

解开安全的锁链：软件定义安全的战略和实践

SESSION ID: MAN-T08

赵 粮

首席战略官
绿盟科技

@赵粮, @绿盟科技 新浪微博



层出不穷，无处不在的安全威胁



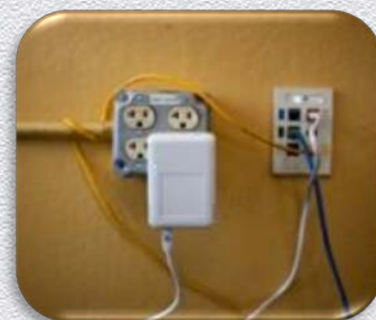
攻击被清除了没有？入侵深度？

攻击从什么时候发生的？还会再发生吗？

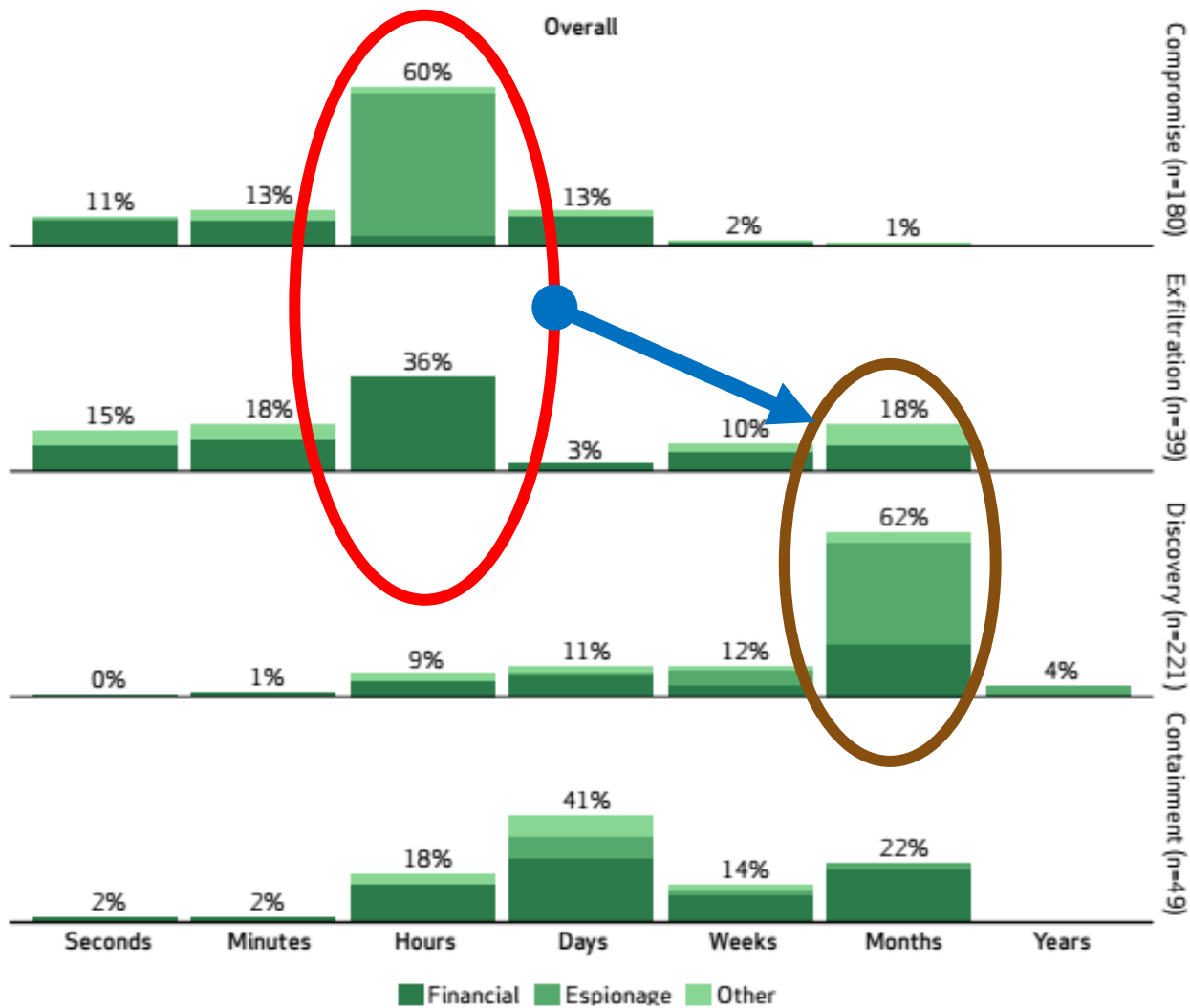
损失有多大？未来如何避免或控制损失？

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

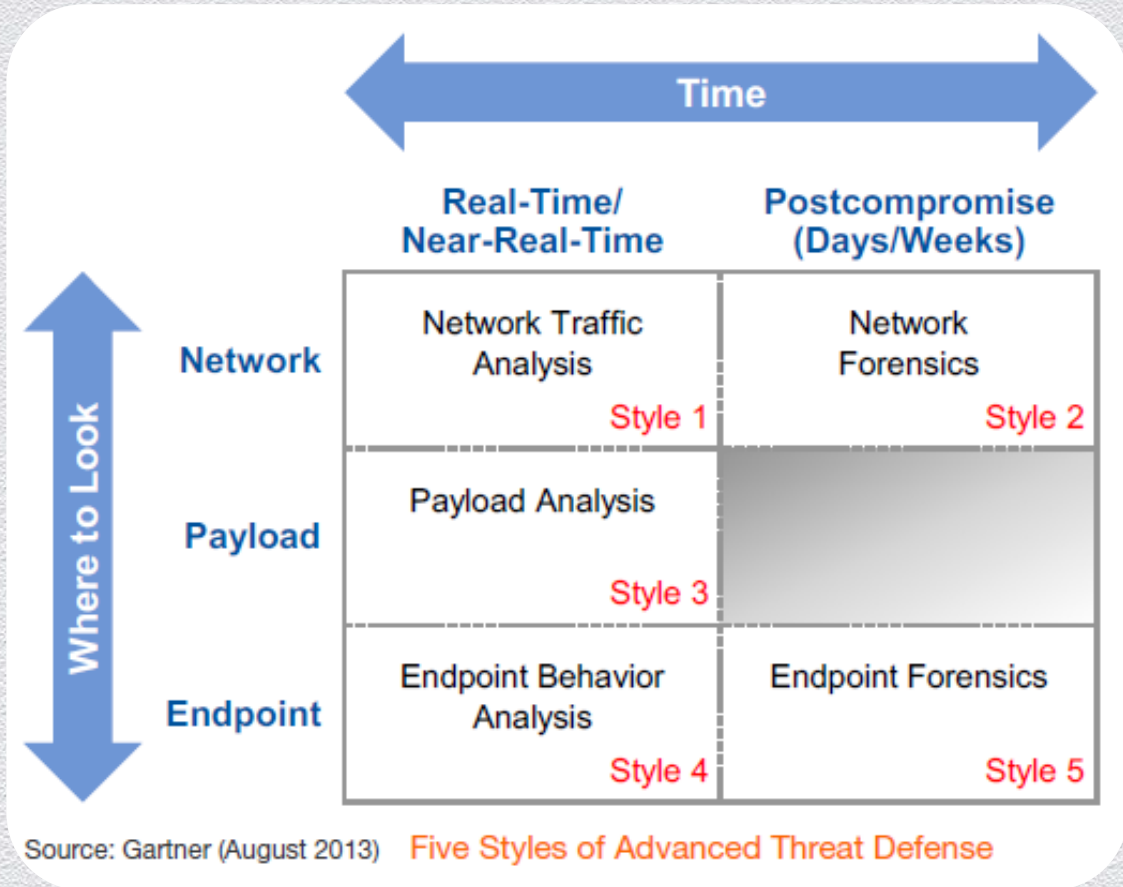
看似琳琅满目，用时捉襟见肘(1)



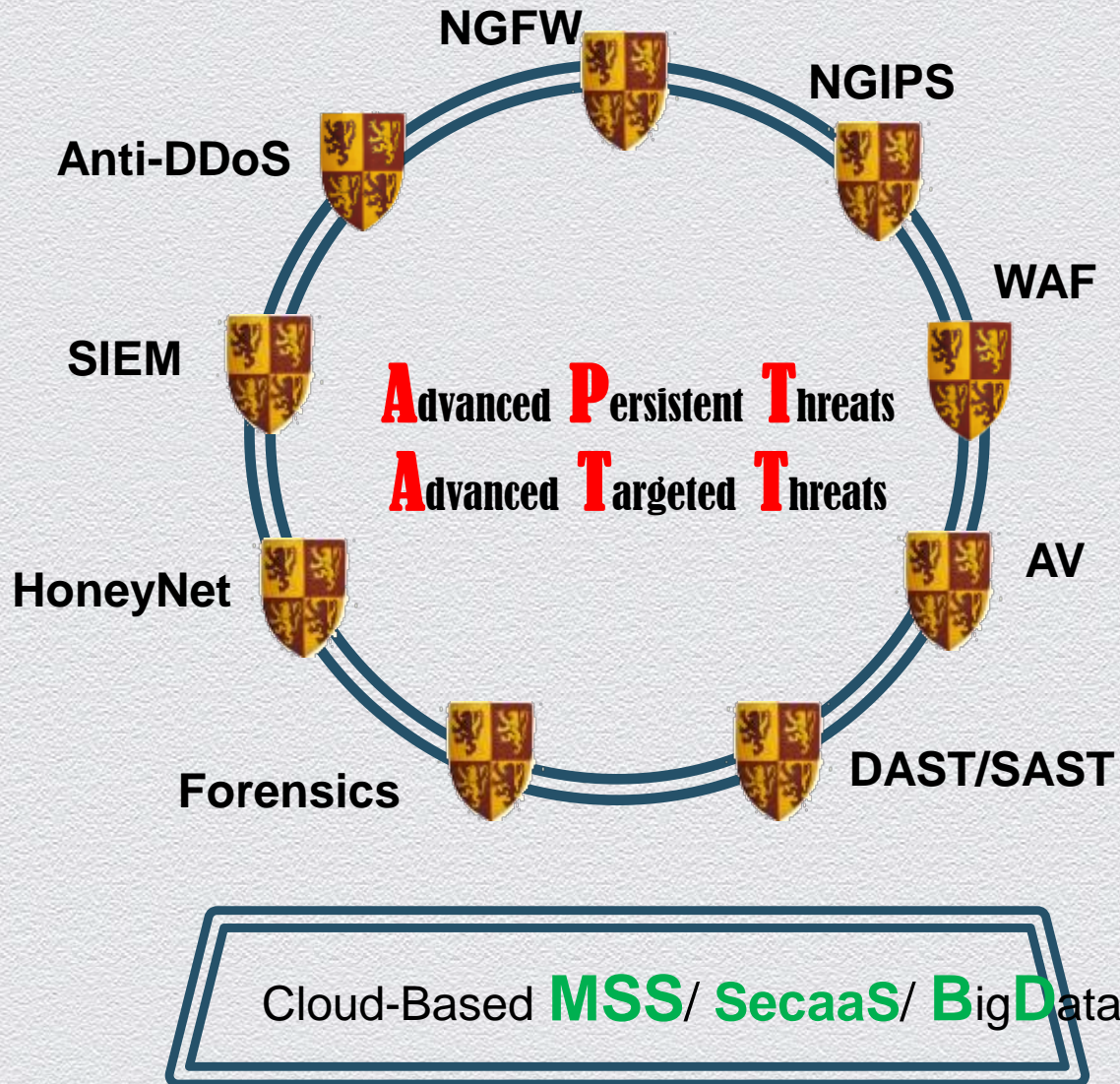
IDS

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**

成效不明；技能知识要求太高；大面积全功能覆盖极其昂贵

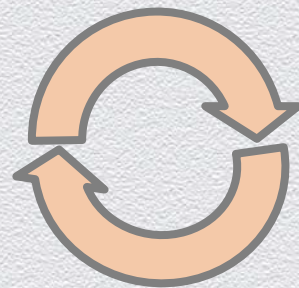
- **More is Slower**

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…

解决之道 – 战略和实践

>>> 成效不明

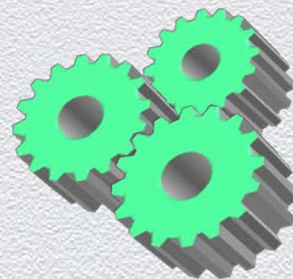
众多安全产品所需的知识技能太高，遇到威胁难以响应。



闭环

>>> 复杂的人工操作

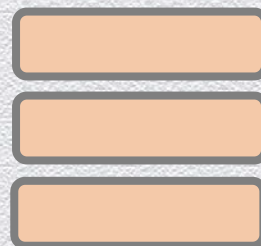
缺少协同，开放性不足，无法进行更新变化...



自动化

>>> 封闭而缺少协同

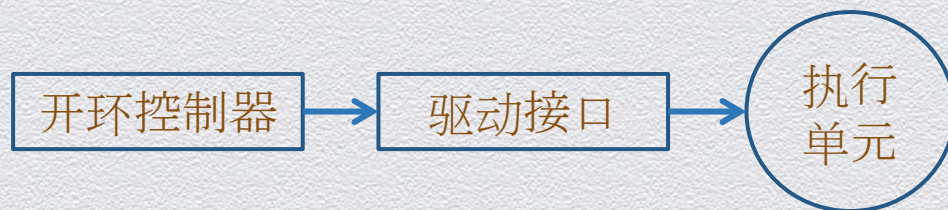
安全的覆盖面固化，或者不足，或者过度。面对灵活变化的威胁，无法聚焦应对



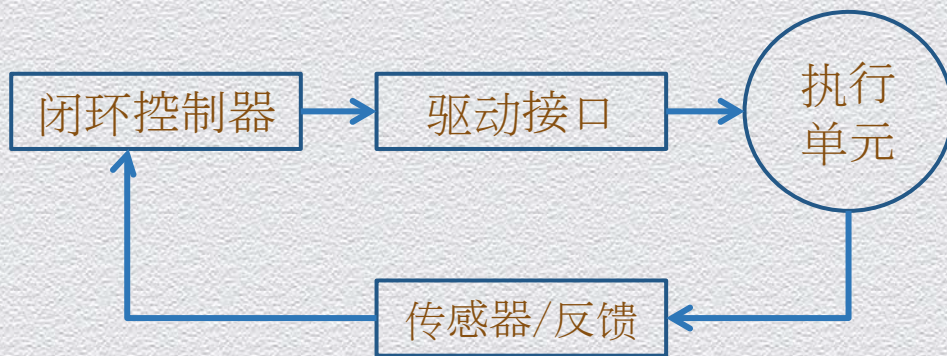
软件定义

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

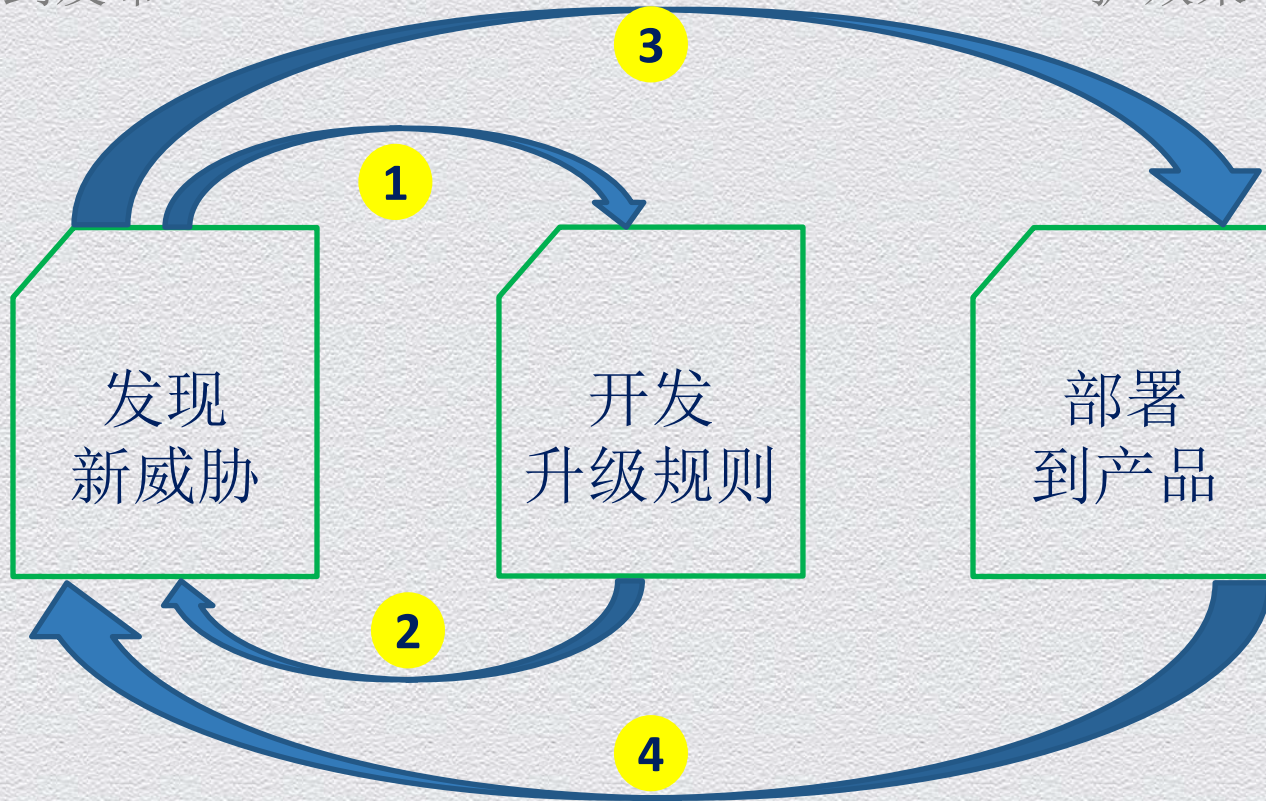
从威胁
到威胁消减
最终安全效果



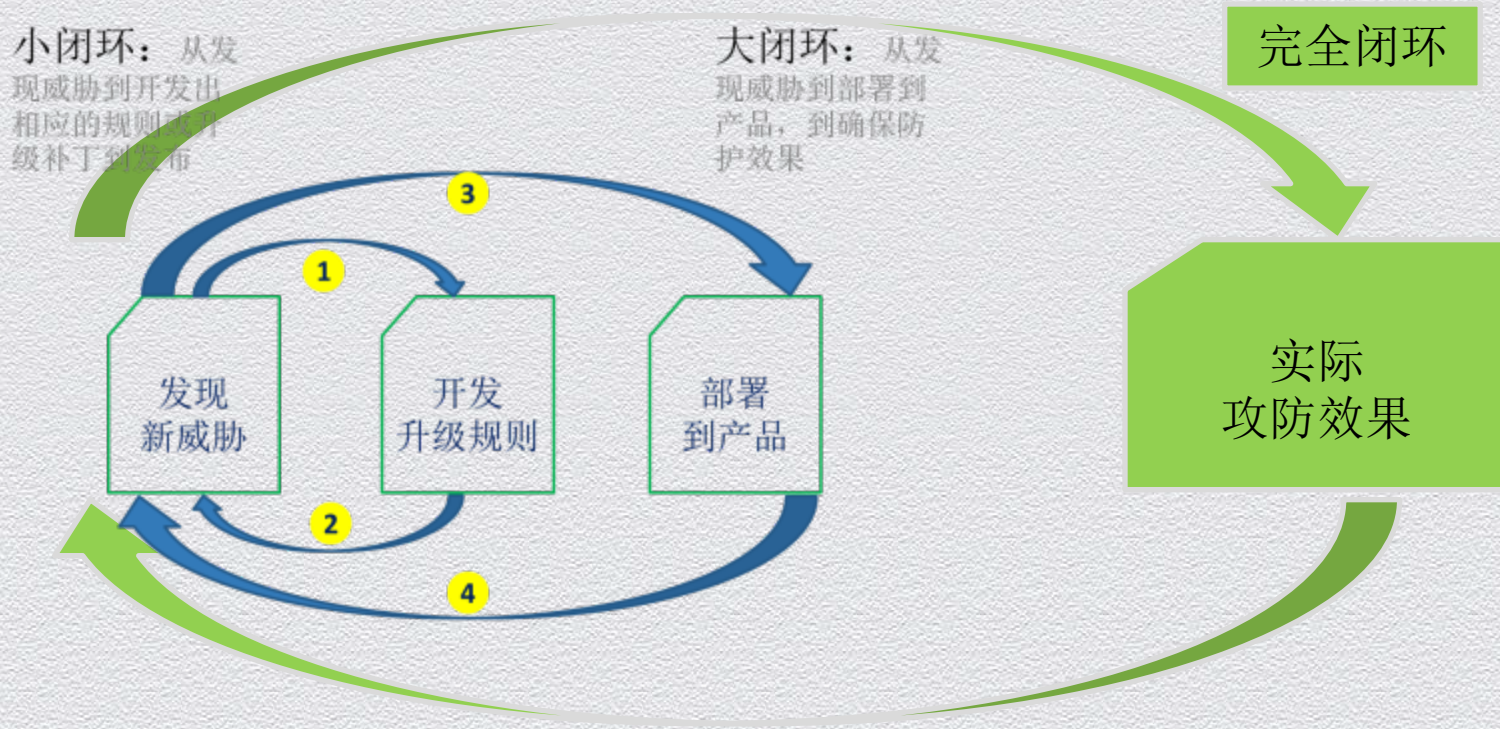
安全智能之闭环流程示意（大小闭环）

小闭环：从发现威胁到开发出相应的规则或升级补丁到发布

大闭环：从发现威胁到部署到产品，到确保防护效果

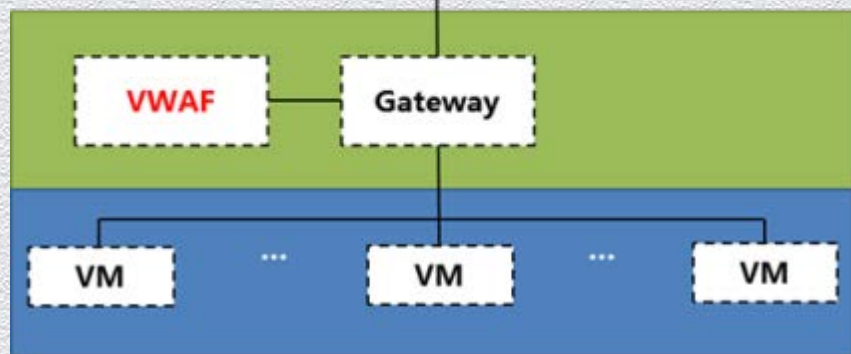
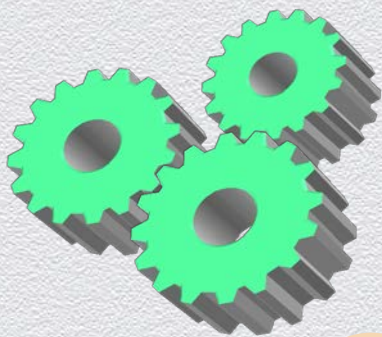


完全闭环运营是攻防技术的必然发展



- ⌚ 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

自动化是做到更快/更便宜的必选



沿着更好，更快，更便宜的路径，其实...

网络
存储
计算

- Network Boot
- Central Configuration
- Automated Patch Mgmt

- | | | |
|--------|---------|-----|
| Linux | Windows | |
| VMware | KVM | Xen |

- | | | |
|------|----|-------------|
| Dell | HP | Super Micro |
|------|----|-------------|

- | | |
|-------|-----|
| Intel | AMD |
|-------|-----|



安全？

SDN时代的一种安全战略

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

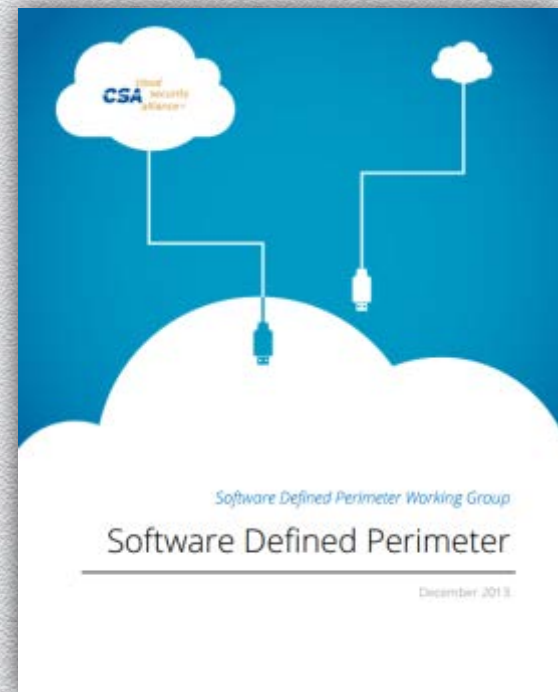
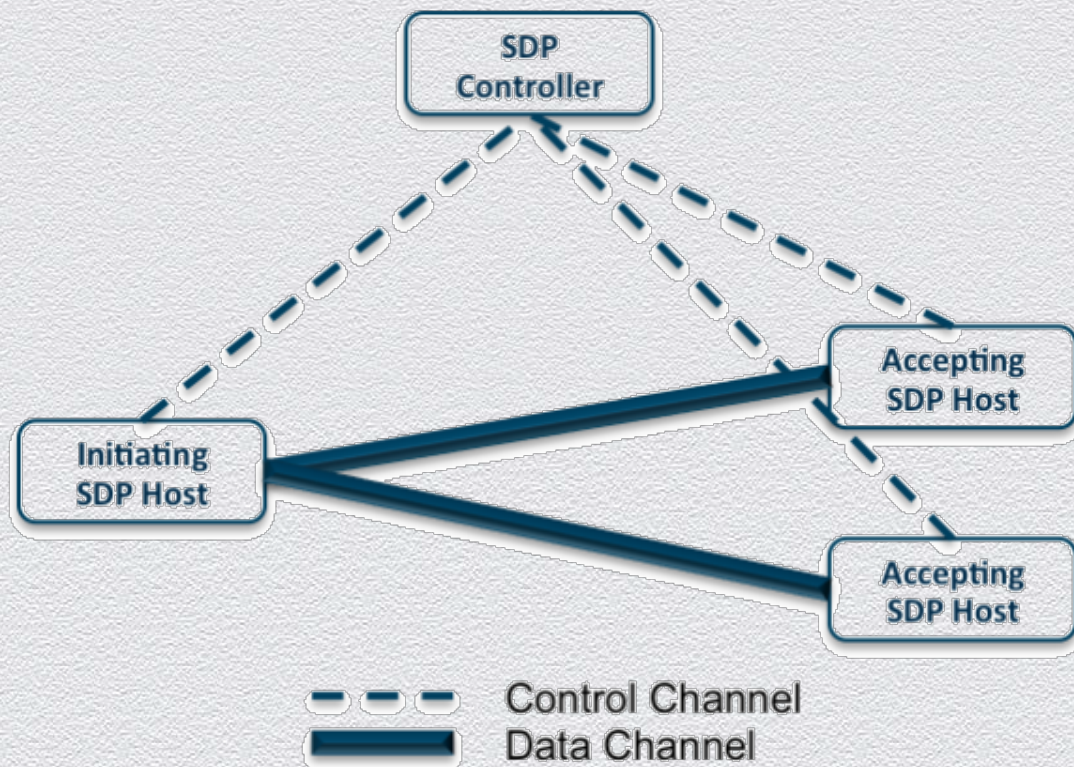
P2: Integrating With the Software-Defined Infrastructure 集成软件定义基础设施

- 通过OpenFlow支持SDN支持和集成
- 加强感知上下文的安全策略
- 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
- *安全不必全都软件化
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+S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

云安全联盟发布的软件定义边界SDP项目



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

点击<http://www.cloudsecurityalliance.org>下载

攻防状态空间与自动化(1)

攻防手段

专家
诊断



非常昂贵, 可能涉及手工操作, 响应速度较慢, 可以执行溯源和根源分析、清除等

\$\$\$

深度
检测



比较昂贵, 涉及Payload复杂深度计算, 例如NGIPS, 沙箱蜜罐、取证分析等

\$\$

一般性
监控分析



低成本的广谱措施, 例如各种基于流的监视分析和日志系统

\$



Clear



Cleared



Suspect Attacked/Attacker

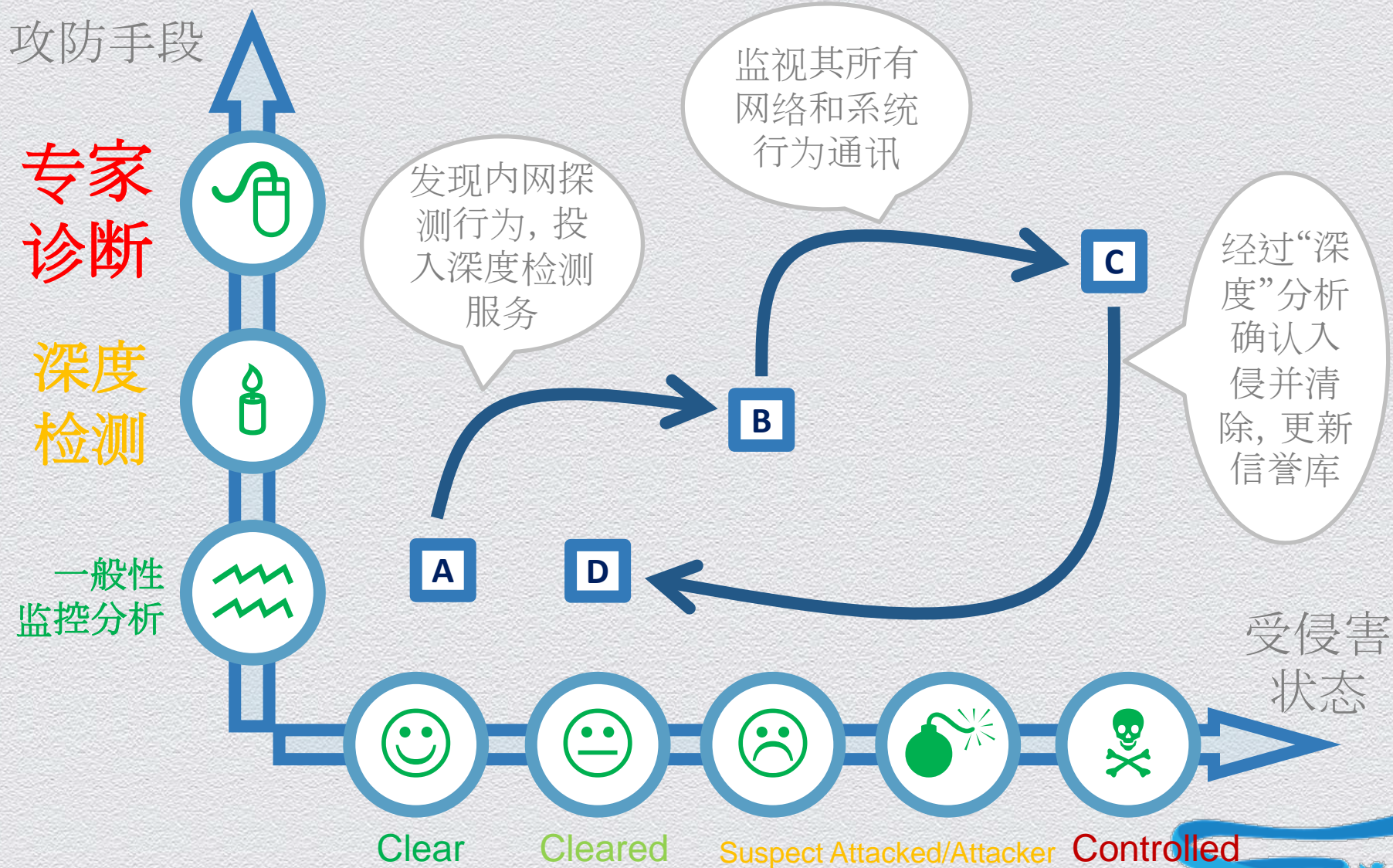


Controlled



受侵害
状态

攻防状态空间与自动化(2)

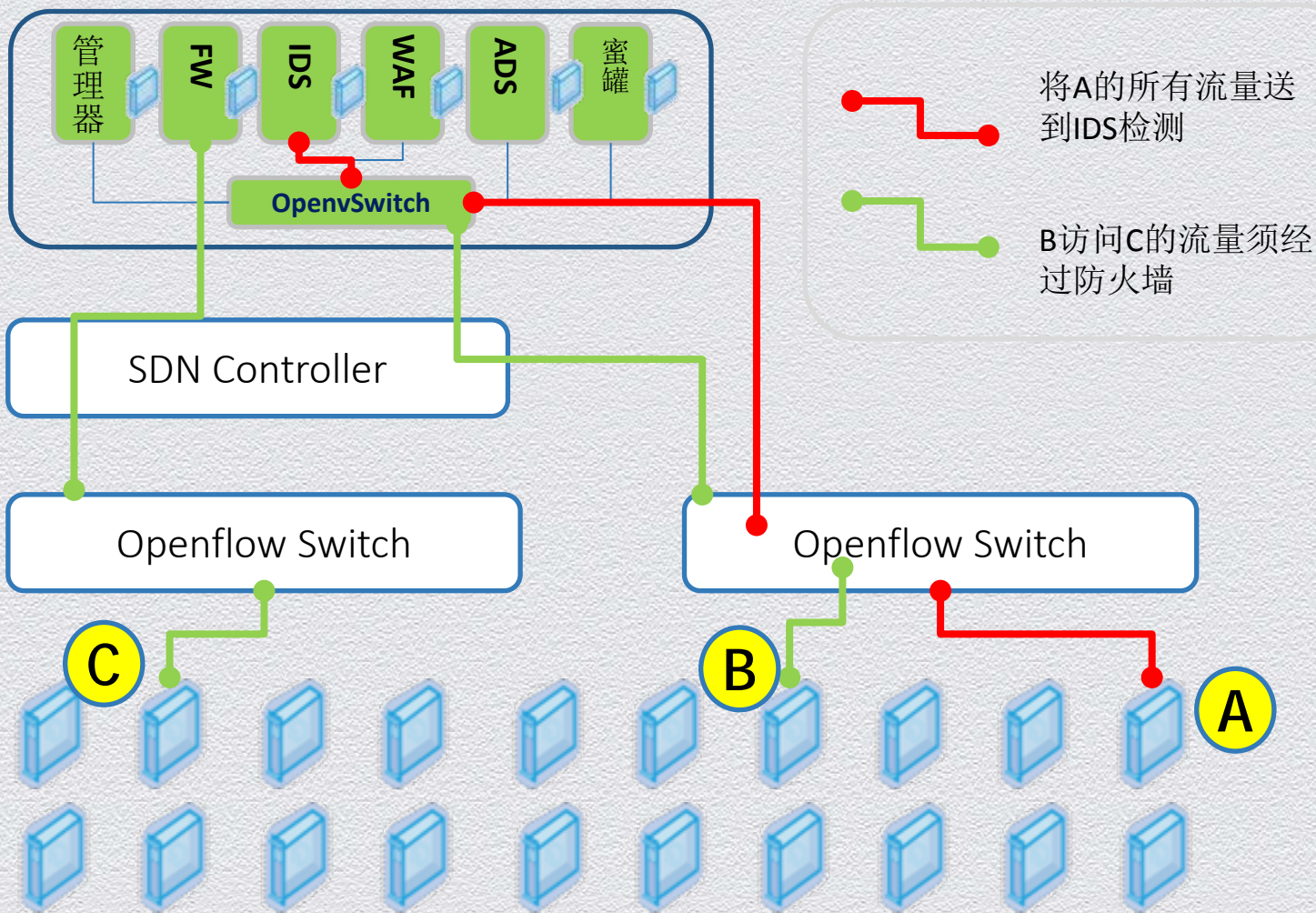


SDN/OF下的安全构想(1) - VSA

安全服务层

控制层

基础设施层

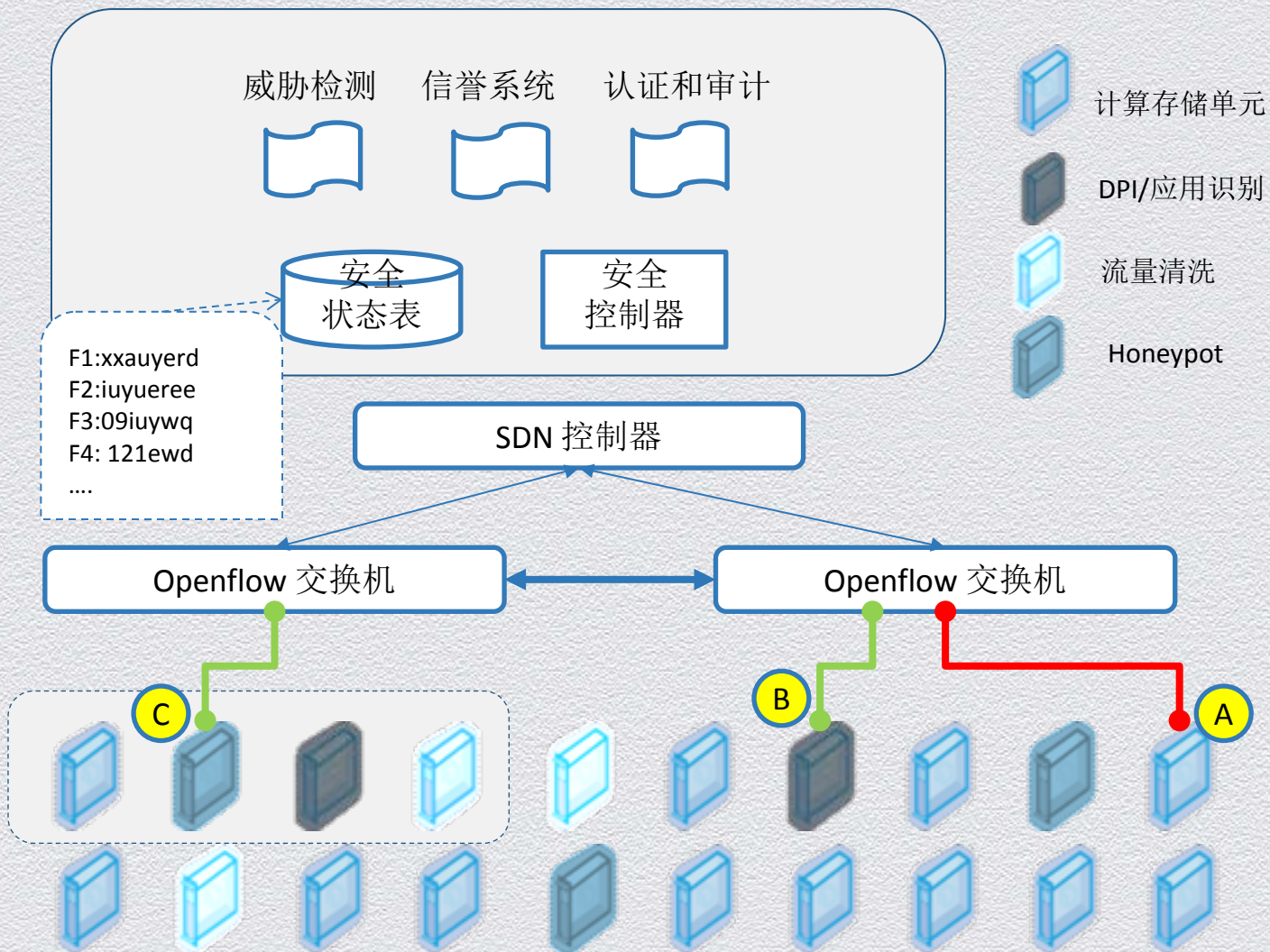


SDN/OF下的安全构想(2) - SDS

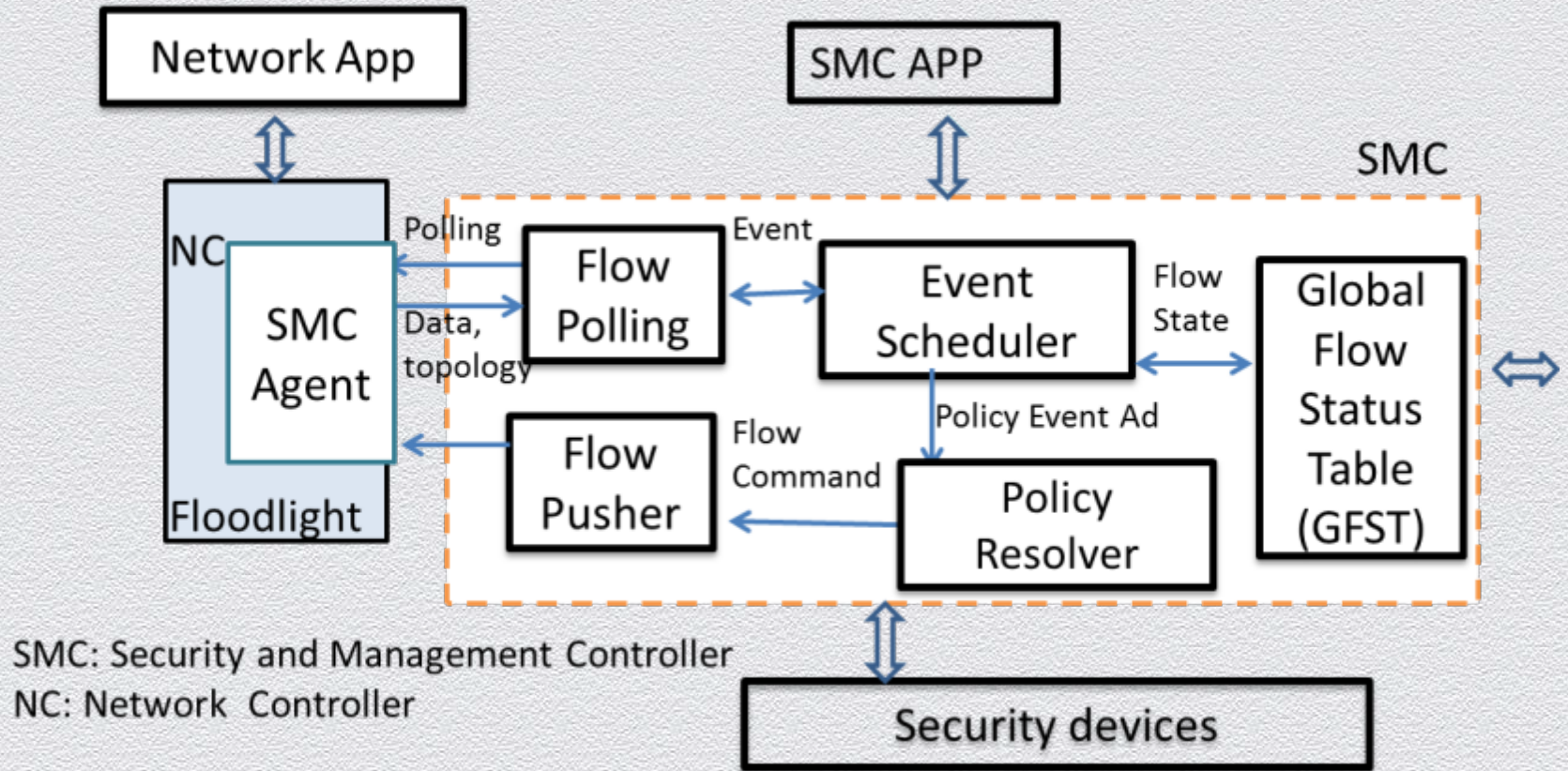
安全服务层

控制层

基础设施层



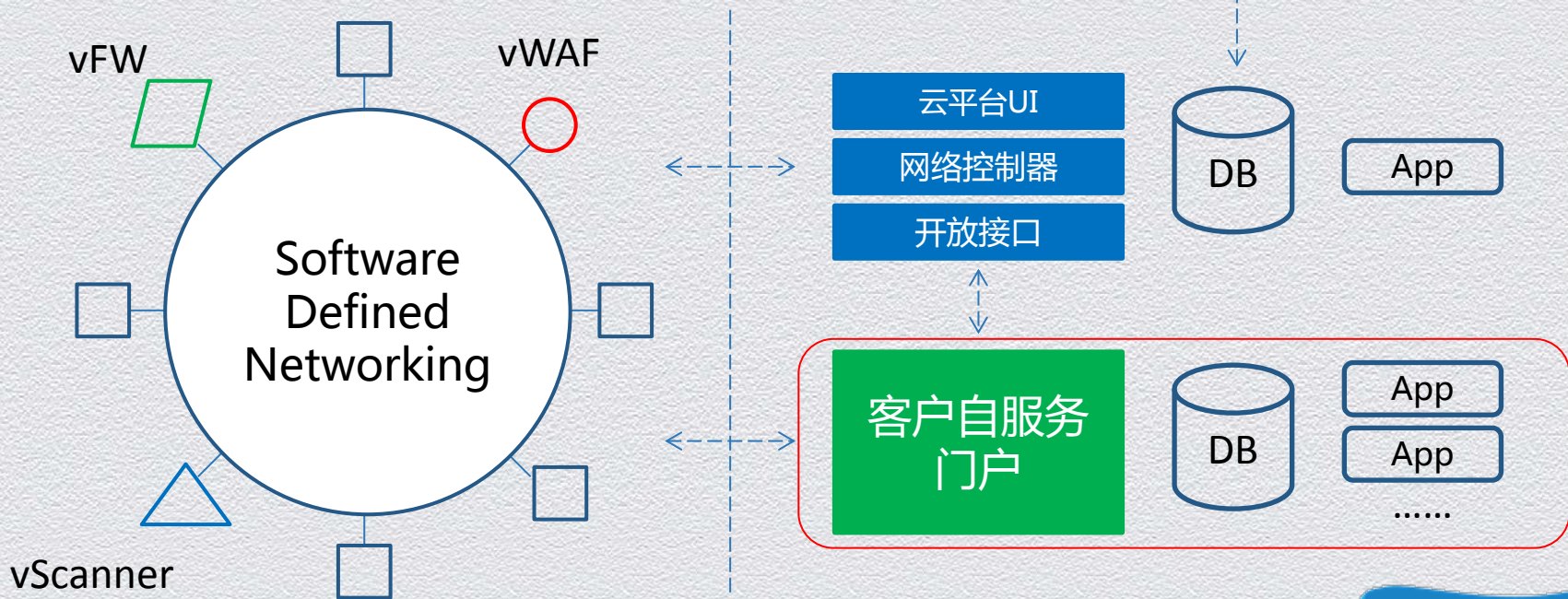
安全控制器、开放性、可编程性



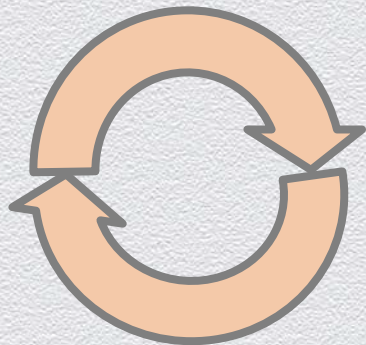
AUTOMATION ⬆️ = MONEY ⬇️ + TIME ⬇️ = WIN THE V

安全控制器、开放性、可编程性

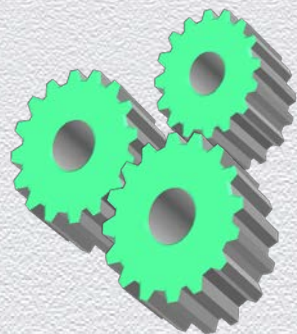
- 安全服务、控制和数据平面分离
- 安全设备通过开放接口抽象重组
- 在适当时间、位置部署适当安全服务, 安全策略实时闭环调优



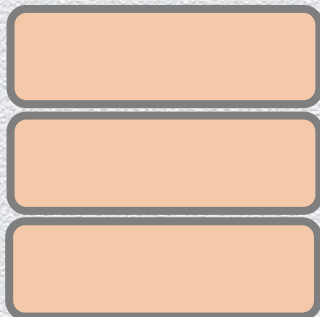
结束语 – 解开安全的锁链



- 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

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



解开安全的锁链：
软件定义安全的
战略和实践