ALL DAY DEVOPS

NOVEMBER 6, 2019

Lukasz Radosz CPO @Cloudentity

DevSecOps Enabled Micro-Perimeter API Protection

ADDO
ALL DAY DEVOPS

DevSecOps Enabled Micro-Perimeter API Protection

How to apply declarative configuration model for API Authorization, story about people, processes and tools...

System Owner	Date	Citation
Brazil Fed of Indus - ElasticSearch API exposed	11/23/18	https://www.zdnet.com/article/brazils-largest-professional-association-suffers-massive-data-leak/
Urban Massage - ElasticSearch API exposed	11/27/18	https://techcrunch.com/2018/11/27/urban-massage-data-exposed-customers-creepy-clients/
SKY Brasil - ElasticSearch API exposed	11/29/18	https://www.zdnet.com/article/sky-brasil-exposes-data-of-32-million-subscribers/
Atrium Health - ElasticSearch API exposed	11/29/18	https://www.securityinfowatch.com/healthcare/news/12438109/personal-data-of-more-than-2m-patients-compromised-in-atrium-health-data-breach
Data&Leads	11/29/18	https://www.bankinfosecurity.com/blogs/data-leads-site-disappears-after-data-exposure-alert-p-2687
LandMark White Limited	2/13/19	https://www.computerworld.com.au/article/657662/landmark-white-blames-exposed-api-data-breach/ https://www.programmableweb.com/news/landmark-white-api-breach-may-have-exposed-loan-details-100000-users/brief/2019/02/13
JustDial Leak	4/17/19	https://thehackernews.com/2019/04/justdial-hacked-data-breach.html
GateHub Cryptocurrency Wallet Hack	6/6/19	https://gatehub.net/blog/gatehub-preliminary-statement/
Venmo transactions Leaked	6/16/19	https://techcrunch.com/2019/06/16/millions-venmo-transactions-scraped/

Big scary slide

By 2022 API abuses will be the attack vector most responsible for data breaches within enterprise Web applications. - Gartner

Over half of the OWASP Top Ten API Security vulnerabilities related authentication and authorization. – OWASP https://www.owasp.org/index.php/OWASP_API_Security_Project

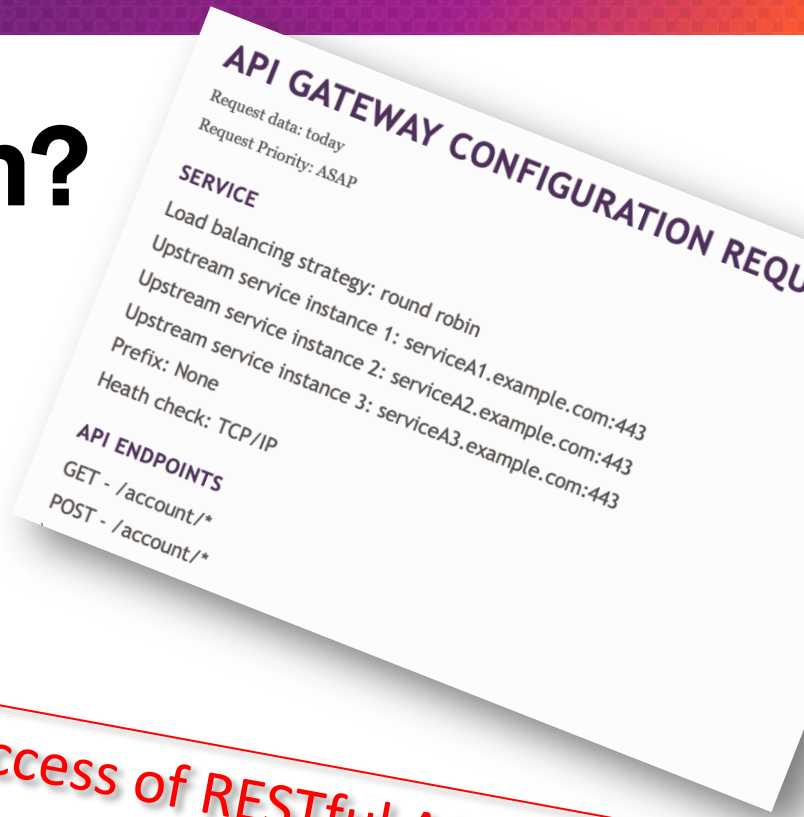
2/3rds of the companies are struggling with access control and authorization for the APIs. - Gartner

60% of the companies have insufficient API access controls in their production systems. - F5 Labs

3 patterns of API compromises: 1) large platforms with lots of third-party integrations, 2) mobile apps, 3) monolithic apps modernization process. During – F5 Labs

So why it's such a big problem?

- ❑Manual configurations
- ❑Complexity
- ❑Lack of tools
- ❑APIs Wild Wild West
- ❑Miscommunication between security and development team



Success of RESTful APIs is at fault here!

So how can we fix it?

Werner Vogels, AWS CTO 2017
AWS: ReInvent

"Security is all of our jobs now. It's no longer just the security team.

If you're doing continuous integration and continuous development, you have to make sure everyone is a security engineer"

To the rescue

Everyone Becoming A Security Engineer Is Not The Answer

Slowing the pace of developers will impact:

- ❑Business growth
- ❑Innovation
- ❑Technology adoption
- ❑Smaller Dev teams = Junior Devs with less oversight
- ❑And they will make more mistakes

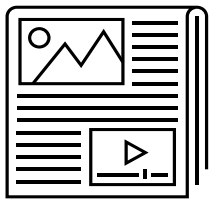
Guardrails instead of responsibility shift

Let’s start with people

Developers

Operations

Security & Governance



ADDO
ALL DAY DEVOPS

Security & Governance

Regulation

Corporate Policies

Risk Acceptability

Privacy & Consent

Audit and visibility

Operations

Load balancing, routing, service discovery

Application Level Authorization

Data/Object Level Authorization

Workloads and API publishing

Monitoring

Developers

Code

Configure

Test

Build

Release

Continue to process and methodologies

ADDO
ALL DAY DEVOPS

Security & Governance

- ✓ **Corporate global policies**
- ✓ **Policy Templates**
- ✓ **Best Practices**

- ✓ **Security peer review**

- ✓ **Generate API Security tests**

- ✓ Security testing
- ✓ **Access control testing**
- ✓ **Authorization testing**

- ✓ **Security and authorization configuration artifacts**

- ✓ **Security & authorization**

- ✓ **Monitor access, authorization, privacy**

Operations

- ✓ Infrastructure as code templates
- ✓ Networking as a code templates
- ✓ **API Publishing as a code templates**

- ✓ **Infrastructure peer review**

- ✓ **Generate API Infrastructure tests**

- ✓ Infrastructure testing
- ✓ Load testing
- ✓ **API Rate limiting testing**

- ✓ Infrastructure configuration artifacts

- ✓ Infrastructure & networking

- ✓ Monitor infrastructure

Developers

- ✓ Application Code
- ✓ **Authorization as a code**
- ✓ **API Publishing as a code**
- ✓ Infrastructure as a code

- ✓ Application artifacts
- ✓ **Configuration artifacts**

- ✓ Application testing
- ✓ Integration testing
- ✓ **API testing**

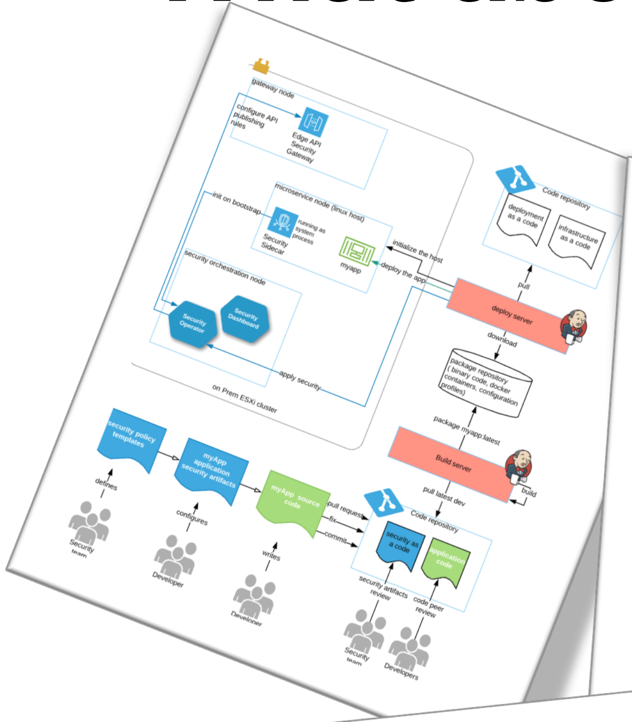
- ✓ Application artifacts

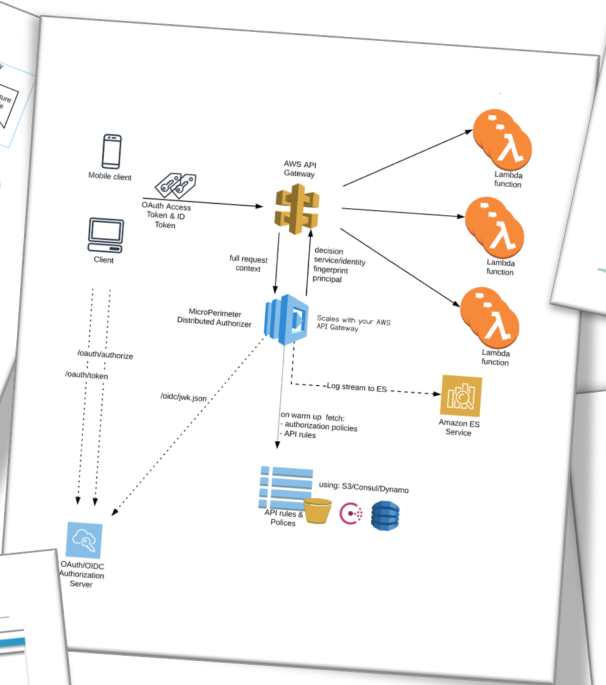
- ✓ Apps & services

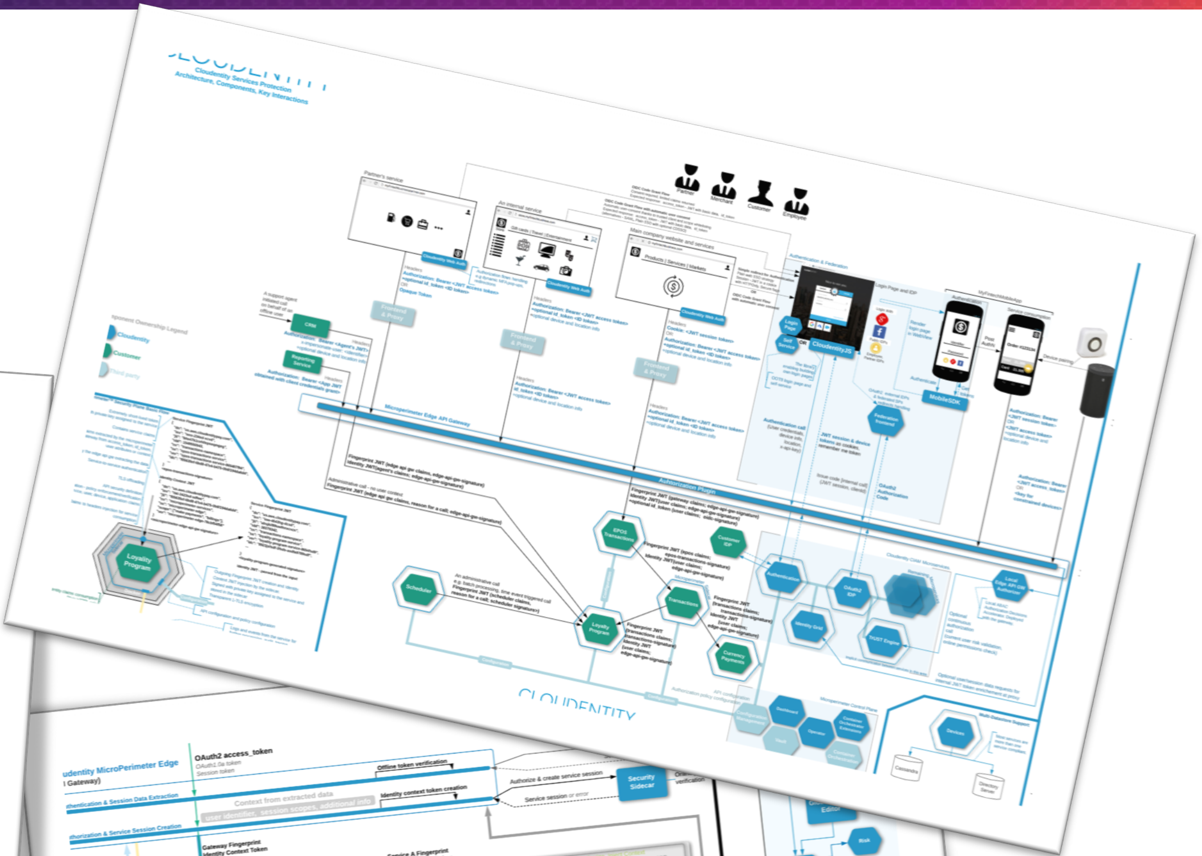
- ✓ Monitor application

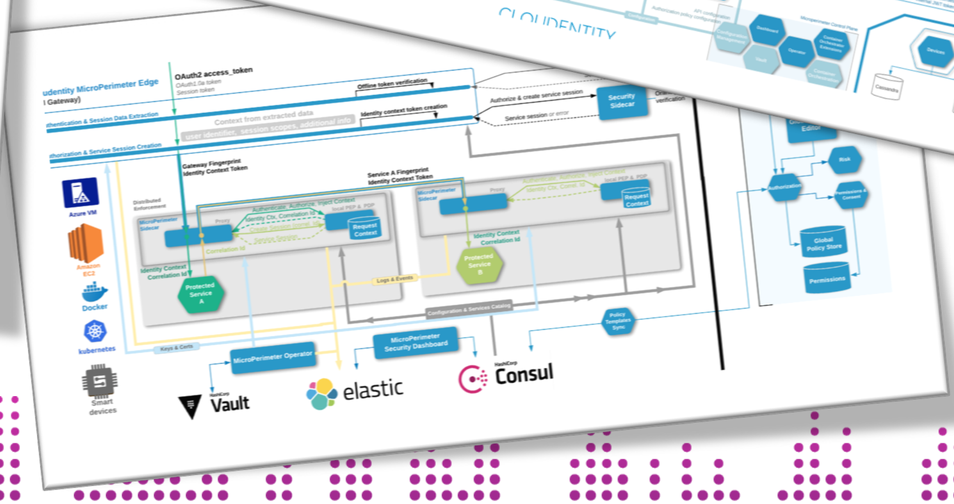
Plan | Code | Build | Test | Release | Deploy | Operate | Monitor

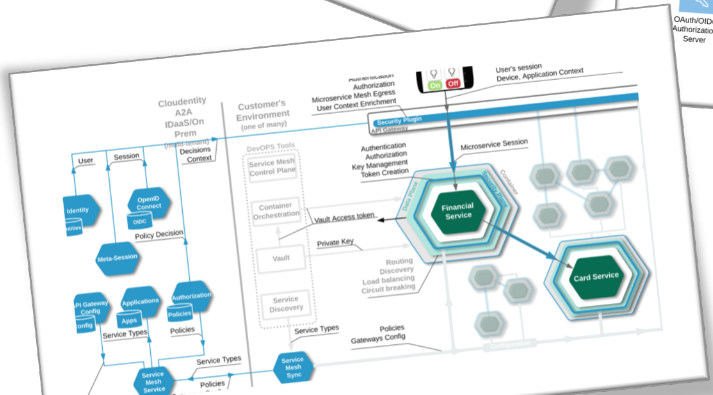
What about tools ?

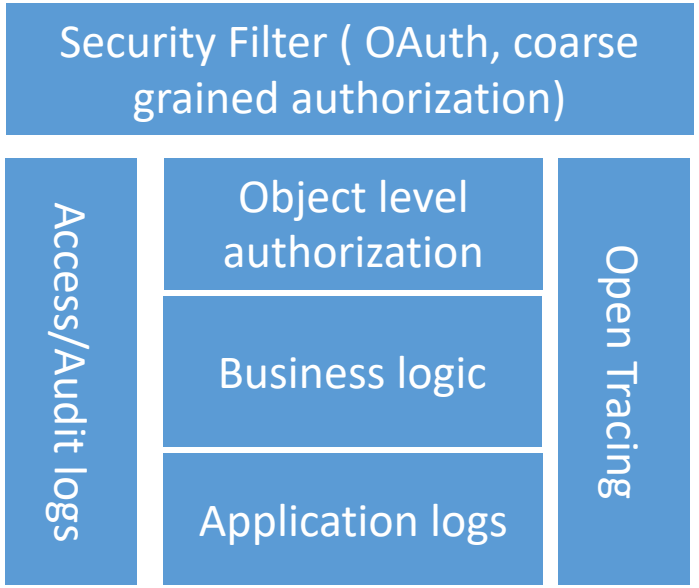










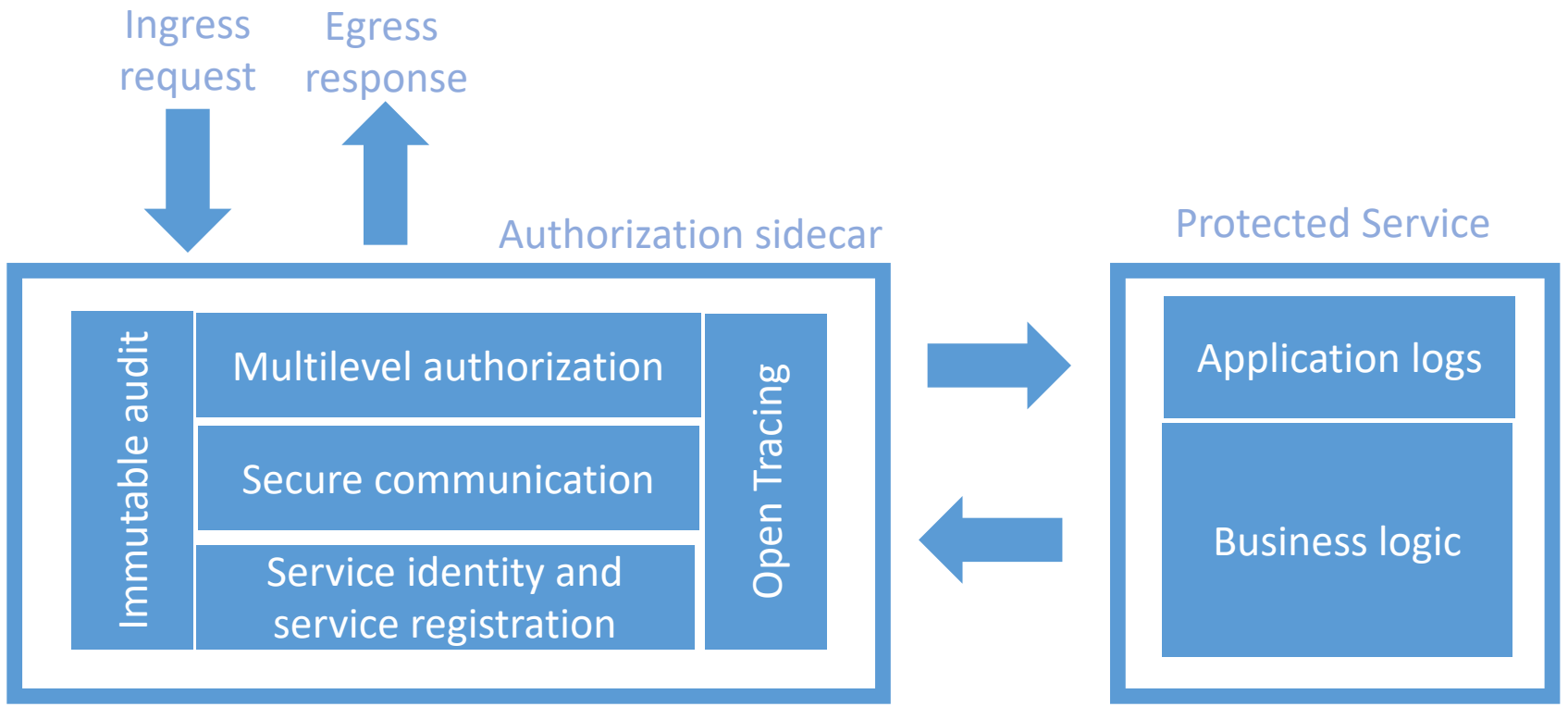


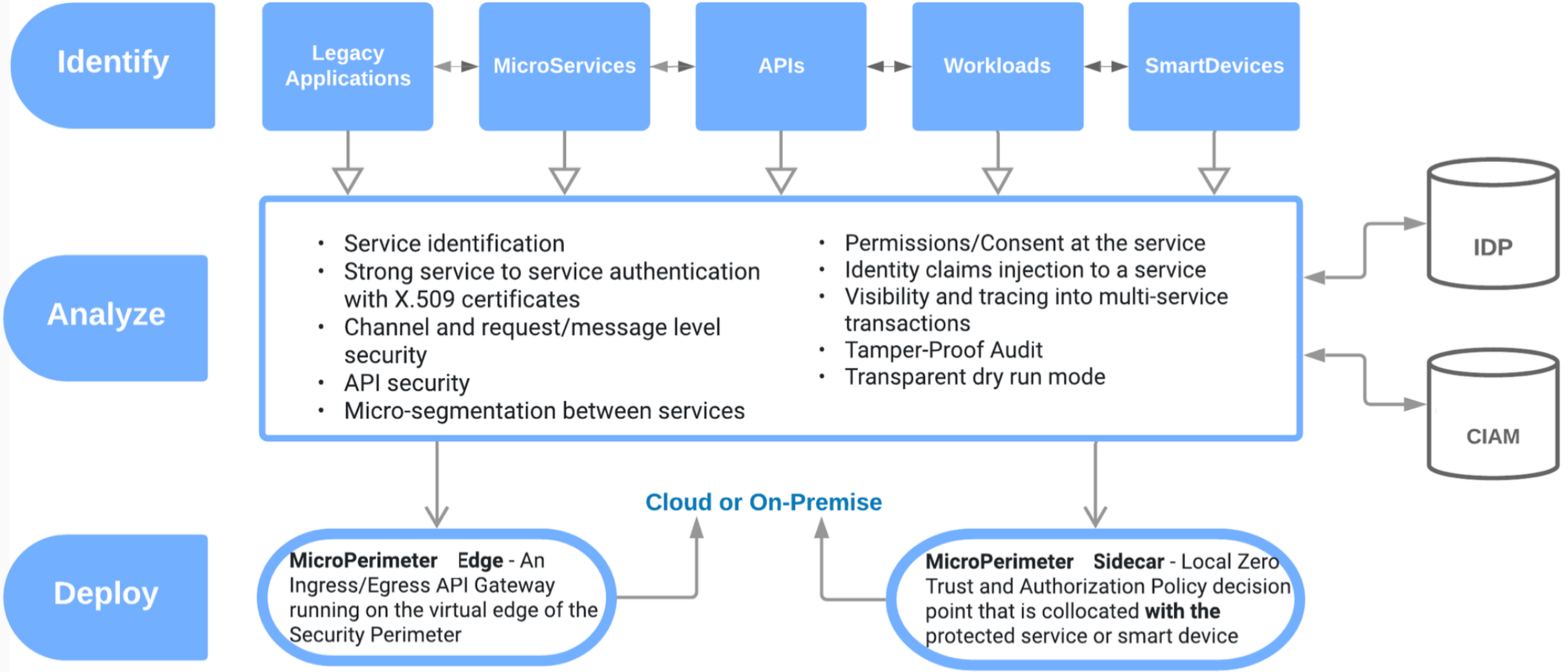
To secure each service one needs
(on top of a business function):

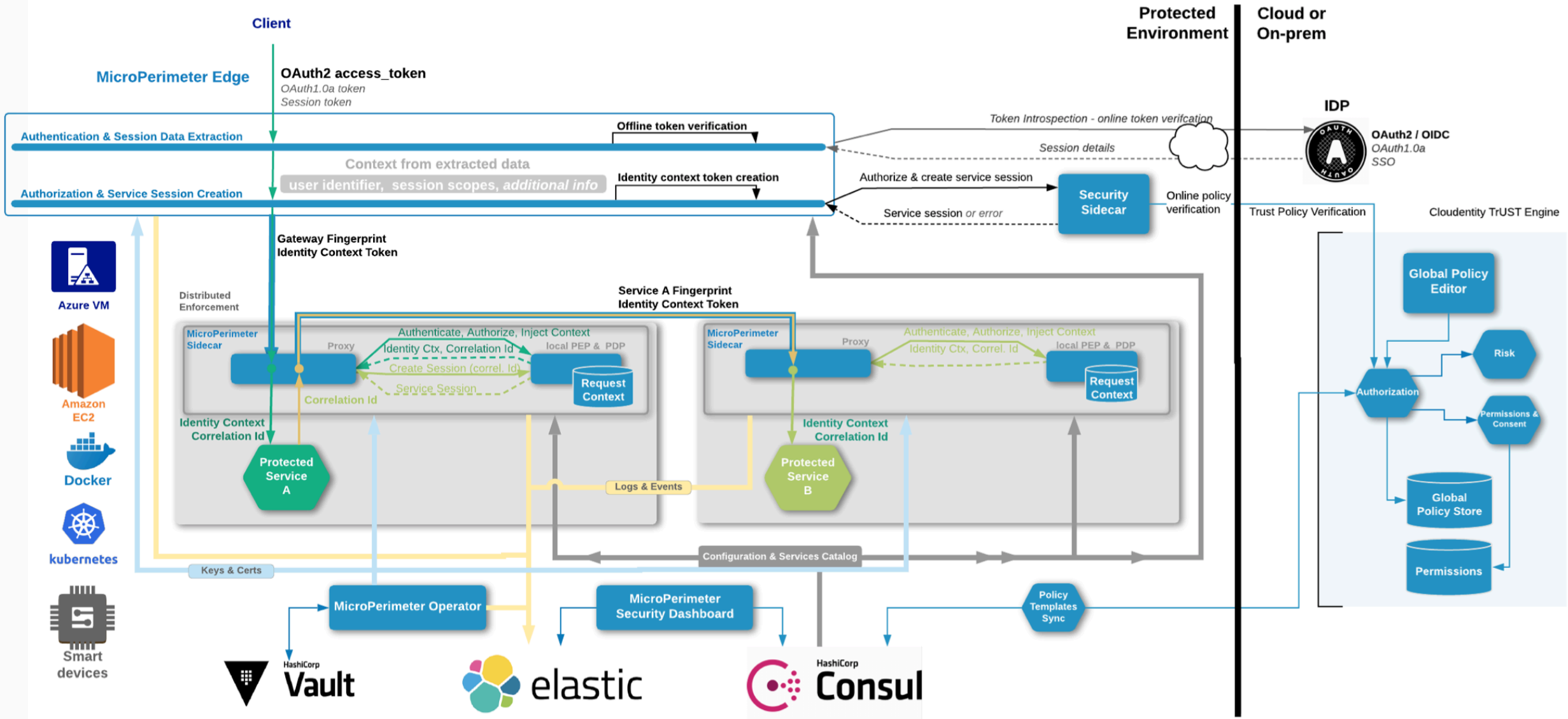
- ✓ Request authentication
- ✓ Request authorization
- ✓ Service registration and service identity
- ✓ API inspection
- ✓ Access/logs

Benefits of that approach

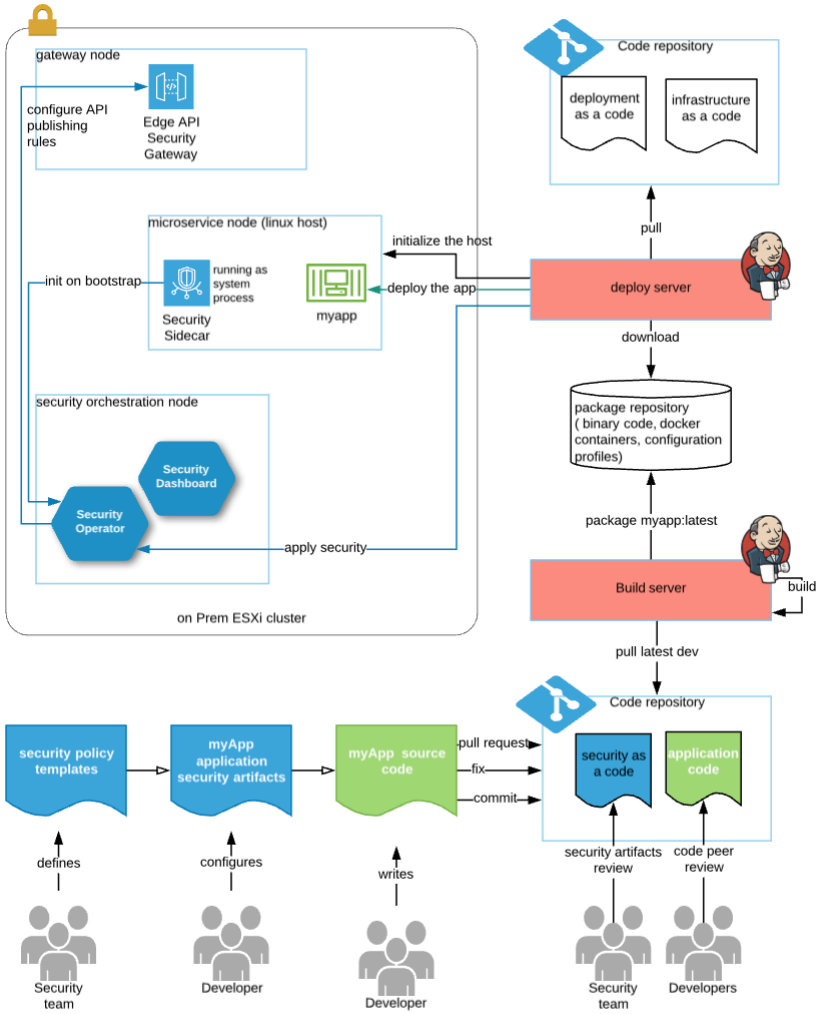
- ✓ Extensible APIs and Microservices
- ✓ Authorization as Code
- ✓ Code Reduction
- ✓ Security Guardrails




Identify
Legacy Applications
MicroServices
APIs
Workloads
SmartDevices
Analyze
Service identification
Strong service to service authentication with X.509 certificates
Channel and request/message level security
API security
Micro-segmentation between services
Permissions/Consent at the service
Identity claims injection to a service
Visibility and tracing into multi-service transactions
Tamper-Proof Audit
Transparent dry run mode
IDP
CIAM
Cloud or On-Premise
Deploy
MicroPerimeter Edge - An Ingress/Egress API Gateway running on the virtual edge of the Security Perimeter
MicroPerimeter Sidecar - Local Zero Trust and Authorization Policy decision point that is collocated with the protected service or smart device

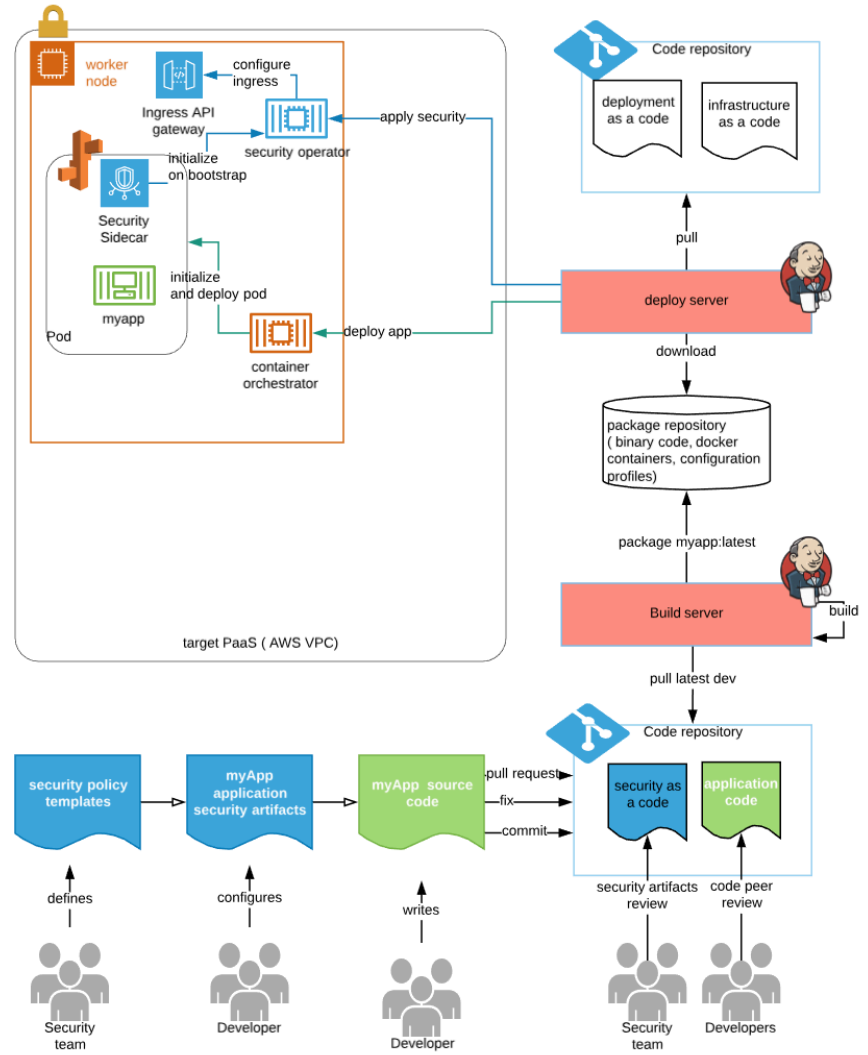

Client
MicroPerimeter Edge
OAuth2 access_token
OAuth1.0a token
Session token
Protected Environment
Cloud or On-prem
IDP
OAuth2 / OIDC
OAuth1.0a
SSO
Token Introspection - online token verifcation
Session details
Authentication & Session Data Extraction
Offline token verification
Context from extracted data
user identifier, session scopes, additional info
Identity context token creation
Authorization & Service Session Creation
Authorize & create service session
Service session or error
Security Sidecar
Online policy verification
Trust Policy Verification
Cloudentity TrUST Engine
Gateway Fingerprint
Identity Context Token
Service A Fingerprint
Identity Context Token
Distributed Enforcement
MicroPerimeter Sidecar
Proxy
Authenticate, Authorize, Inject Context
Identity Ctx, Correlation Id
local PEP & PDP
Create Session (correl. Id)
Service Session
Request Context
Correlation Id
Identity Context Correlation Id
Protected Service A
Protected Service B
Logs & Events
Configuration & Services Catalog
Keys & Certs
Azure VM
Amazon EC2
Docker
kubernetes
Smart devices
MicroPerimeter Operator
MicroPerimeter Security Dashboard
Policy Templates Sync
HashiCorp Vault
elastic
HashiCorp Consul
Global Policy Editor
Risk
Authorization
Permissions & Consent
Global Policy Store
Permissions

Traditional architecture



Not all of us are cloud native!

Microservices based architecture

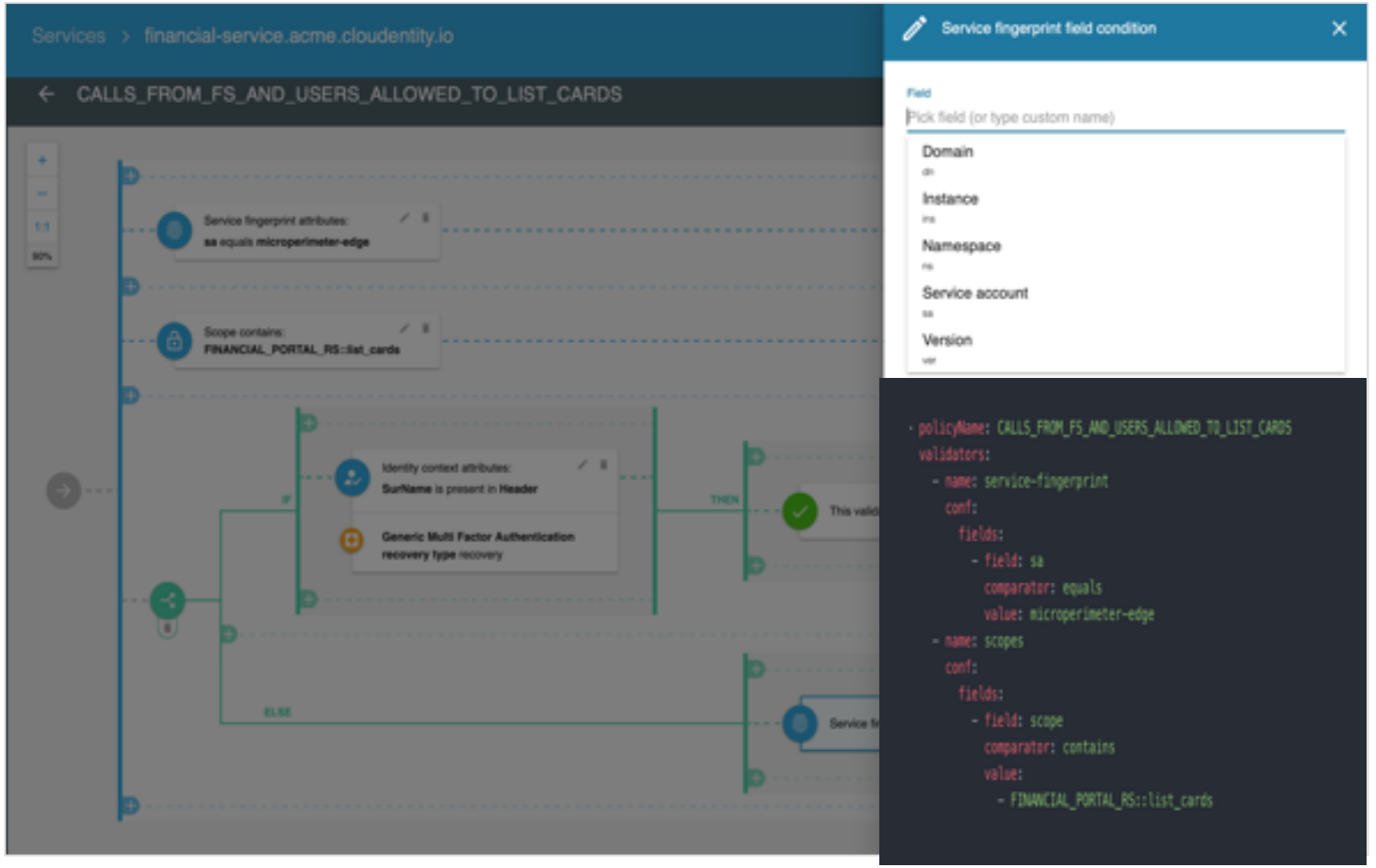


Policies as Code

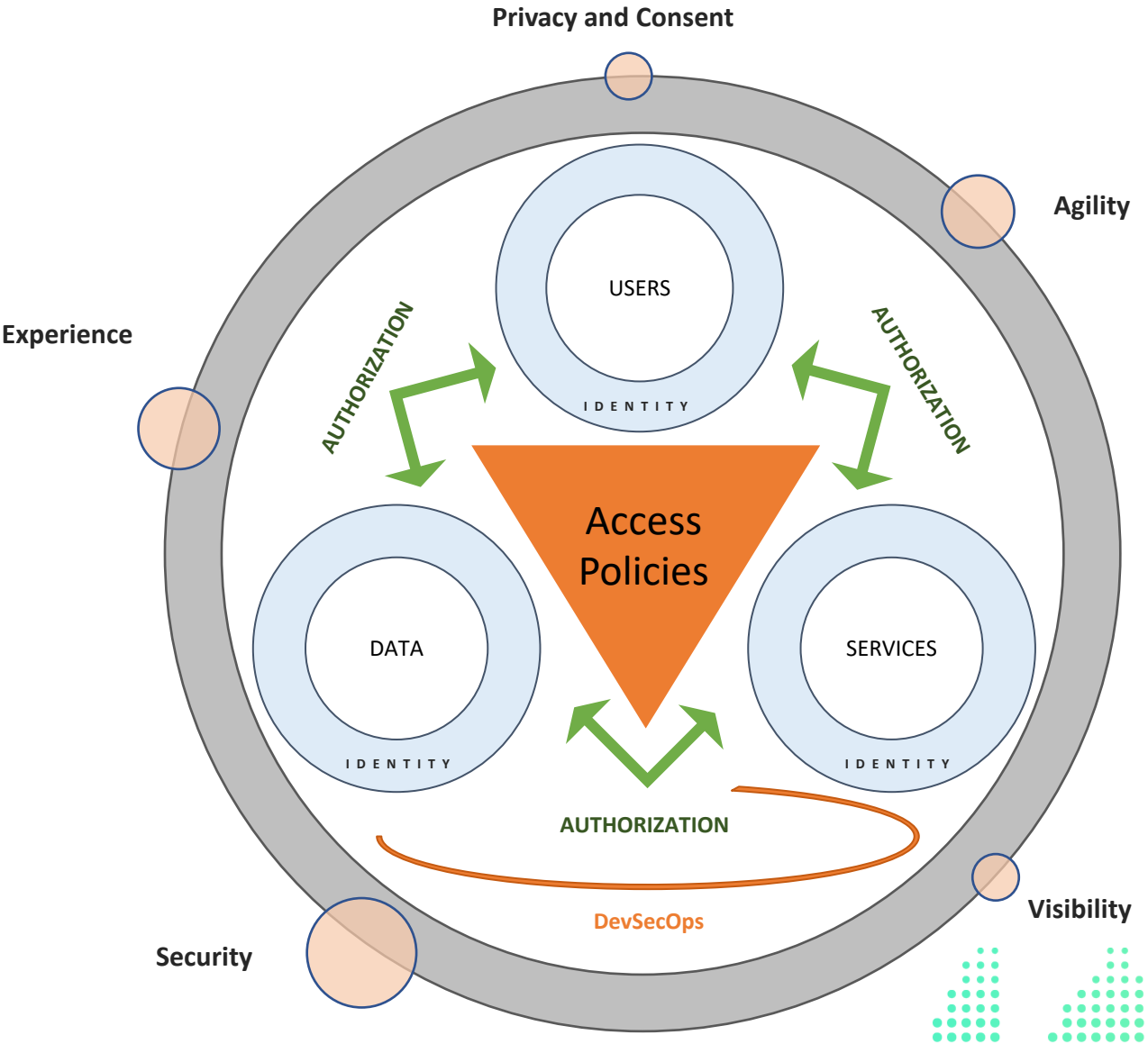
- ❑ JSON object
- ❑ Accessible via APIs
- ❑ Distributable
- ❑ Centrally Managed

Applicable

- ❑ Localhost
- ❑ Dev
- ❑ Pre-Prod
- ❑ Prod



Security is the same regardless of infrastructure & app architecture



Identity is at heart of security and enables you to deliver the modern services **your customers demand…**

All while

*Ensuring the **security** of the data you hold*

*Enhancing the **privacy** of the customers you serve; and*

*Meeting your regulatory and compliance **obligations**?*

Thank you!

About me:

Lukasz Radosz
CPO at Cloudentity
Residing in “cloudy” Seattle, looking forward to snowboarding season to start

Learn more at:
www.cloudentity.com

CLOUDENTITY

RIGHT **PEOPLE**, RIGHT **DATA**, RIGHT **PLACE**, RIGHT **TIME**

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

StateFarm

GOLD SPONSORS

vmware

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure

MEDIA SPONSORS

DZone
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire