    ...
    def get_queryset(self):
        queryset = super(OrderViewSet, self).get_queryset()
        if self.request.user.is_authenticated():
            if self.request.user.is_staff:
                return self.queryset
            return self.queryset.filter(
                Q(organization__accounts=self.request.user) |
                Q(vendor__accounts=self.request.user),
                is_visible=True,
            ).distinct()
       return queryset.none()
```

REAL EXAMPLE

```
class OrderViewSet(SignViewSetMixin, viewsets.ModelViewSet):
    ...
    def get_queryset(self):
        queryset = super(OrderViewSet, self).get_queryset()
        if self.request.user.is_authenticated():
            if self.request.user.is_staff:
                return self.queryset
            return self.queryset.filter(
                Q(organization__accounts=self.request.user) |
                Q(vendor__accounts=self.request.user),
                is_visible=True,
            ).distinct()
        return queryset.none()
```

REAL EXAMPLE — LIBRARIES

- Django REST Framework

REAL EXAMPLE — LIBRARIES

- Django REST Framework
- rest_condition (forked)

REAL EXAMPLE — LIBRARIES

- Django REST Framework
- rest_condition (forked)
- signed viewsets (in-house)

REAL EXAMPLE — LIBRARIES

- Django REST Framework
- rest_condition (forked)
- signed viewsets (in-house)
- patch fields factory (in-house)

REAL EXAMPLE — CODE LOCATIONS

- ViewSet class mixin

REAL EXAMPLE — CODE LOCATIONS

- ViewSet class mixin
- ViewSet permissions list

REAL EXAMPLE — CODE LOCATIONS

- ViewSet class mixin
- ViewSet permissions list
- ViewSet get_queryset method

REAL EXAMPLE — CODE LOCATIONS

- ViewSet class mixin
- ViewSet permissions list
- ViewSet get_queryset method
- Serializer fields (not depicted)

REAL EXAMPLE — CODE LOCATIONS

- ViewSet class mixin
- ViewSet permissions list
- ViewSet get_queryset method
- Serializer fields (not depicted)
- Permission classes (not depicted)

1. WHY REST
2. STATE OF REST
3. PAIN POINTS

4. THE FUTURE

EMBETTERMENT

- Better tokens and signed URLs

EMBETTERMENT

- Better tokens and signed URLs
- Combined list/object permissions

EMBETTERMENT

- Better tokens and signed URLs
- Combined list/object permissions
- Permission organization

chewse

Jeff Schenck CTO & Co-Founder

twitter **@jeffschenck**
email **jeff@chewse.com**