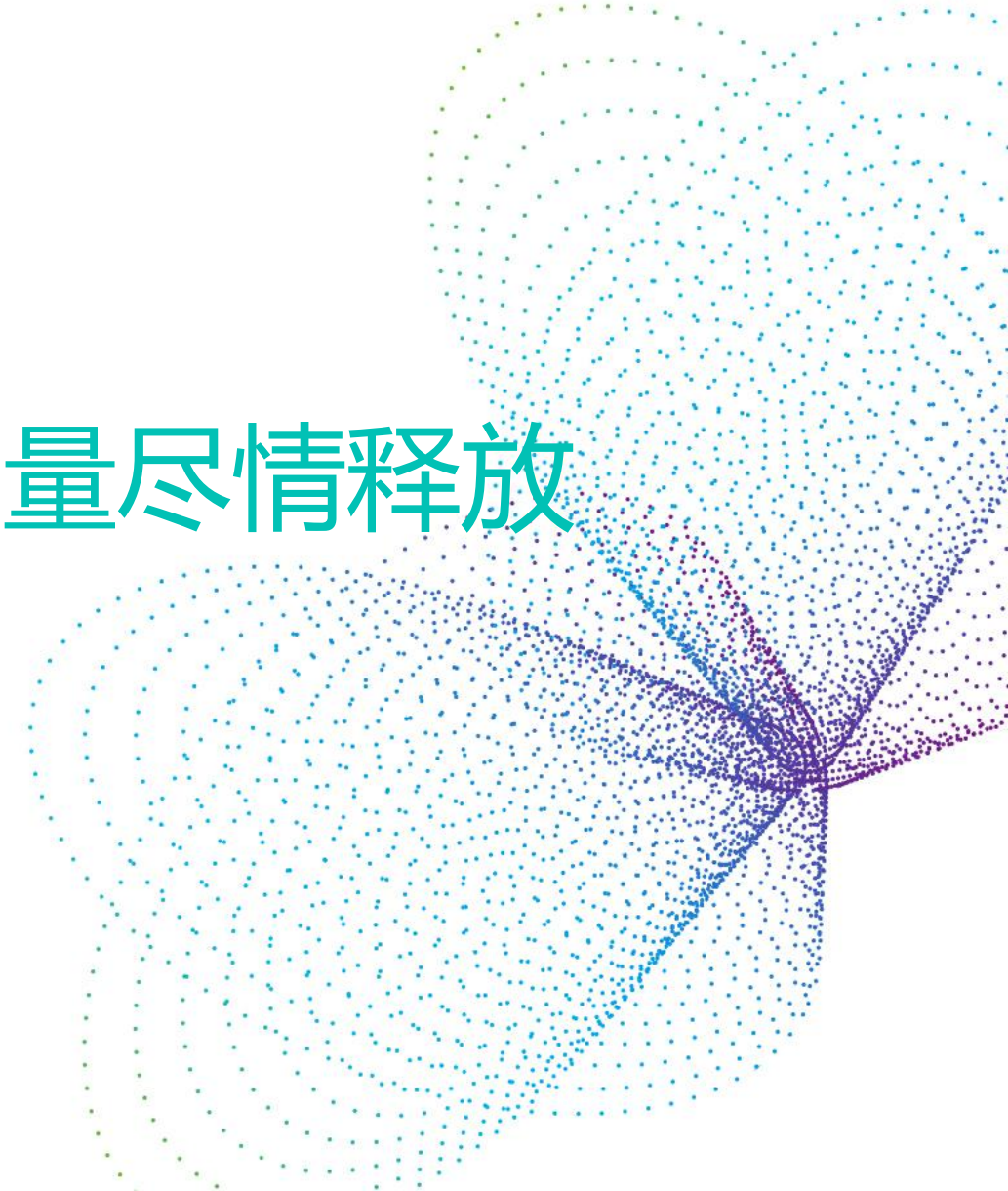
CAICT 中国信通院

TRUCS2019
TRUSTED CLOUD SUMMIT
可信云大会
中国·北京　2019.7.2-3

云原生安全，让创新的能量尽情释放

演讲人：杨海涛
Pivotal云计算资深架构师



要速度还是要安全?

科技大大提升了创新的速度并且可以带来全新的客户体验

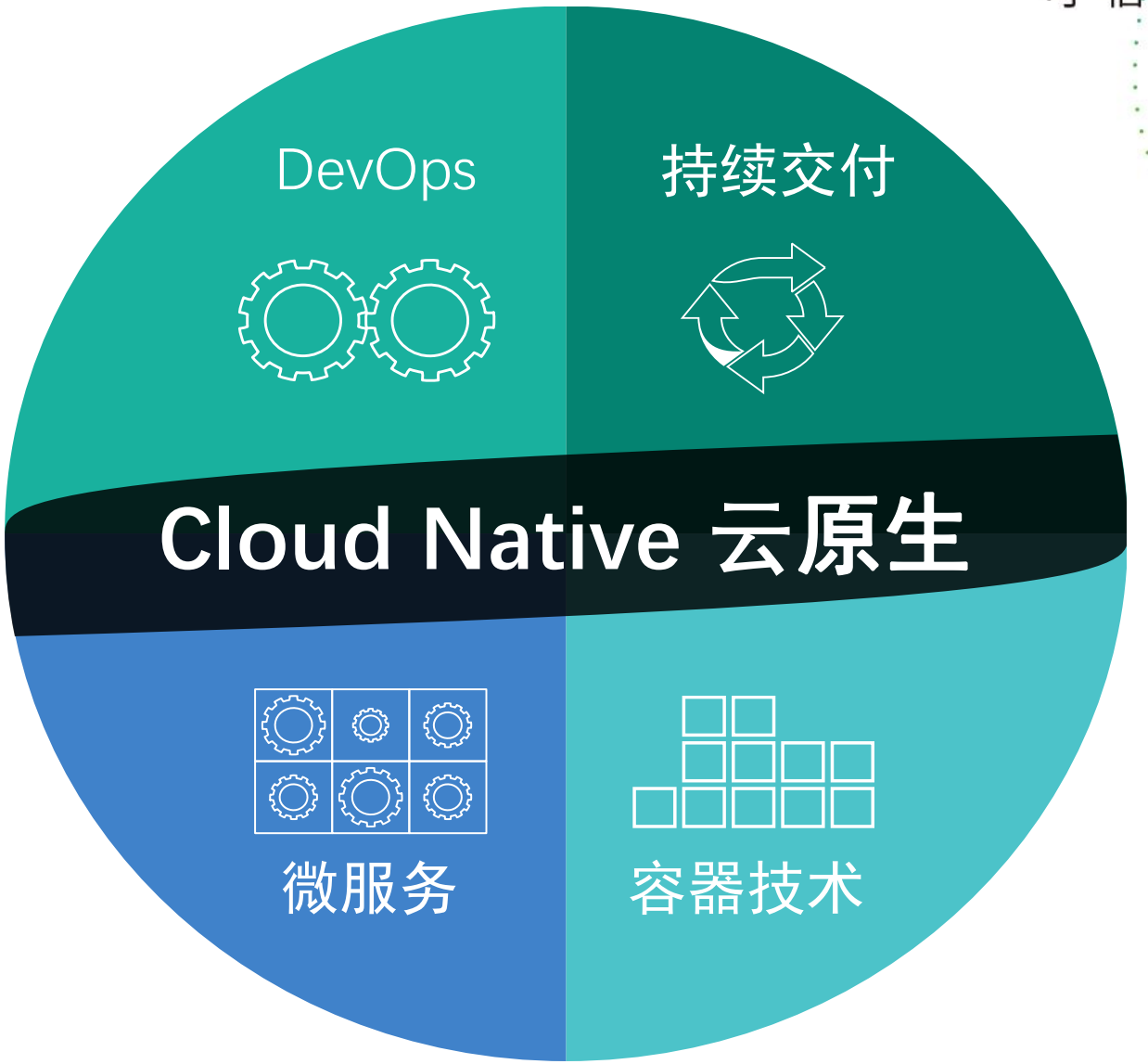
速度

vs

网络攻击从频率, 复杂性以及破坏后果等各方面都在显著上升

安全

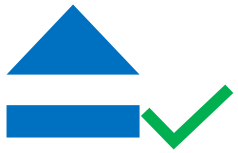
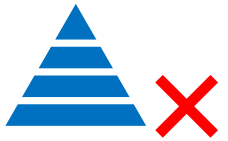
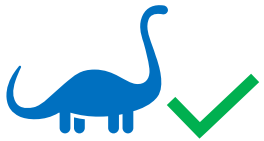
云原生的特征



Pivotal

传统企业安全工具的困境

传统安全工具：

	传统应用环境(包括IaaS)	云原生环境
应用数量		
应用部署频率		
平台架构		
平台状态		

Pivotal

现代安全的目标

对业务和用户减少风险

实践

- 对核心系统一定要打上所有重要的安全补丁
- 经常轮换服务的密钥
- 移除可能有重大影响的配置项

让安全容易落地，更加简单

实践

- “安全是默认的”
- 与具体云平台无关
- 不可变基础设施
- 可以消费的服务 (IAM, 日志, 证书, 密钥)

对恶意行为可以进行检测并快速作出反应

实践

- 日志和监控
- 对于行为的综合监控
- 最小化的软件
- 自动触发反应

遵循行业规范

实践

- 内嵌的操作系统
- 继承控制
- 使用现有的身份认证系统
- 可以审计的配置代码
- 多租户

Pivotal

云原生安全：速度 + 安全

Pivotal

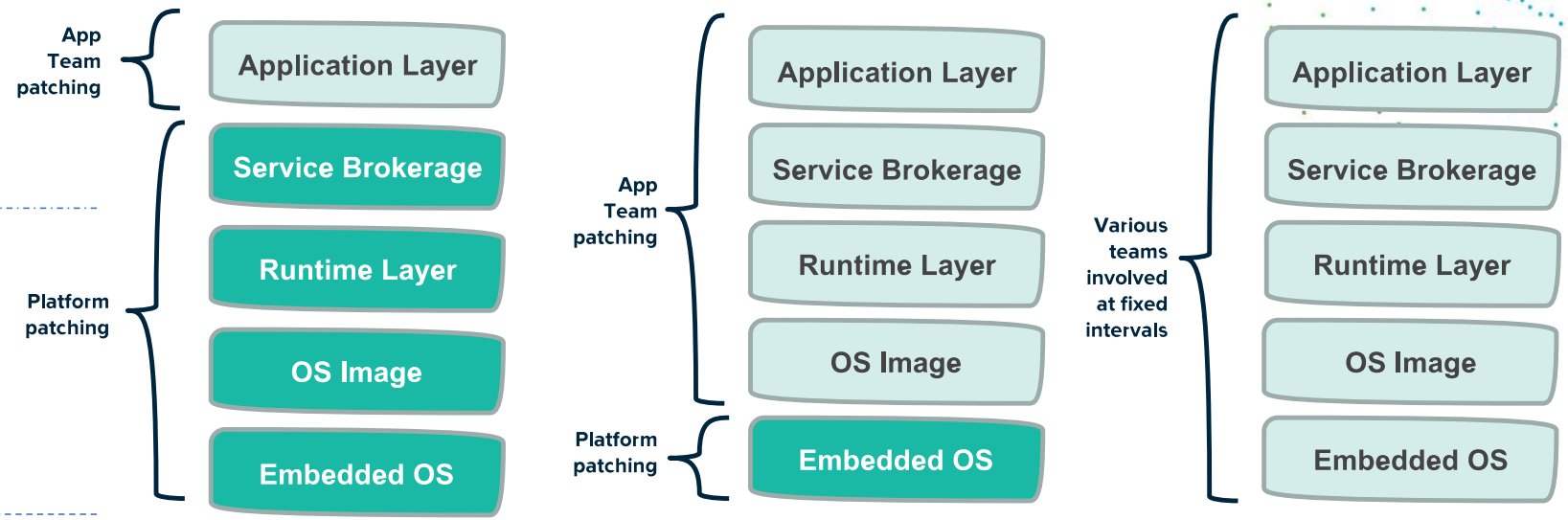
大规模降低风险的平台层手段

等级保护2.0

NIST

PCI DSS COMPLIANT

CIS Center for Internet Security®



平台安全

安全内置: 加密, 身份认证服务, 日志, 操作系统隔离, 不变的基础设施

最佳实践: 0停机打补丁, 定期更换密码和运行环境

全自动化更新来减少人工错误带来的风险

IaaS

私有云1 私有云2 公有云1 公有云2 公有云3

Pivotal

云原生安全的四要素

修补

只要有新的版本，马上升级有漏洞的软件系统.

Repair

重新部署

经常性的重新部署服务器和应用

Repave

轮换

经常性的轮换用户密钥, 这样它们只在短期有效.

Rotate

内置合规性

内嵌操作系统，对应用的控制来自于平台, 简化审计.

减少您的平均修补时间 | 抵御更高级的驻留性的网络攻击 | 减少泄漏密钥的风险

"3R"

Pivotal

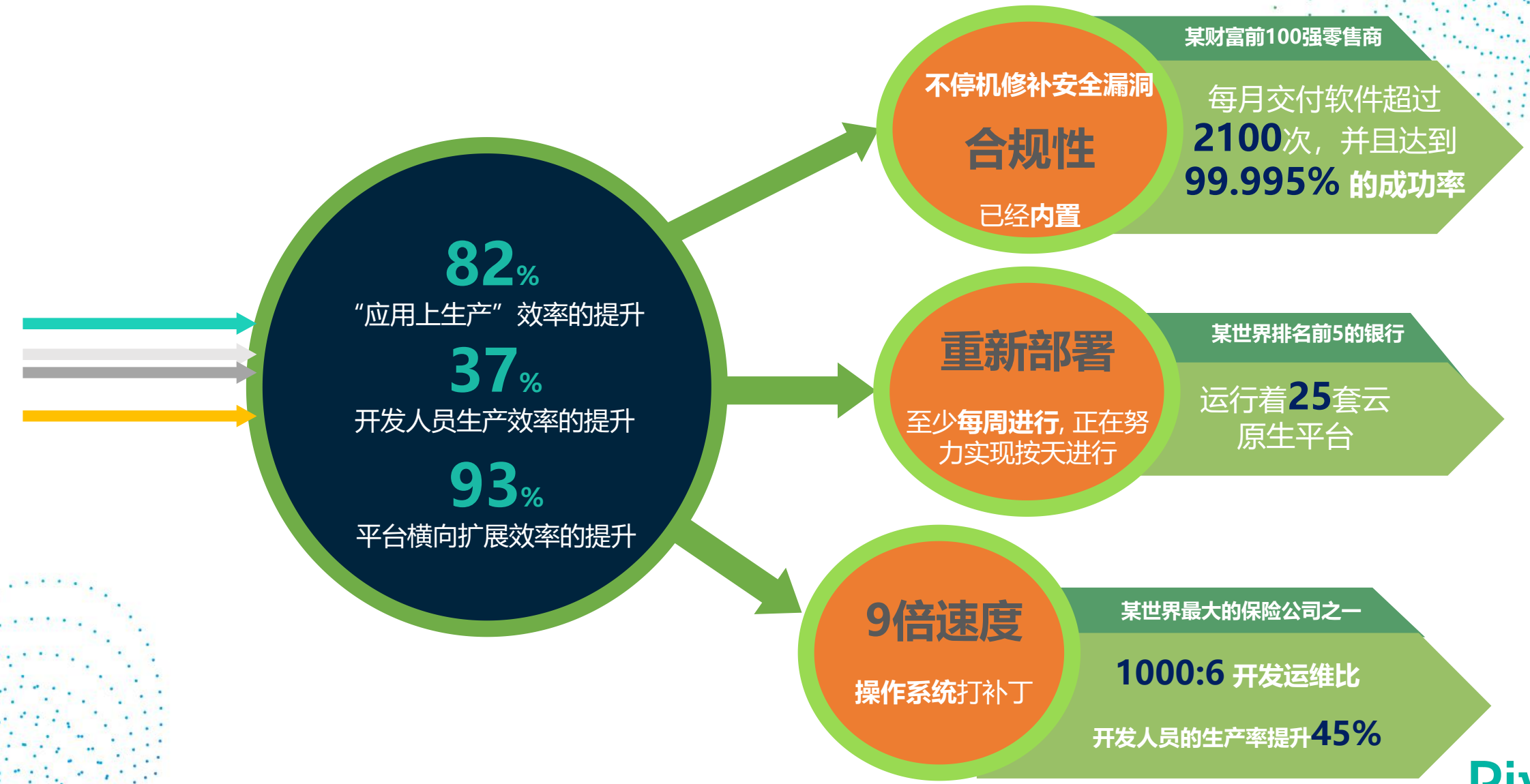
平台的DevOps对安全带来的好处

快速的软件发布速度	更快地打补丁
不可变基础设施	更快地恢复 对生产系统减少人为修改 更小的攻击窗口 更容易实现故障的跨云可重现
Configuration as Code	更高的一致性，易于审计 持续的安全监控
平台产品化	对安全问题有更大责任

Pivotal

云原生安全的好处显而易见

TRUSTED CLOUD SUMMIT
可 信 云 大 会



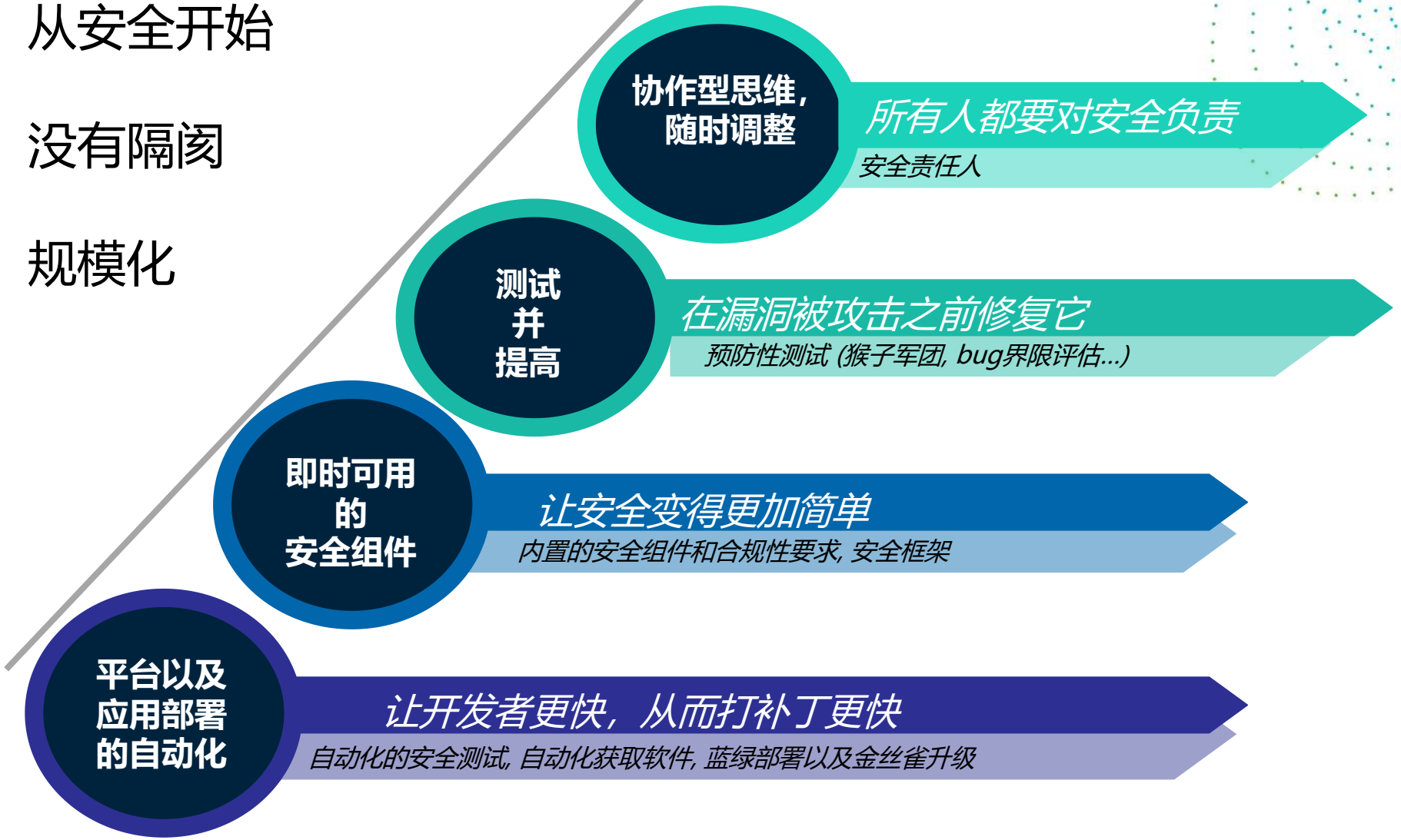
Pivotal

超越平台:
持续改进的结果和指标衡量

从安全开始

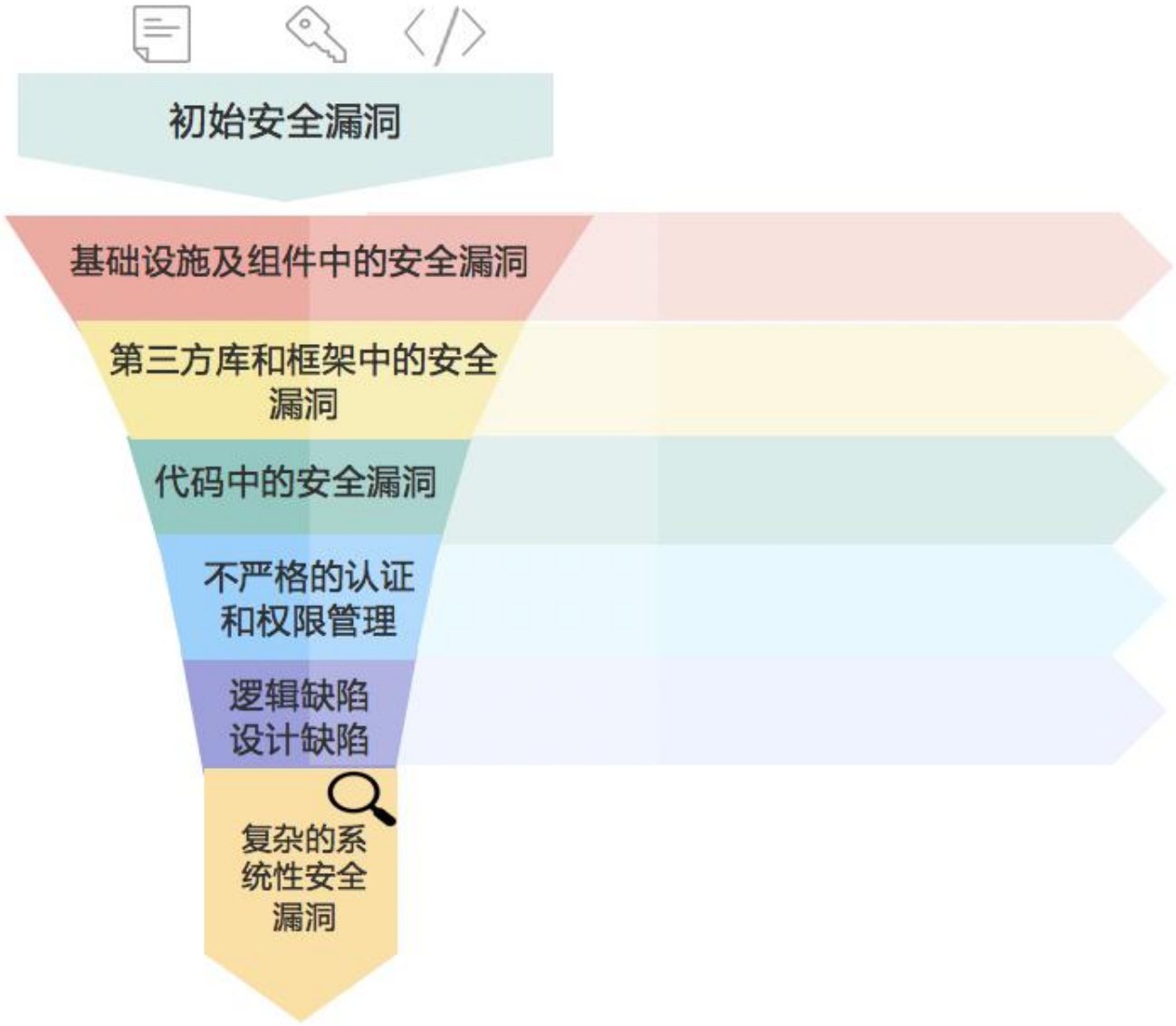
没有隔阂

规模化



Pivotal

深度防御的最佳实践



实现

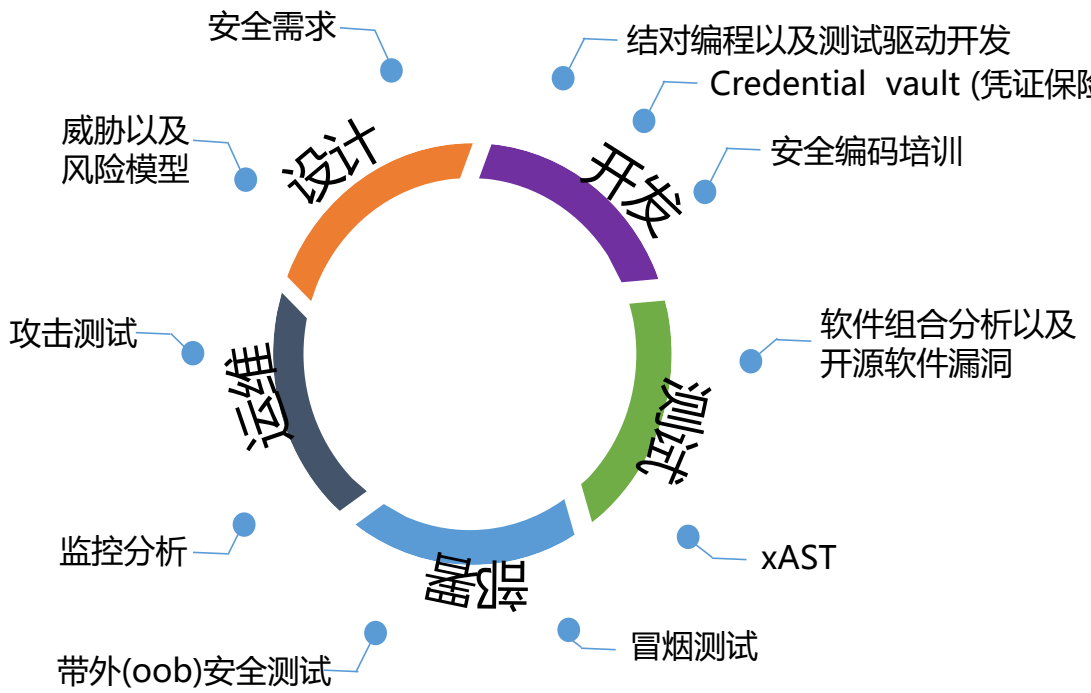
- 更多来自平台的本地化控制
- 尽可能自动化
- 尽快修复测试中发现的问题
- 持续对全栈进行侵入式测试
- 积极评估并调整改进计划

避免

- 不断叠加各种软件工具
- 试图用一个方案解决所有问题
- 用手工的方法去配置和部署安全解决方案 (防火墙, 应用防火墙, 网络加密...)
- 忽视主动检测的力量: 这才是防范攻击的最有效办法

Pivotal

通过全流程管理机制，全面管控应用风险



重点 方法	威胁以及风险模型：避免系统级漏洞
	安全编码培训：避免代码实现中的漏洞
	软件组合分析以及开源软件漏洞（Source Composition Analysis & Open Source Security）：确保第三方安全
	xAST(SAST/DAST/IAST): 通过白盒，黑盒以及交互测试，寻找应用实现中的漏洞
	OOB（Out-Of-Band Testing）：防止SQL注入，命令注入等恶意攻击
	攻击测试（Adversarial Testing）：模拟真实的网络攻击，测试系统健壮度

Pivotal

持续改进的路径：定义安全目标和指标

安全流程: 提升速度，快速修复问题

- 打补丁的速度
- 检测的时间 / 恶意窥探的时间
- 软件发布效率 (编码的时间 vs 测试的时间)
- 测试工具的正确性 (False Positives / False Negatives)

系统弹性: 提高响应和恢复的速度

- 平均恢复时间
- 上一次系统重建的时间?

降低风险: 从源头进行控制

- 测试覆盖率 (TDD)
- 打补丁的周期
- 凭证和密码轮换的周期
- 已经找到并测试过的安全风险场景
- 生产环境下的人工变更次数

组织领导者:

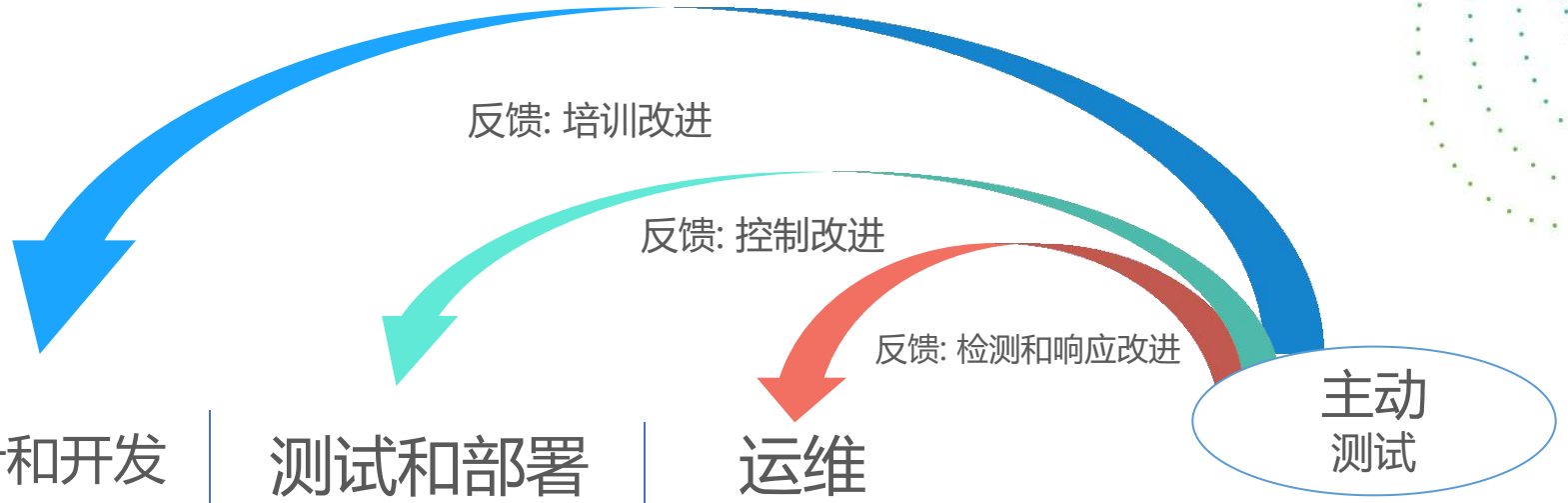
安全的DevOps

持续改进计划


持续改进的重要原则：平台保持开放，符合标准，与开源社区同步！
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path
l.cncf.io
CLOUD NATIVE COMPUTING FOUNDATION
CLOUD NATIVE Landscape
Amplify
Pivotal

主动防御策略

在被攻击之前找到漏洞: 主动测试



设计和开发

安全编码培训
威胁模型
安全框架
安全情报交换

测试和部署

TDD
xAST / RASP
单元测试

运维

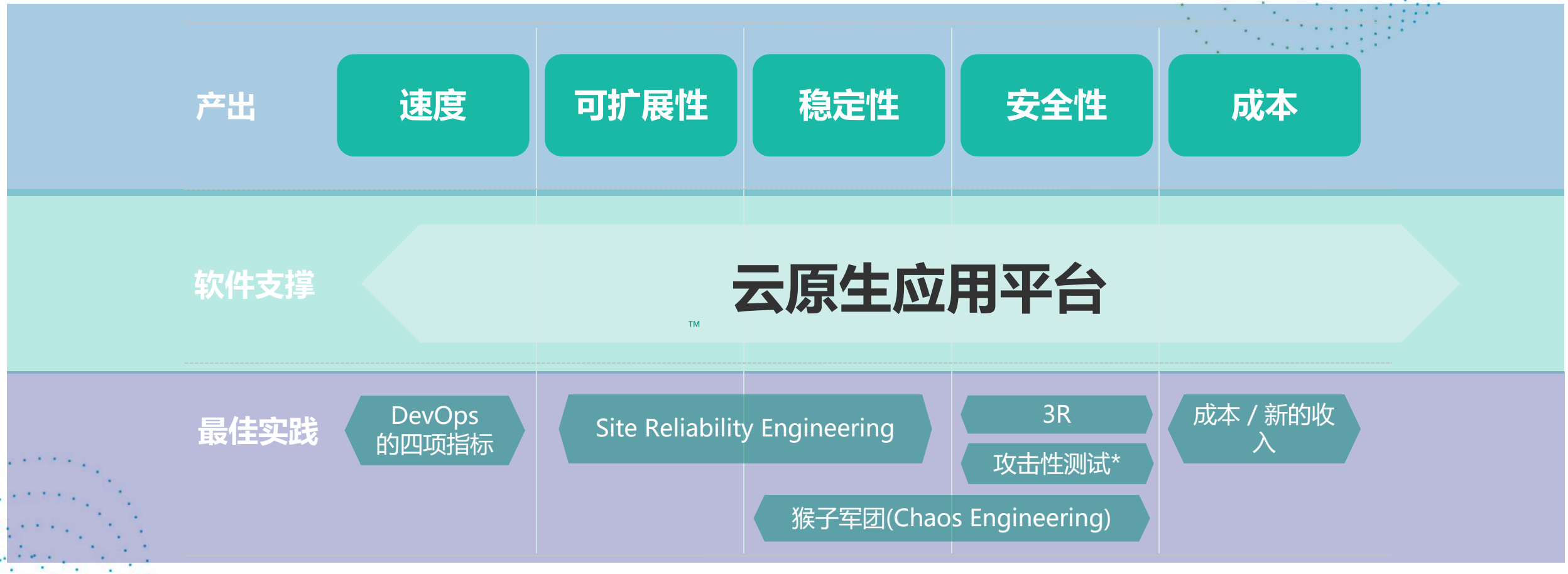
日志监控
防御模型
行为分析
自适应身份认证
安全响应编排（Response Orchestration）

主动检测还是事后补救？ 这直接决定了安全问题只是一个威胁，还是会变成灾难性的事故。减少检测和修复的时间应是整个组织的共同目标

* RASP(Runtime Application Self-Protection): 运行时应用自我保护机制

Pivotal

信任但是要验证: 平台之外的最佳实践

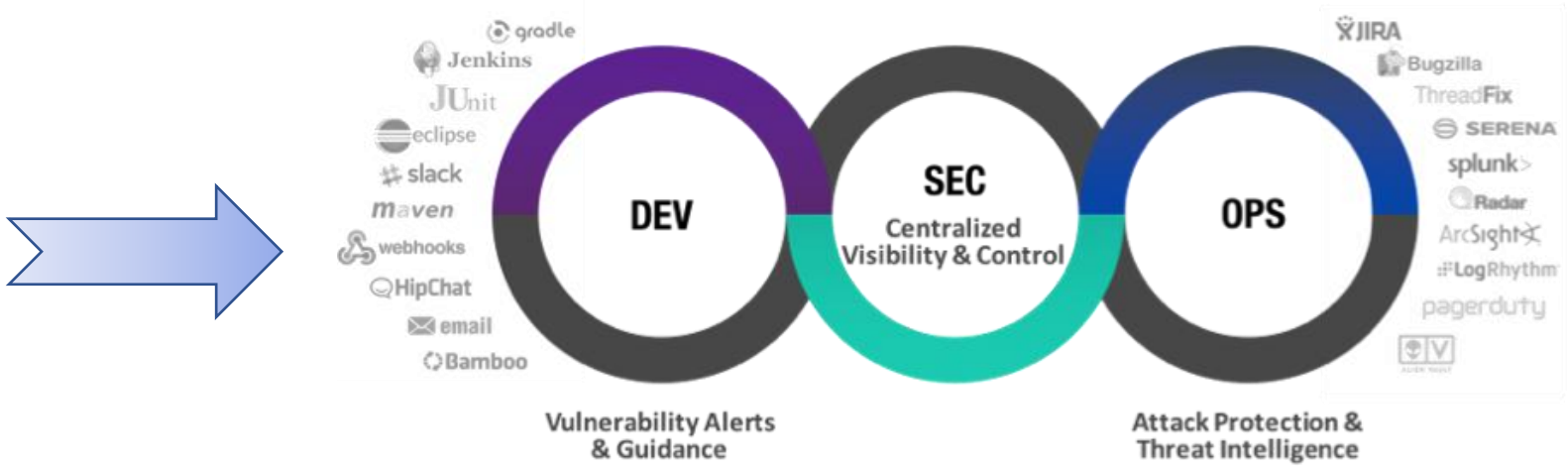


* *攻击性测试：包括漏洞举报奖励, 安全对抗团队, 模拟攻击, 穿透性测试等*

Pivotal

安全威胁不断演进

将您的平台视作一个持续改进的产品，满足不断变化的用户需求，同时沉着应对日益严峻的安全威胁。



Pivotal

博采众长

内外兼修

日益精进

Thank You!

TRUSTED CLOUD SUMMIT
可 信 云 大 会

- 官方微信：pivotal_china
- 中文官网：Pivotal.io/cn
- 技术咨询：400 135 8900
- 电子邮件：greaterchina_marketing@pivotal.io
- 白皮书下载：

  https://cn.content.pivotal.io/white-papers

Pivotal