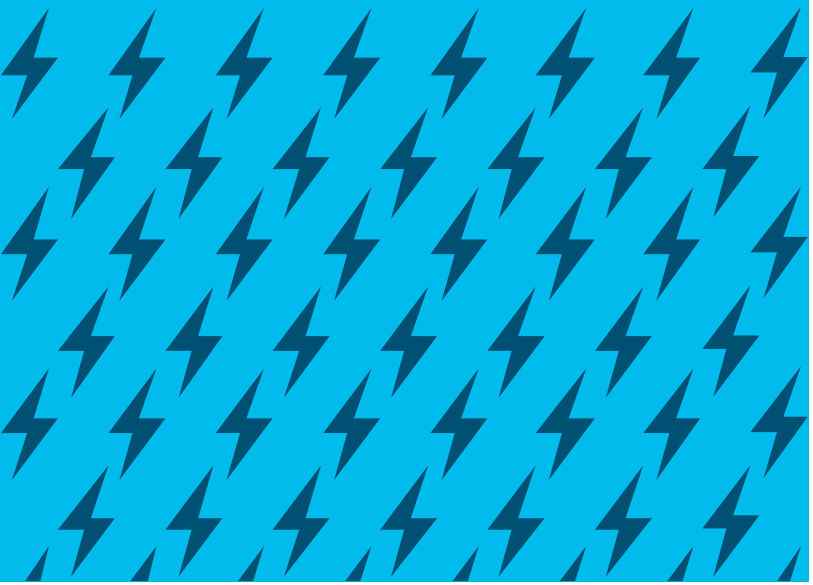
Application Security Trends

Agenda



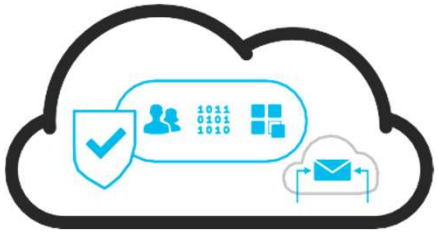
- Introduction
- Challenges
- Cisco’s approach
- Use cases.
- Conclusion

Security for a cloud first world

Security to get to the cloud

Secure Internet Gateway (SIG)

Security for SaaS apps

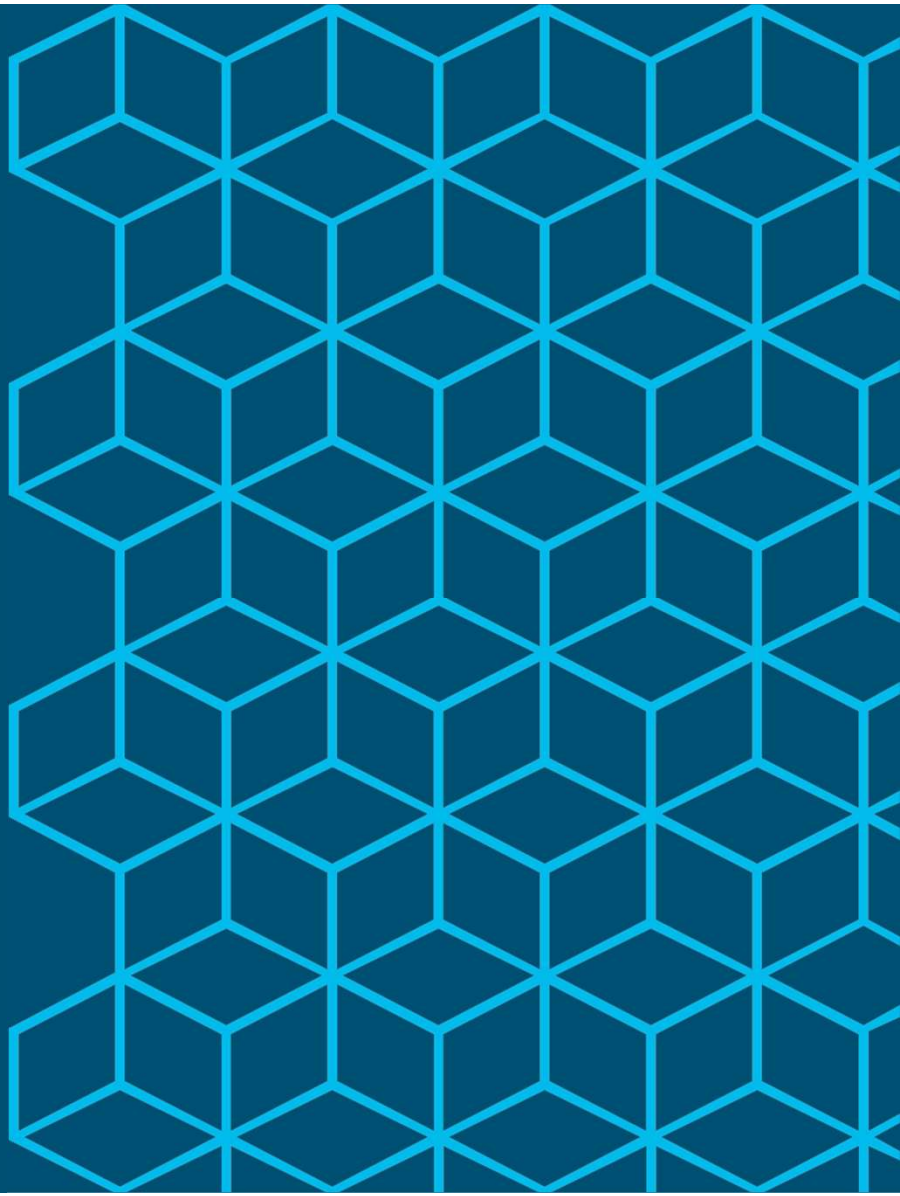


User, data and app security

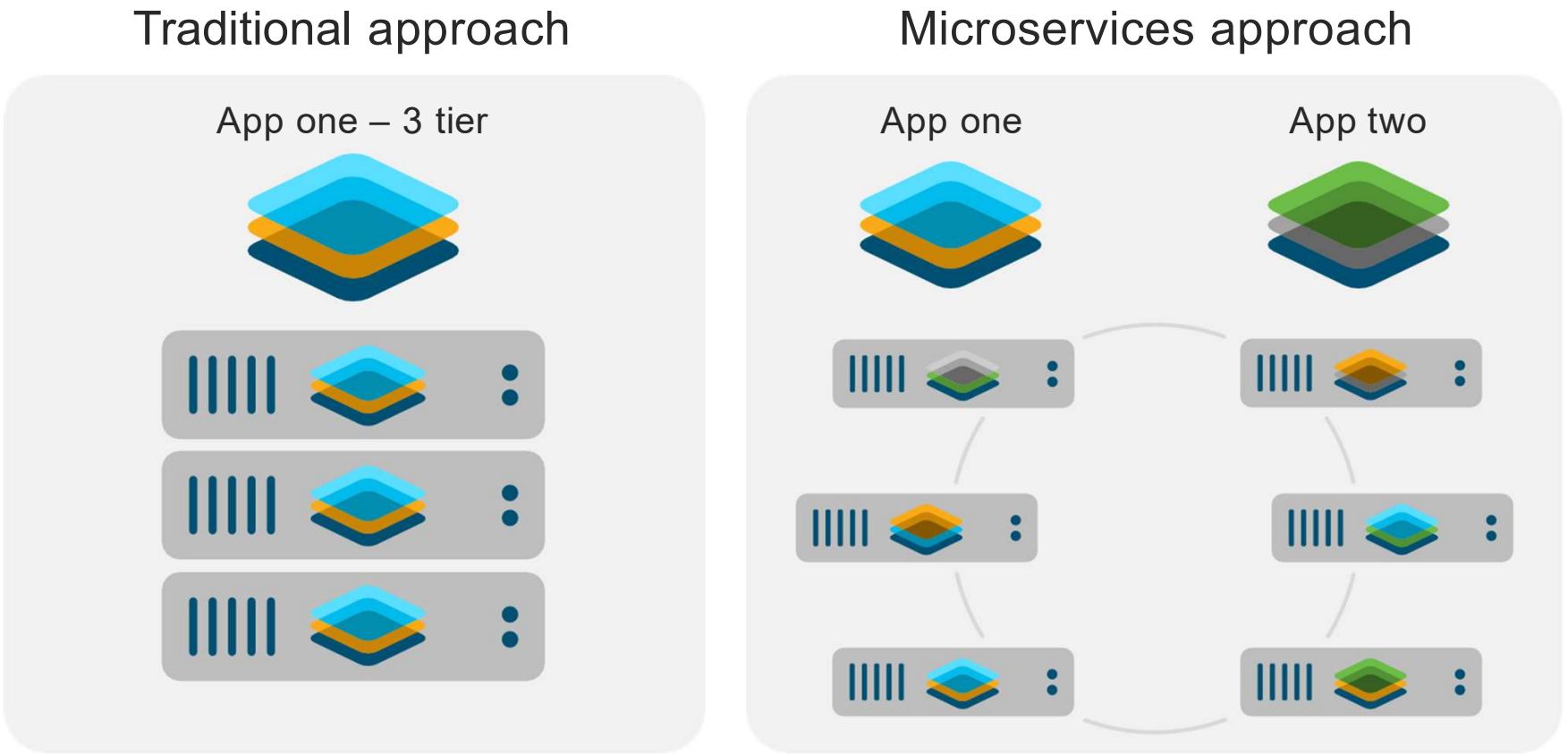
Security for your apps

Application & Workload Security

Challenges in securing cloud-native applications

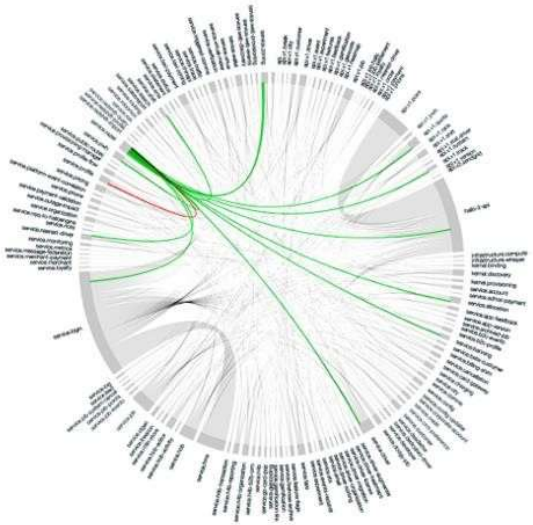


Application architecture is changing



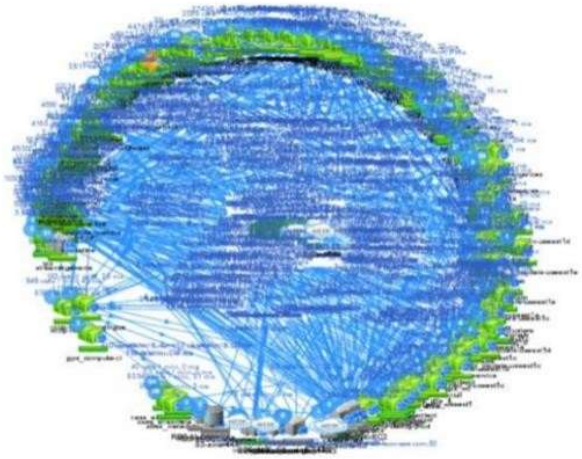
Microservices in real world

450+ microservices



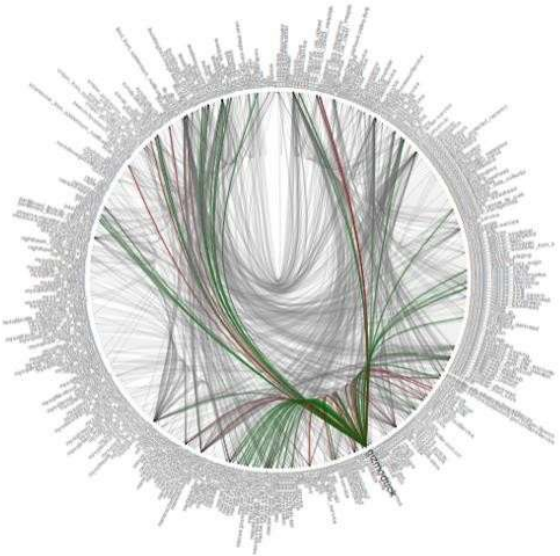
HAILO

500+ microservices



NETFLIX

500+ microservices



Protecting a moving target: applications

Two worlds

Application security
= *application* problem

Application

Compute,
Storage, Network

Application security
= *infrastructure* problem

Many challenges

1. Applications are changing and run everywhere
2. Lack of visibility and consistency of controls
3. Application deployments drive infrastructure
4. Application teams outnumber security 100:1

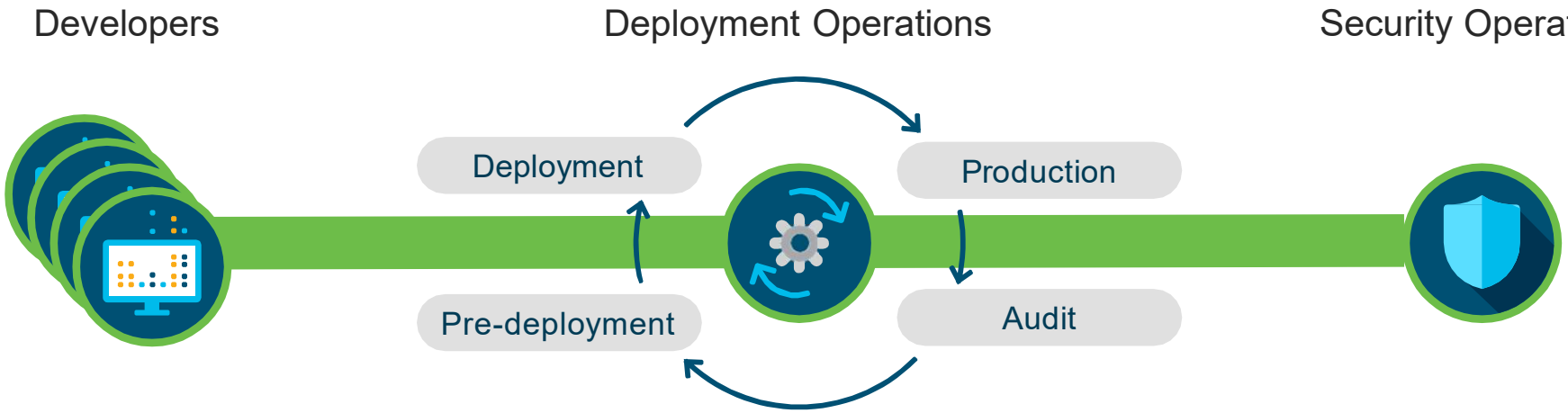
How to protect a workload in the cloud?

"SECURITY PREFERS A SYSTEM POWERED OFF AND UNPLUGGED"
- DEVELOPER

"…THOSE STUPID DEVELOPERS"
- SECURITY PERSON

Imagine a world where security and DevOps cooperated

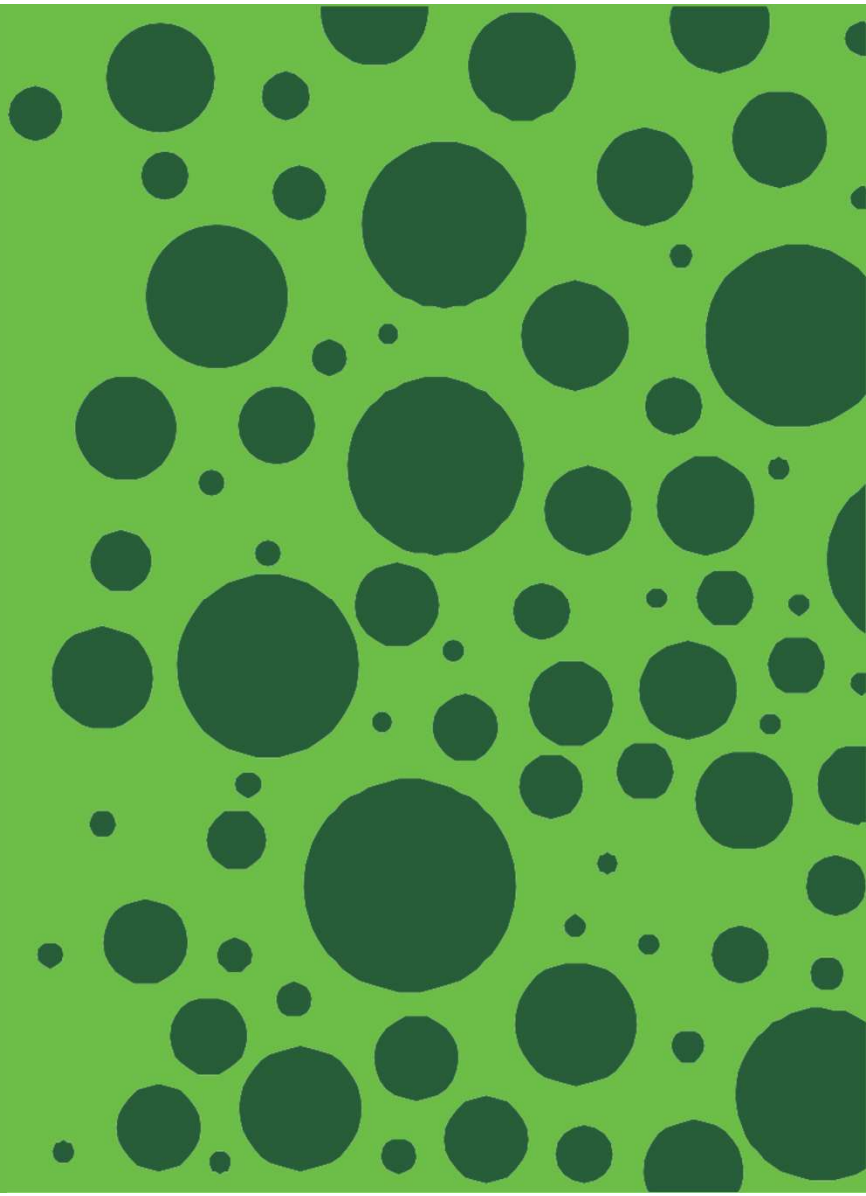
What would this world look like?



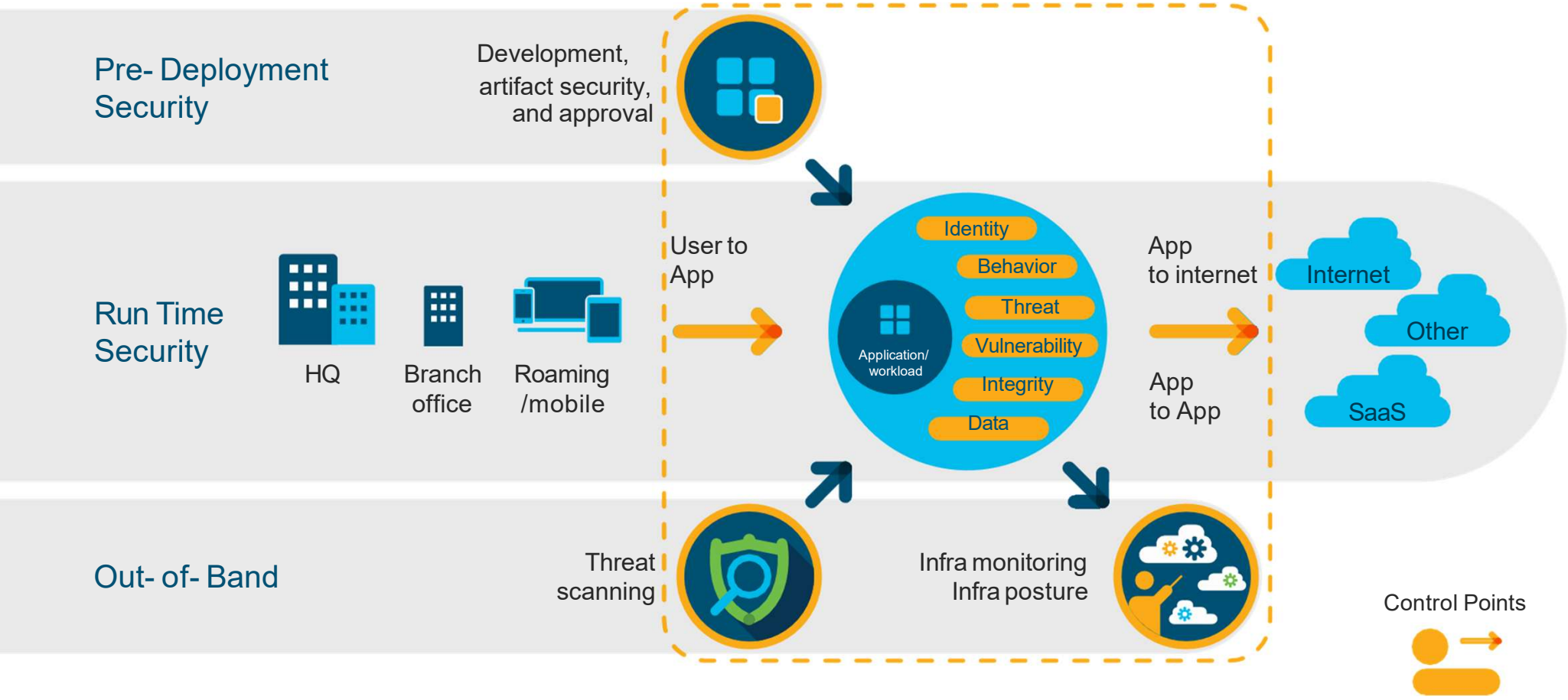
Outcomes

- Less Friction
- Secure Dev process
- Greater Visibility and Control
- Continuous compliance
- Tailored incident response
- World Peace!!!

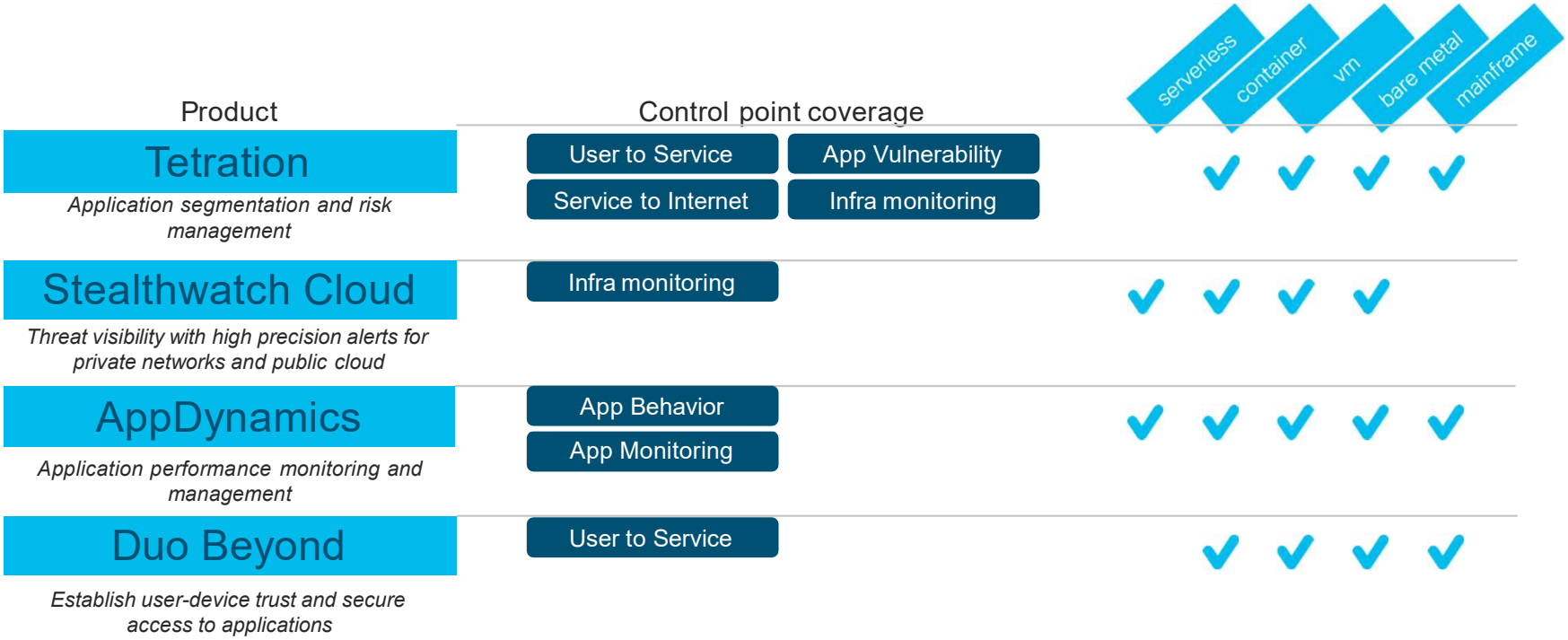
Cisco’s Approach



Cisco framework for application first security



App/workload security products today



Good Coverage today across control points and workload formats, but…

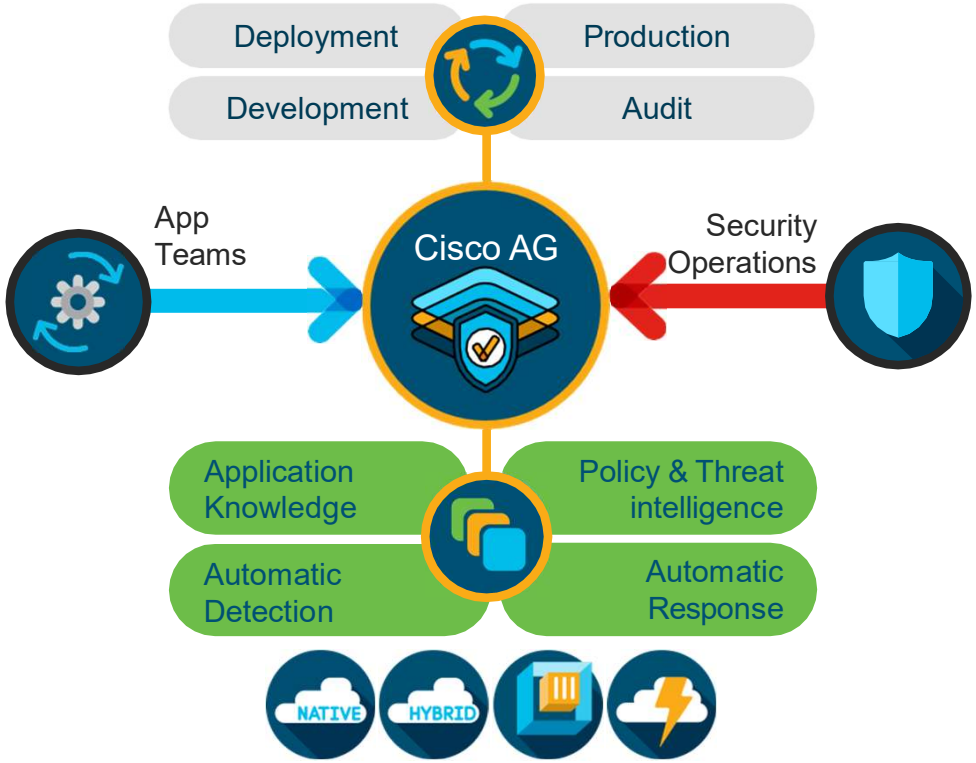
Add control points to “shift security left”

Planning is in progress

- Teams brought together
- To secure any native/hybrid application
- Throughout app lifecycle
- Anywhere the app runs

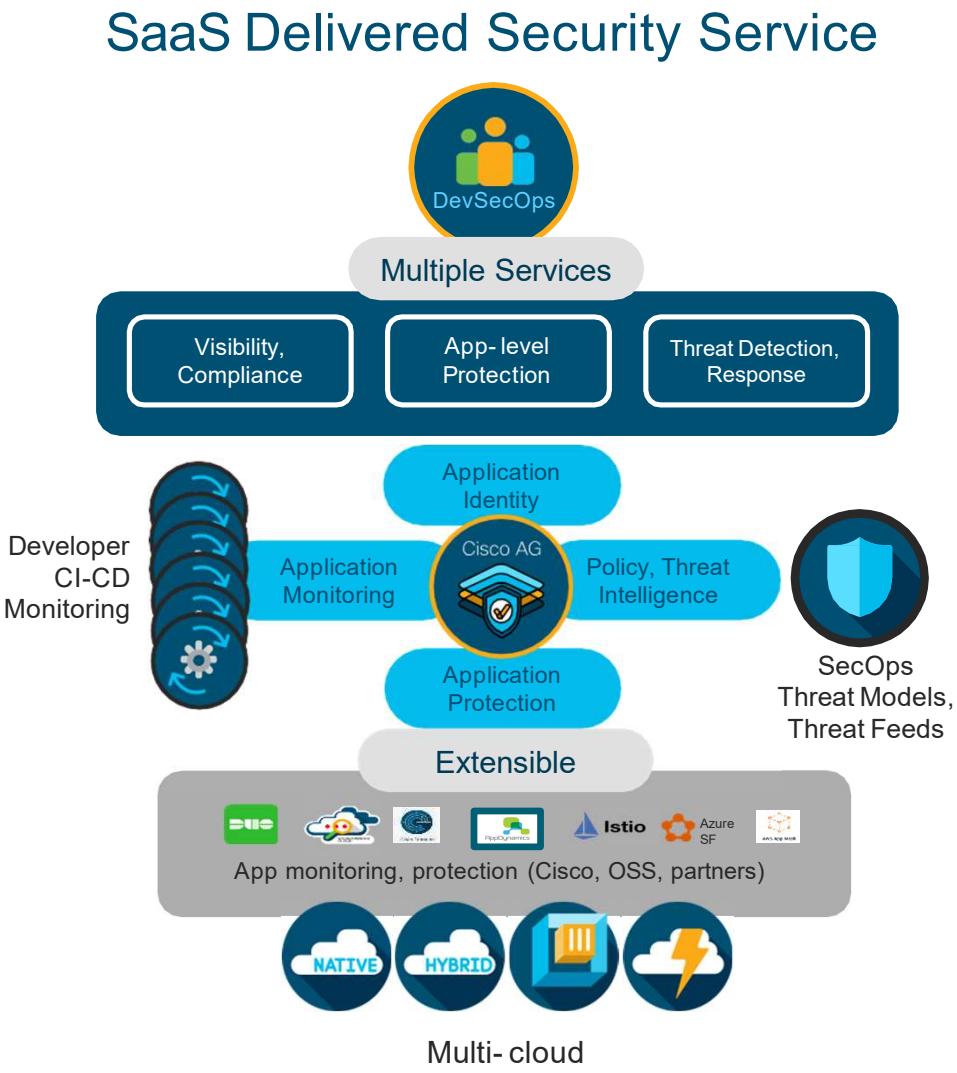
Closer Continuous Tailored to app

Project: Cisco AG

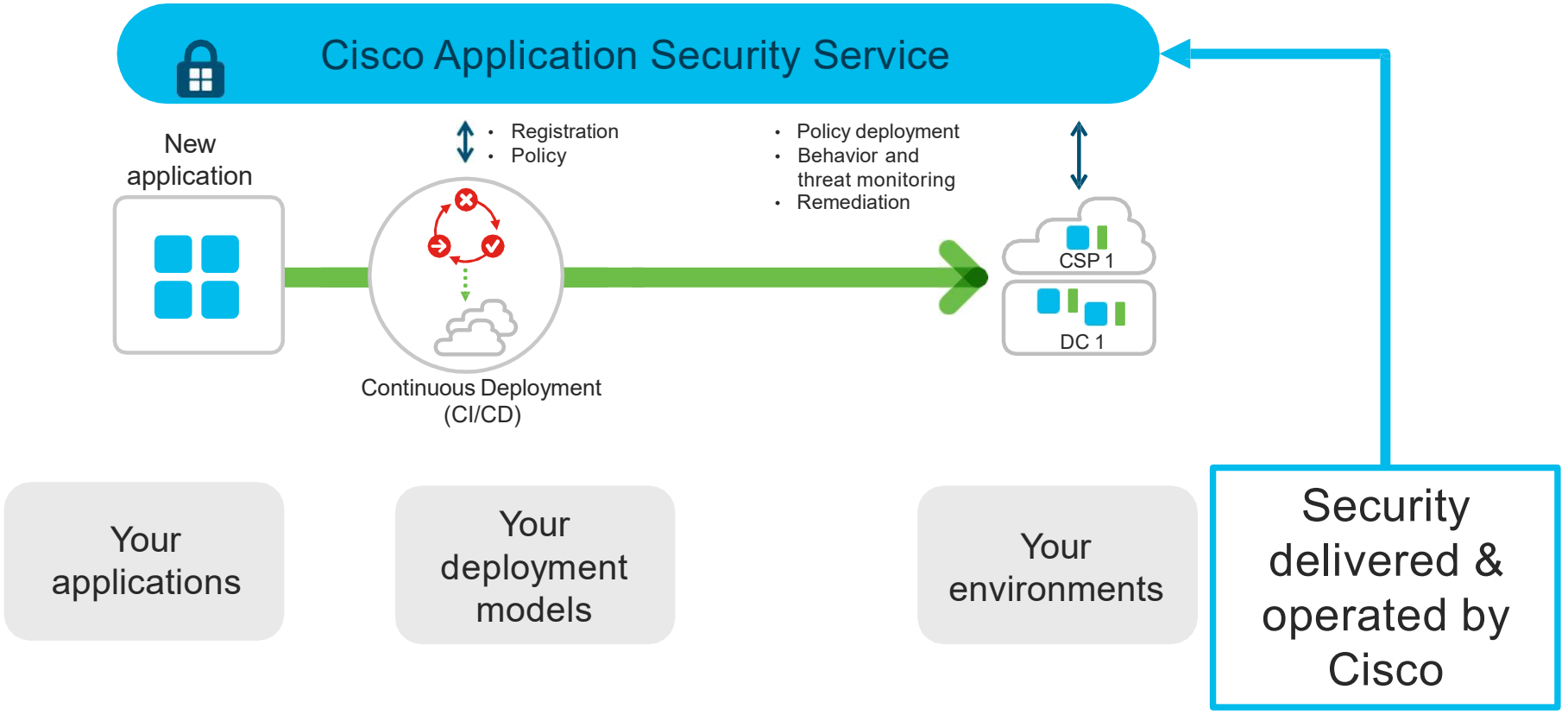


Project AG details

- Auto-learn app knowledge from CI-CD metadata, monitoring tools, developer input
- Acquire security knowledge from policy input, threat models/feeds
- Automatic security implementation using native app-level controls



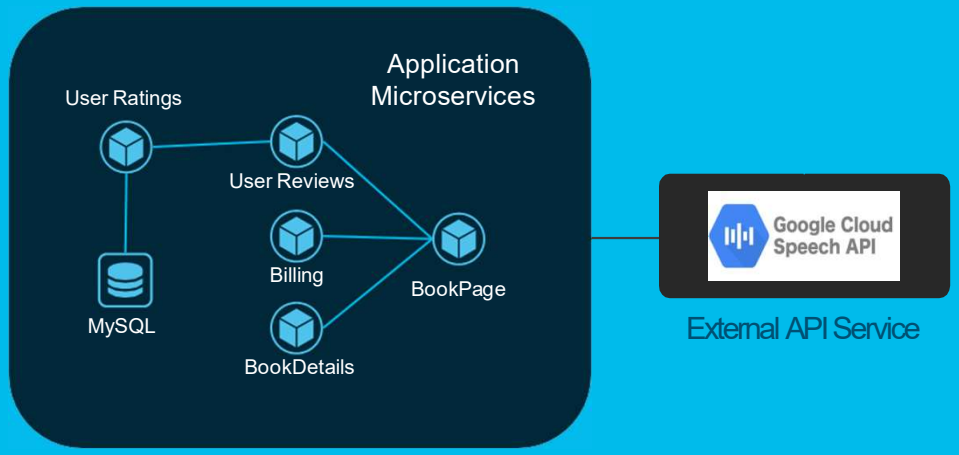
Project AG in a nutshell



Use cases

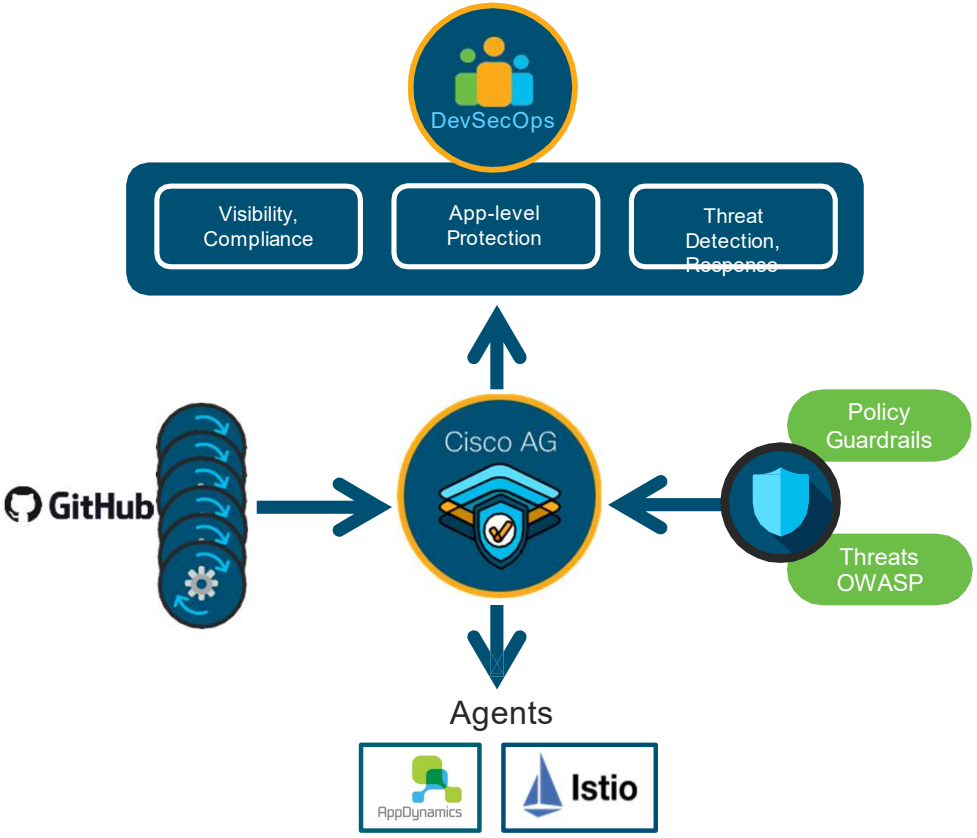
Demo application

Micro-services based, running on K8s



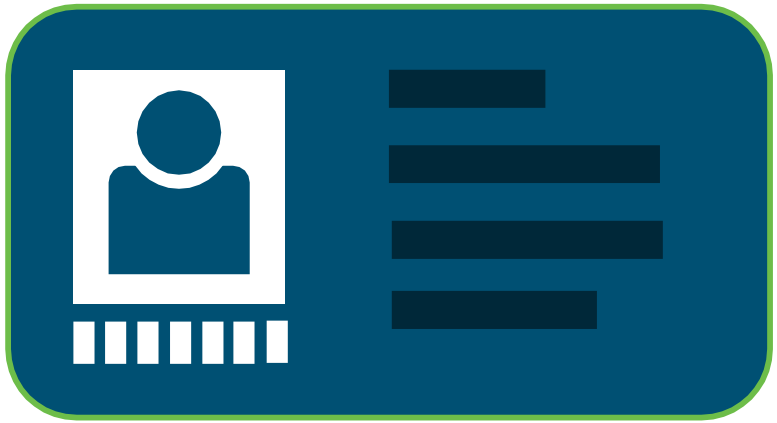
Demo app: Bookinfo

Demo Setup



Demo Customer Profile

- Developing new and migrating existing applications to cloud
- Adopting DevOps methods agile development
- Evolving existing security process and tools to accommodate move to cloud



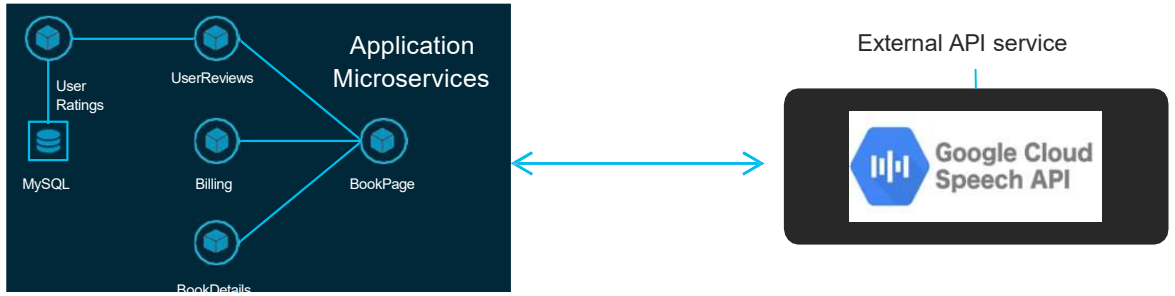
Use case: App visibility and API Governance

How to continuously visualize the app; validate compliance, API usage?

Compliance problem
Point in time process

- Cloud services evolve rapidly
- App architecture evolve rapidly
- Micro-services and DevOps are accelerator of this trend

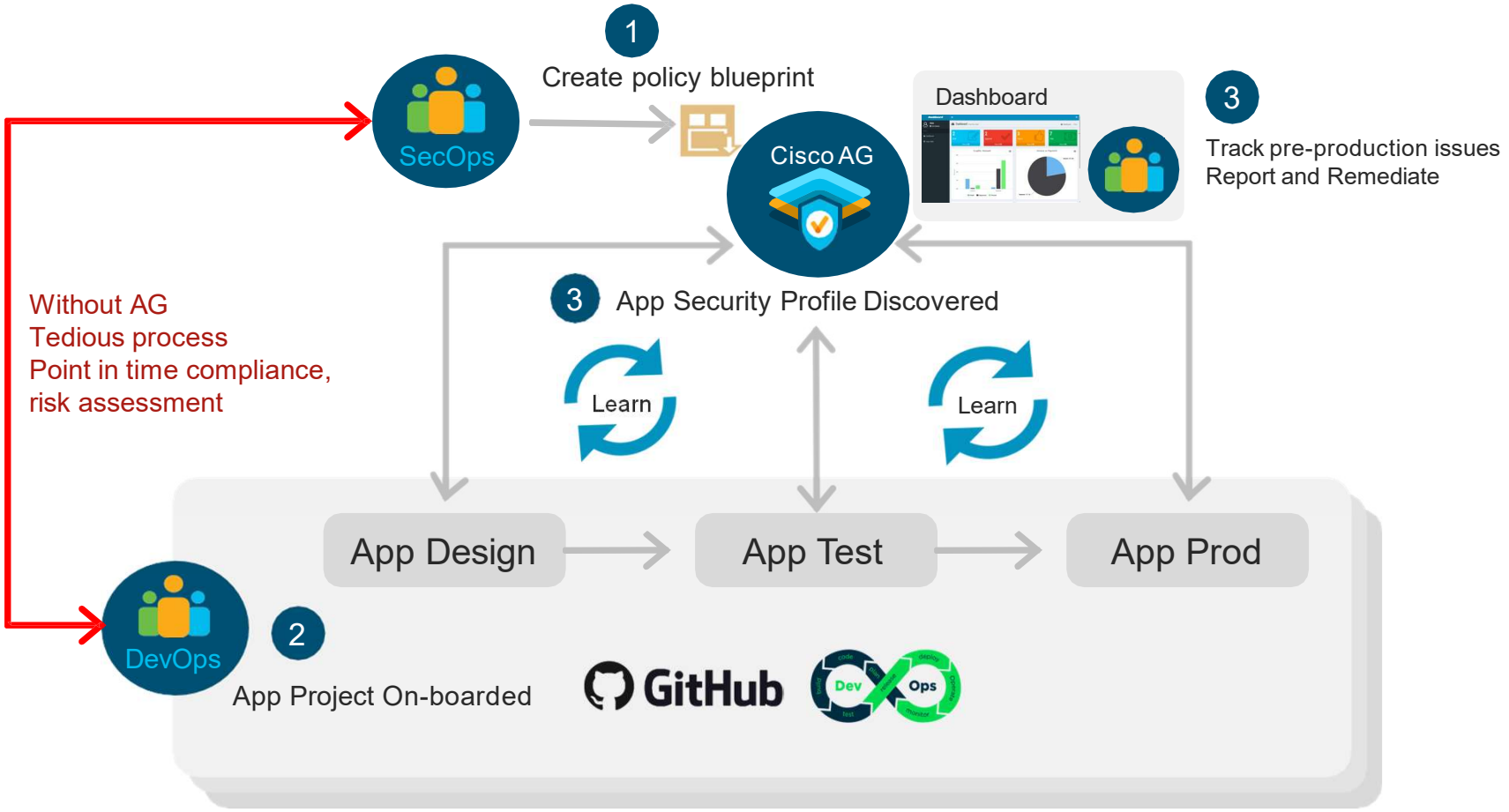
Infosec and application lead



Demo application

Data compliance issue: Certain Google Speech API downloads customer data to Google Cloud

AG pre-production workflow



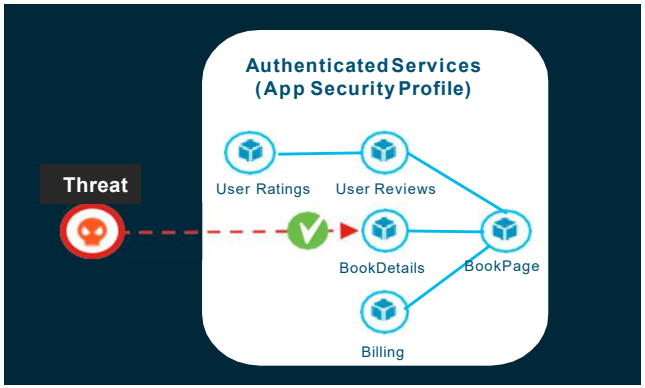
Use case: Threat detection, Response

How to filter out the noise, pinpoint the application breaches?

Threat Monitoring problem
Which threats are getting inside?

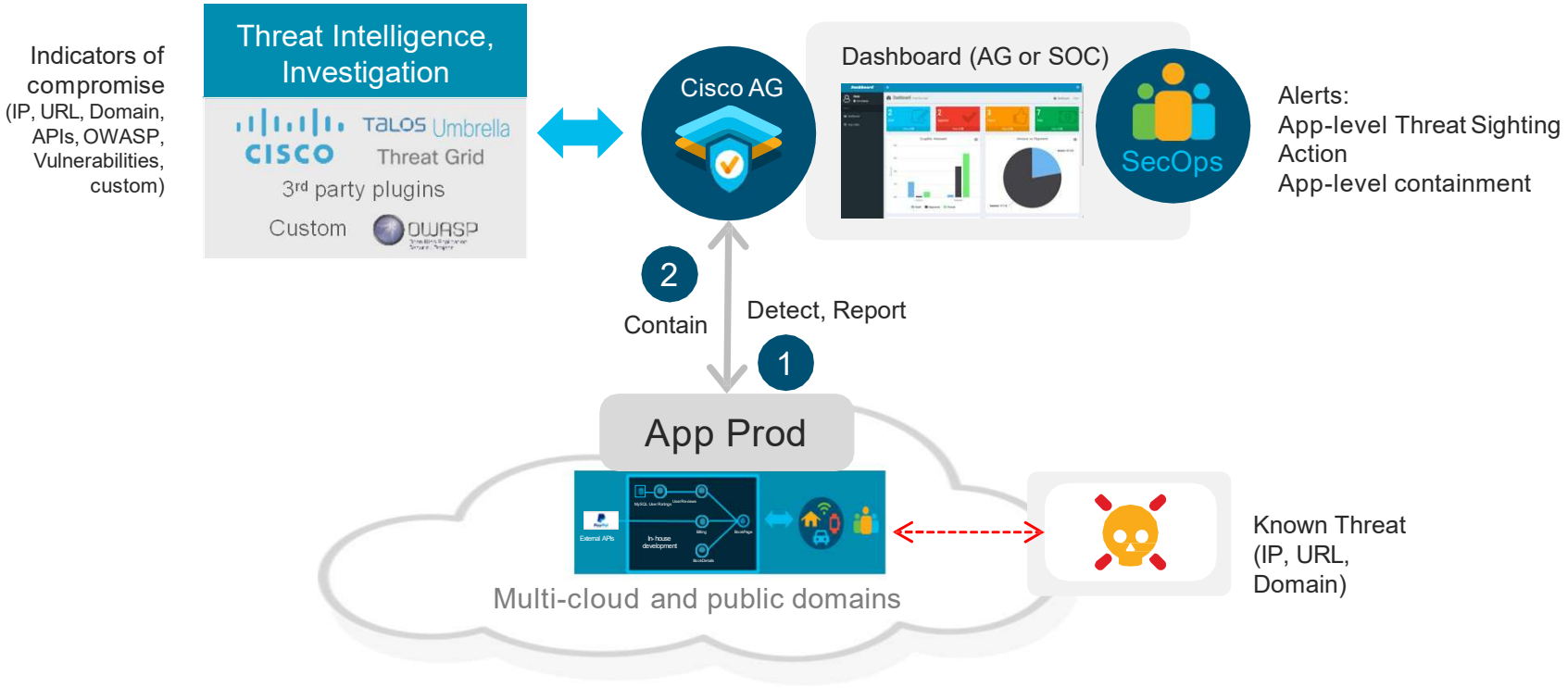
- App-level encryption hides threats
- Increased attack vectors due to open, distributed app architectures

Incident Response / DevSecOps



Threat detection and response – demo for OWASP top 10

App in production: threat detection, response



AG using agents adopted by DevOps

RASP emulation (Runtime Application Self Protection)

AppDynamics

- RASP security agent, provides task-level visibility inside app transactions
- Detects Top OWASP attacks, app transactions indicating interaction with external threats
- Platform agnostic, native app agent can be distributed separately or as an APM extension

Coordinated threat visibility, response at app-level

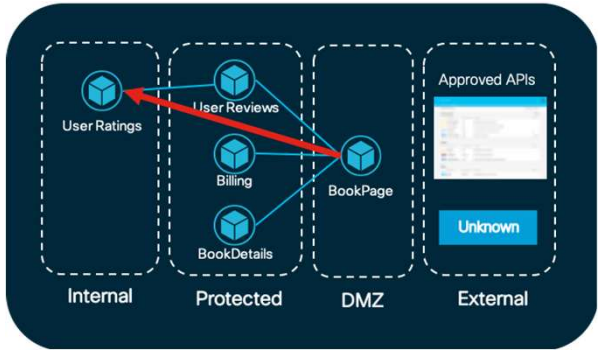
Use case: App protection in multi-cloud

How to block lateral movement across cloud domains?

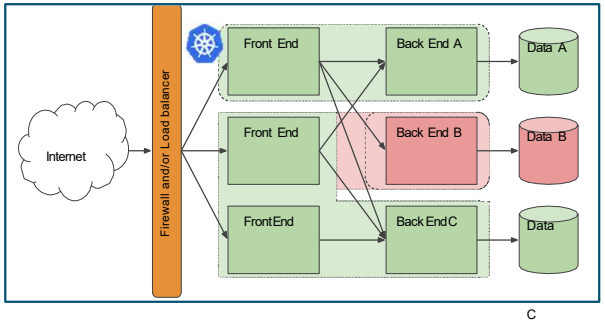
Segmentation problem
Infrastructure, Perimeter-based

- Cloud native apps require open multi-cloud communication
- Dynamic micro-services, distributed across multi-cloud
- No infrastructure controls for serverless, external APIs

InfoSec and application lead



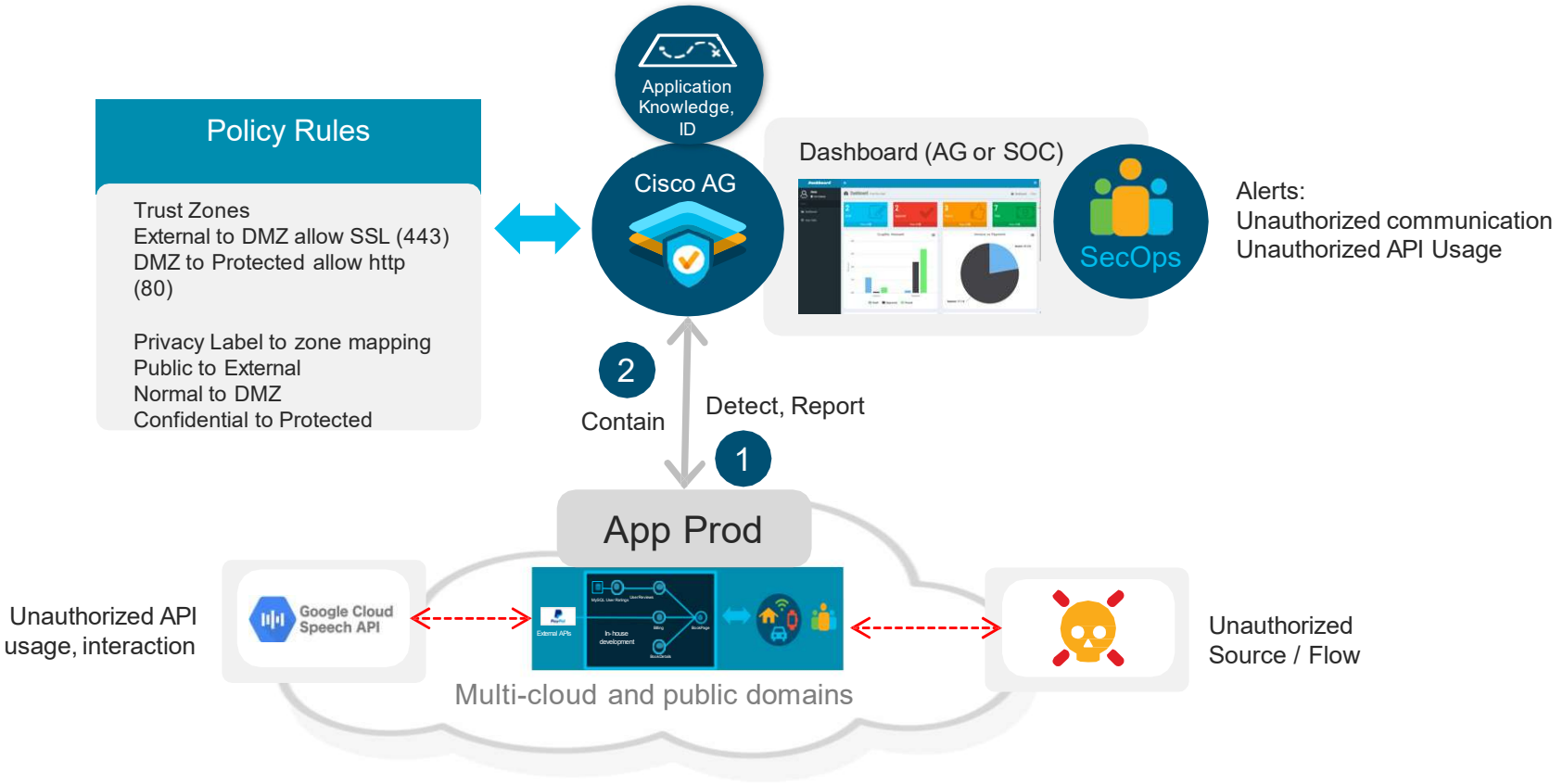
Customer 1



Customer 2

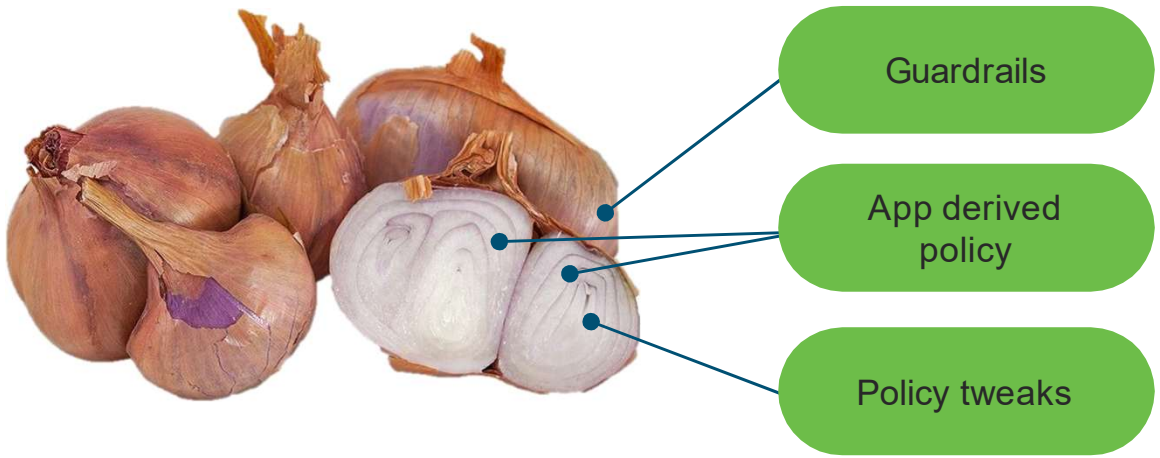
Trust zones demo: Zero Trust, multi-cloud environment

App in production: AG identity, policy-centric protection



How policy is determined and layered

Think of onions – every one starts with a skin (*guardrails*) and has layers (*derived and tweaked*) policy

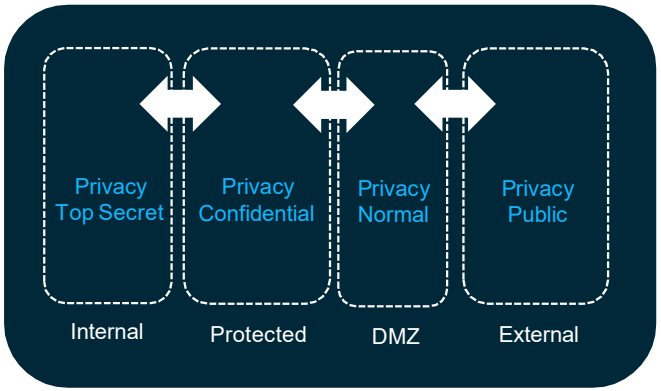


Determined by

- SecOps
- Automation
- App Team or SecOps

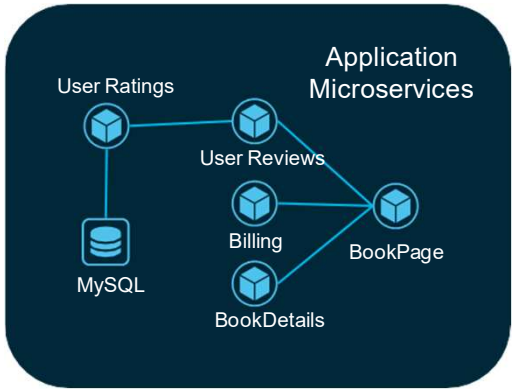
How policy is implemented – trust zones example

Security persona



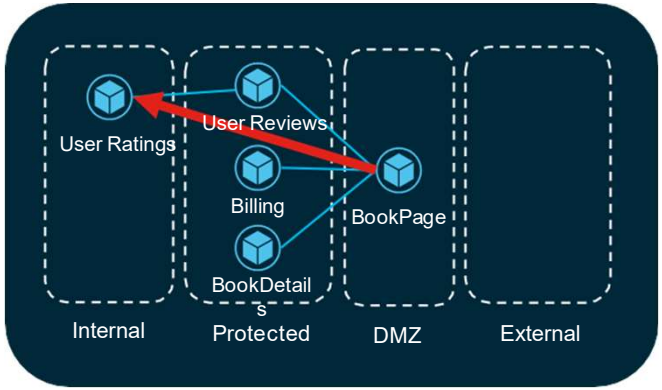
Guardrails – all app projects

Automatic discovery



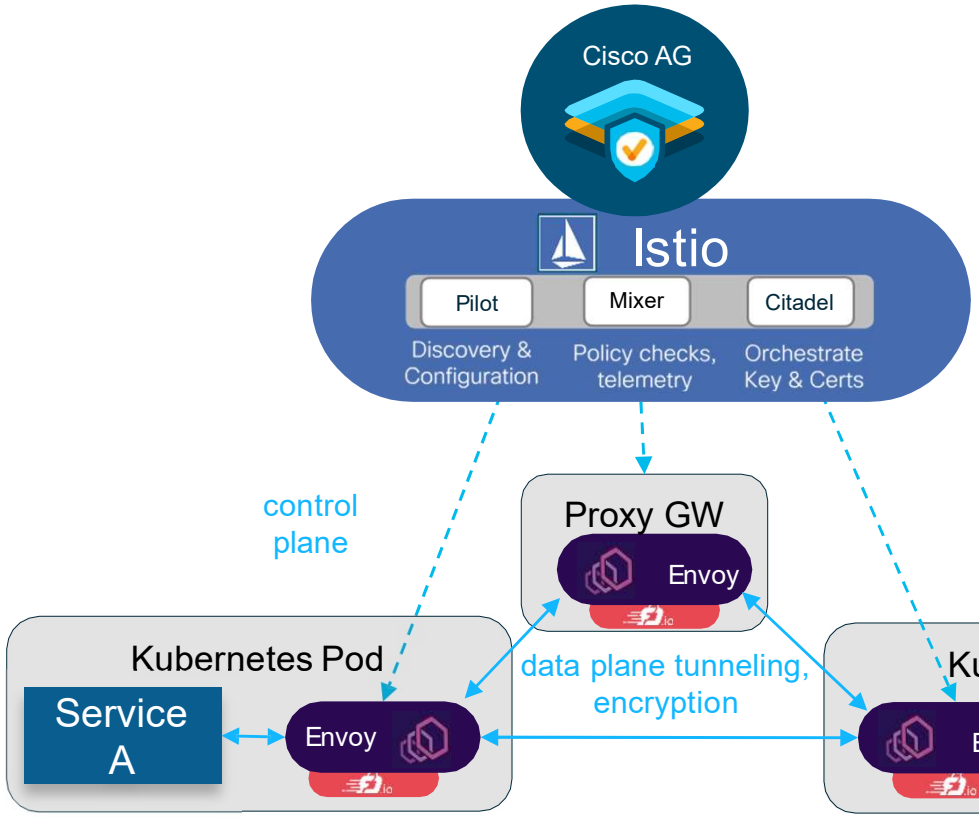
Learned app profile

Automatic enforcement



Derived app segmentation

AG using agents adopted by DevOps



Istio

- Open source software supported by Cloud Community, deployed for 4 years in Webscale
- Provides L7, API infrastructure for handling service-to-service/Internet communication
- Platform agnostic, native Envoy agent delivers with the app code DevOps and security tools

Consistent protection at micro-service level

Recap

- Embed security early and continuously in application lifecycle – ride along with CI/CD
- Application-level enforcement regardless of where the app runs
- Continuously monitor app behavior, detect and react to deviations

…and all of this while providing value to the developers AND security teams

Project AG Value Proposition