PULSANT

DevOps & Continuous Compliance

MS Azure Hybrid Workshop 2018

Pulsant
Business Unlimited

LAYERV
A Pulsant Company

ABOUT ME

Javid Khan – CTO of LayerV

- 18 years IT sector experience
- Technology Delivery across multiple £50+M projects
- Successful delivery of multiple global private cloud platforms
- Technical ‘hands on’ background

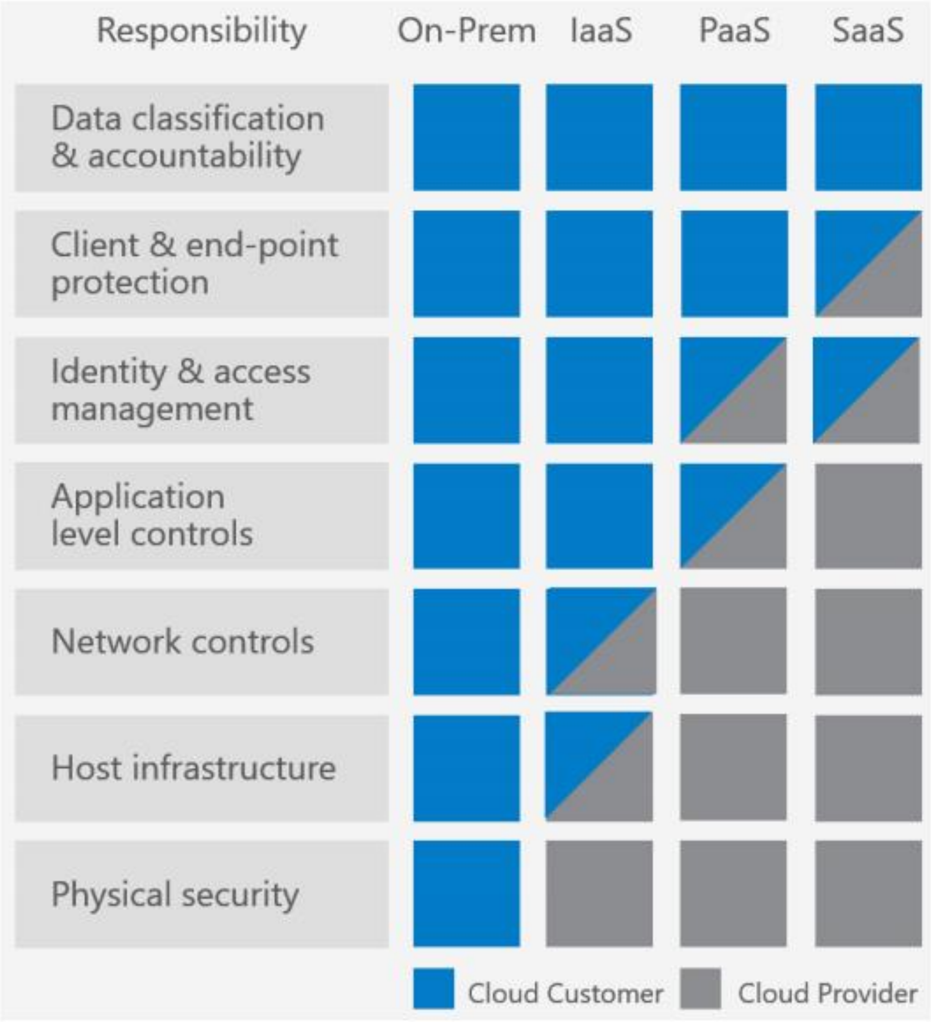
@javidkhan

@jav1d

LAYERV A Pulsant Company

Pulsant Business Unlimited

Azure Shared Responsibility Model



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

- Customer is accountable to ensure their solution and its data is securely *identified*, *labeled*, and correctly *classified* to meet any compliance obligation
- With an IaaS service model, for capabilities such as virtual machines, storage, and networking, is the customer’s responsibility to configure and protect the data that is stored and transmitted
- When using IaaS-based solution, data classification must be considered at all layers of the solution
- Compliance also requires that customers audit all deployed virtual machines within their solutions

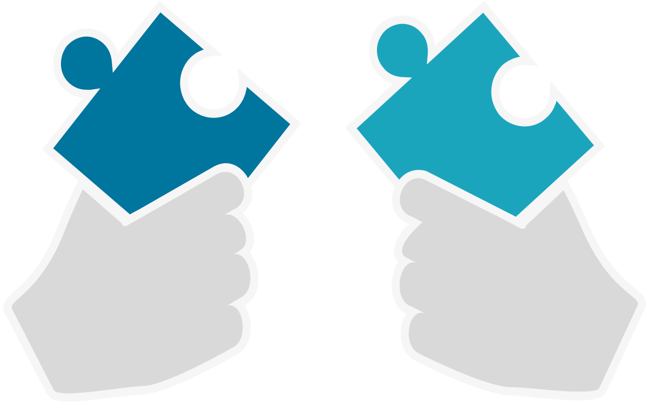
IaaS Customer Responsibilities

- Application Security & SDL
- Access Control
- Data Protection
- O/S Baselines, Patching, AV, Vulnerability Scanning
- Penetration Testing
- Logging, Monitoring, Incident
- Response
- ISMS Programmatic Controls
- Certifications, Accreditations & Audits

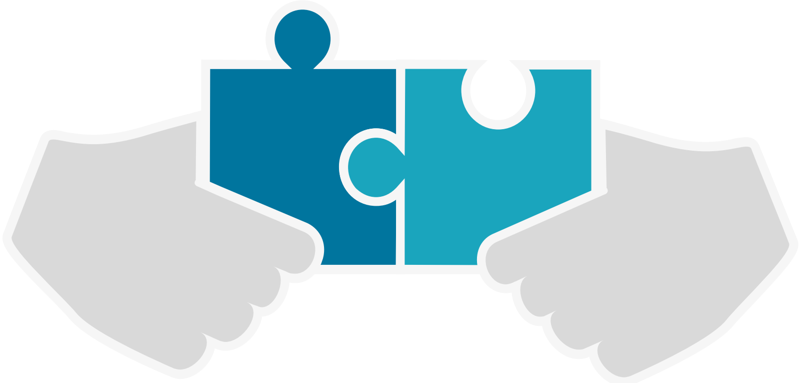
Compliance Approach

- Identify Your Organisation's Obligations and Responsibilities
  - ISO 27001:5, NIST 800-53, FedRAMP, SSAE 16 (SOC 1, SOC 2), PCI, HIPAA, EUMC and numerous others
- Adopt a Standard Control Set
  - Cross-referenced, extensible
- Establish Policies and Standards
  - Aligned to controls and lifecycle
- Document System(s) in Scope
  - Physical datacenters, Network, Infrastructure, Services and Components
- Develop narratives for each control
  - Hundreds++
- Test Control Design & Execution
  - Standardization and centralization to scale and drive best practices
- Identify Exceptions and Issues
  - Strive for excellence and drive continuous improvement
- Determine Risk Exposure
  - Not everything is critical and high risk
- Define Remediation Goals and Plans
  - Time, Quality, Effort
- Monitor the System
  - Define metrics, targets, decisions and performance indicators
- Report on Compliance Status
  - Map to obligations, responsibilities, asks and decisions

Compliance - Problem & Solution

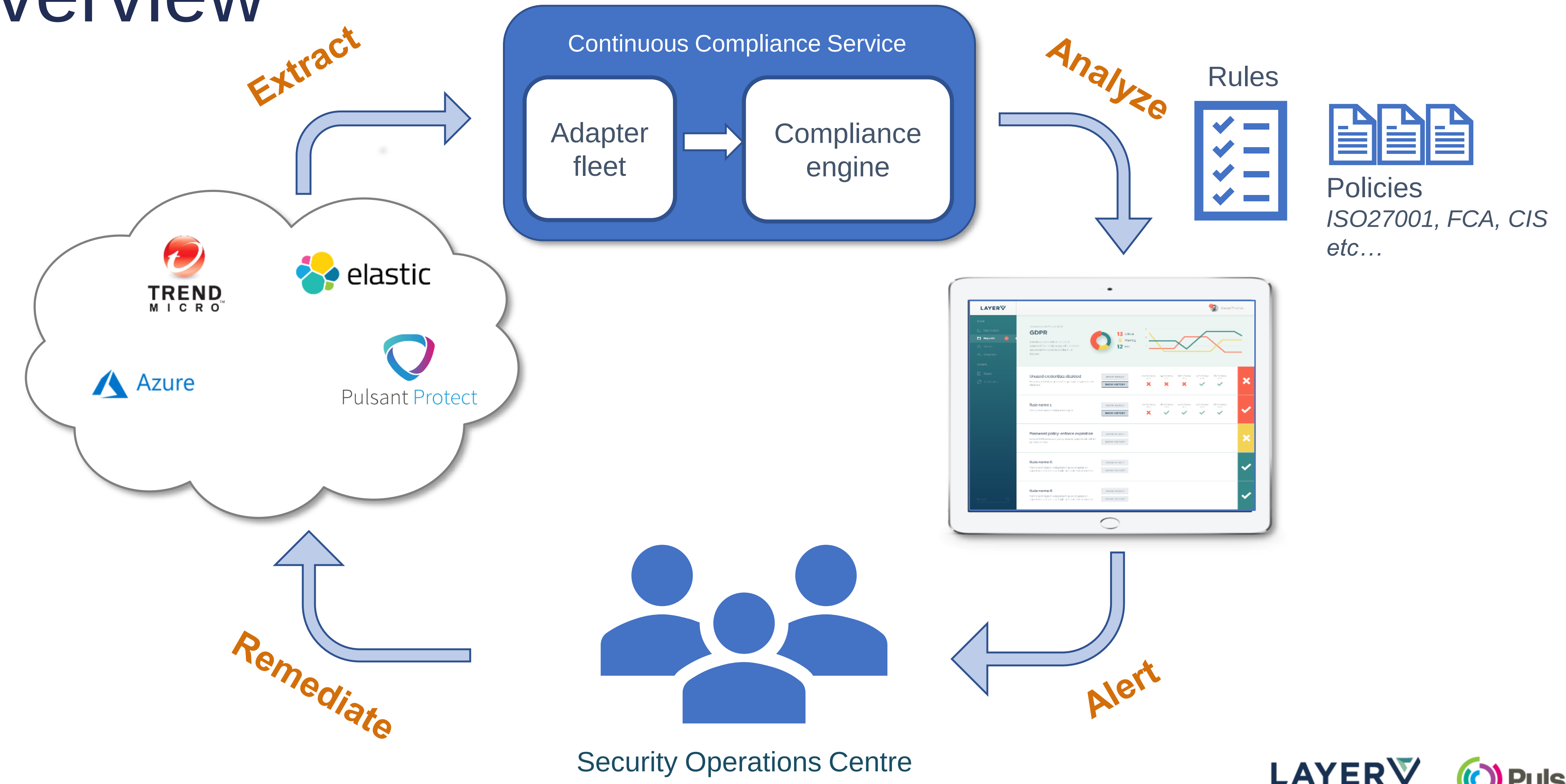


- **Risk** and **Reputation** therefore **COST!**
- Lack of **Compliance Visibility**
- Compliance affects **multiple systems** across **multiple tech stacks**
- Compliance **misunderstood**
- Too much **Manual effort**
- Off the shelf tools too **monolithic**



- ✓ Compliance state for **any** system and **any** data source
- ✓ **Dynamic** and **powerful** compliance engine
- ✓ Automated remediation mechanisms
- ✓ Aggregated view of the **whole** estate
- ✓ Near **real-time** assurance
- ✓ Historical data and trends

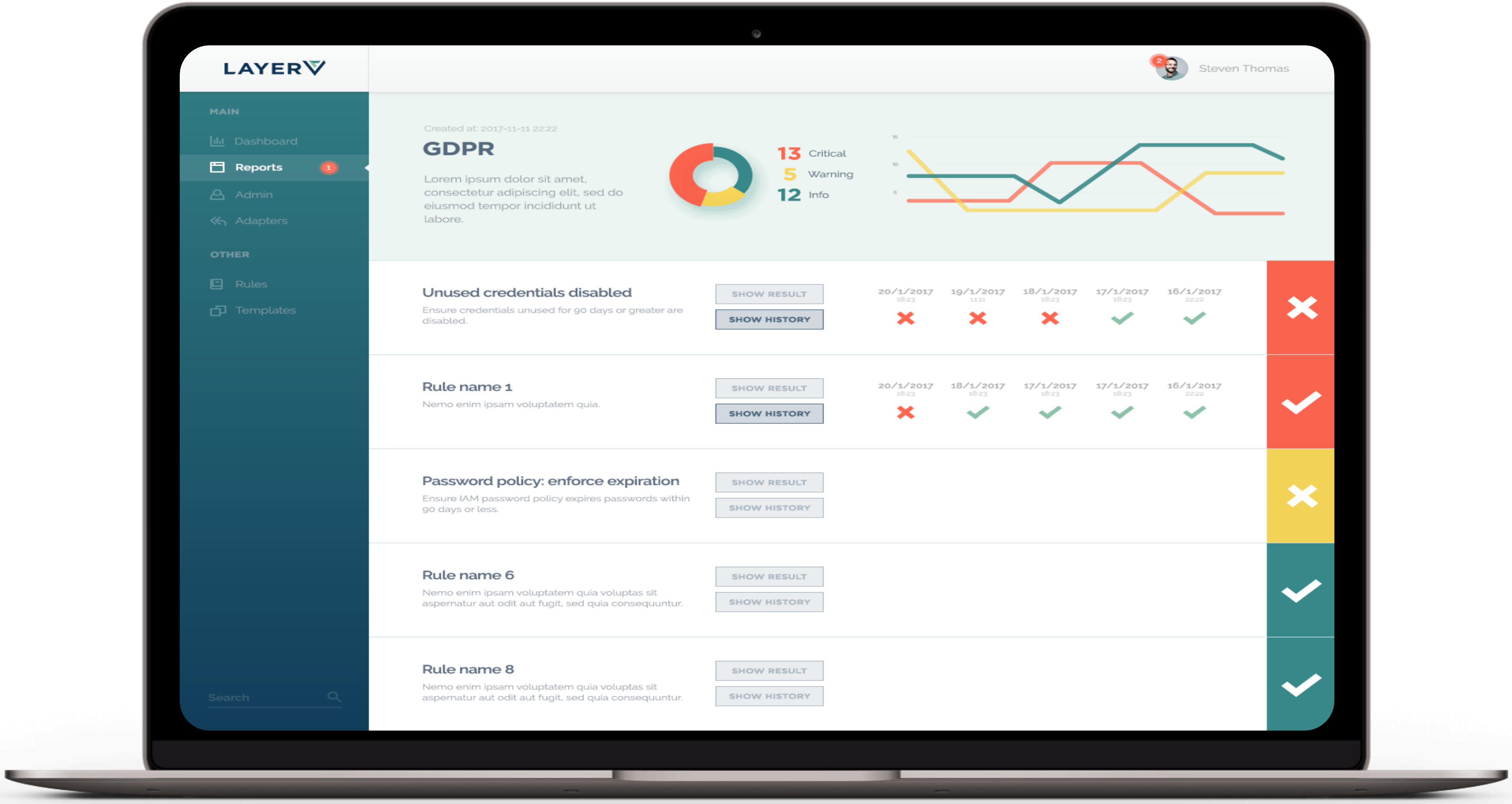
Overview


Extract
Continuous Compliance Service
Adapter fleet
Compliance engine
Analyze
Rules
Policies
ISO27001, FCA, CIS etc…
TREND MICRO
elastic
Azure
Pulsant Protect
Alert
Remediate
Security Operations Centre

Key Benefits

- Ready-to-use compliance templates
- ANY cloud, product, system
- Highly configurable & adaptable
- Single pane of glass
- Near real-time & continuous visibility
- Historical data and trends
- Proof of active monitoring for auditors
- Human and machine-readable output

CONTINUOUS COMPLIANCE



Created at: 2017-11-11 22:22

GDPR

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.

13 Critical
5 Warning
12 Info

		20/1/2017 18:23	19/1/2017 11:11	18/1/2017 18:23	17/1/2017 18:23	16/1/2017 22:22	
Unused credentials disabled Ensure credentials unused for 90 days or greater are disabled.	SHOW RESULT SHOW HISTORY	✗	✗	✗	✓	✓	✗

		20/1/2017 18:23	18/1/2017 18:23	17/1/2017 18:23	17/1/2017 18:23	16/1/2017 22:22	
Rule name 1 Nemo enim ipsam voluptatem quia.	SHOW RESULT SHOW HISTORY	✗	✓	✓	✓	✓	✓

Password policy: enforce expiration
Ensure IAM password policy expires passwords within 90 days or less.
SHOW RESULT
SHOW HISTORY
✗

Rule name 6
Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur.
SHOW RESULT
SHOW HISTORY
✓

Rule name 8
Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur.
SHOW RESULT
SHOW HISTORY
✓

Sample Policies

CIS Azure Benchmarks

GDPR technical controls (AWS/Azure)

Azure network security

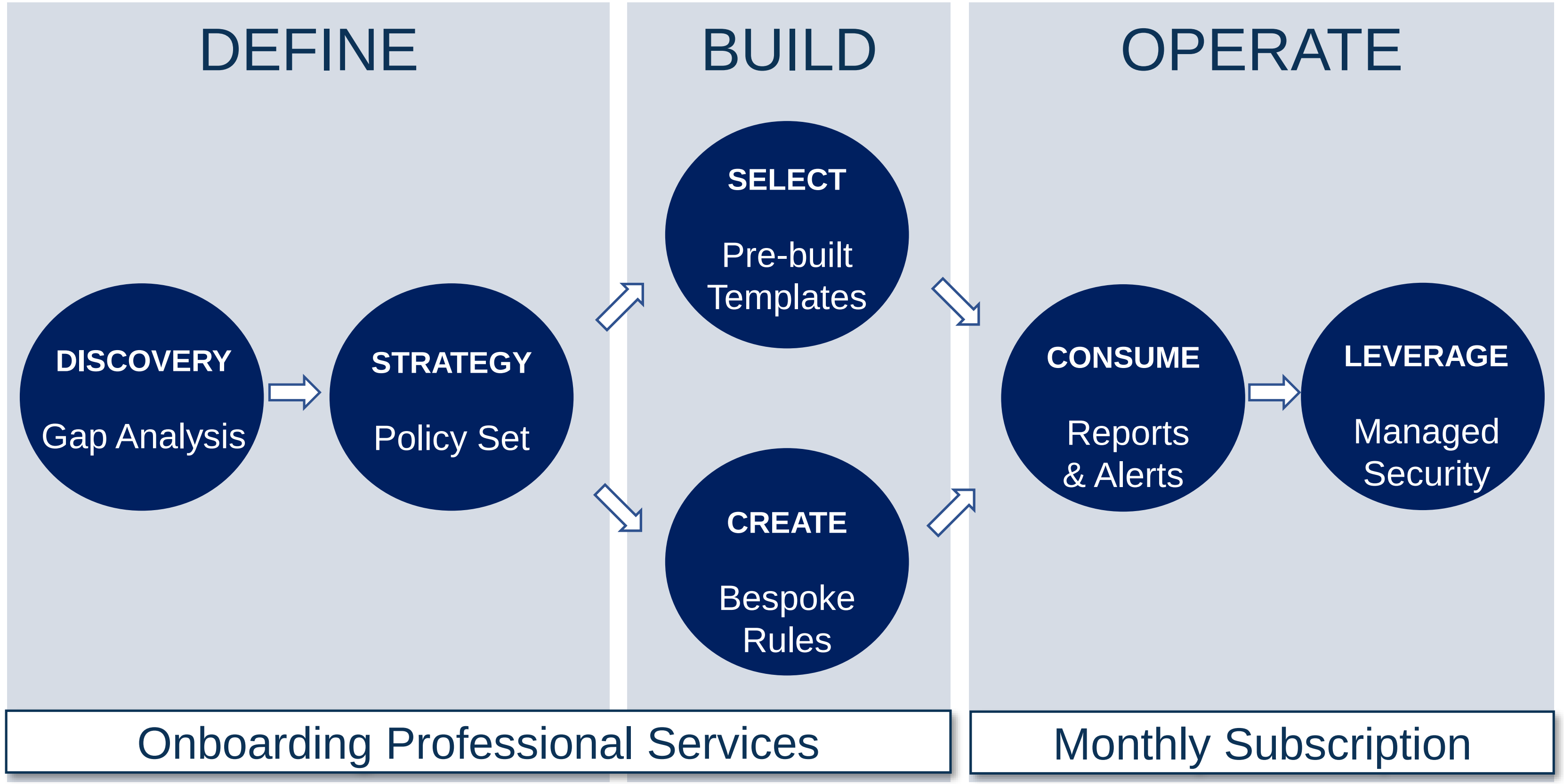
Any bespoke customer policy

ISO27001 selected controls

PCI-DSS selected controls

FCA selected controls

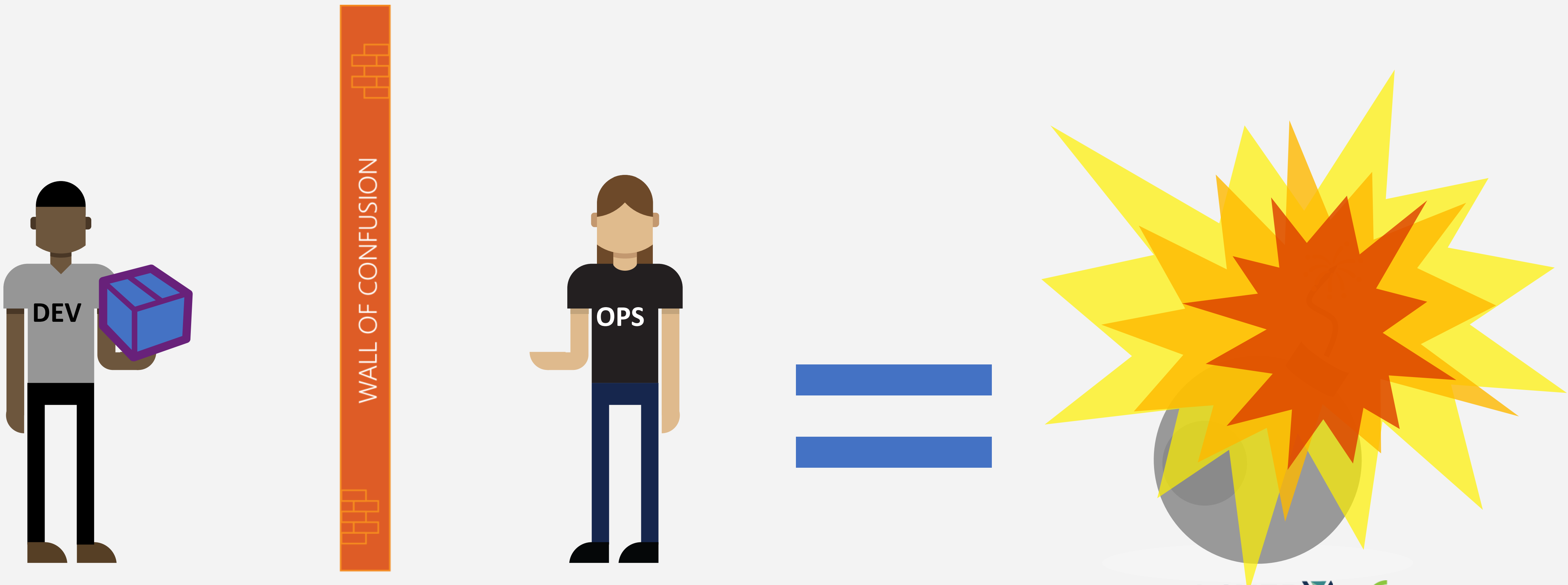
Onboarding


DEFINE
BUILD
OPERATE
DISCOVERY
Gap Analysis
STRATEGY
Policy Set
SELECT
Pre-built Templates
CREATE
Bespoke Rules
CONSUME
Reports & Alerts
LEVERAGE
Managed Security
Onboarding Professional Services
Monthly Subscription

To Summarise..

KEY TECHNICAL CAPABILITIES	BUSINESS BENEFITS
Central Auditing and Logging	Near Real-time 360º Managed Security Platform
Granular management of identities and access controls	“Out of the box” Comprehensive Security Coverage
Comprehensive monitoring for cloud platform, OS, applications and services	Confidence in your Cloud Security
Full integration with SIEM (Security Incident and Event Management)	Ensure compliance of your cloud against regulatory and industry requirements such as FCA, ISO27001, PCI
	Single Pane of Glass Dashboard

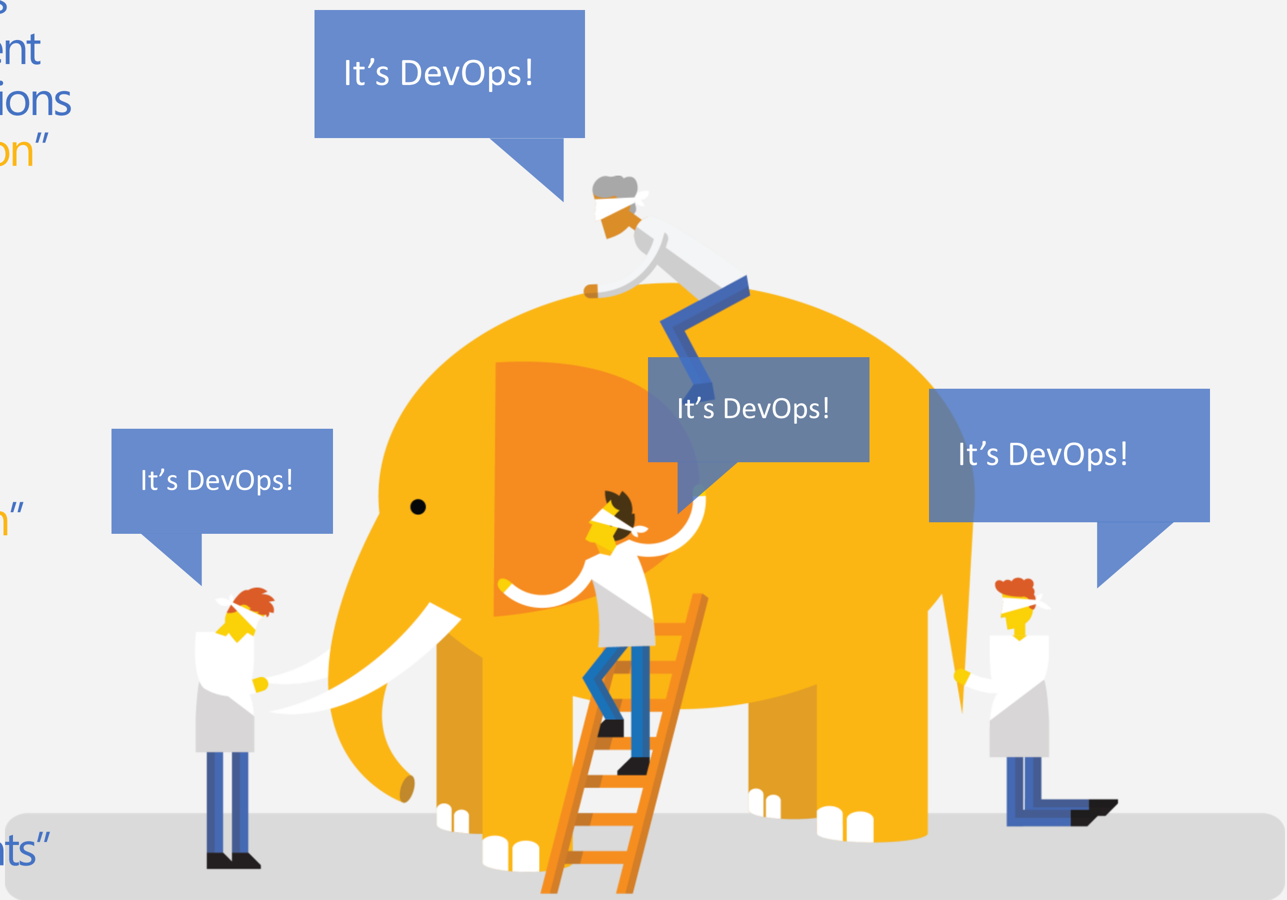
Traditional Development & Operations



"**DevOps** is development and operations collaboration"

"**DevOps** is using automation"

"**DevOps** is small deployments"

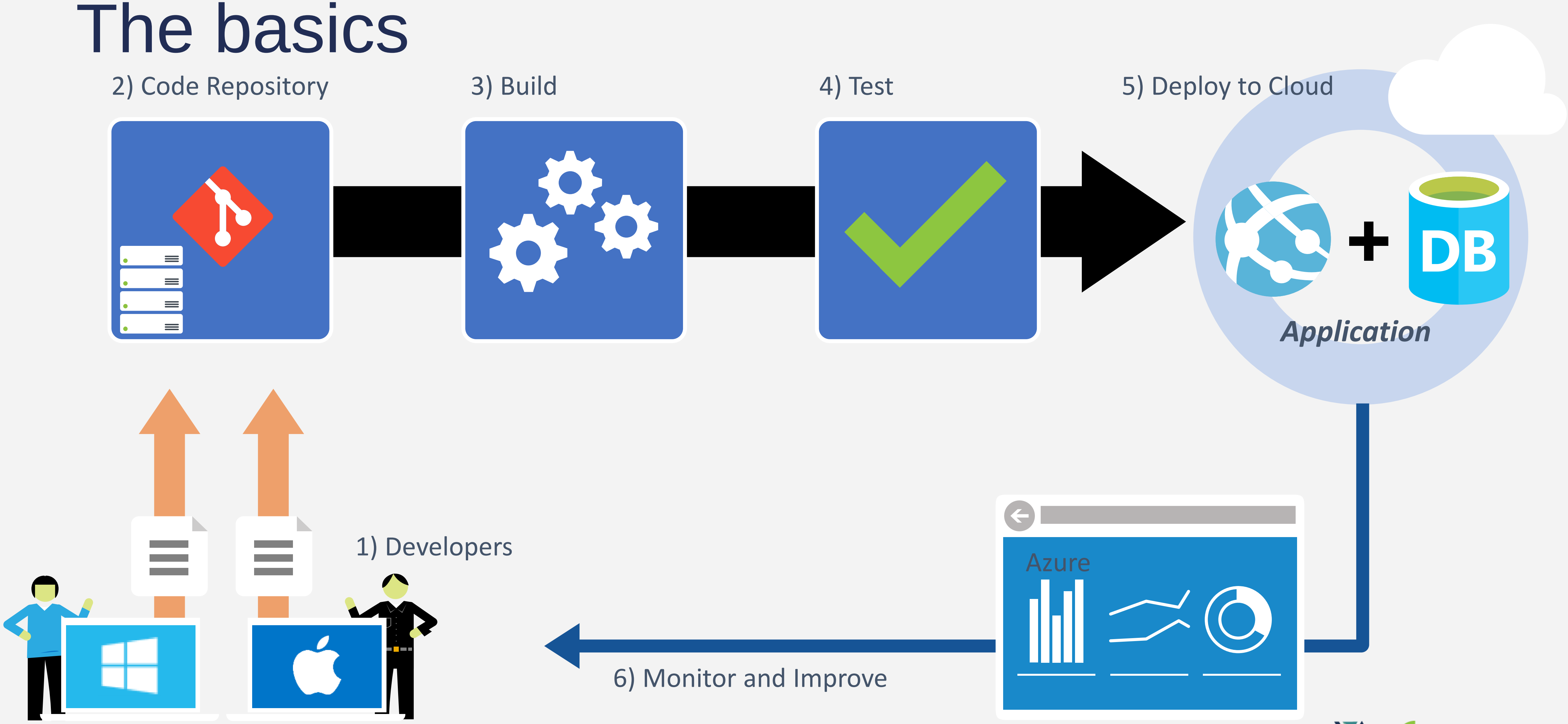


"**DevOps** is treating your infrastructure as code"

"**DevOps** is feature switches"

"Kanban for Ops?"

The basics



2) Code Repository

3) Build

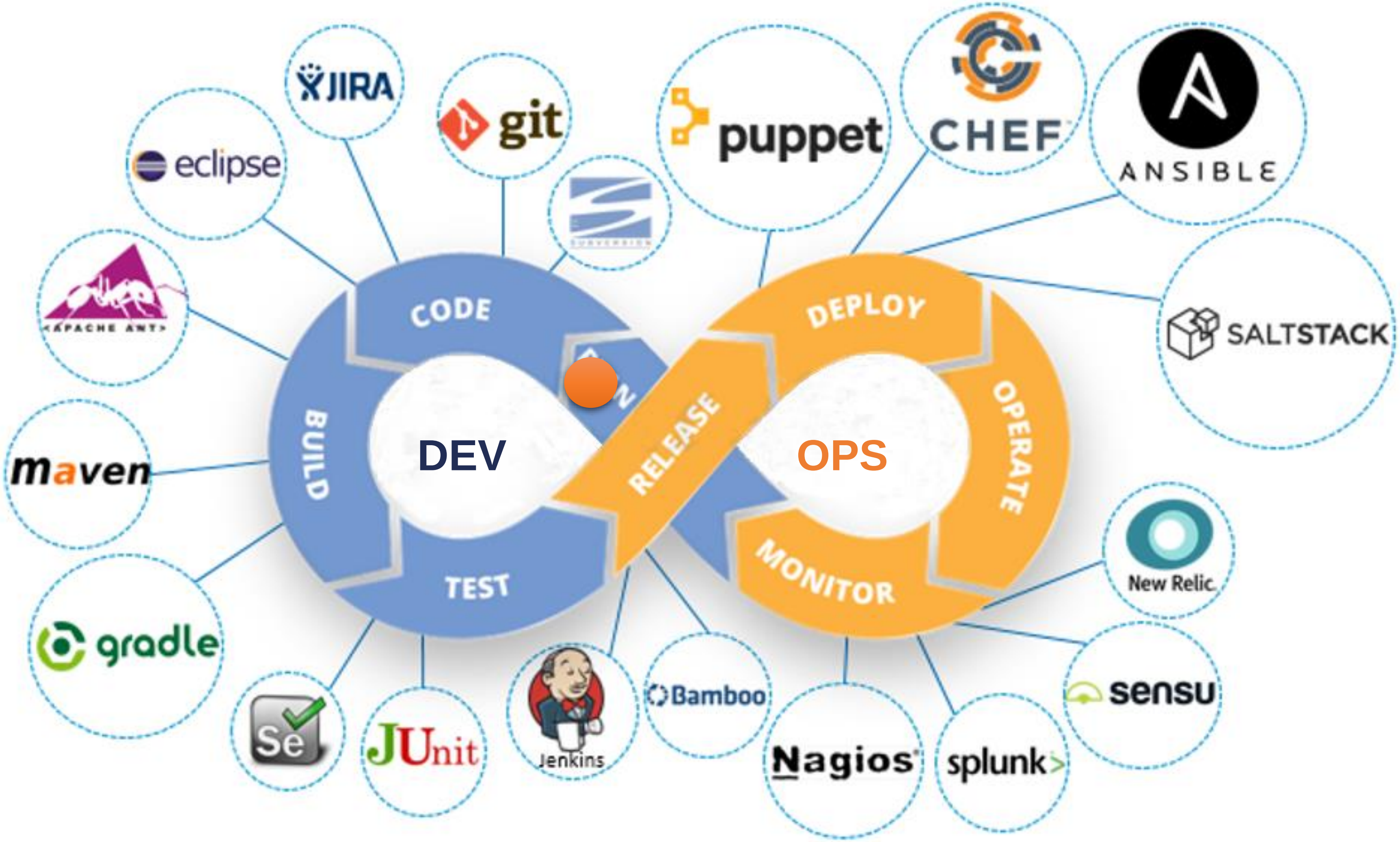
4) Test

5) Deploy to Cloud

1) Developers

6) Monitor and Improve

Lifecycle

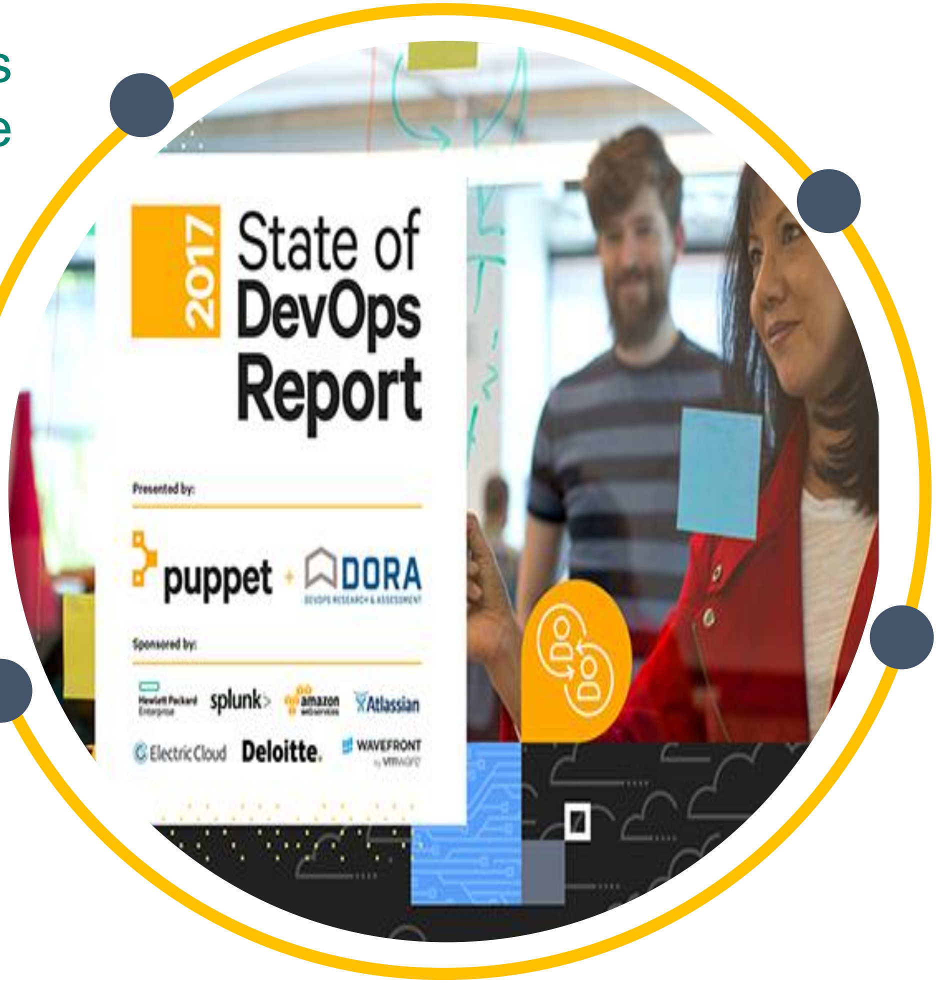

DEV
OPS
CODE
BUILD
TEST
PLAN
RELEASE
DEPLOY
OPERATE
MONITOR
JIRA
git
eclipse
APACHE ANT
maven
gradle
Se
JUnit
Jenkins
Bamboo
puppet
CHEF
ANSIBLE
SALTSTACK
New Relic
sensu
splunk>
Nagios

Benefits

Strong IT Performance is a competitive advantage

Firms with high-performing IT organisations were 2x as likely to exceed their profitability, market share, and productivity goals

DevOps Practices improve IT performance



2017

State of DevOps Report

Presented by:

puppet + DORA

Sponsored by:

Hewlett Packard Enterprise splunk> amazon web services Atlassian

ElectricCloud Deloitte. WAVEFRONT by vmware

Deploy code 46x faster

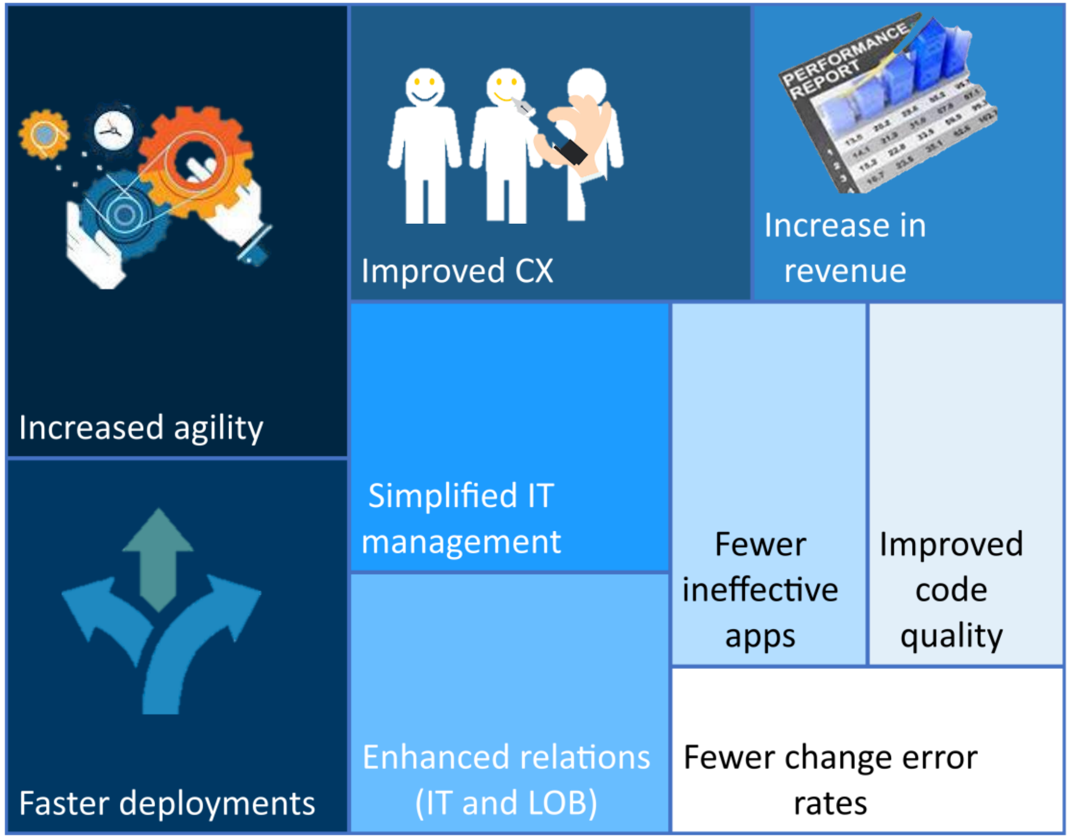
and with 440x shorter lead time as compared to their lower-performing peers

Have 60x fewer failures

and recover from failure 96x faster as compared to their lower-performing peers

Source: https://puppetlabs.com/

Drivers of DevOps Adoption



Increased agility

Improved CX

Increase in revenue

Faster deployments

Simplified IT management

Enhanced relations (IT and LOB)

Fewer ineffective apps

Improved code quality

Fewer change error rates

What are the primary drivers of wider DevOps adoption?

Speed and Throughput

Quality

Costs

Source: *European DevOps Survey*, 2016

Drive change across..

People

Unified Teams

Culture

"BiZ" Value and Metrics

Technology

Flexible, Secure, Automated

Business

Align-ment

Process

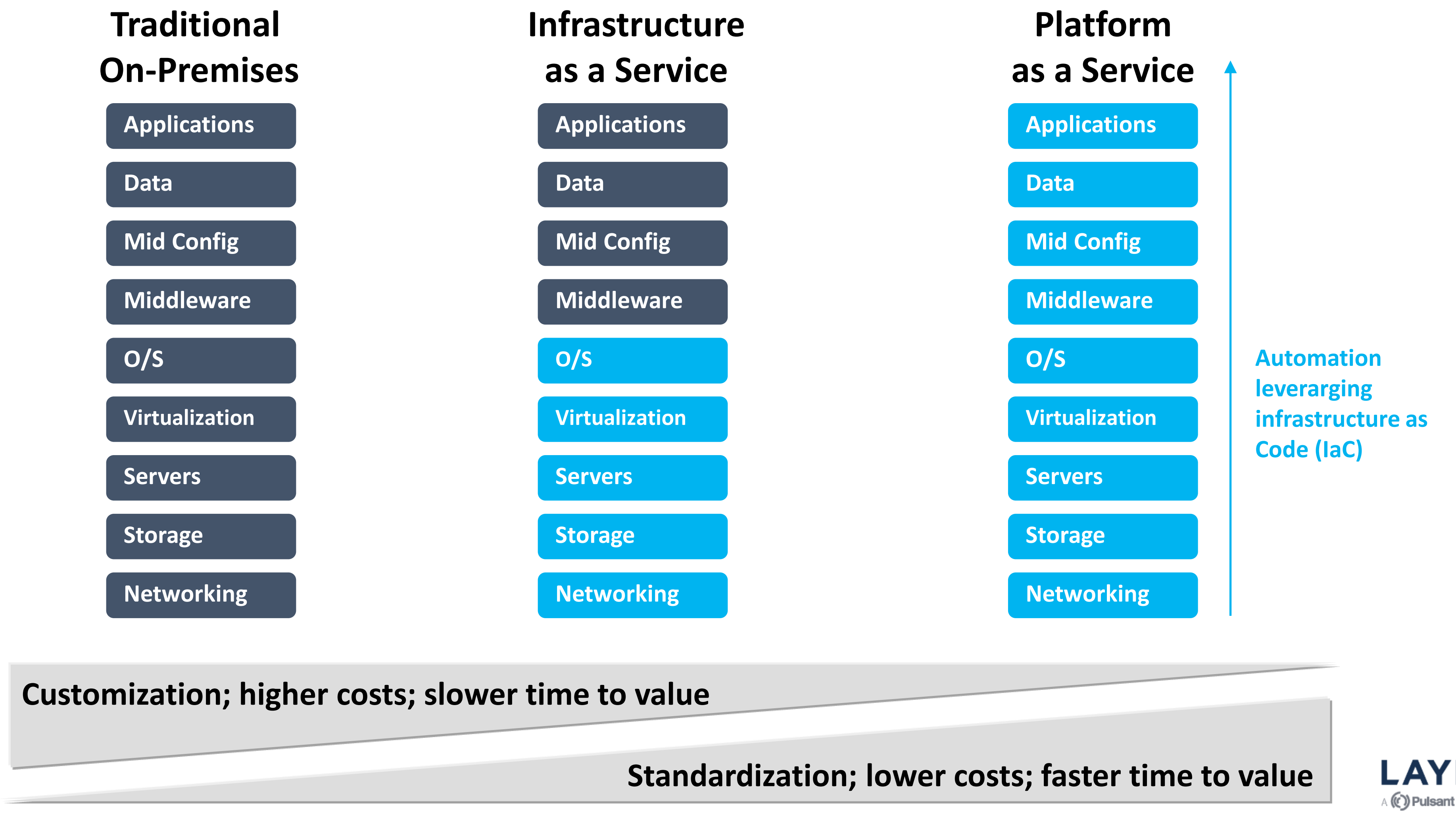
Standardsation

List of DevOps Practices

- Infrastructure as Code (IaC)
- Continuous Integration
- Automated Testing
- Continuous Deployment
- Release Management
- App Performance Monitoring
- Load Testing & Auto-Scale

- Availability Monitoring
- Change/Configuration Management
- Feature Flags
- Automated Environment De-Provisioning
- Self Service Environments
- Automated Recovery (Rollback & Roll-Forward)
- Hypothesis Driven Development
  - Testing in Production
  - Fault Injection
  - Usage Monitoring/User Telemetry

Automating for faster delivery with DevOps and cloud



Traditional On-Premises	Infrastructure as a Service	Platform as a Service
Applications	Applications	Applications
Data	Data	Data
Mid Config	Mid Config	Mid Config
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking

Automation leverarging infrastructure as Code (IaC)

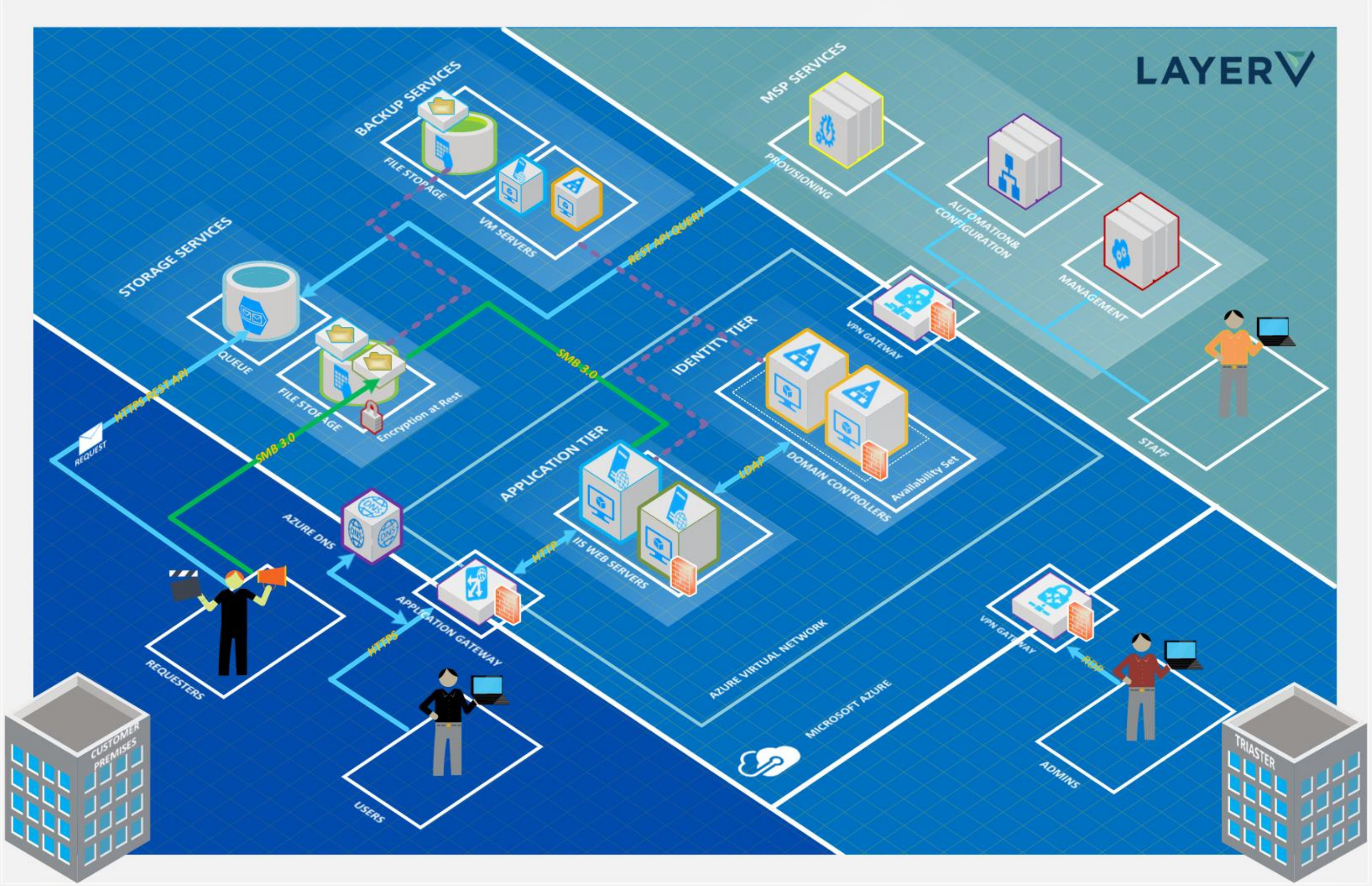
Customization; higher costs; slower time to value

Standardization; lower costs; faster time to value

DEVOPS

Case Study

TRIASTER



SaaS BPM Collaborative Solution

Challenges

- Hardware/VMWare based solution running on mixed vendors
- 5 week Onboarding!
- Operational complexities

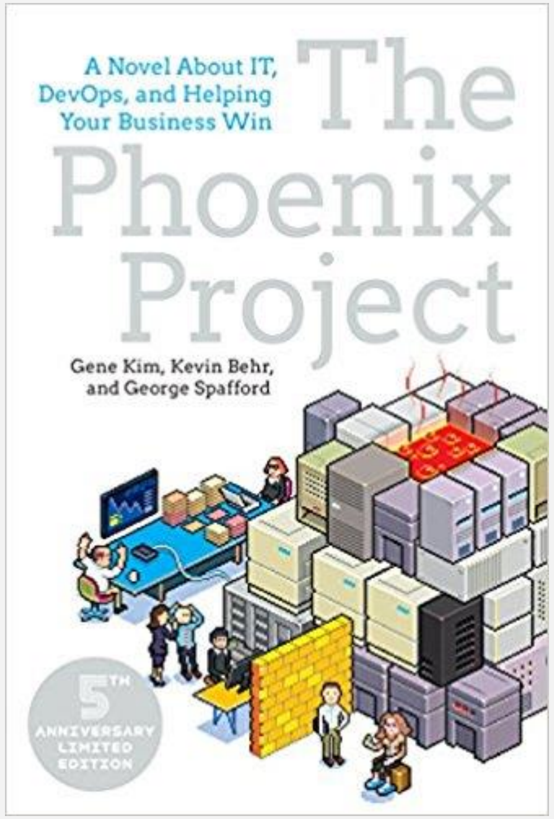
Solution

- Azure based stack
- Fully automated infrastructure deployments
- Self serving provisioning
- **5min deployments**

LAYERV A Pulsant Company

Pulsant Business Unlimited

Worth a read..


A Novel About IT, DevOps, and Helping Your Business Win
The Phoenix Project
Gene Kim, Kevin Behr, and George Spafford
5TH ANNIVERSARY LIMITED EDITION

The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win

Happy DevOps