Basil Policy-as-code Platform

Ron Herardian

(ISC)² East Bay Chapter Fall Conference, November 8, 2019

Organic Press Coverage

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

CSO
ChiefSustainabilityOfficer

Intellyx™

WIKIBON

BusinessWire
A Berkshire Hathaway Company

RSAConference

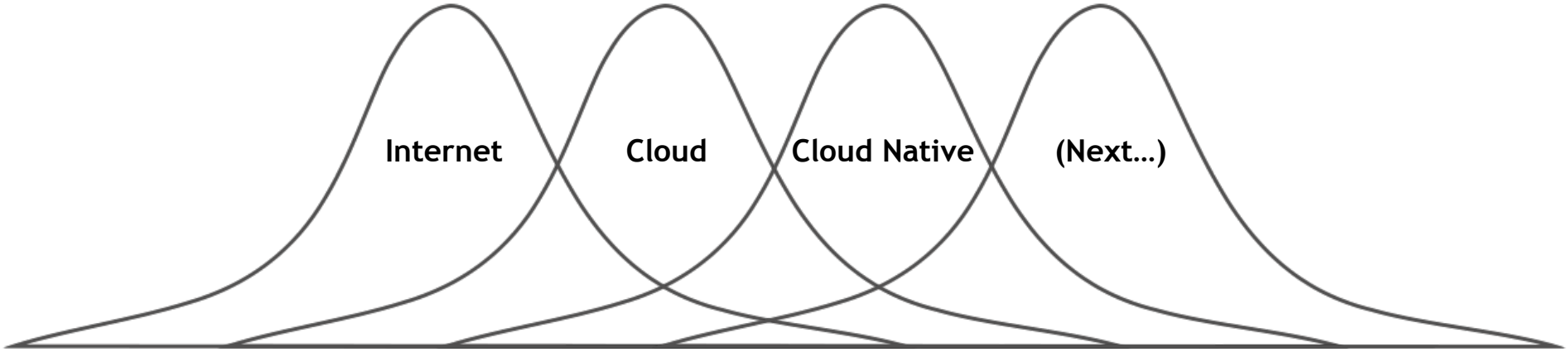
the cyberwire

VentureBeat

MarketWatch

Is every business a software business?

- Cloud
- Cloud Native



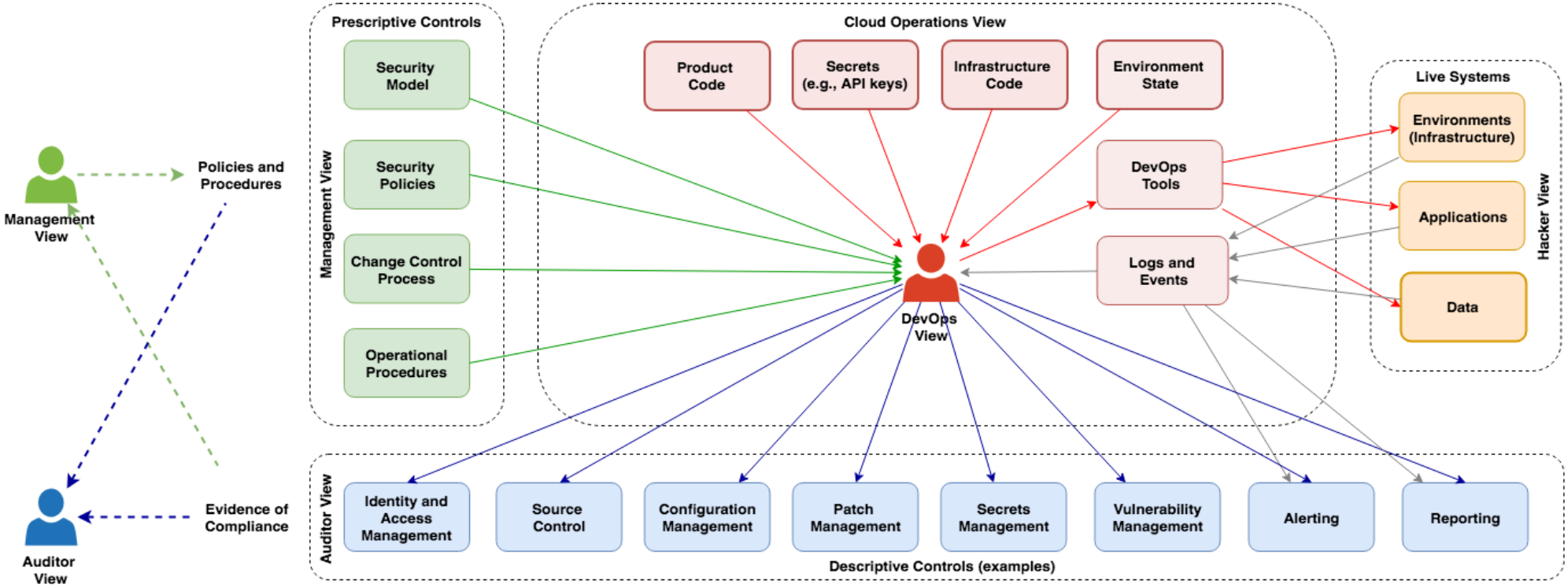
Cloud Challenges

- How are security controls unified?
- How are policies enforced?
- Who is accountable?

Policy vs. Execution

- Policies and procedures not followed
- Impacts on application availability / up time
- Security incidents
  - Insider negligence, IP theft, cyberattacks, data breaches
- Technical solutions use 'find and fix' strategy
- The damage is already done

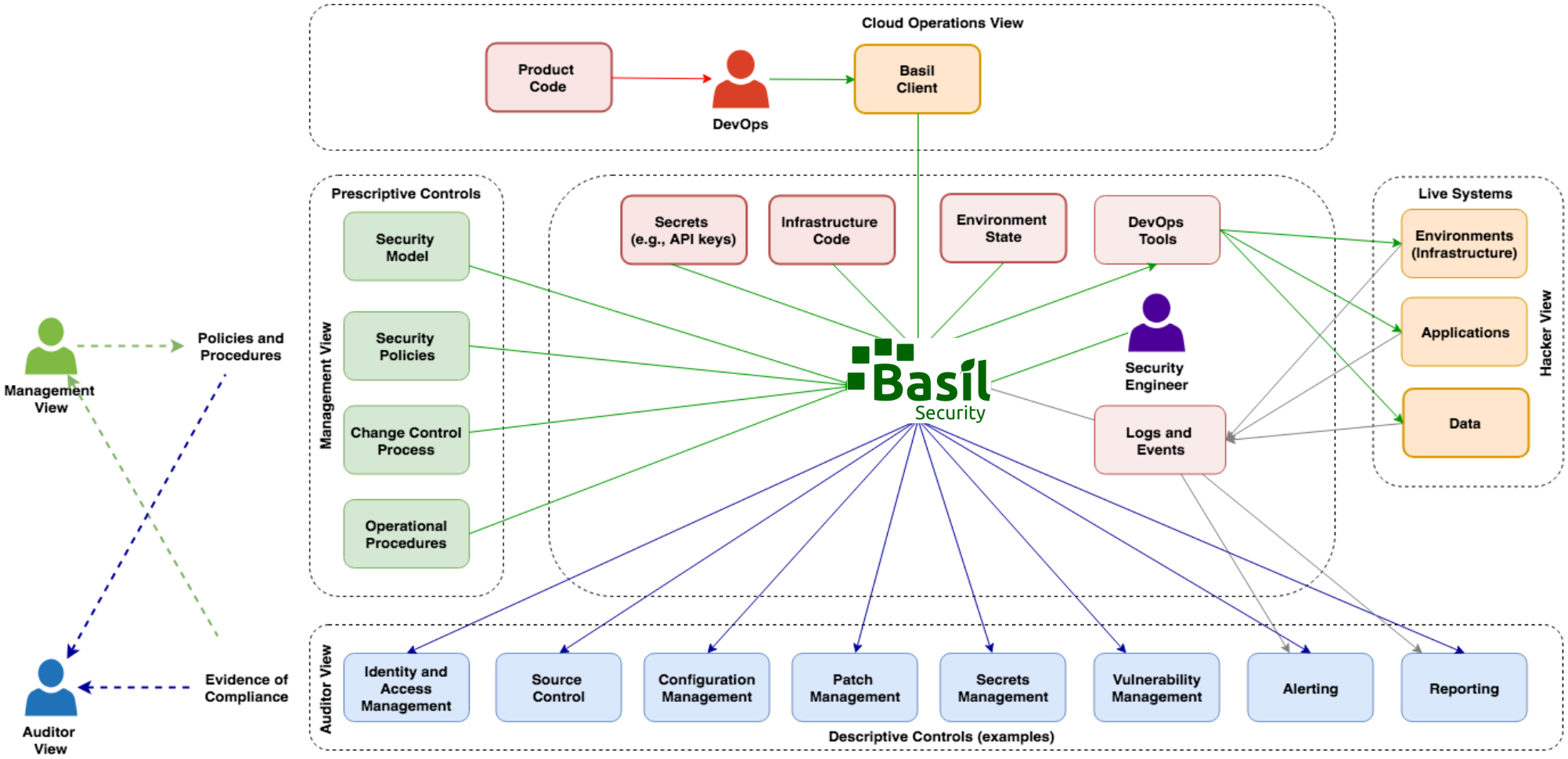
Illusion of Control (lots of things can go wrong)



Basil to the Rescue

- Common policy language
- Enforce policies before the fact
- Make policies smarter (context aware)
- Policy traceability / chain of integrity

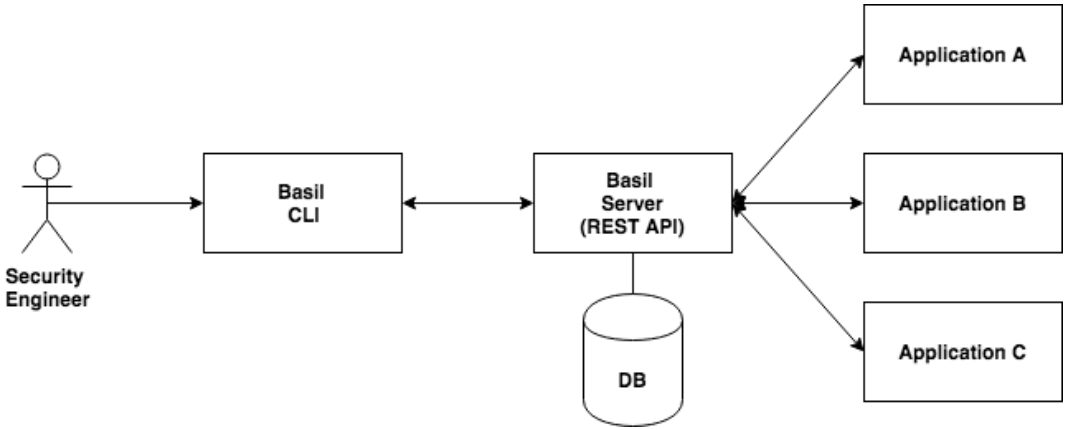
Actual Control



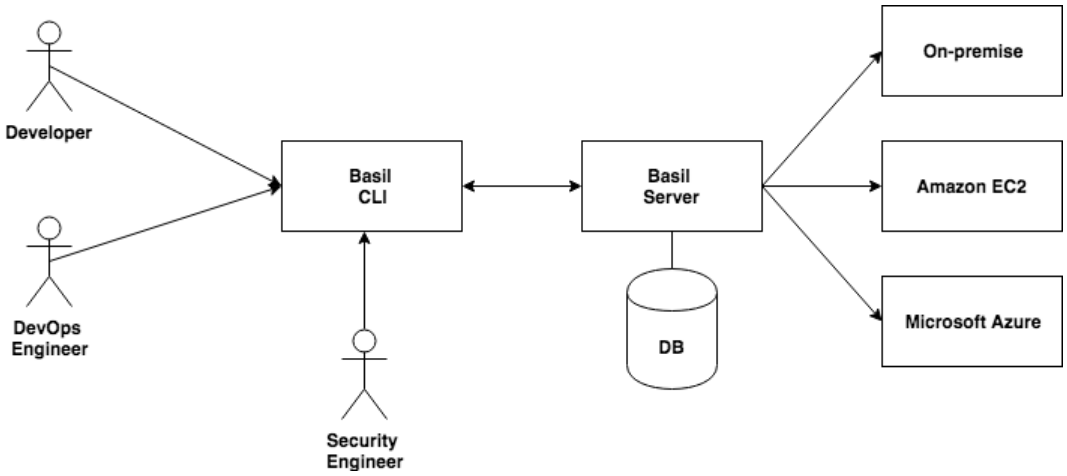
Use Cases

- Application security (via REST APIs)
- Automation, e.g., using events such as webhooks
- Development and operations (DevSecOps)
- Hardware configuration security, e.g., using reverse SSH proxy tunneling
- Policy-based information classification
- Multi-level data encryption

DevSecOps Use Case

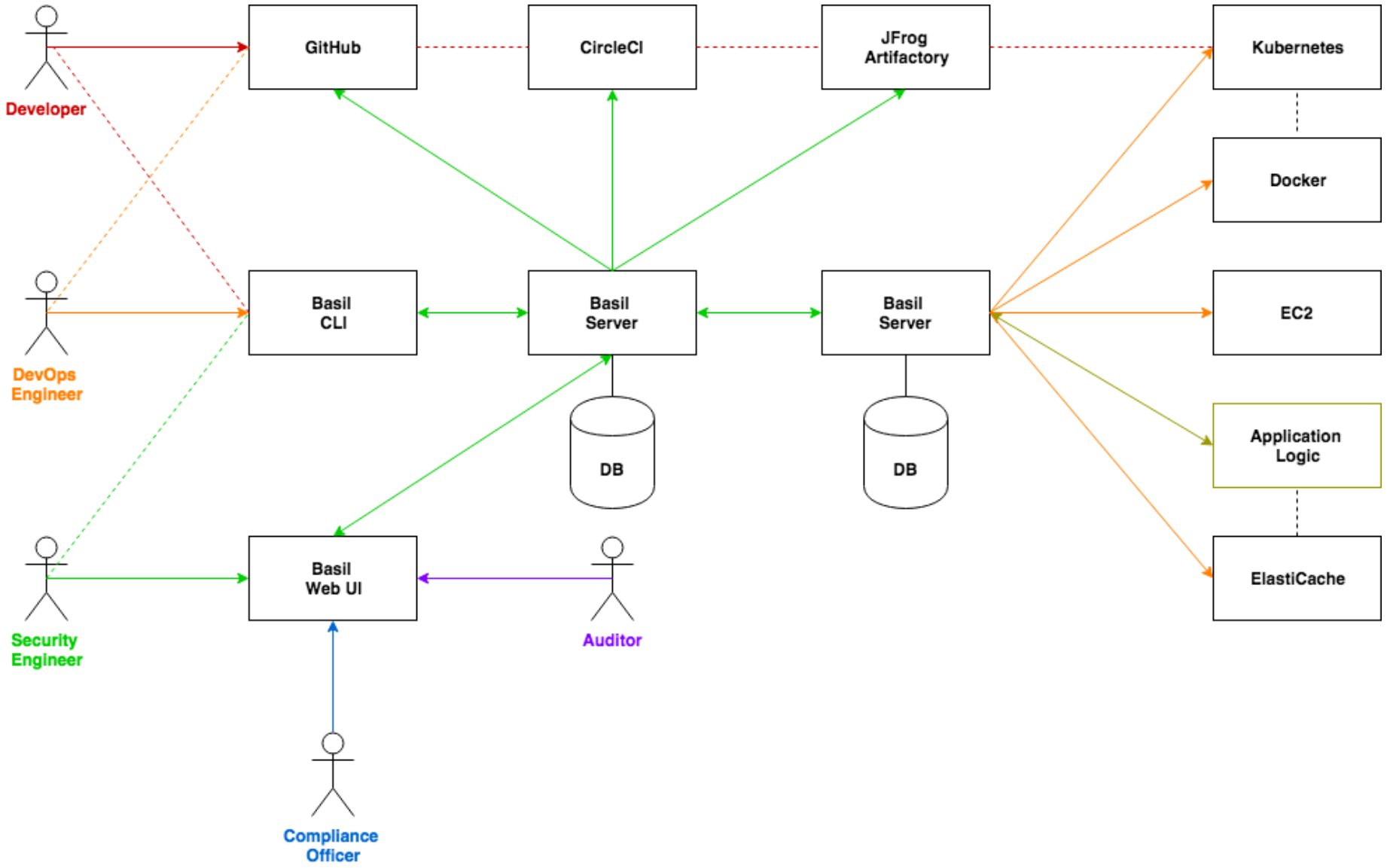


Machine-to-machine: Application stack or CI/CD



Human-to-machine: Systems and environments

Unified Controls / Chain of Integrity



Before and After (DevOps -> DevSecOps)

	Before	After
Procedures / workflows	Can’t be enforced	Automatically enforced
Accountability	No guarantee	Guaranteed
Configurations	Can be inconsistent	Consistent
Secrets	Accessible, not secure	Secure
Run code without review	Anyone can run code	Review enforced
Malicious acts	Anyone can do damage	Attacks prevented

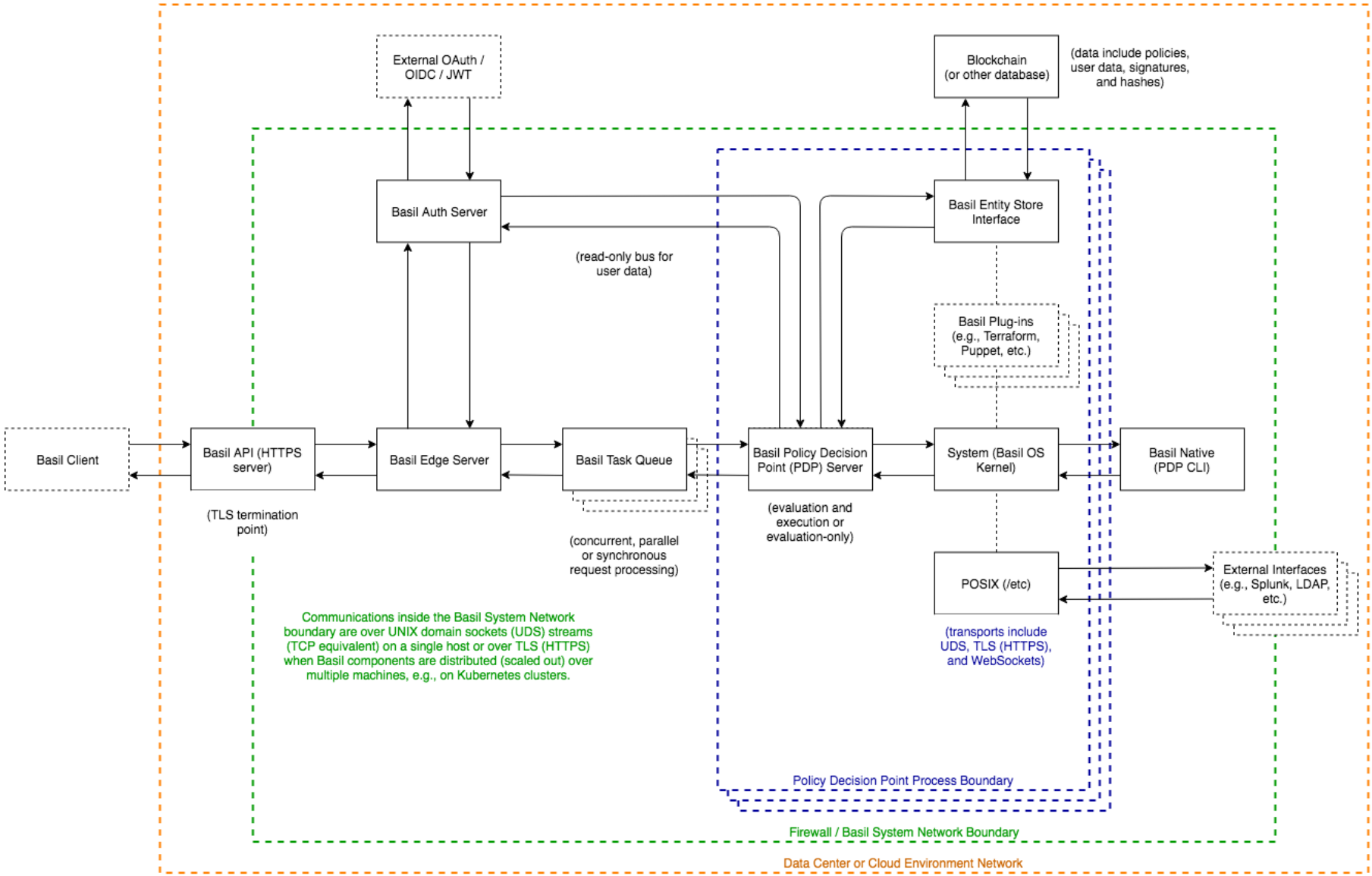
Who Cares?

Basil Feature	Compliance	Security	Development	Operations
Policy integrity across domains	Y	Y	_	_
Unify security controls	_	Y	Y	Y
Stateful and event-driven policies	_	Y	Y	Y
Secure secrets handling	Y	Y	_	Y
Non-repudiation	Y	Y	_	Y
Multi-party approval	Y	Y	_	Y
Machine-to-machine automation	_	_	Y	Y
Audit time travel	Y	Y	_	_
Guaranteed log integrity	Y	Y	_	_
Extendable integrations	_	Y	Y	Y
Enforcement before the fact	Y	Y	Y	Y
Distributed state machine	_	Y	_	Y

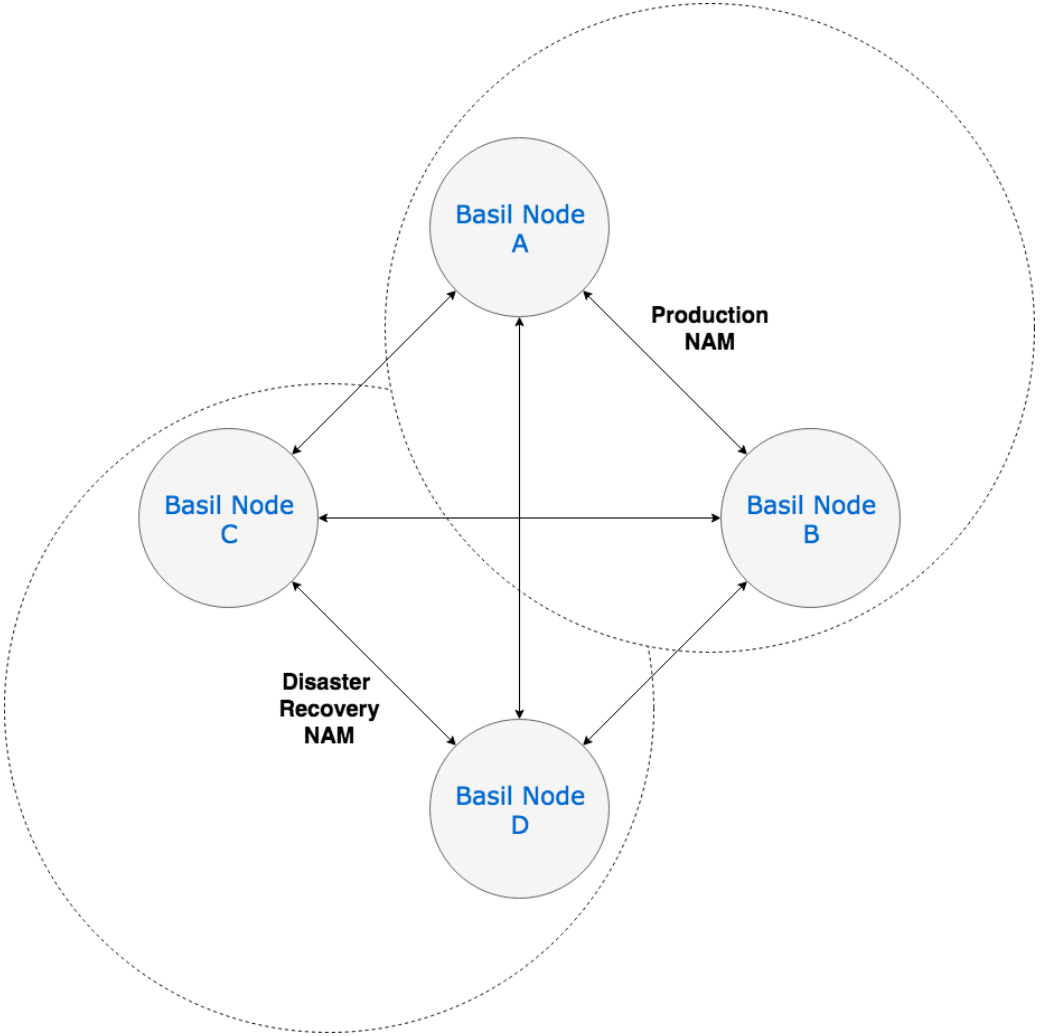
Technology

- Distributed command and control
- Control software, systems, data access
- Policy programming language
- Attribute based access control (ABAC)
- Stateful or event-driven
- Extendable plugin system
- Blockchain data store
- Pervasive use of cryptography
- Operates under DoD D-DIL conditions

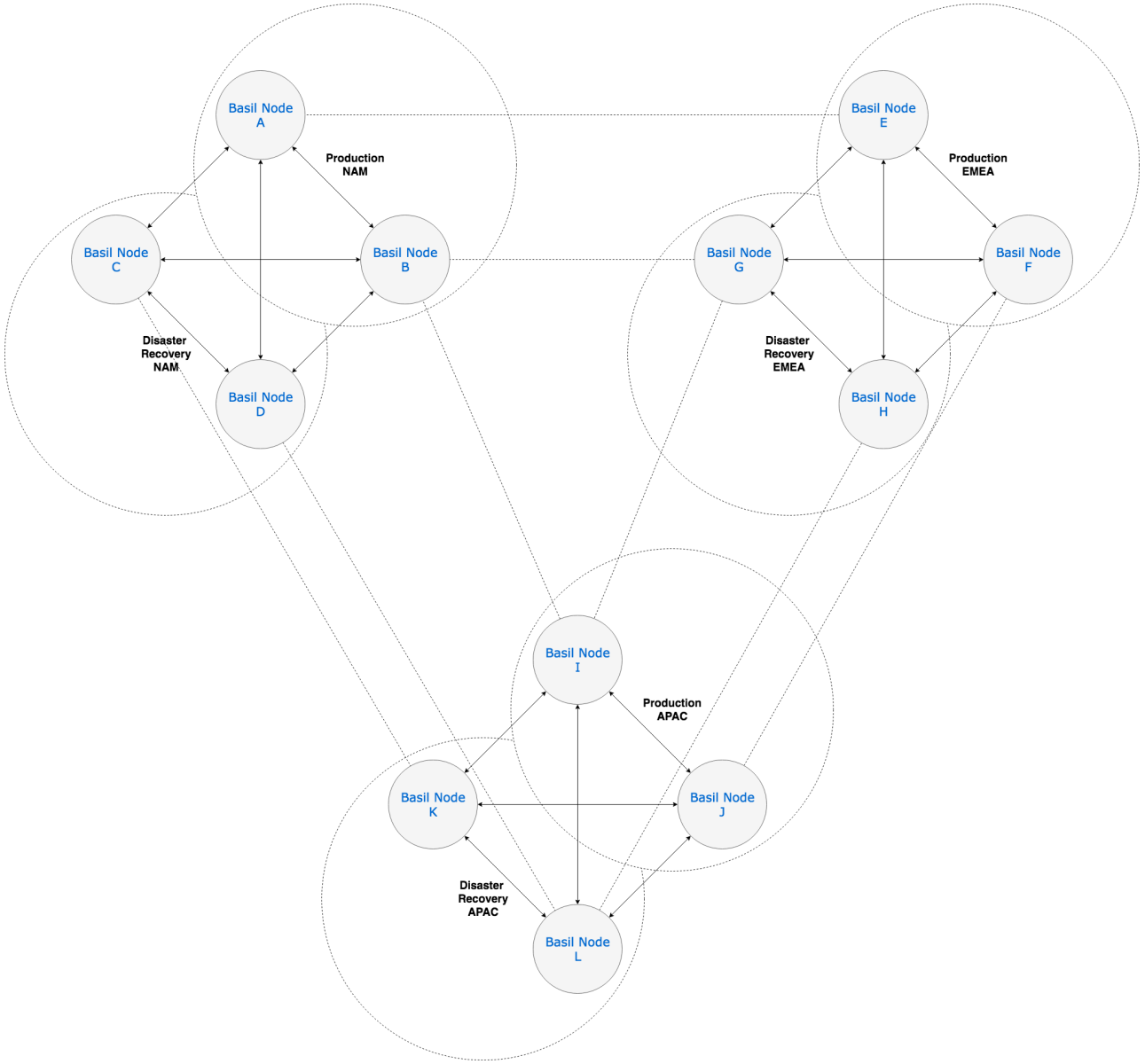
Basil Scale-out Architecture



Example Basil Node Deployment



Basil at Scale



Ron Herardian, ron@basilsecurity.com, +1 408 766 4487 mobile