解开安全的九连环：闭环、自动化和软件定义

Security Unchained: Closed Loop, Automated, and Software Defined

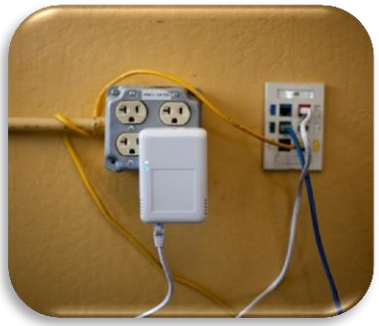
赵 粮

首席战略官，绿盟科技

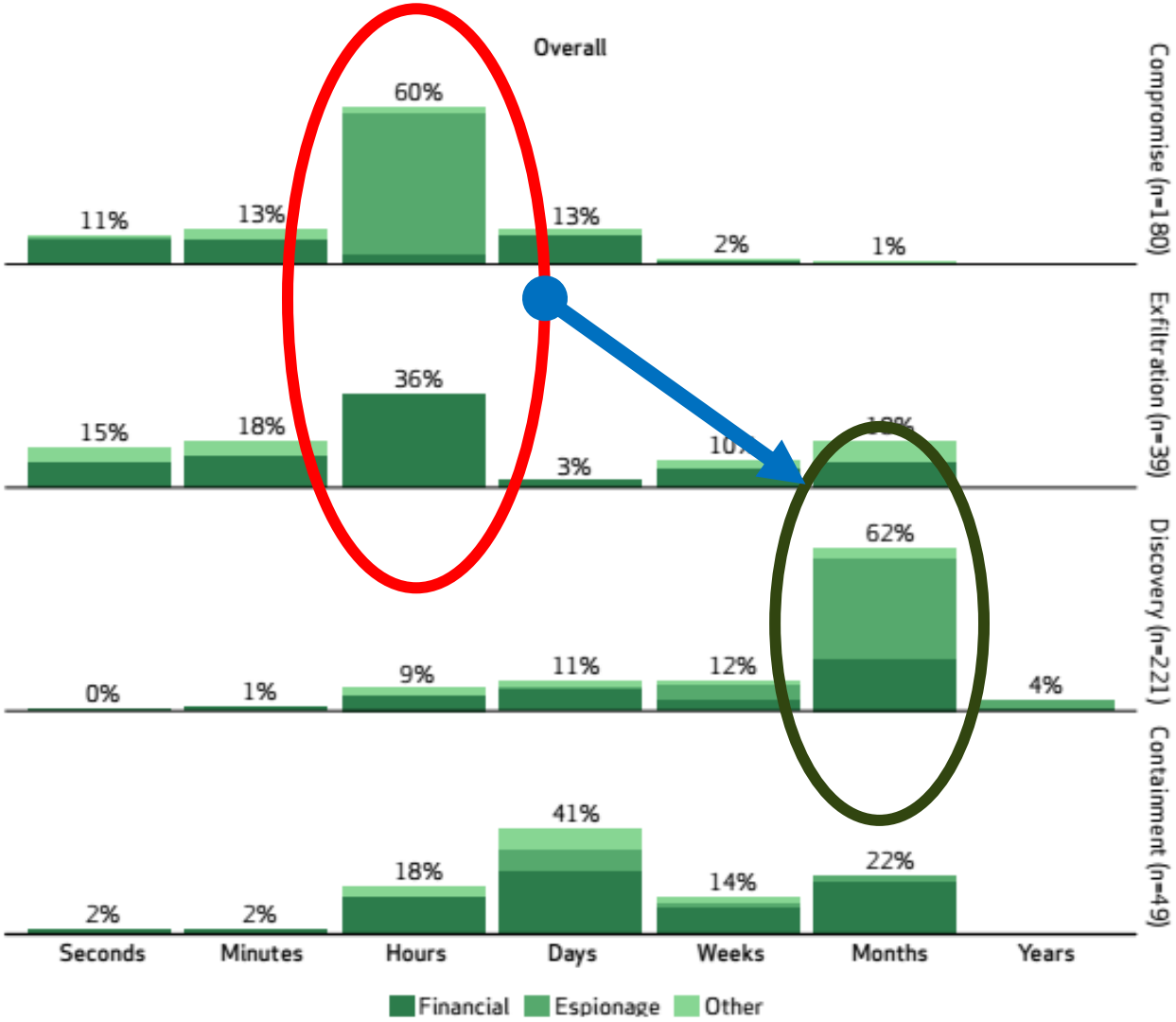
April.24 2014

层出不穷，无处不在的安全威胁

- 攻击被清除了没有？入侵深度？
- 攻击从什么时候发生的？还会再发生吗？
- 损失有多大？未来如何避免或控制损失？
- 当前安全资源投入足够吗？有效吗？
- 应该DIY还是外包？…



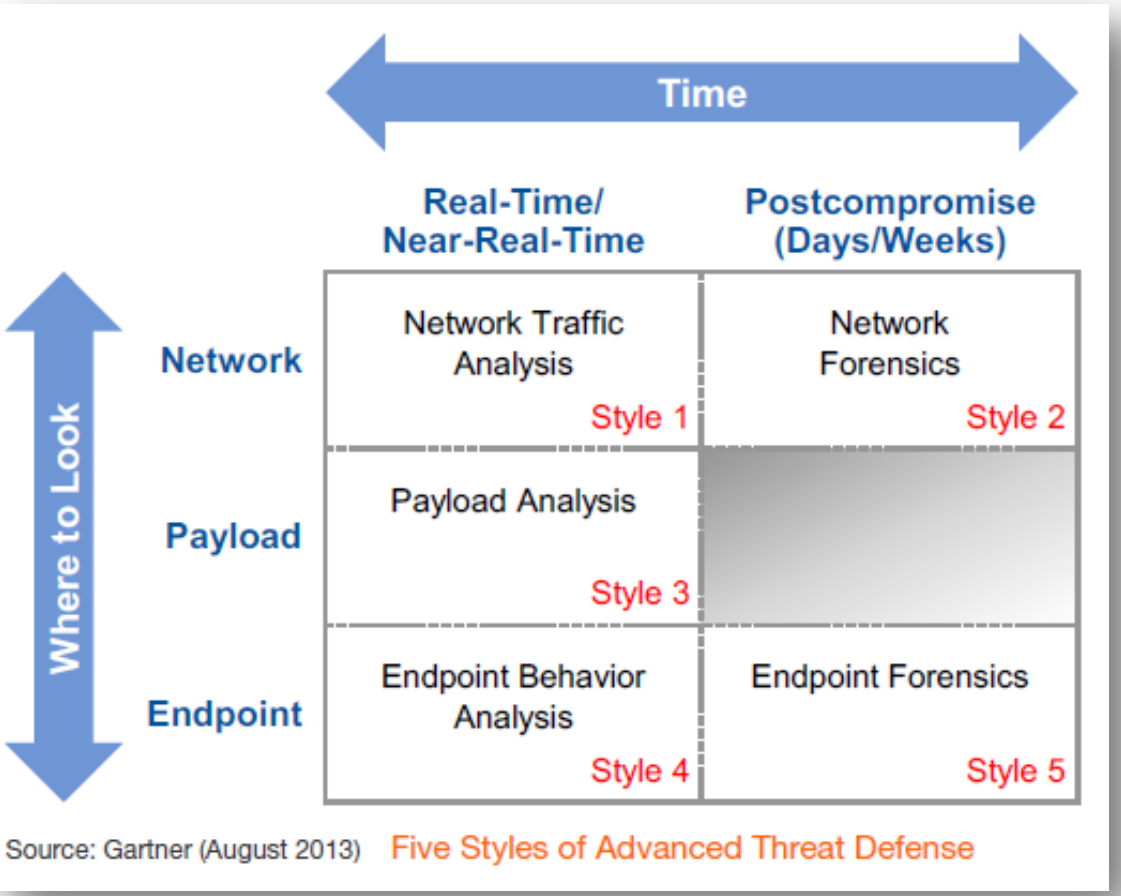
从小时到数月 – 可怕的时间窗口



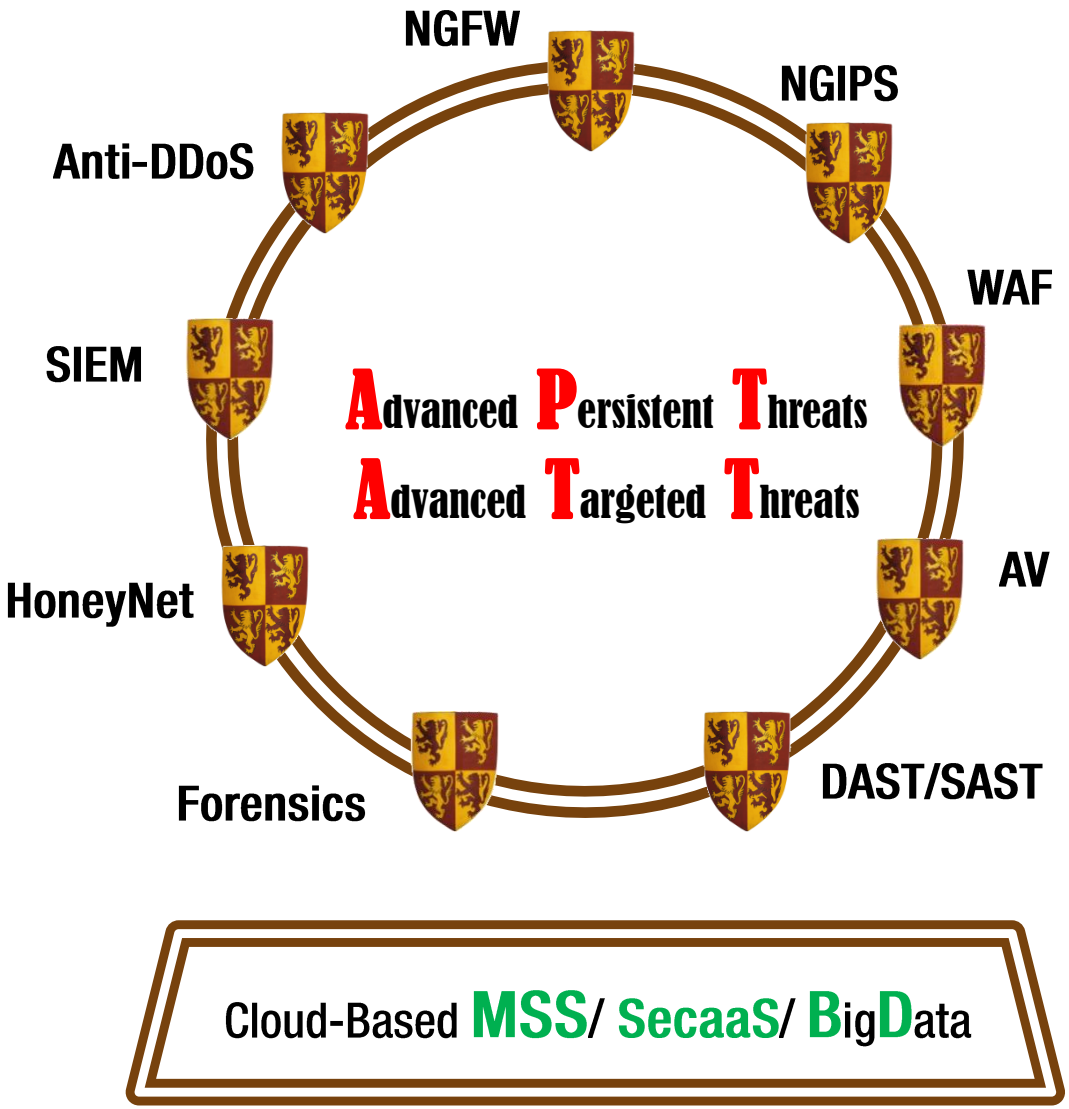
Data Source: Verizon DBIR 2013

看似琳琅满目，用时捉襟见肘(1)

- IDS
- Anti-Virus
- SIEM



看似琳琅满目，用时捉襟见肘(2)

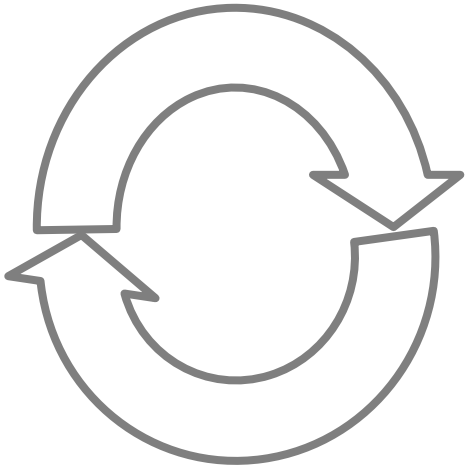


看似琳琅满目，用时捉襟见肘(3)

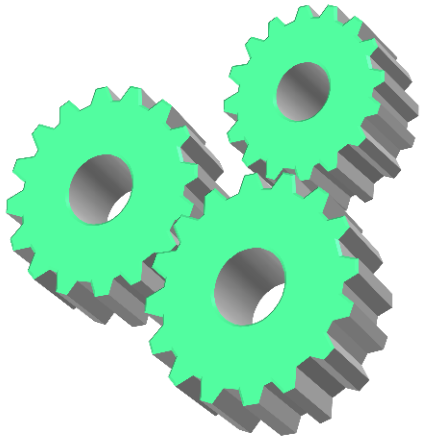
- **More is Less**
  效果不明；技能知识要求太高；大面积全功能覆盖极其昂贵

- **More is Slower**
  缺少协同、大量手工操作，整体响应很慢；开放性不足，更新无法快速现场完成…

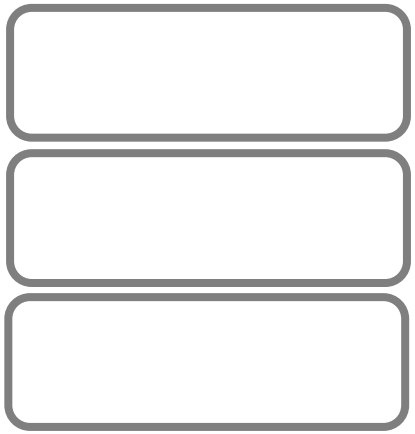
闭环、自动化和软件定义



闭环



自动化



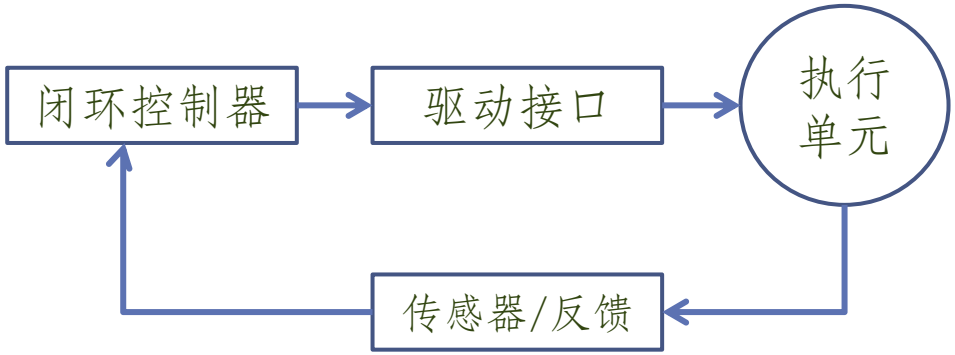
软件定义

闭环成为标配 ~ RSA2014

闭环与开环

～开环～
闭环眼睛瞄准

～闭环～
安全云智能实现积累反馈带来校准和实时更新



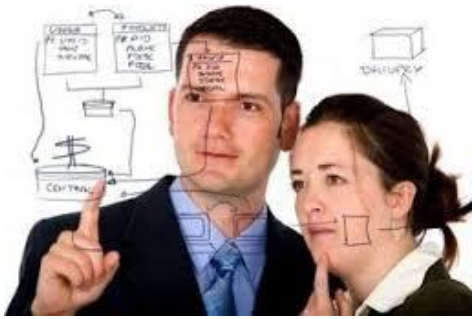
智能闭环和运营闭环

智能

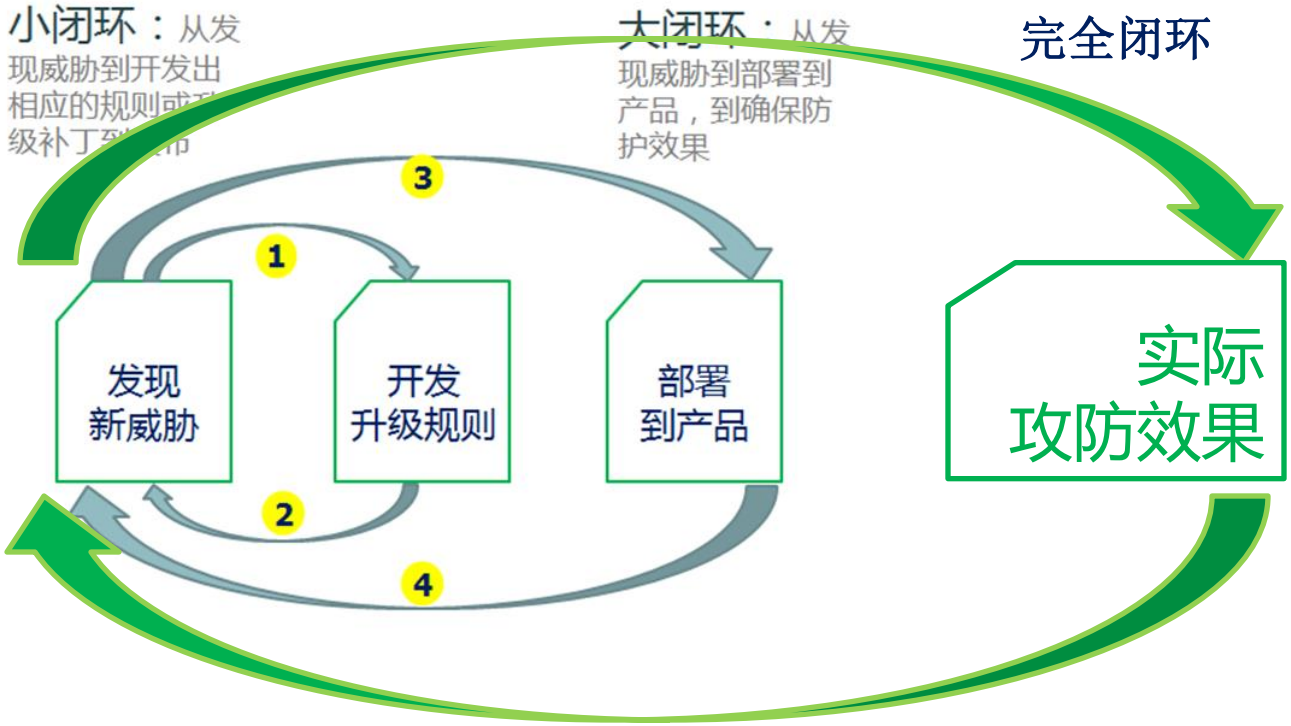
从威胁
到防护规则
到成效验证

运营

从威胁
到威胁消减
最终安全效果



闭环运营帮助用户和安全提供商共赢



- 及时评价防护效果，优化防护措施
- 从小闭环走向大闭环、完全闭环

闭环是下一代安全七个关键特性的核心

NSFOCUS

威胁感知
- 全天候，24x7，多源头
- 基于产品协同及智能分析

可视化
- 安全也能所见即所得
- 揭示虚拟空间的风险

闭环运营
- 及时评价防护效果，优化防护措施

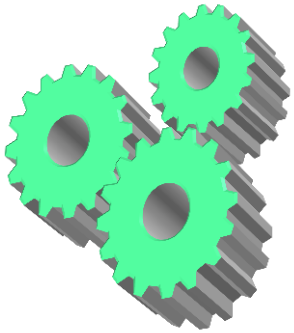
异常检测
- 基于行为模型与安全信誉的异常检测
- 结合采用静态和动态应用安全测试技术

安全协同
- 人人为我，我为人人
- 基于安全智能的合力
- 1+1>2

安全云
- 基于云计算的交付
- 保护云，也使用云

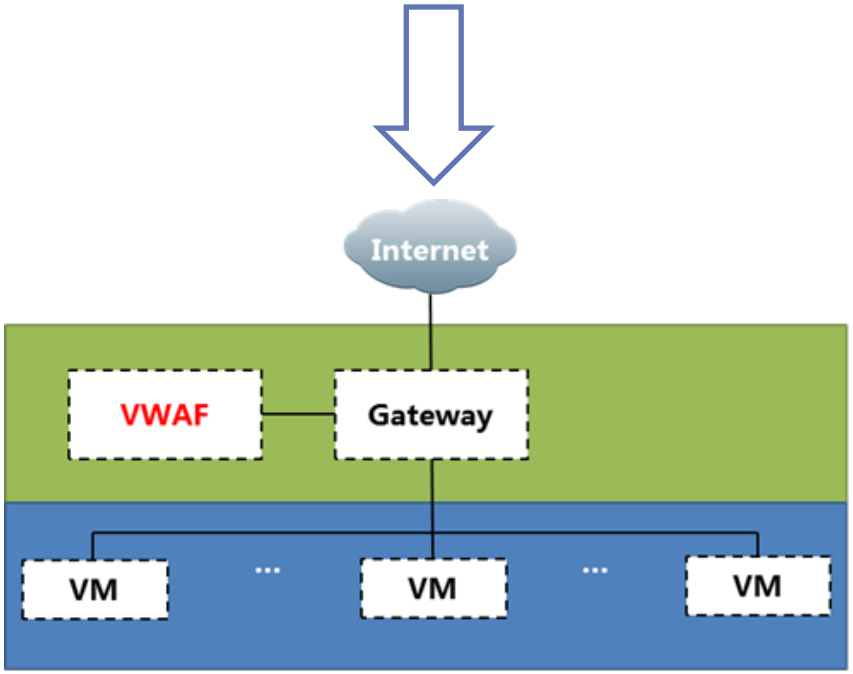
虚拟化
- 面向云计算环境的安全产品虚拟化
- 虚拟化环境应用部署

自动化是做到更快/更便宜的必选

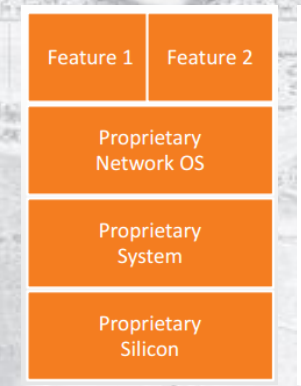


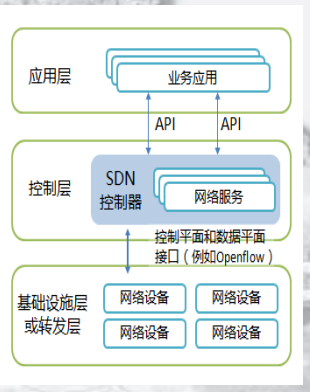
1

2



沿着更好，更快，更便宜的路径，其实...





网络

存储

计算

安全？

- Network Boot
- Central Configuration
- Automated Patch Mgmt

Linux | Windows

VMware | KVM | Xen

Dell | HP | Super Micro

Intel | AMD

Strategy for Security in SDN Age by Gartner

NSFOCUS

P1: Securing Software-Defined Data Centers
保护软件定义数据中心

- 解码/解密/深度检查相关新协议，e.g. OpenFlow, VXLAN, NVGRE，etc.
- 保护控制器和可编程通信接口
- 确保Controller和网元通信安全和完整性
- 保护安全策略的一致性以及SOD
- 提供策略调整的审计、日志和监视
- 将安全管理控制平面和数据运行平面分离

P2: Integrating With the Software-Defined Infrastructure
集成软件定义基础设施

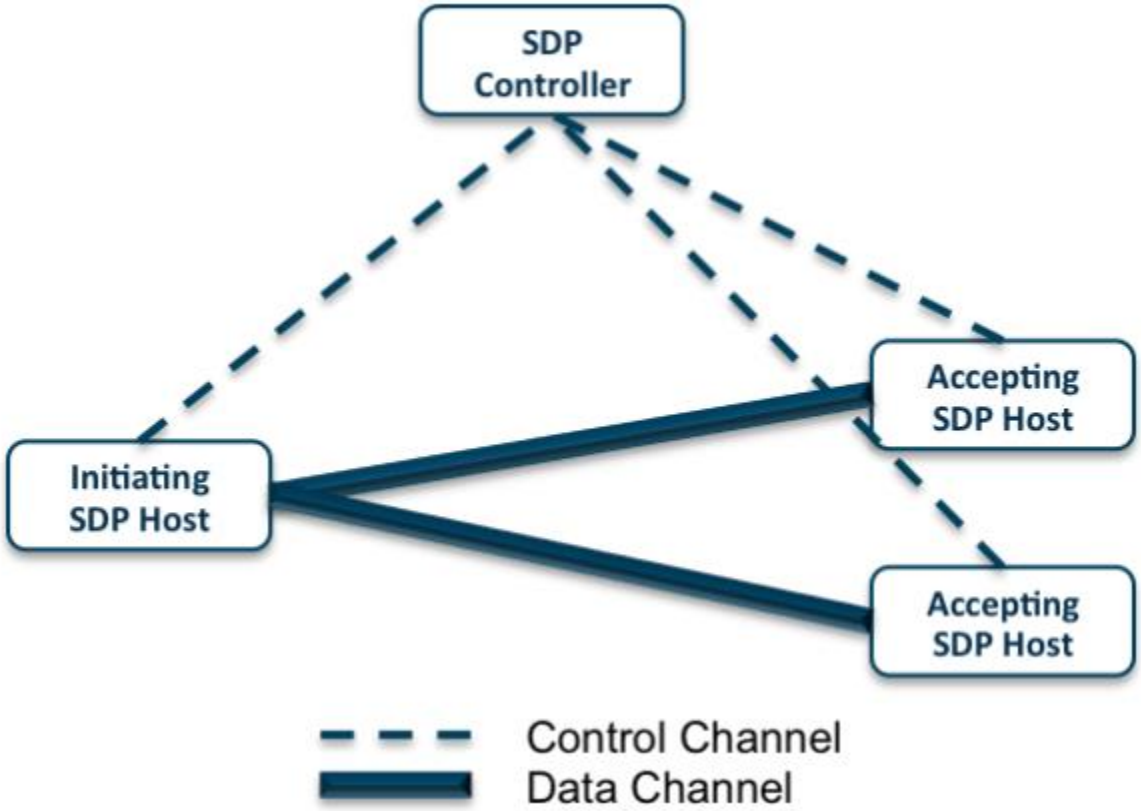
- 支持SDN awareness and integration via OpenFlow
- 加强Context aware security policies
- 基于逻辑属性的安全策略，而不是物理属性
- 使用RESTful or JSON APIs自动化

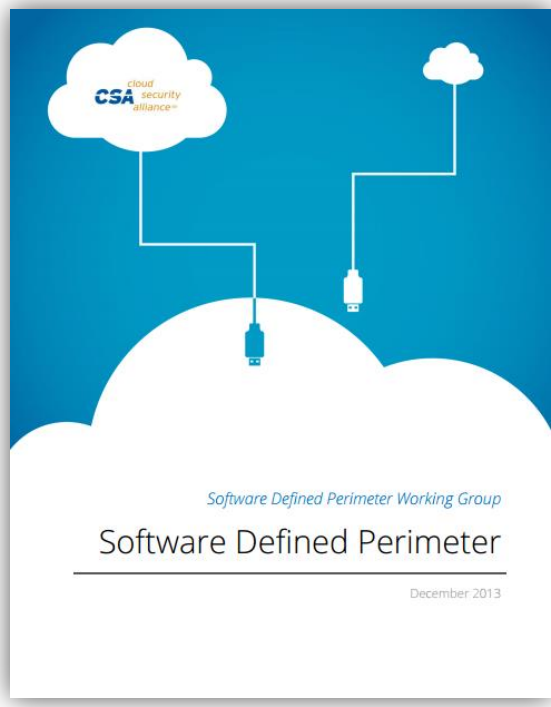
- Security doesn't have to all move to software.

P3: Evolving Into Software-Defined Security
演化到软件定义安全

- 安全管理平面和安全数据平面分离
- 将出现安全管理器，集中管理安全SLA/策略/属性
- 全局管理，而不是某个安全设备
- P+V混合按需部署优化
- 与其它SDx控制器双向集成
- 关注策略和风险，而不是基础设施的编程

Software Defined Perimeter by CSA



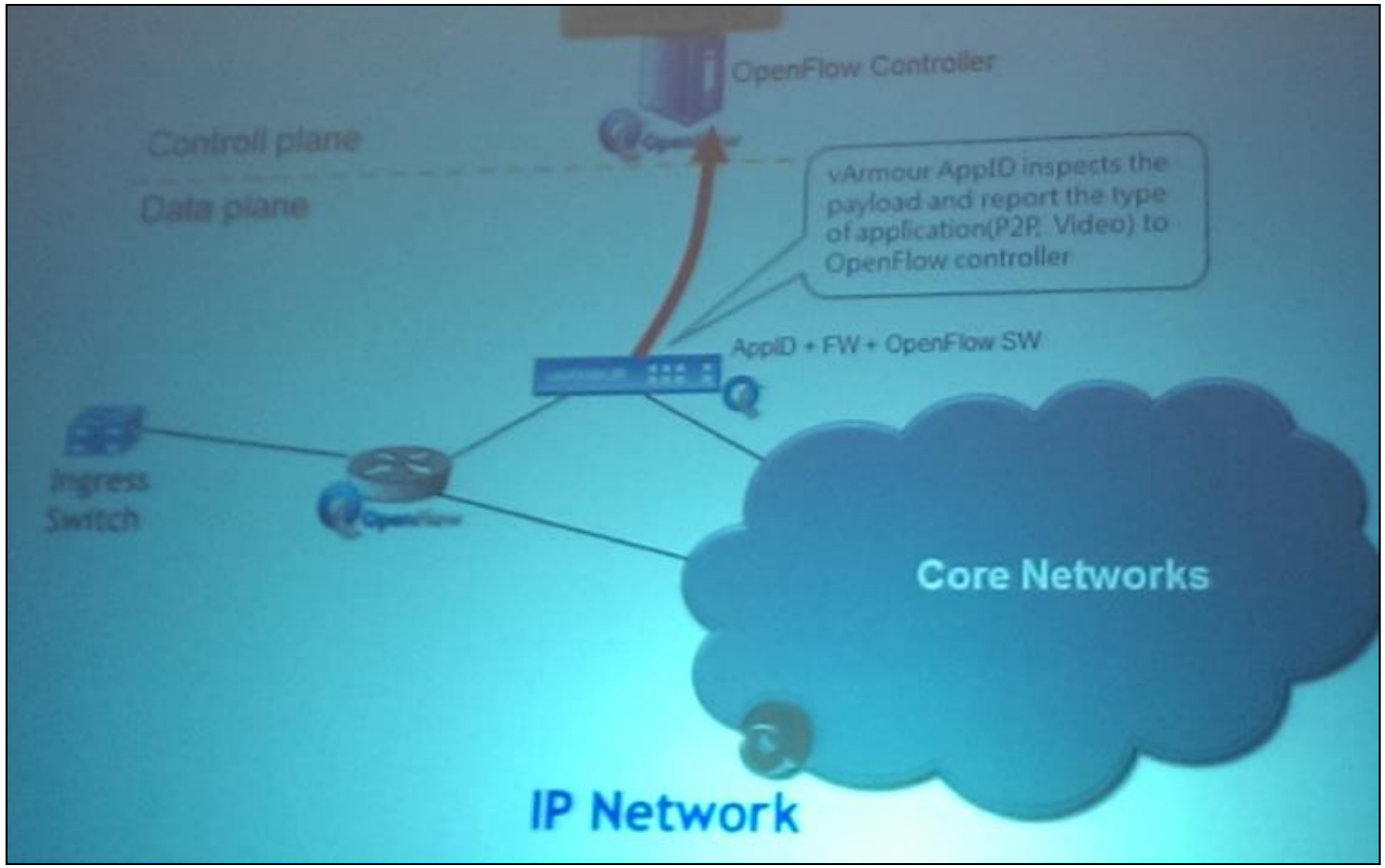


- NIST, DoD, CIA, Coca-Cola…
- BYOD, SaaS, IaaS…

点击http://www.cloudsecurityalliance.org下载

SDN/SDS架构带来新的机遇

- 一种混合设备
- 网络安全+交换机
- 内容识别(AppID)探测载荷类型后，报告给控制器，获得指令后，直接处理。后续数据包按照预定路径直接通讯



Software Defined Protection by Checkpoint

Software Defined Protection by Checkpoint

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

自动化

可视化

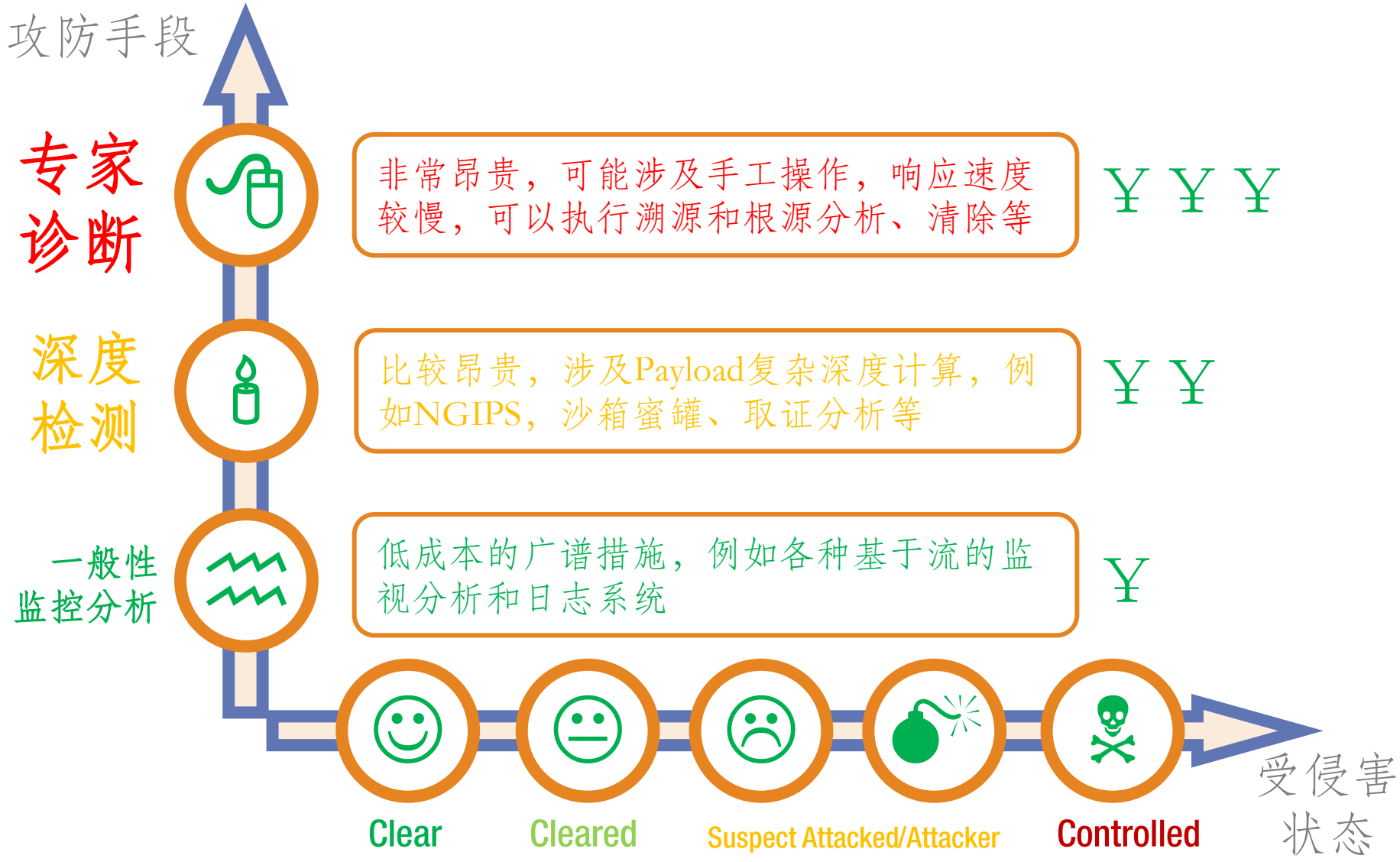
模块化

管理层

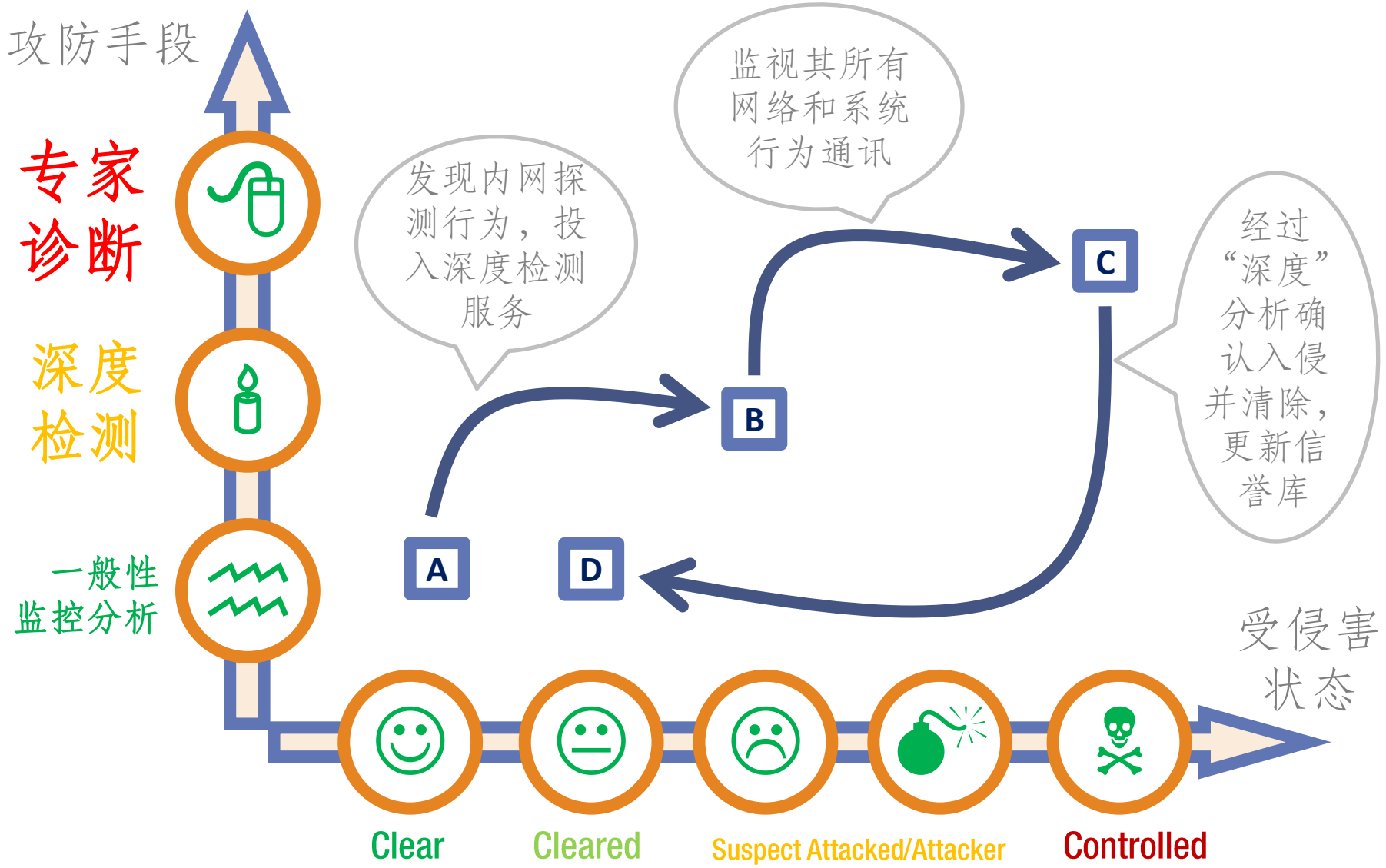
控制层
(安全策略，威胁情报)

执行层
(各安全执行点)

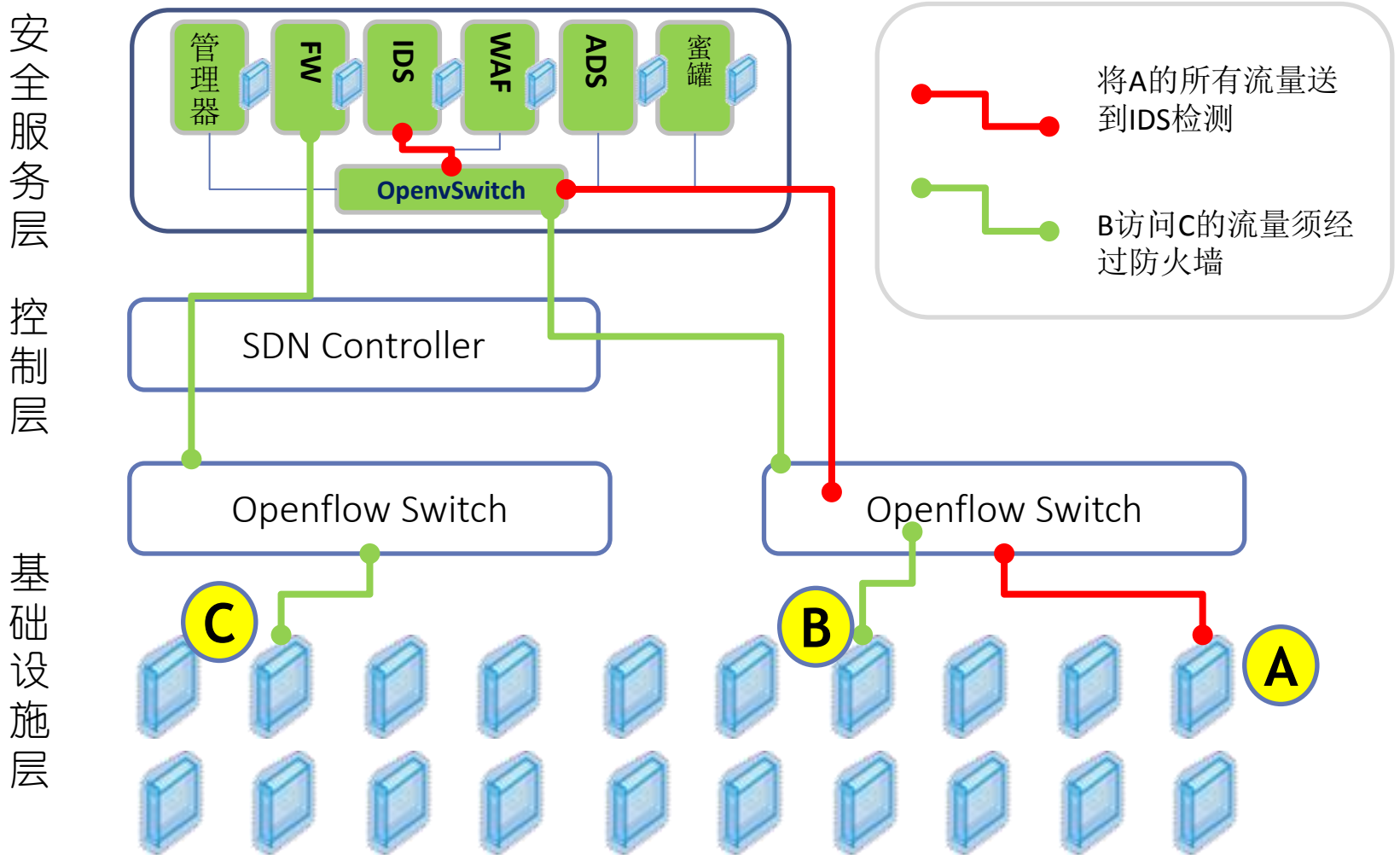
攻防状态空间与自动化(1)



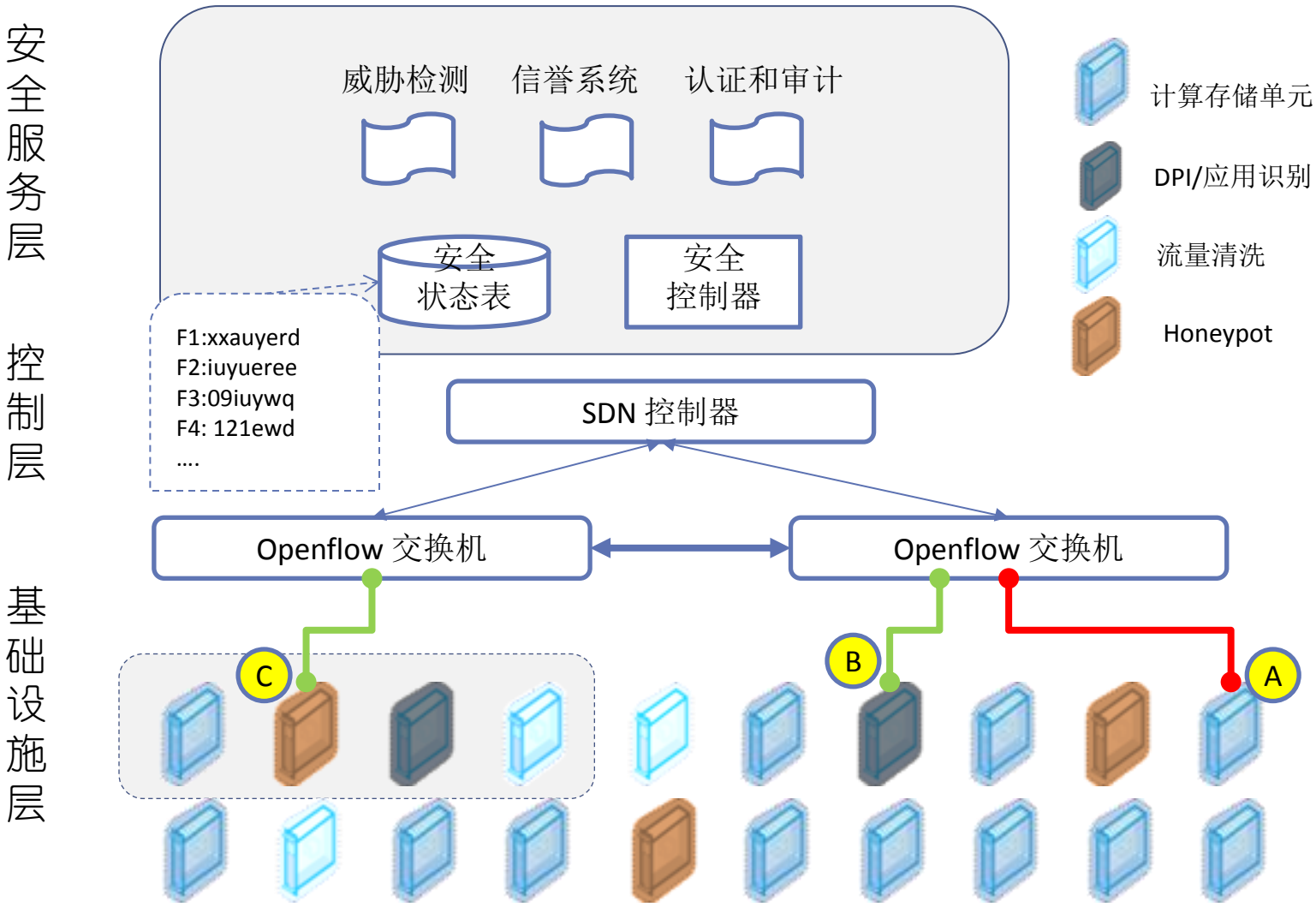
攻防状态空间与自动化(2)



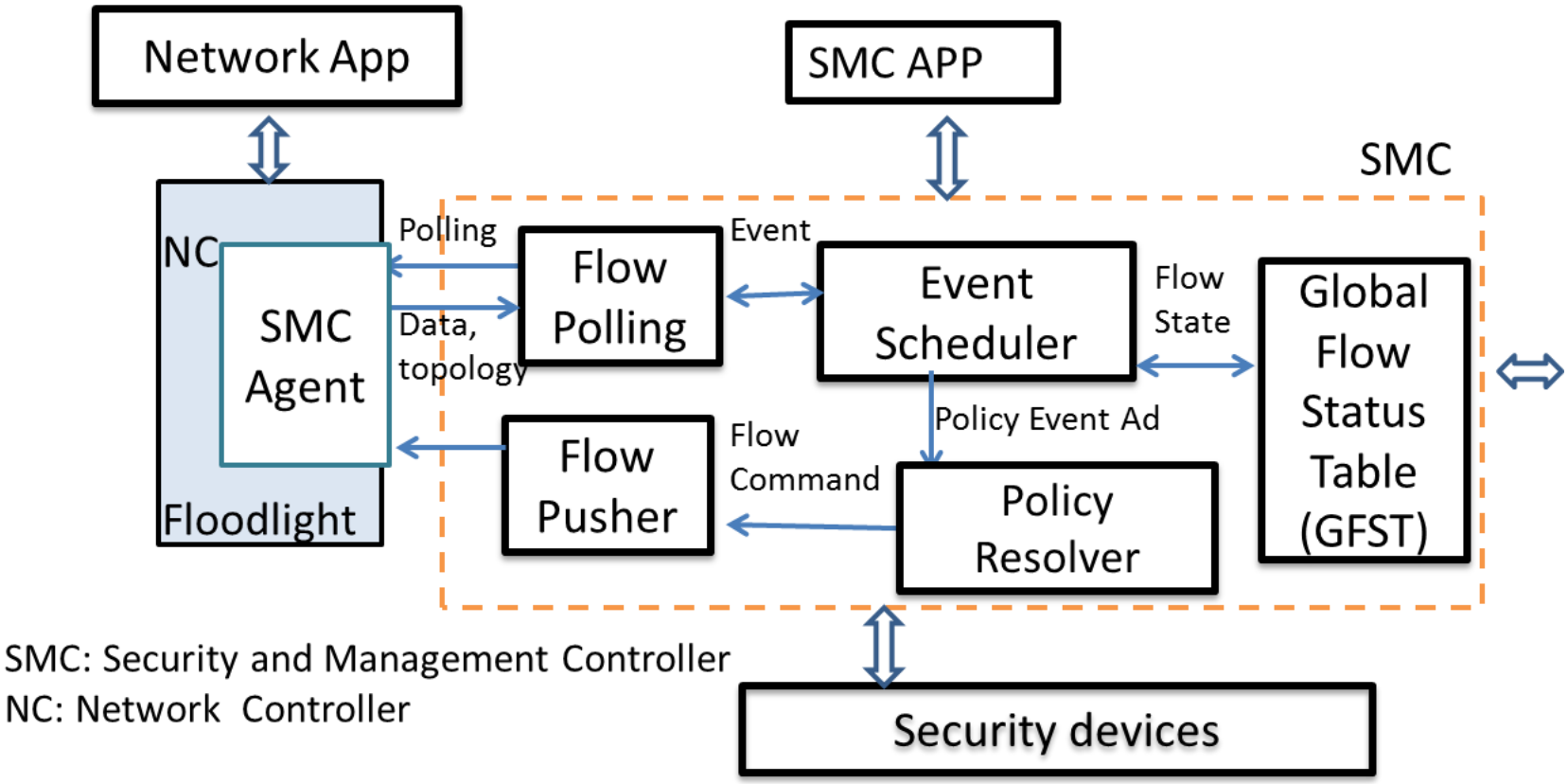
SDN/OF下的安全构想(1) - VSA



SDN/OF下的安全构想(2) - SDS



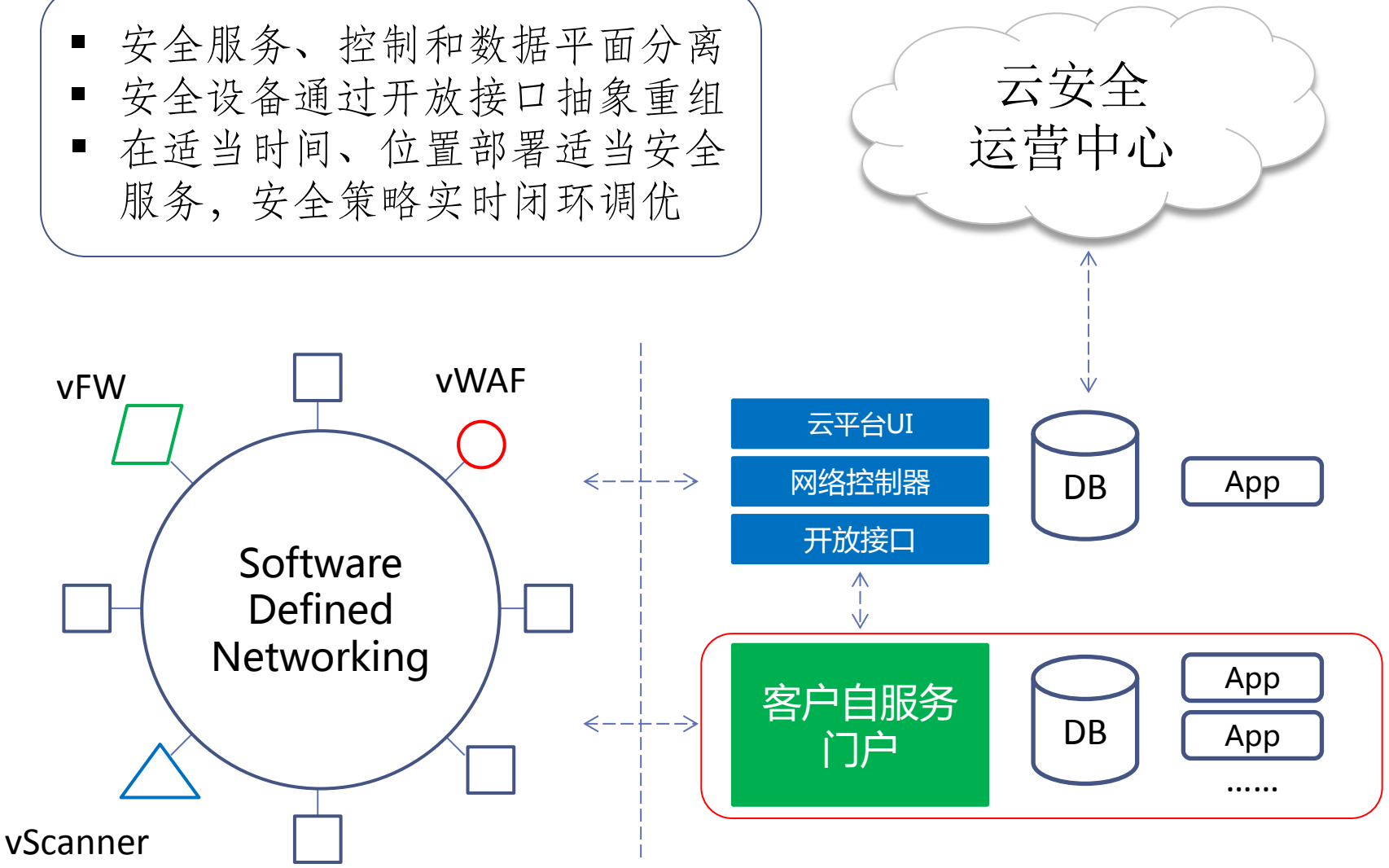
安全控制器、开放性、可编程性



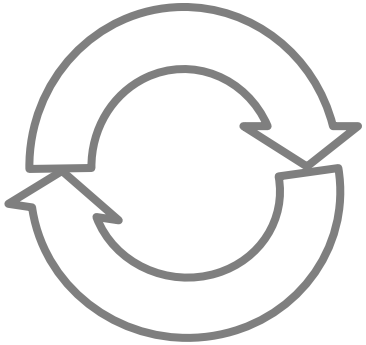
AUTOMATION ↑ = MONEY ↓ + TIME ↓ = WIN THE WAR

安全控制器、开放性、可编程性

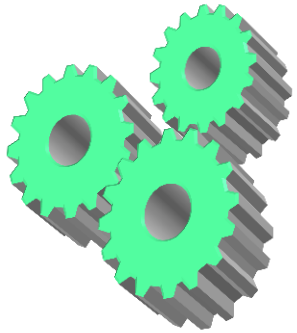
- 安全服务、控制和数据平面分离
- 安全设备通过开放接口抽象重组
- 在适当时间、位置部署适当安全服务，安全策略实时闭环调优



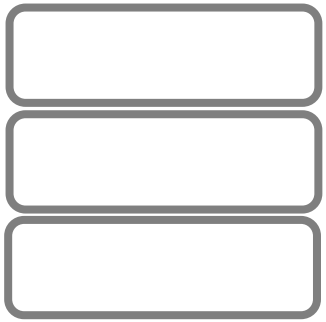
结束语 – 解开安全的九连环



- 闭环是保证安全成效的必然发展
- 智能闭环和运营闭环是两种形态



- 自动化开通部署（P+V+S）
- 自动化的策略调整和调度



- 软件定义本质上是分层、开放、服务重组、操作前置
- 软件定义帮助实现更快/更便宜的安全

NSFOCUS

谢谢 Thank You 謝謝 Vielen Dank Gracias Merci Beaucoup
ありがと 감사합니다 Obrigado ขอบคุณ Terima kasih