OWASP
Open Web Application Security Project

安全可知、可控与超融合安全应用技术

铱迅信息 杨谦

Contents

目 录

1. 安全痛点综述

2. 安全可知

3. 安全管控

4. 安全应急与恢复

5. 总结

OWASP
Open Web Application Security Project

安全痛点综述

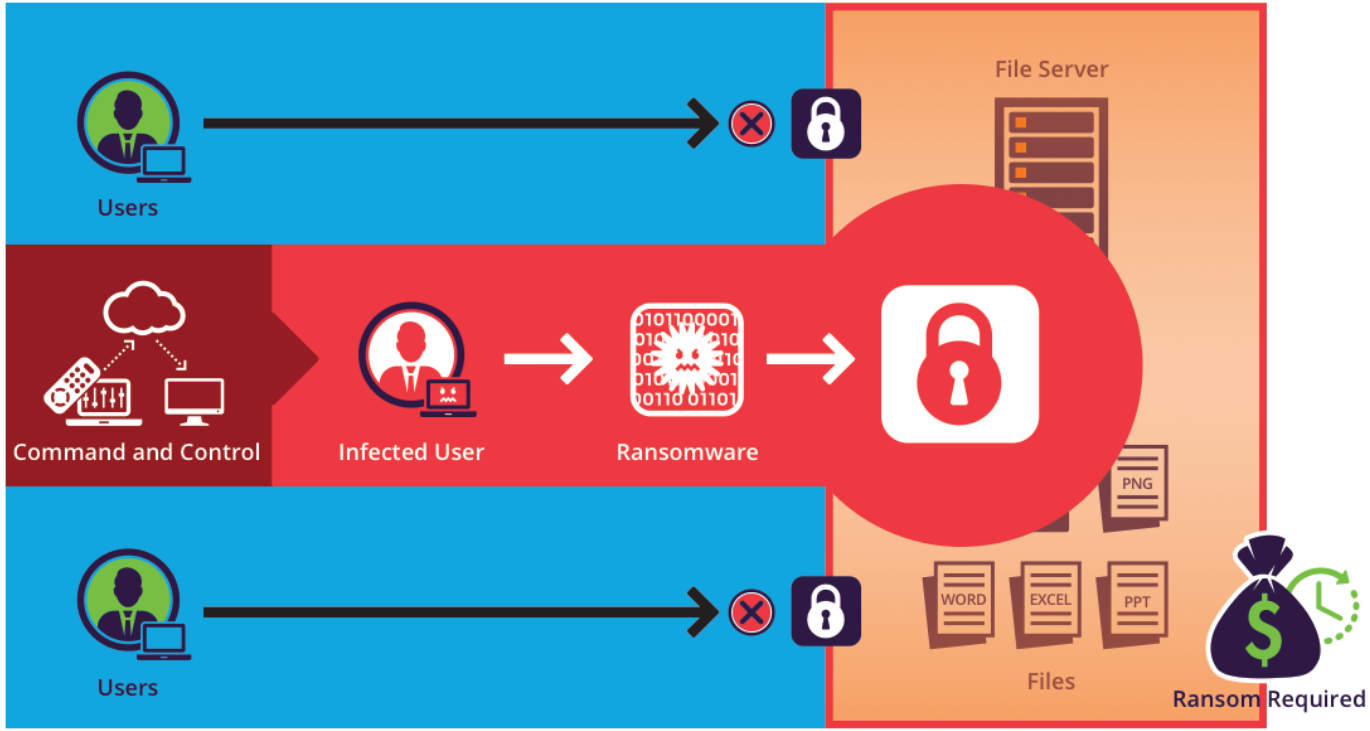
铱迅信息技术股份有限公司

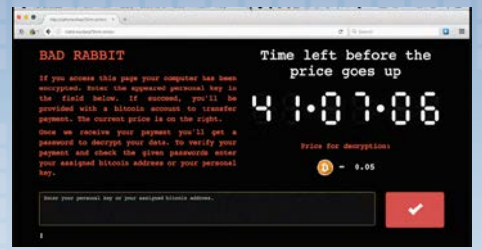
安全漏洞层出不穷

Drupal 6,7,8等多个子版本存在远程代码执行漏洞。
攻击者可以利用该漏洞攻击Drupal系统的网站，执行恶意代码，最后完全控制被攻击的网站，该漏洞就是：CVE-2018-7600。

OWASP
Open Web Application Security Project

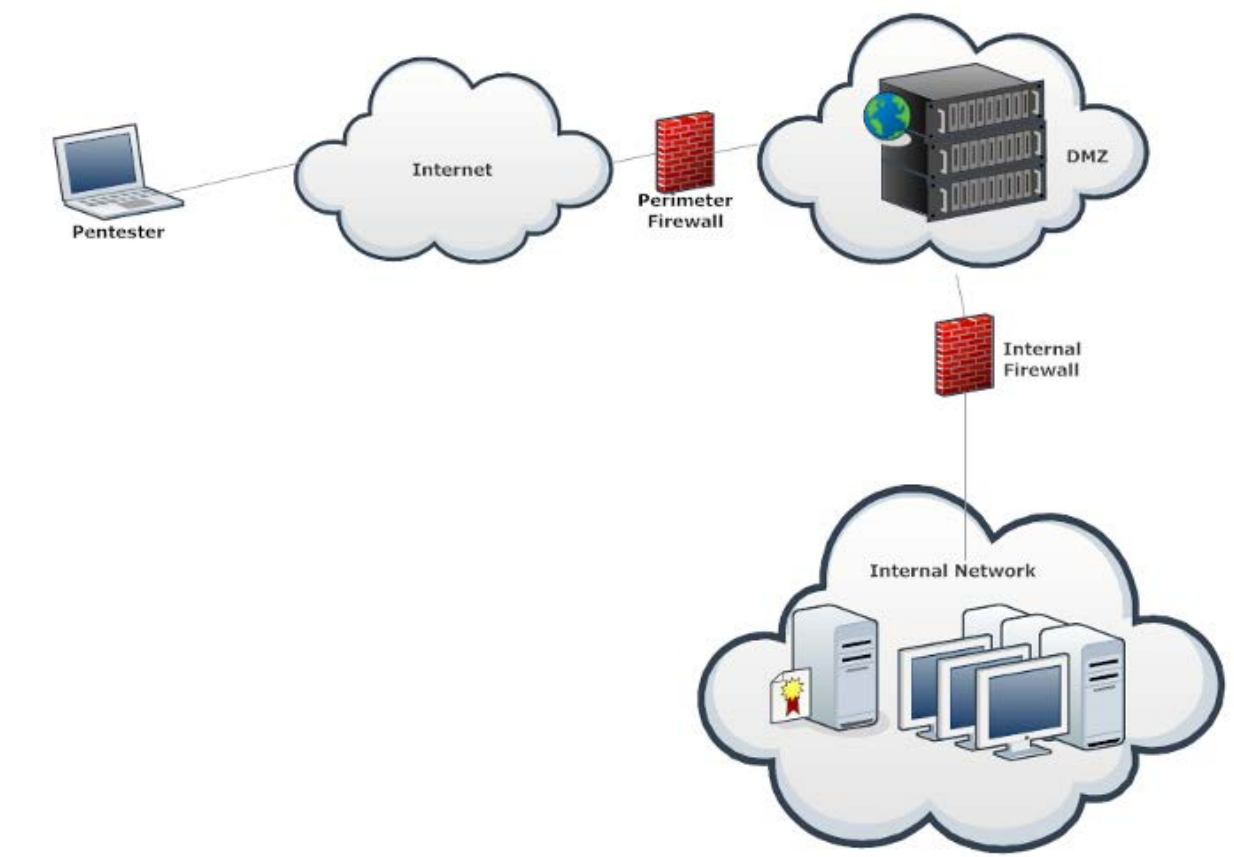
勒索病毒横行

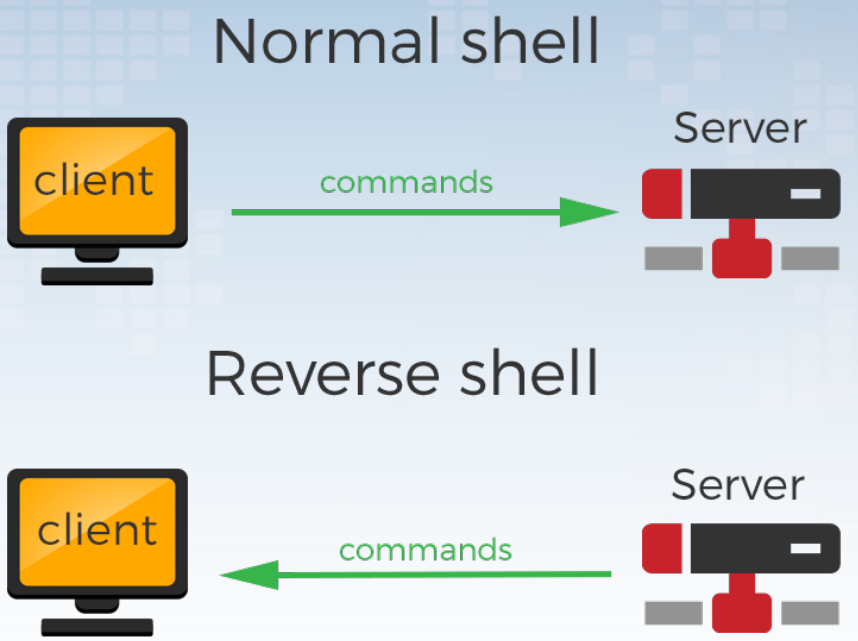




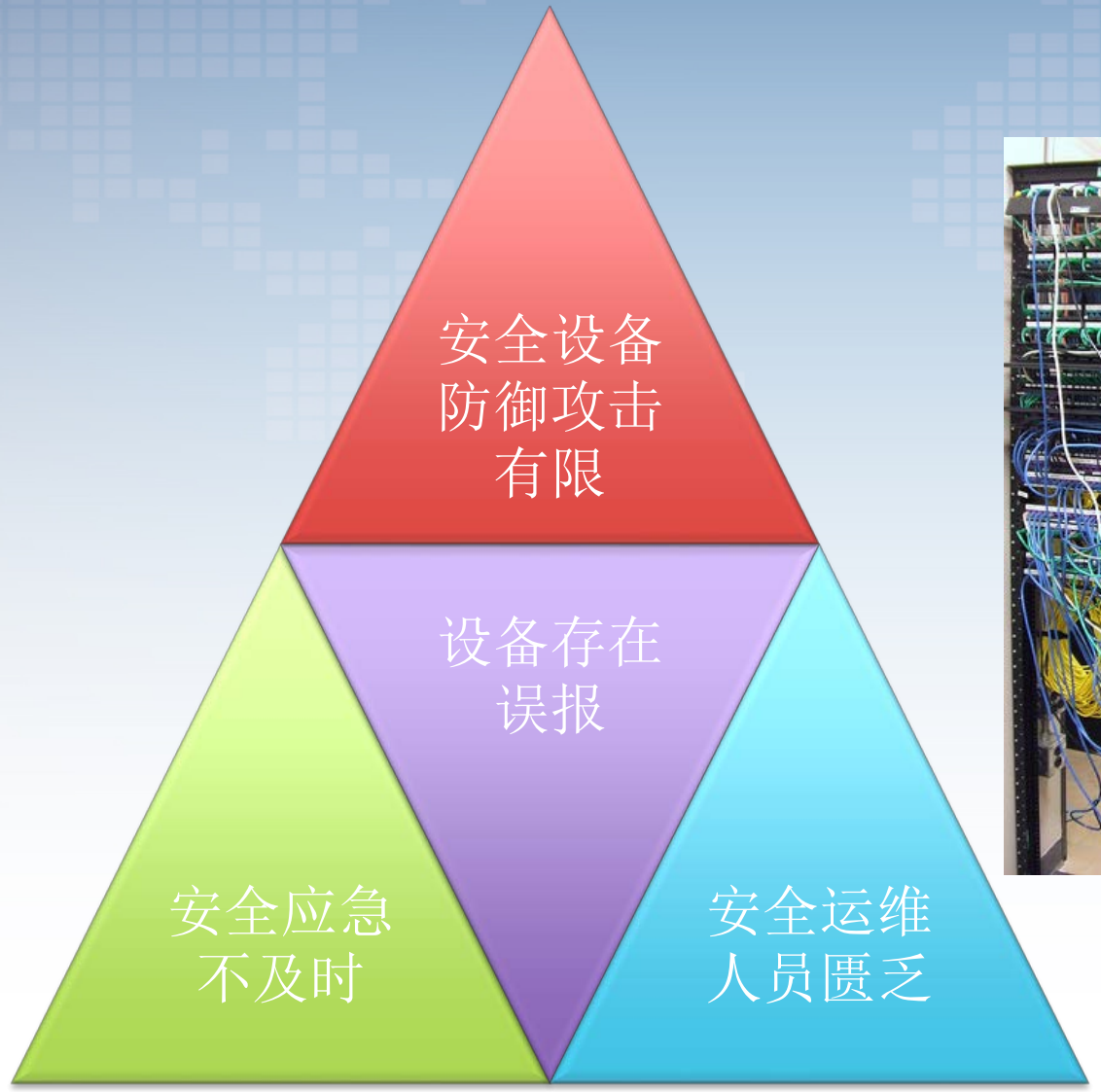
OWASP
Open Web Application Security Project

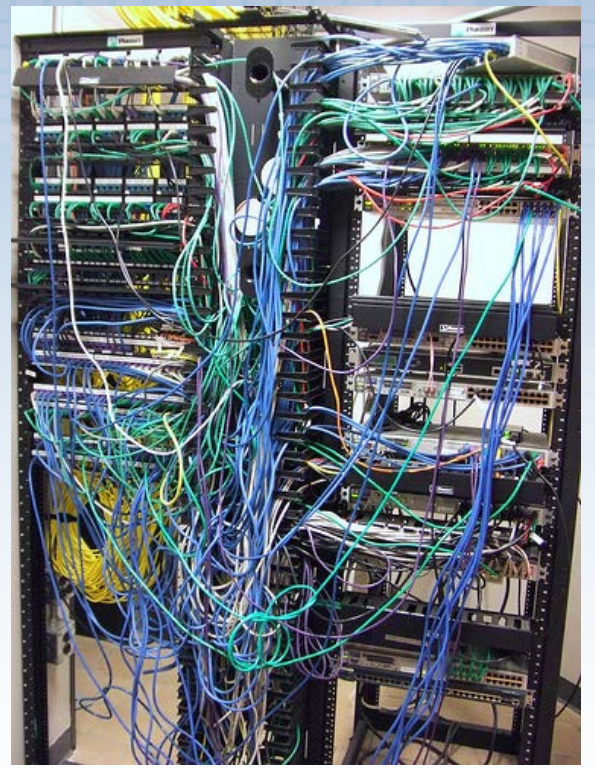
无法找出内网跳板肉鸡





安全现状





仅仅使用安全设备，面对当今错综复杂的安全问题显得束手无策

安全事件发生，无法分析原因和溯源

凤凰网财经 > 财经滚动新闻 > 正文

安全专家：币安遭遇“黑客+金融”式割韭菜 交易所是重灾区

2018-03-10 06:30:07

来源：新京报-财经频道

0人参与 0评论

原标题：安全专家：币安遭遇“黑客+金融”式割韭菜 交易所是重灾区

新京报快讯 (记者刘素宏)3月7日夜里，世界交易量排名第二的虚拟币交易平台币安(Binance)被黑客攻击，大量账户中的虚拟币被交易成比特币。数字货币交易平台币安的交易量在遭遇黑客攻击后不降反升。根据区块链业内人士介绍，交易手续费占数字货币交易所盈利的最主要部分。而根据币安官方网站公布，通常币安的交易手续费率为0.1%。按此粗略计算，币安每日的交易费收益在千万级。

本次币安所遭遇的黑客攻击与以往网络攻击有何不同?区块链去中心化特征下，遭遇网络攻击后损失是否会加大?用户如何加强个人防护?就此，寻找中国创客专访腾讯云云鼎实验室的掌门人董志强(网络ID：killer)，以及腾讯云云鼎实验室高级安全工程师喻峰。

币安回应黑客攻击事件：无法回滚交易 自行交易用户损失自担

2018-03-08 16:30:20

来源：凤凰网财经WEMONEY 作者：刘四红 2人参与 2评论

凤凰网WEMONEY讯 3月8日，数字货币交易所币安（Binance）针对3月7日晚VIA/BTC交易异动，触发自动停止提币事件进行了回应说明。

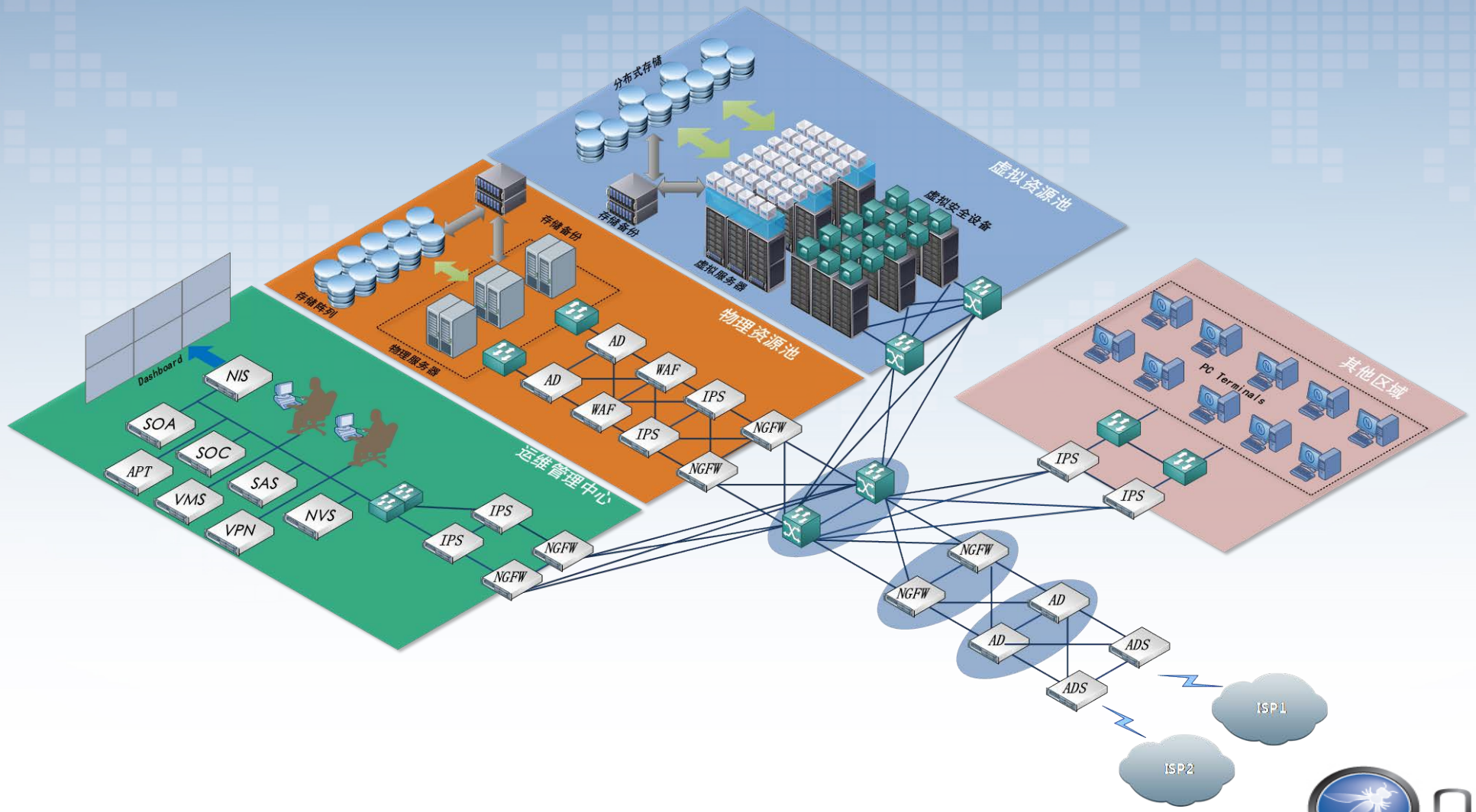
同时，币安一内部工作人员告诉凤凰网WEMONEY，在此次黑客攻击事件中，如果用户是因为被盗带来损失，币安将会进行处理；但如果是自行交易用户则不做处理。

OWASP Open Web Application Security Project

安全可知

铱迅信息技术股份有限公司

传统的网络



安全可知

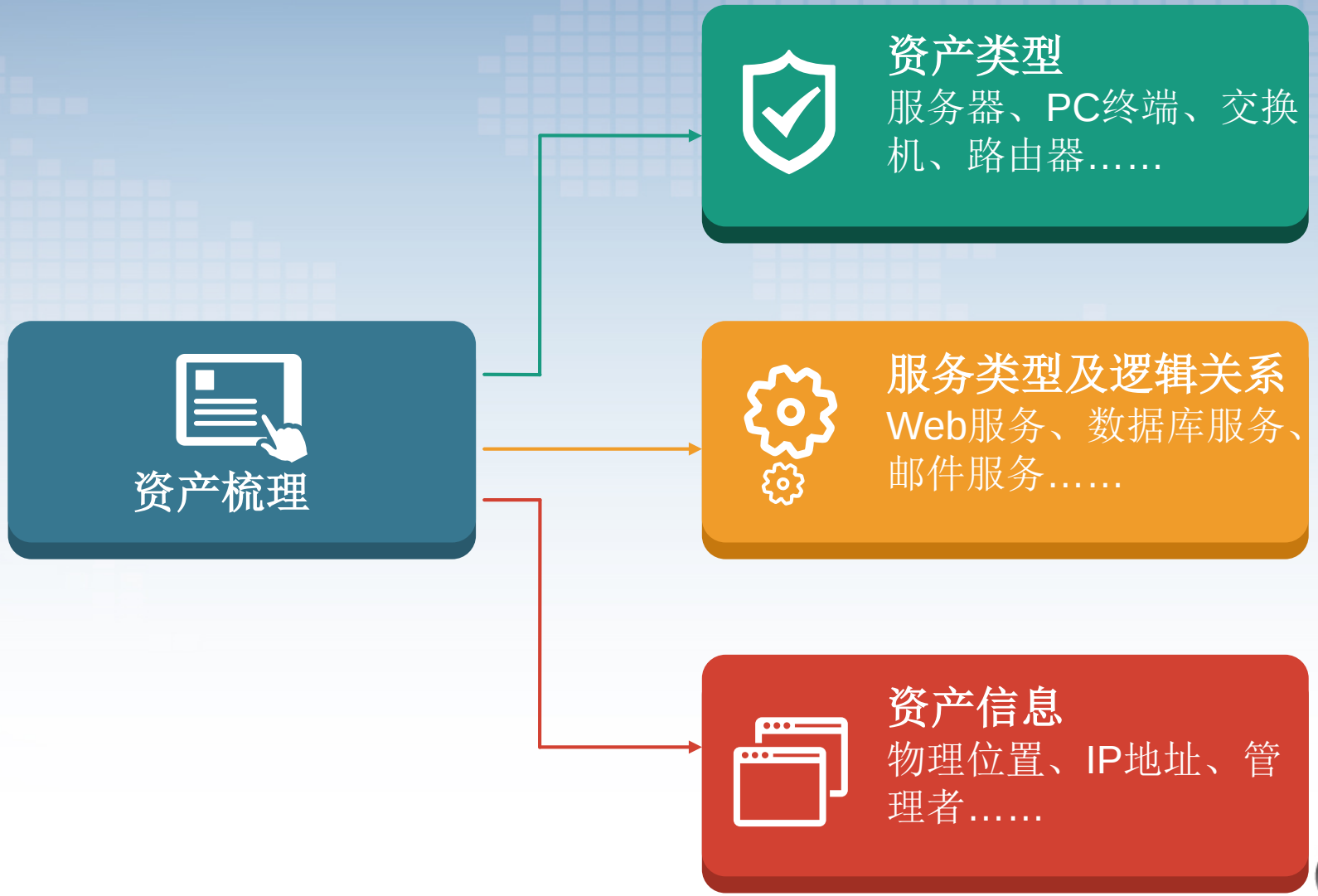
资产及漏洞识别

资产及漏洞识别

1. 定期识别主机、端口、域名、应用及中间件
2. 安全漏洞识别
3. 基线安全

资产及漏洞识别

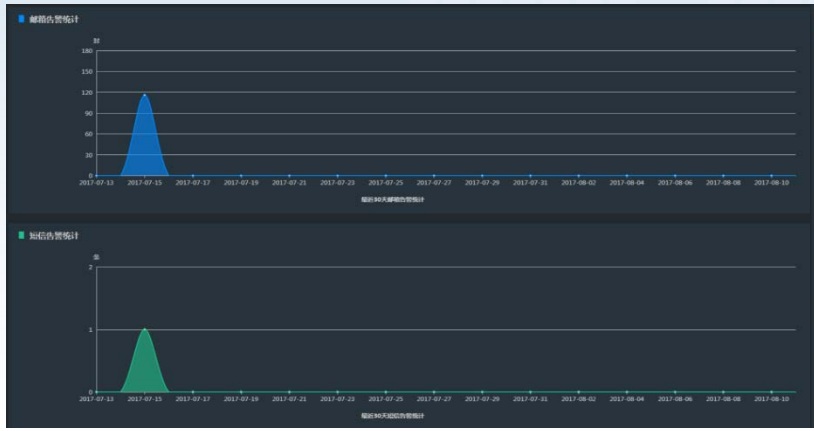
资产及漏洞识别

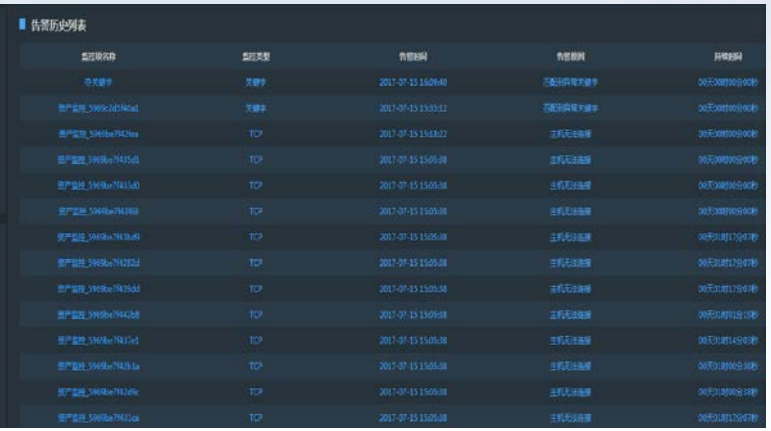


资产及漏洞识别

资产梳理

- 自动发现资产、感知资产信息
添加资产至监控任务进行实时管控





OWASP
Open Web Application Security Project

安全漏洞识别

- 漏洞扫描：操作系统、数据库、Web、弱口令等多个维度漏洞。

主机漏洞扫描
操作系统漏洞
数据库服务器漏洞
邮件服务器漏洞
网络设备漏洞
……

常用应用软件漏洞扫描
Vmware漏洞
KVM漏洞
Server-U漏洞
Lotus漏洞
……

Web漏洞扫描
SQL注入漏洞
跨站脚本漏洞
文件上传漏洞
代码执行漏洞
……

弱密码扫描
3389
SQL Server
ORACLE
SSH
……

OWASP
Open Web Application Security Project

基线安全

基线安全

类别	账号类	口令类		授权类
名称	应删除或锁定与设备运行、维护等工作无关的账号	对于采用静态口令认证技术的设备，口令长度至少6位，并包括数字、小写字母、大写字母和特殊符号4类中至少2类	对于采用静态口令认证技术的设备，帐户口令的生存期不长于90天	在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限
检查方法	设定被允许的帐号，一旦发现非法帐号，产生配置违规告警	检查/etc/default/passwd的配置，PASSLENGTH = 6 #设定最小用户密码长度为6位 ，MINALPHA=2；MINNONALPHA=1（表示至少含两个字母和一个非字母）	检查/etc/default/passwd的配置，MAXWEEKS=13 密码的最大生存周期为13周	etc/passwd、/etc/group必须所有用户都可读，root用户可写，/etc/shadow 只有root可见

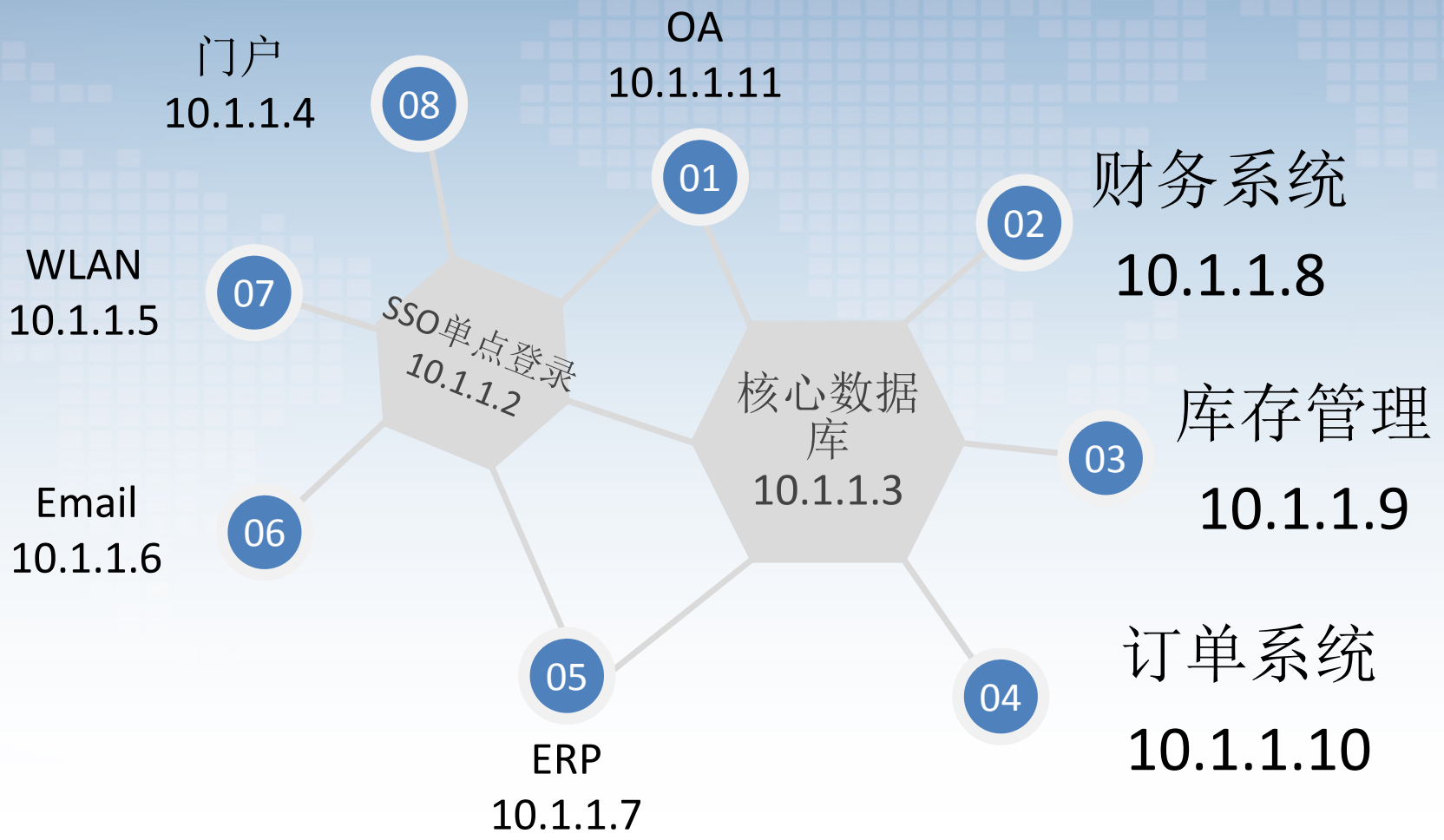
资产关系图绘制

资产关系图绘制

1. 应用依赖关系
2. 服务依赖关系
3. 网络关系

资产关系图绘制

应用依赖关系



服务依赖关系

蜜罐技术+态势感知侦测内网跳板

态势感知-技术架构

态势感知-检测威胁-安全事件采集

网站监控

- 健康监控
- 异常告警
- 挂马监控
- 暗链监控
- 篡改监控
- 关键词监控
- 图片OCR监控

态势感知-检测威胁-安全事件采集

攻击态势可视

- 处理WAF/IPS/NGFW等安全设备日志
- 动态对攻击情况进行展示和溯源

态势感知-检测威胁-安全事件采集

安全态势感知

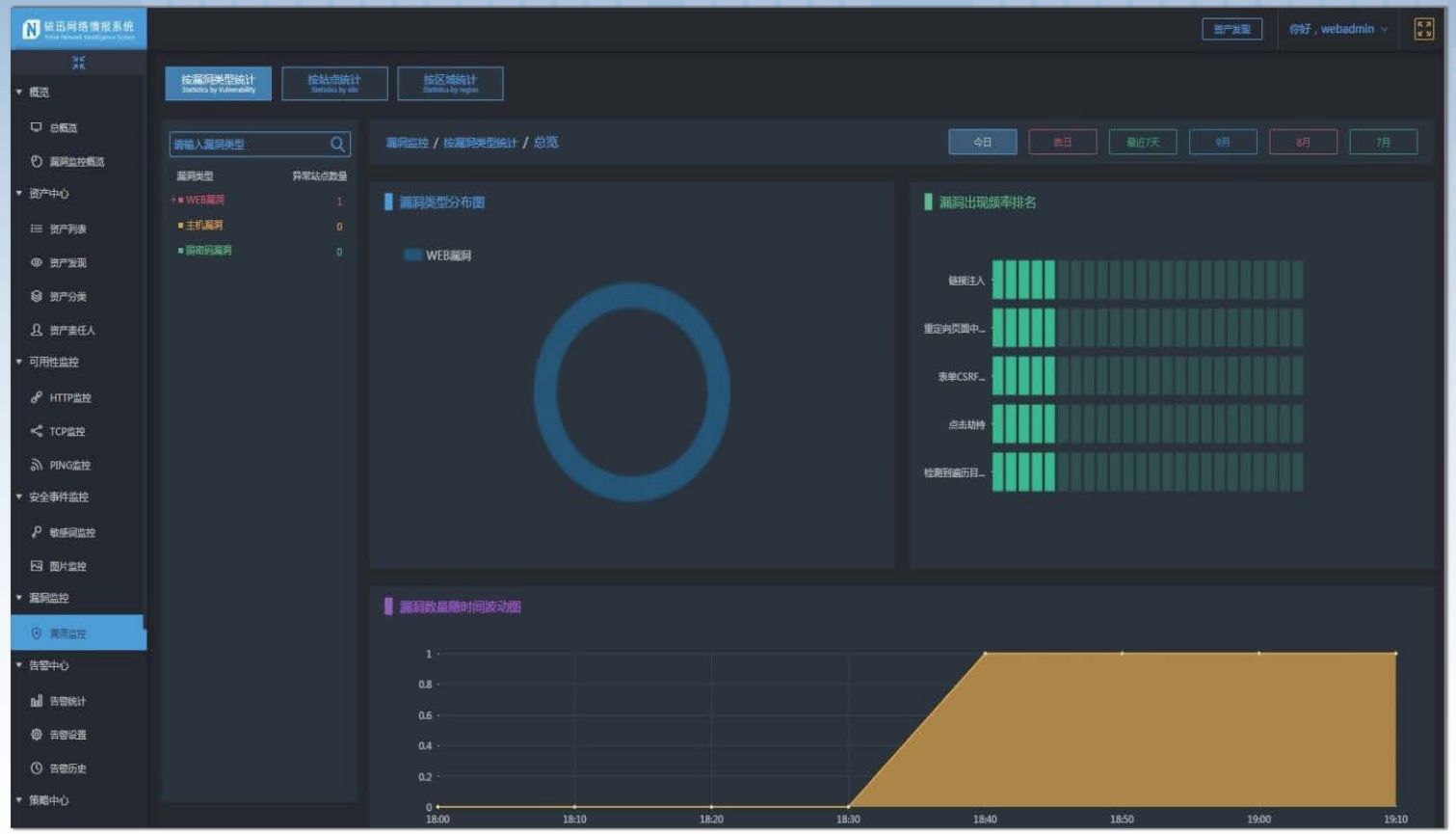
- 实时监测漏洞、暗链、网站挂马、篡改和异常访问情况。
- 数学模型分析安全事件

OWASP
Open Web Application Security Project

态势感知-功能模块-漏洞扫描

漏洞扫描

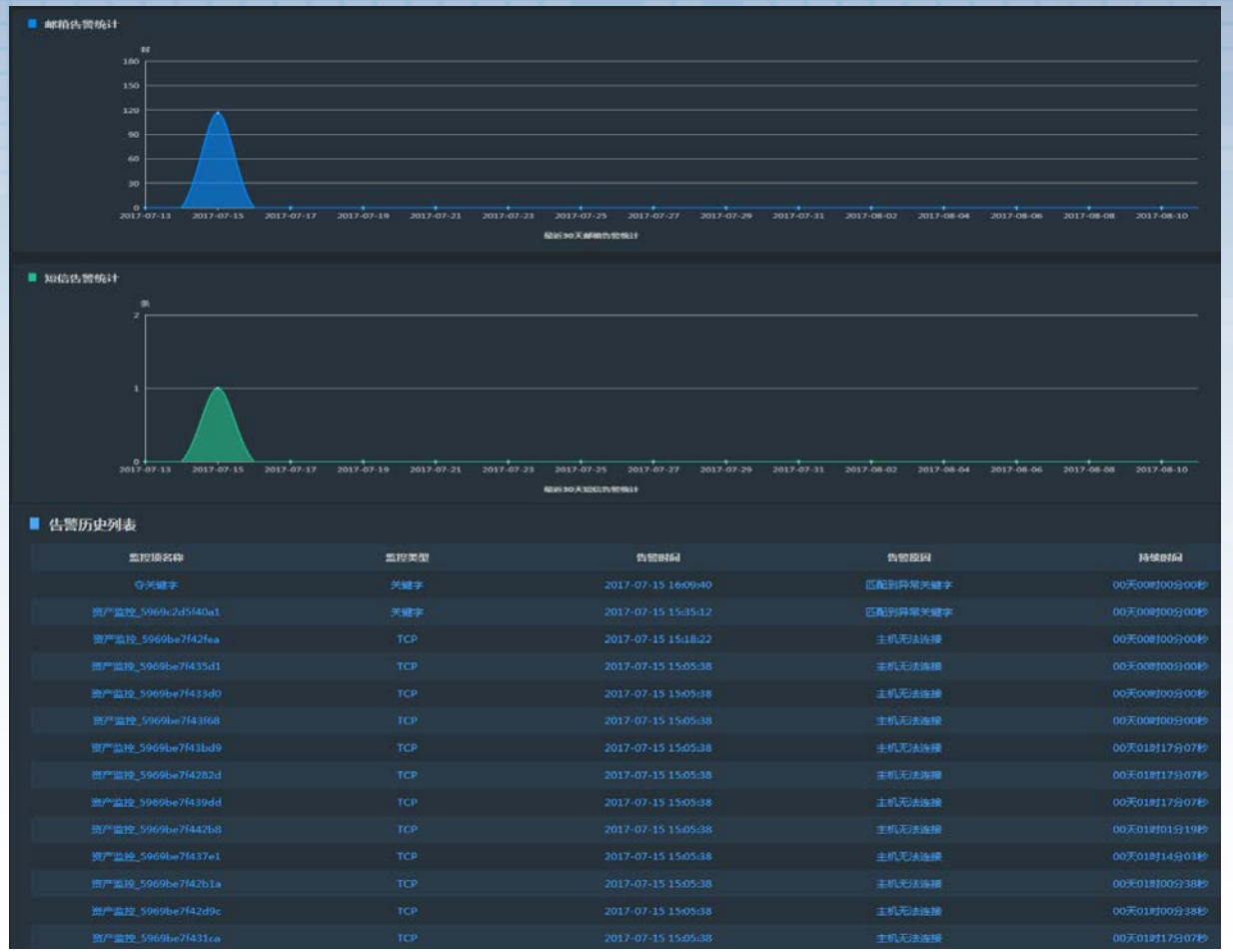
- 扫描Web漏洞
- 扫描系统漏洞
- 扫描弱口令



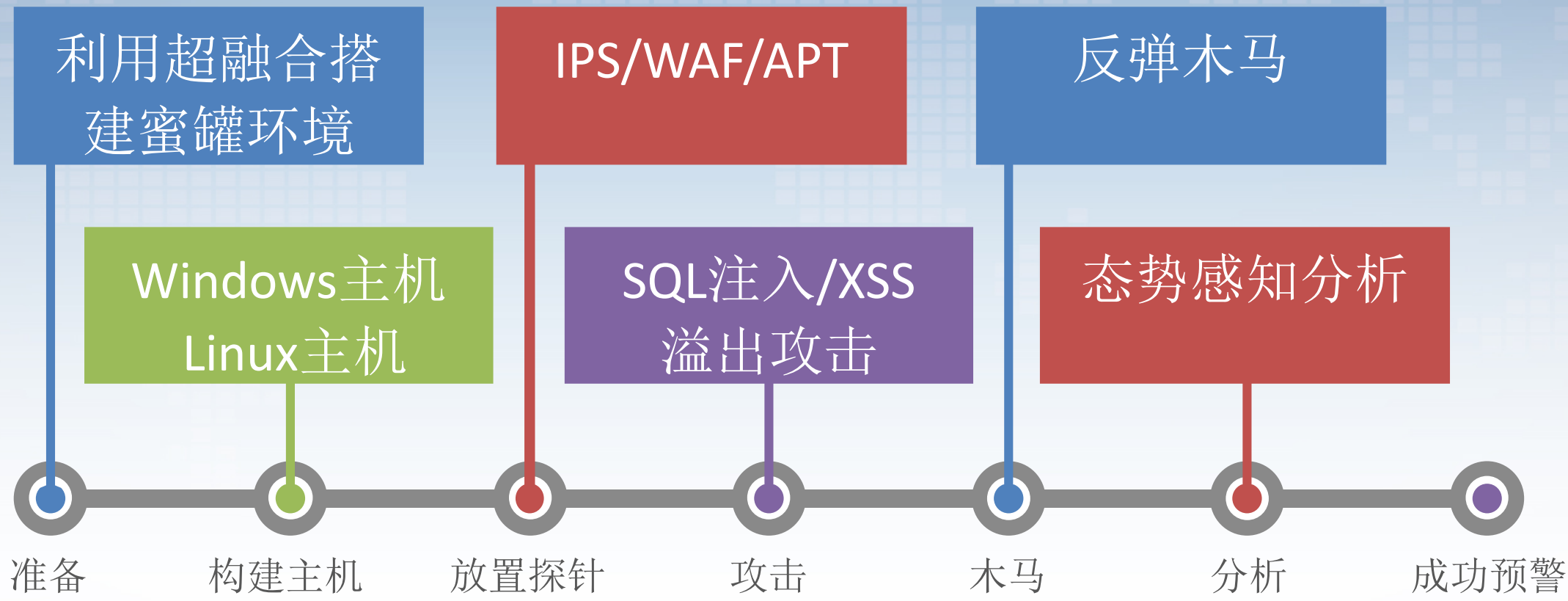
态势感知-检测威胁-安全事件采集

预警平台

- 实时分析挖掘监控目标的各类信息数据
- 分析威胁并及时预警。



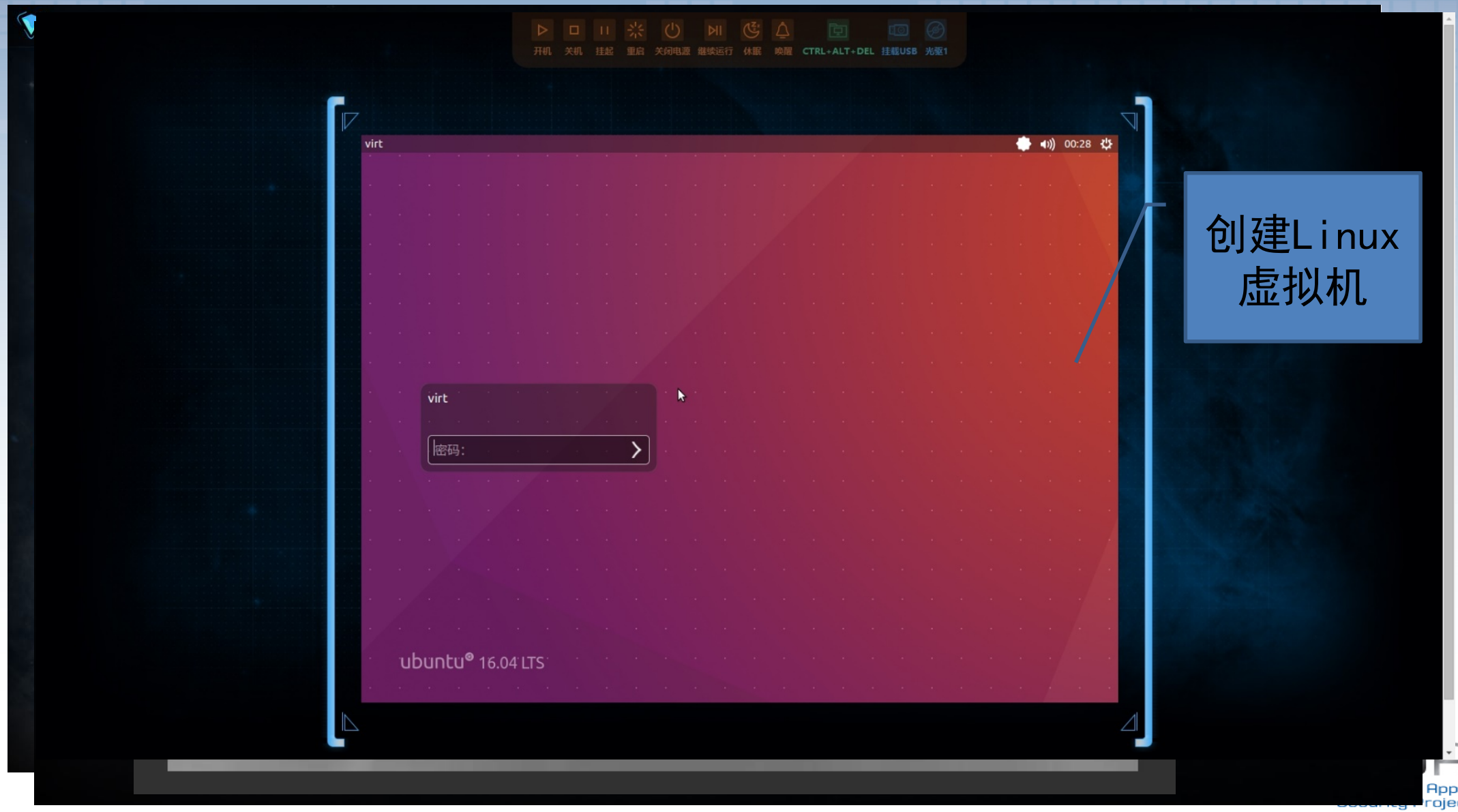
蜜罐技术+态势感知侦测内网跳板



蜜罐技术+态势感知侦测内网跳板

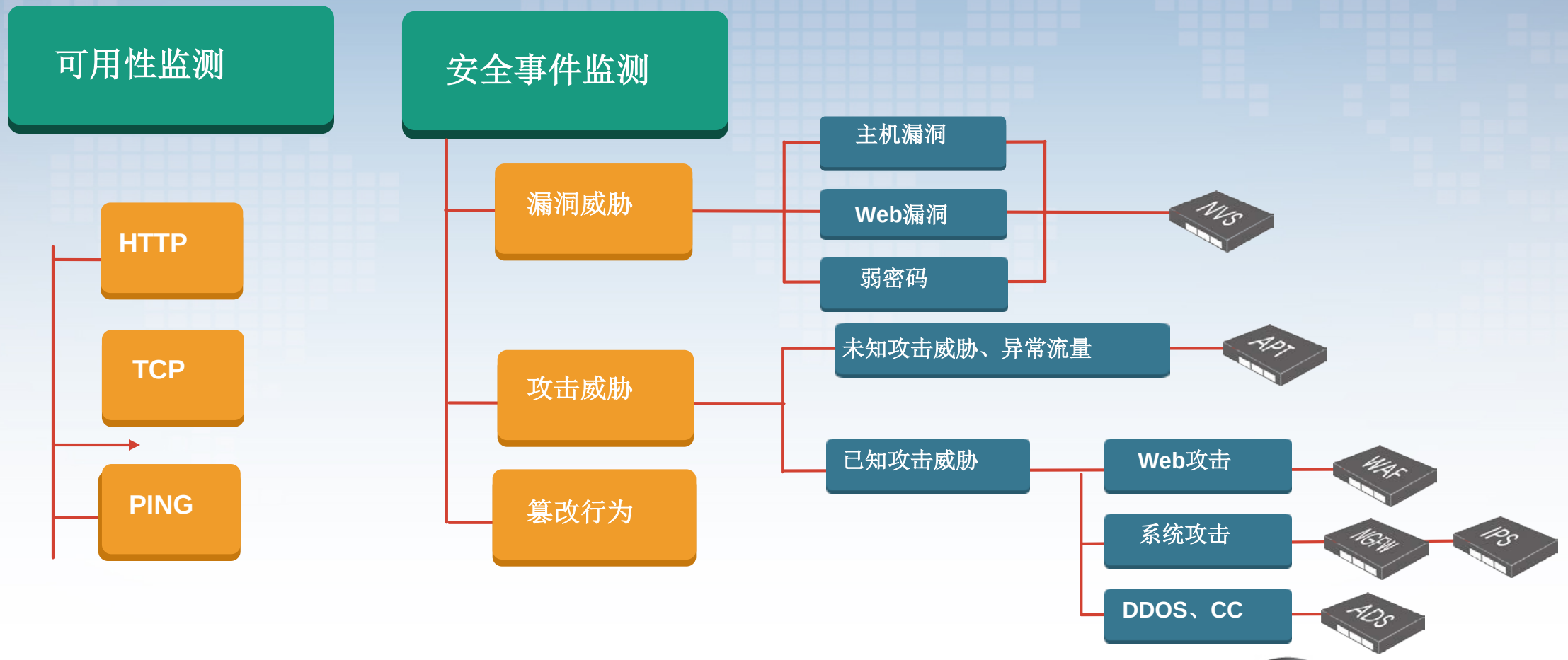
利用超融合技术构建虚拟网络和服务器环境

蜜罐技术+态势感知侦测内网跳板



蜜罐技术+态势感知侦测内网跳板

- 部署采集器：对可用性、安全事件进行监测

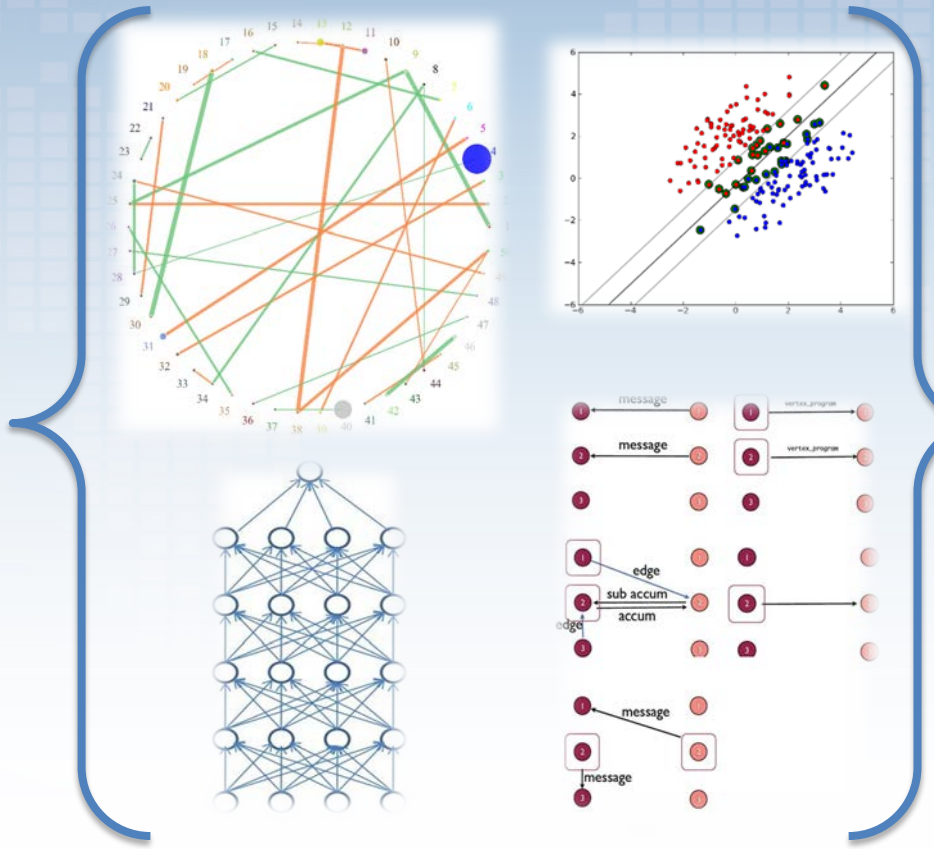


蜜罐技术+态势感知侦测内网跳板

OWASP
Open Web Application Security Project

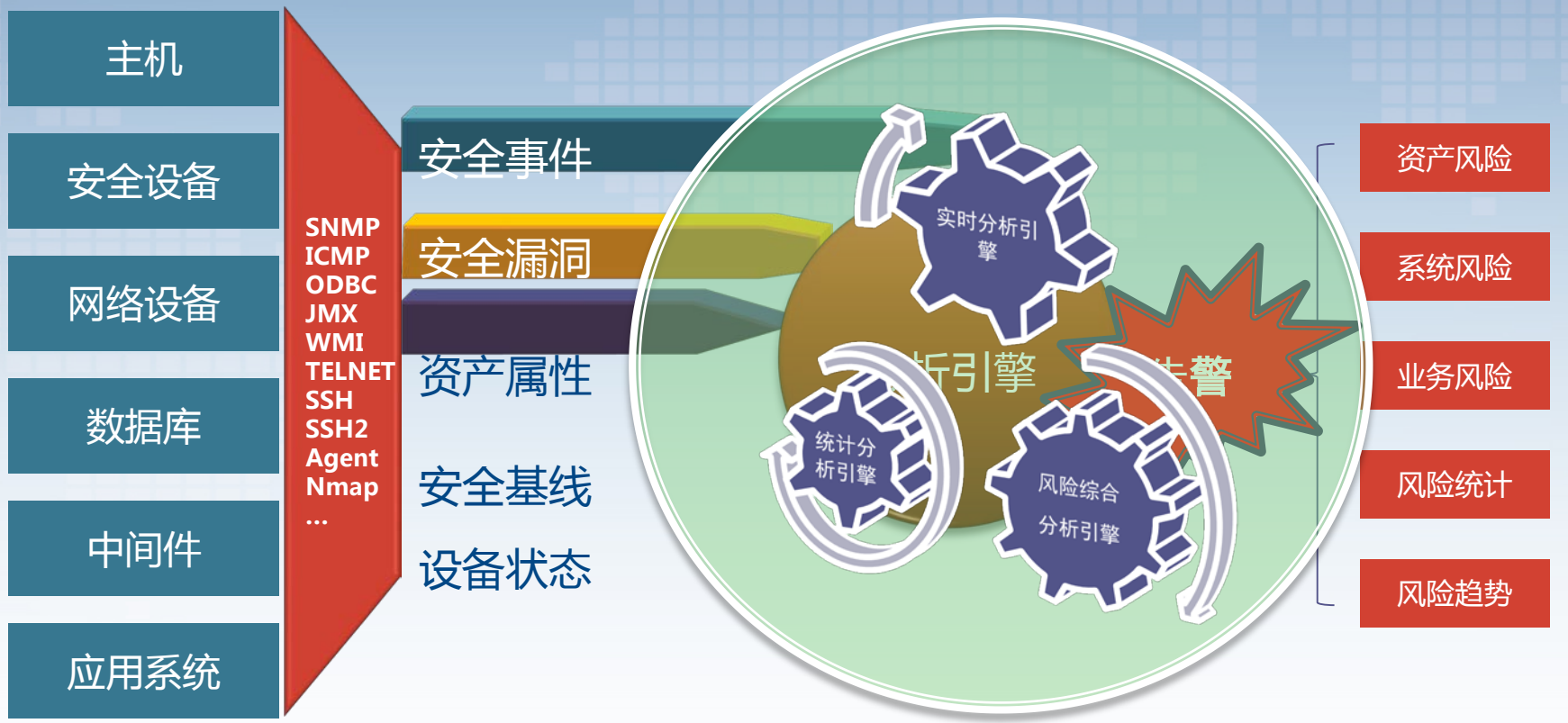
蜜罐技术+态势感知侦测内网跳板

- 安全事件数学分析引擎：采用但不限于神经网络、相关性分析、SVM等方法对安全事件进行分析，并从千万条告警信息中找出有价值的攻击事件。



安全日志实时留存与实时分析告警

安全日志实时留存与实时告警分析



安全对象 → 风险采集 → 存储管理 → 风险分析 → 风险呈现 → 威胁预警

安全日志实时留存与实时告警分析

采集控制器

login failed

login failed

login failed

login failed

login failed

login success

服务器发出的syslog日志

用户服务器

已标准化的原始事件序列

user:root/pwd:bbb

user:root/pwd:bbb

user:root/pwd:bbb

user:root/pwd:bbb

user:root/pwd:bbb

尝试输入账号和密码

关联分析

user:root
pwd:real

核心分析服务器

State1(filter(EventName ==‘登录失败’),60,5,’DIP’)
Followed_by(State1.DIP==State2.DIP)
State2(filter(EventName ==‘登录成功’),60,1,’DIP’)

日志审计工作台

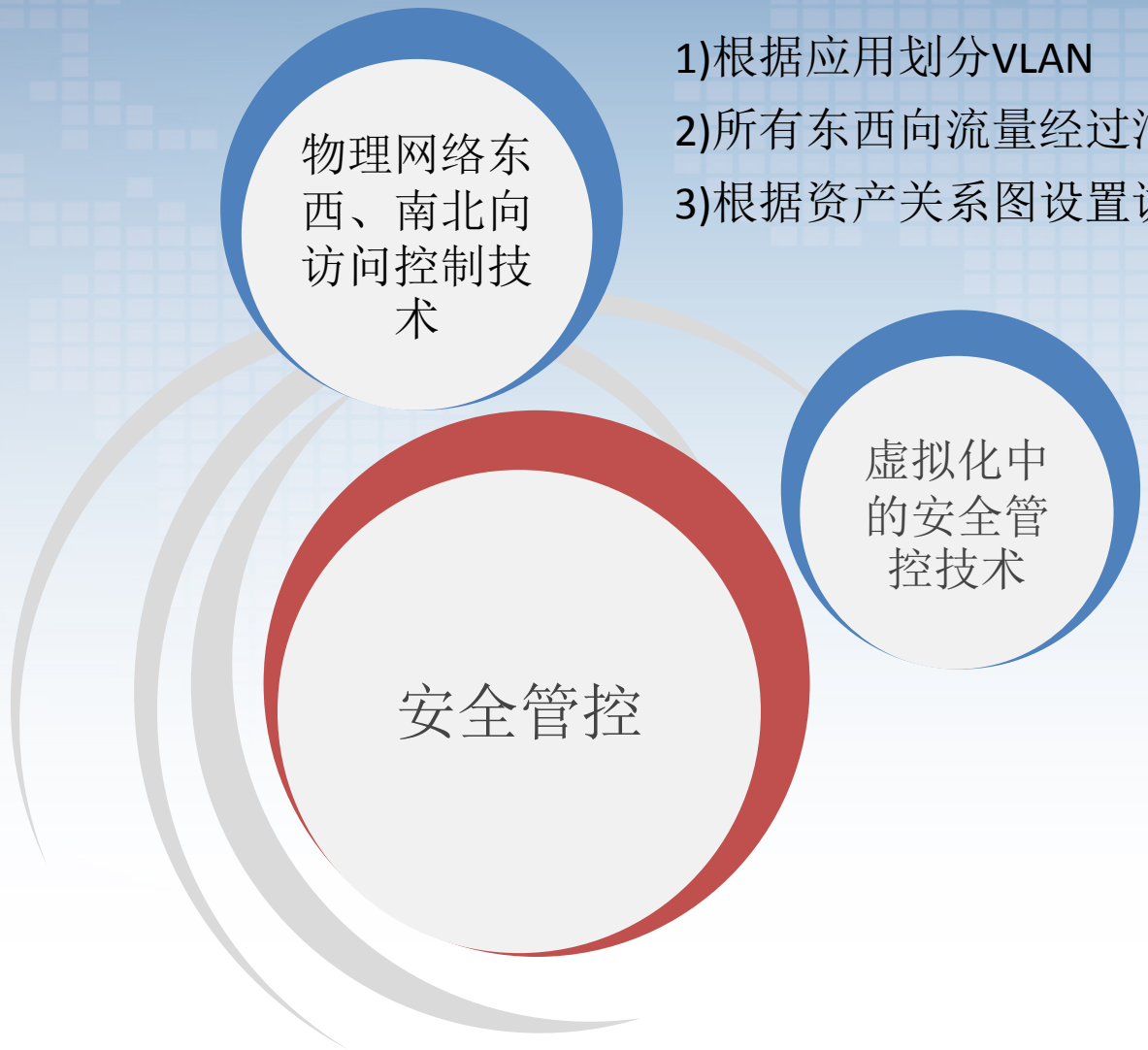
入侵者

OWASP
Open Web Application Security Project

安全管控

铱迅信息技术股份有限公司

安全管控

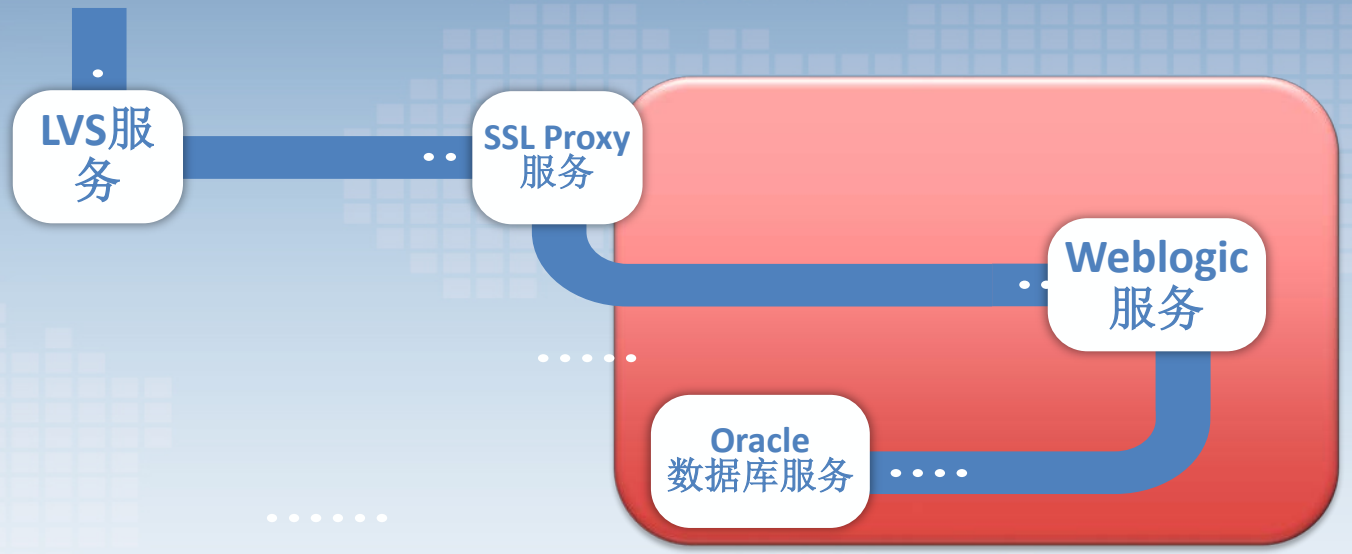


1)根据应用划分VLAN
2)所有东西向流量经过汇聚
3)根据资产关系图设置访问控制策略

1)VXLAN技术
2)SDN软件定义网络技术
3)SDS软件定义安全技术
4)无代理防病毒技术

物理网络东西、南北向访问控制技术

物理网络下高强度的内网东西、南北向访问控制技术



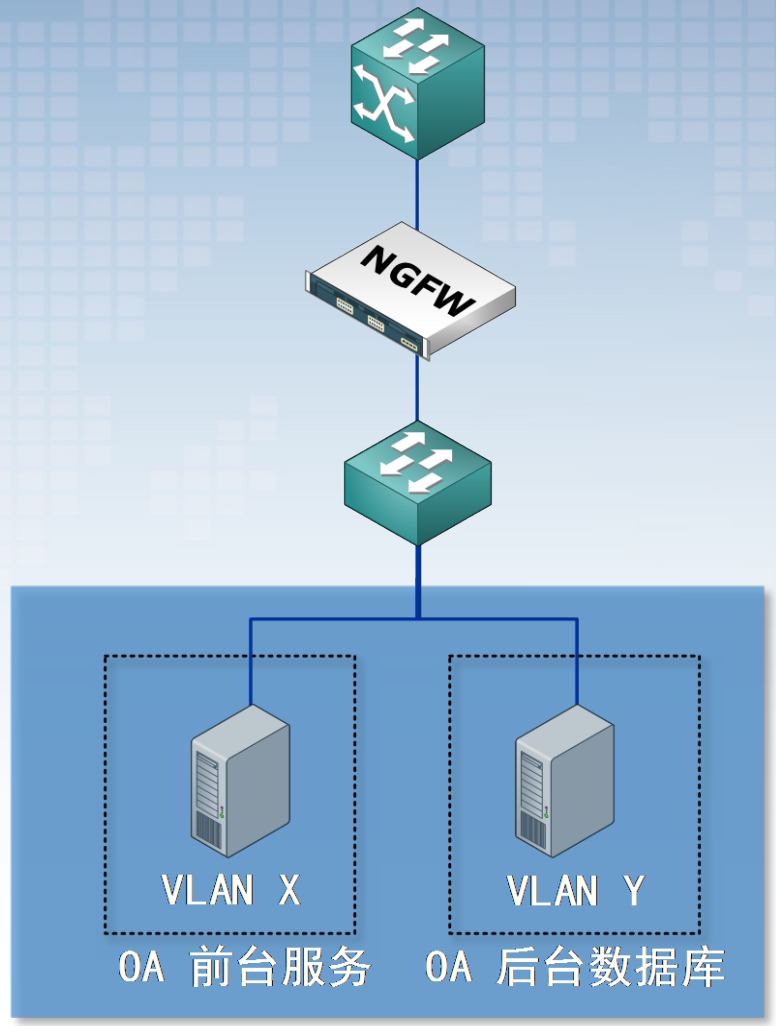
添加 | 删除 | 启用 | 停用 | 上移 | 下移 | 刷新 | 应用 | 冲突检测

序号	名称	描述	是否启用	动作	生效时段
1	允许任意地址访问Web端口	0.0.0.0/0 -> 192.168.1.3:80	已启用	放行	全天
2	允许Web访问Oracle端口	192.168.1.3 -> 192.168.1.10:1521	已启用	放行	全天
3	禁止任意IP访问Oracle服务器	0.0.0.0/0 -> 192.168.1.10	已启用	丢弃	全天
4	禁止任意IP访问Web服务器	0.0.0.0/0 -> 192.168.1.3	已启用	丢弃	全天
5	全部禁止	0.0.0.0/0 -> 0.0.0.0/0	已启用	丢弃	全天

物理网络下高强度的内网东西、南北向访问控制技术

访问控制策略：

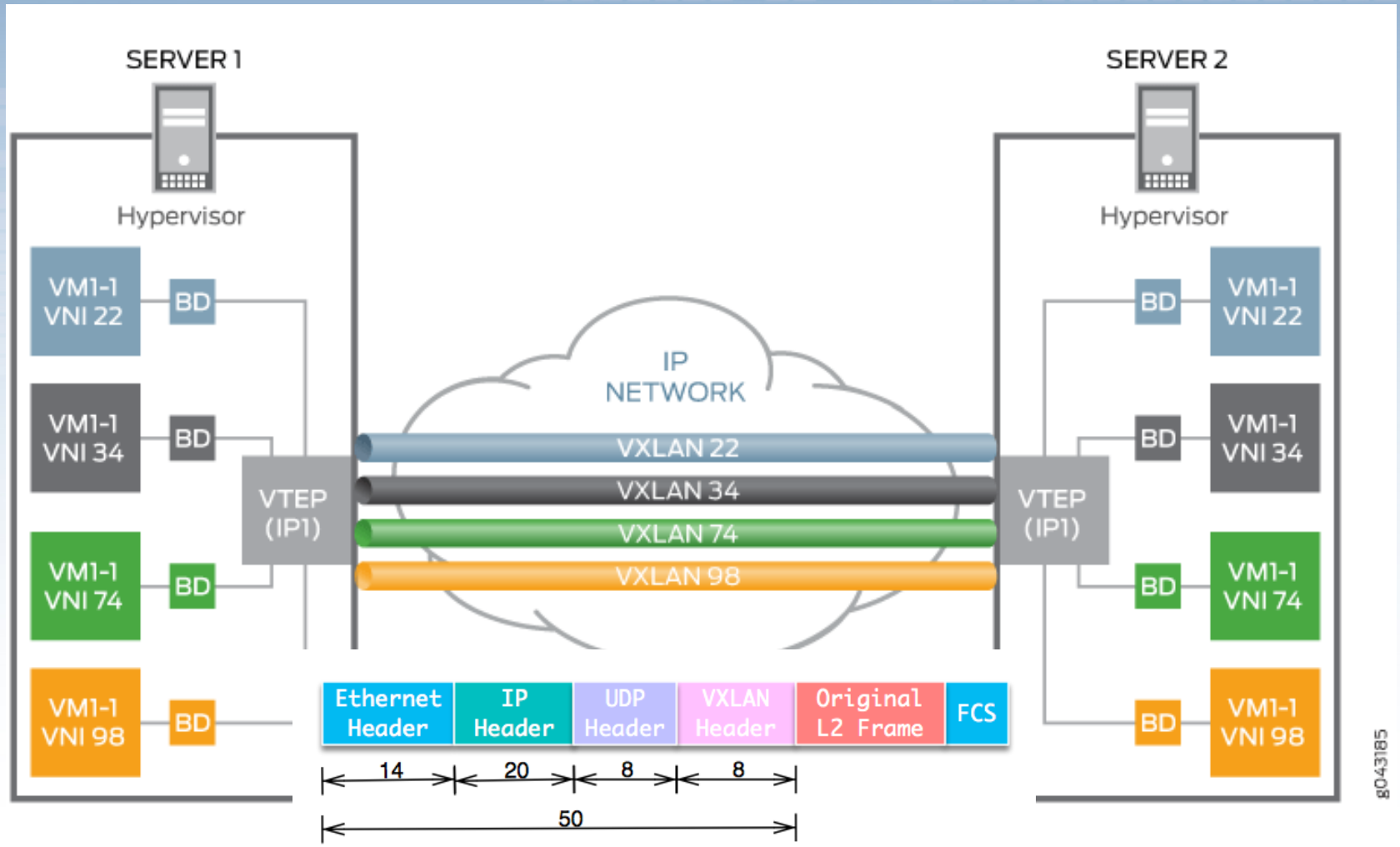
- 允许办公人员访问OA前台服务器的80端口（单向）
- 允许OA前台服务器访问后台数据库的端口（单向）
- 允许管理员IP或堡垒机IP可以访问2台服务器（单向）
- 允许2台服务器向日志发送到综合安全管理平台（单向）
- 其他一律拒绝



物理网络下高强度的内网东西、南北向访问控制技术

虚拟化中的安全管控技术

虚拟化中的安全管控技术-VXLAN技术

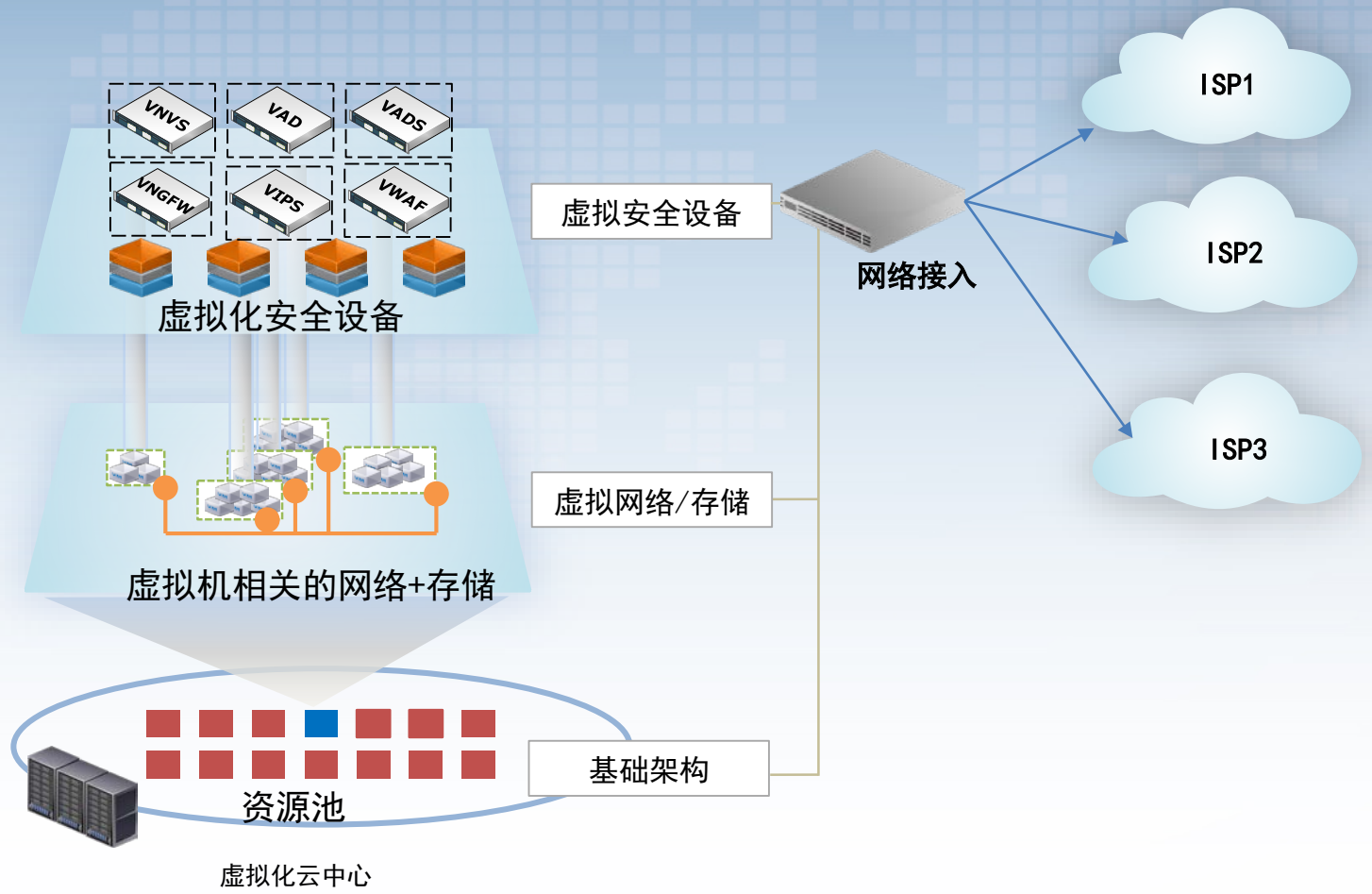


虚拟化中的安全管控技术-SDN软件定义网络技术

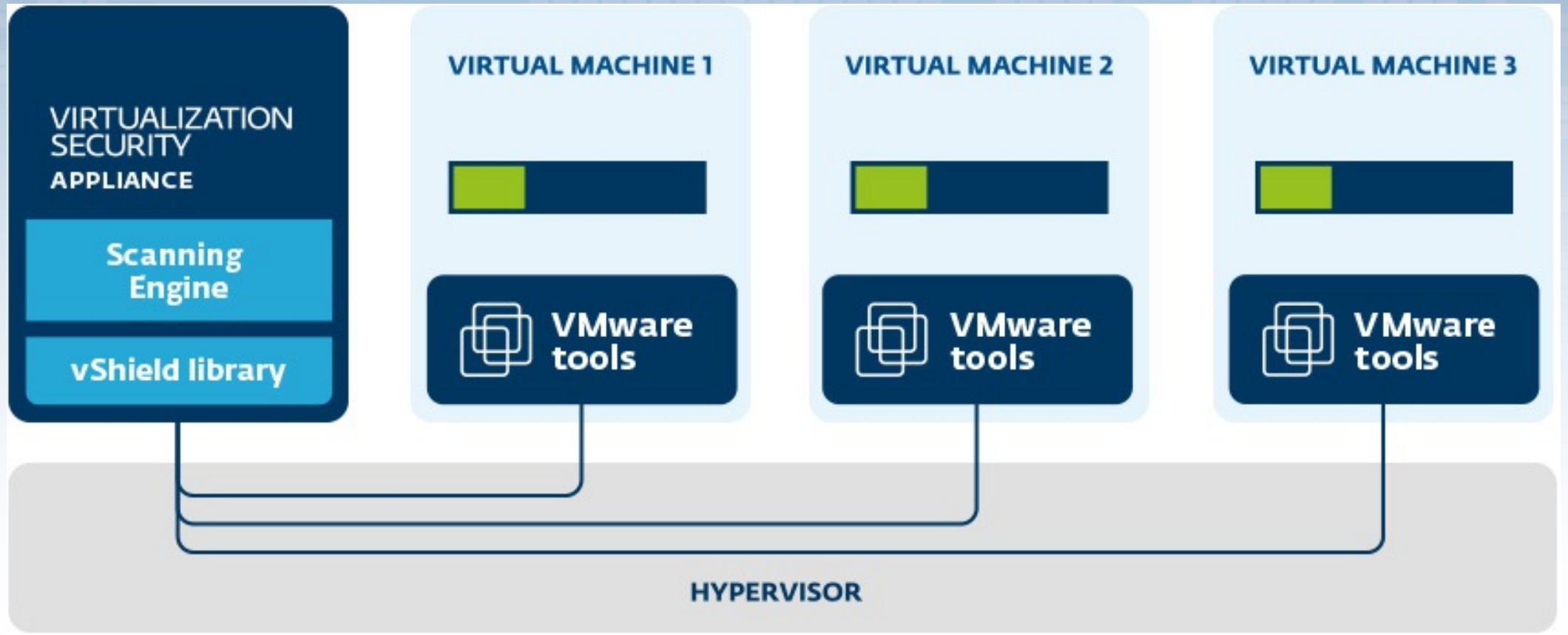
虚拟化中的安全管控技术-SDS软件定义安全技术

软件定义安全

- 软件定义安全技术（SDS），通过利用虚拟化技术，借助标准的计算单元创造一个安全设备。
- 根据一定维度（如应用类型、应用重要性、租户群体等）将虚拟机划分区域，对各个区域进行独立的东西南北向防护。



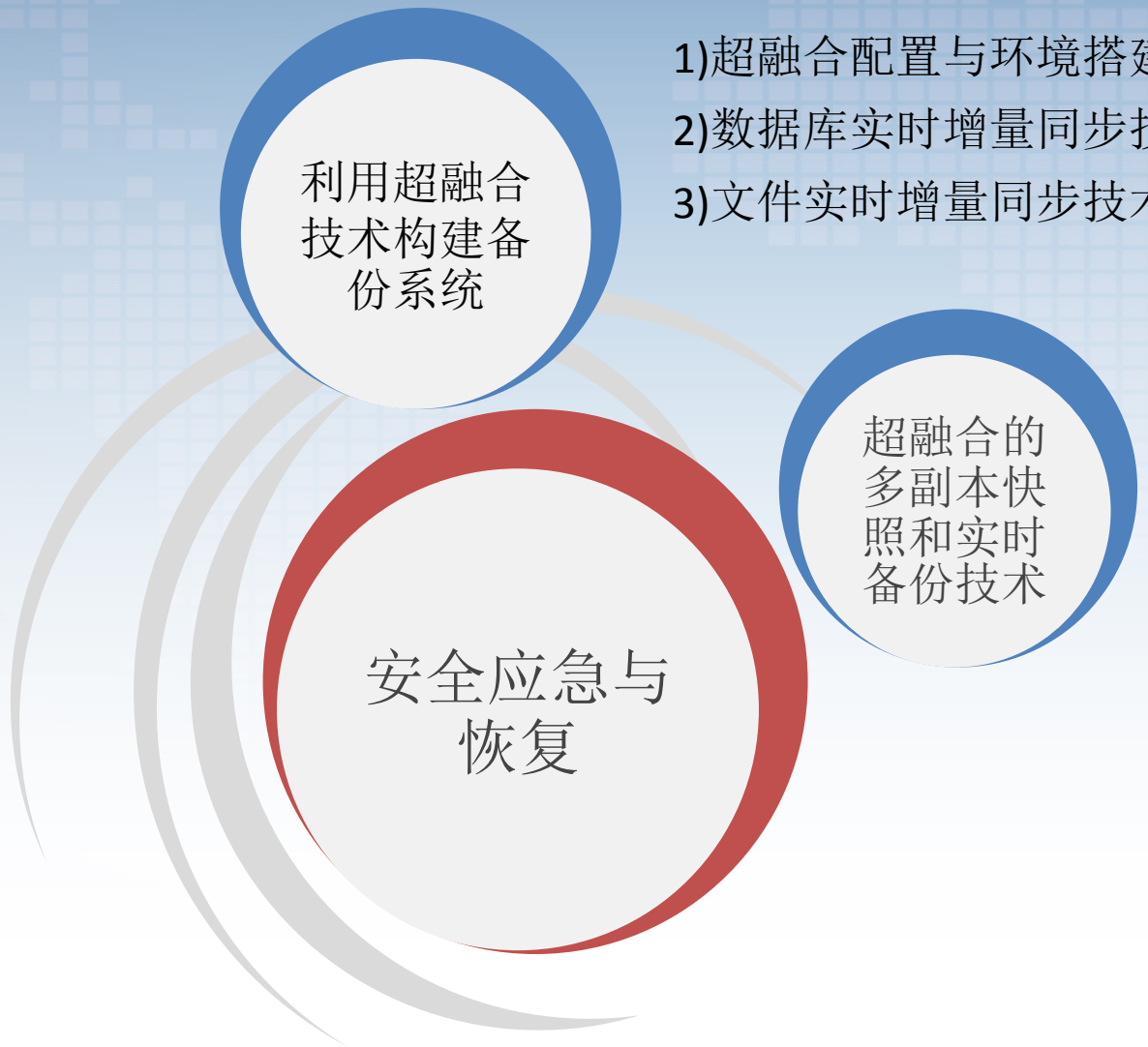
虚拟化中的安全管控技术-无代理防病毒技术



安全应急与恢复

铱迅信息技术股份有限公司

安全应急与恢复

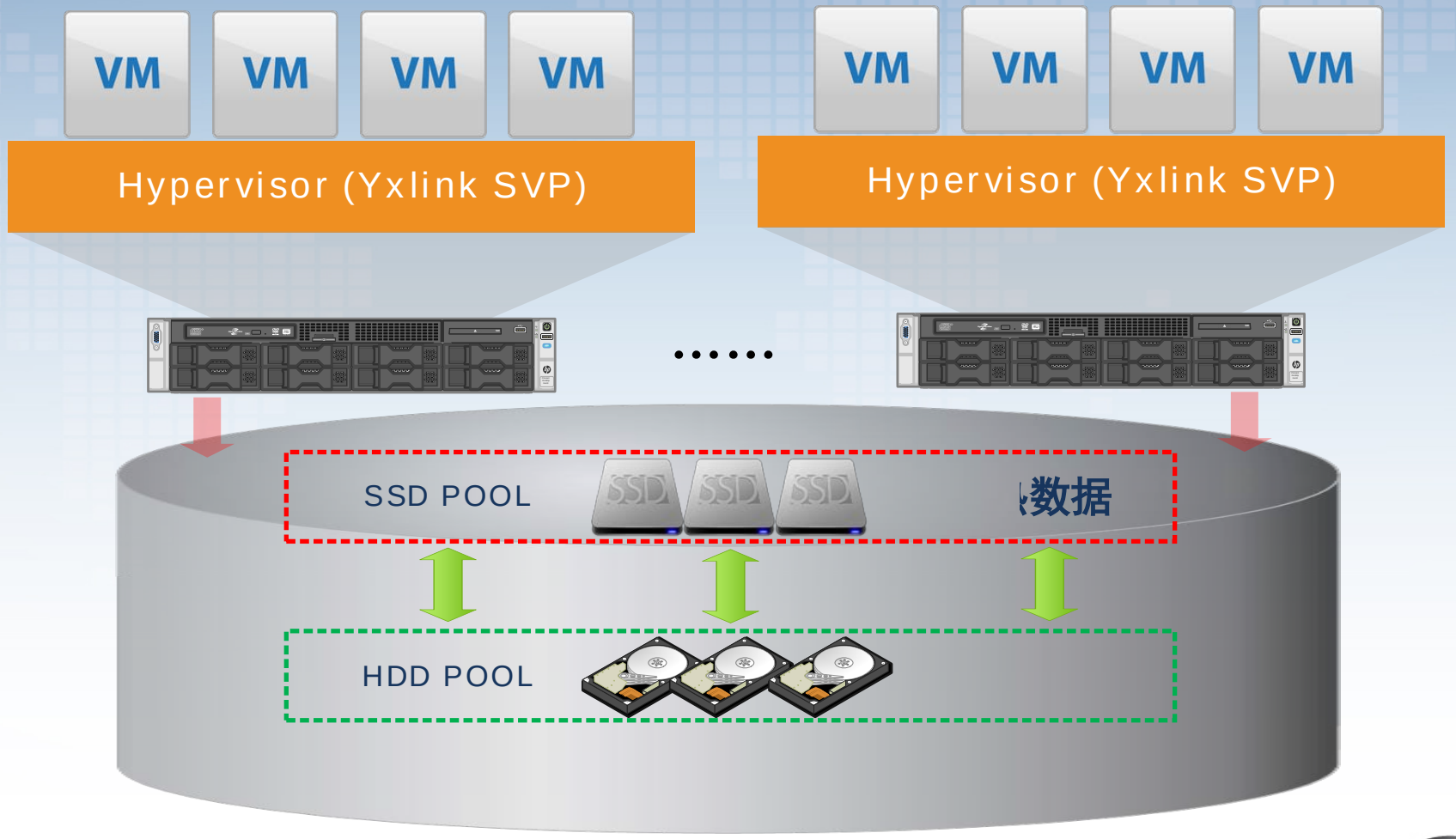


1)超融合配置与环境搭建
2)数据库实时增量同步技术
3)文件实时增量同步技术

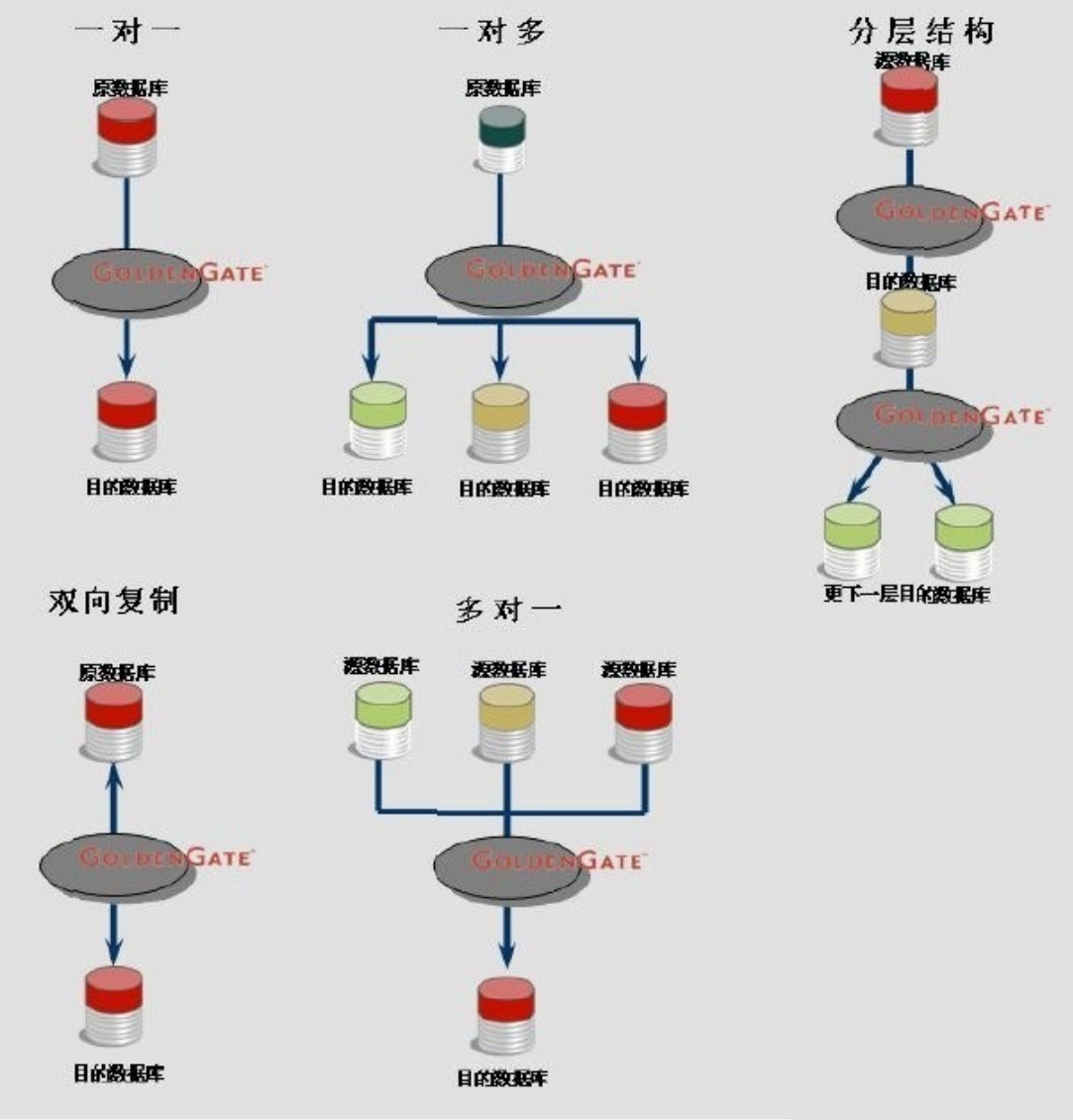
1)超融合的多副本分布式文件系统
2)超融合的磁盘及内存快照技术

利用超融合技术构建备份系统

超融合配置与环境搭建



数据库实时增量同步技术

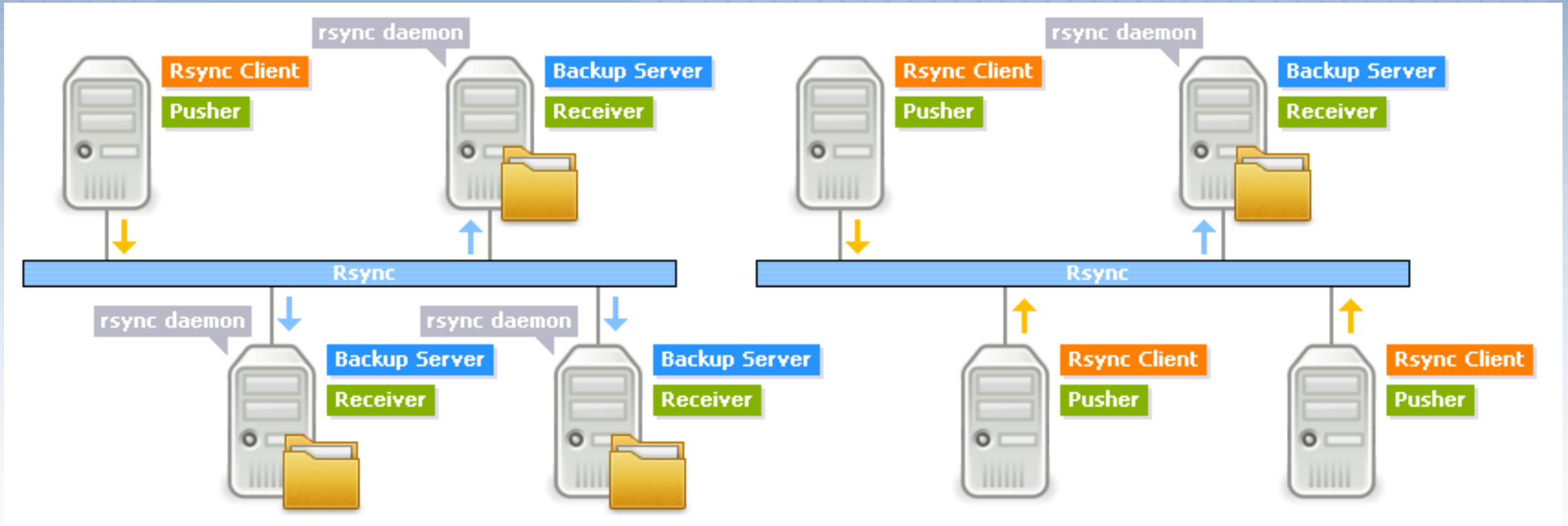


Oracle GoldenGateTDM

可以提供可靠的数据复制：

保证事务一致性
检查点机制保障数据无丢失
可靠的数据传输机制

文件实时增量同步技术



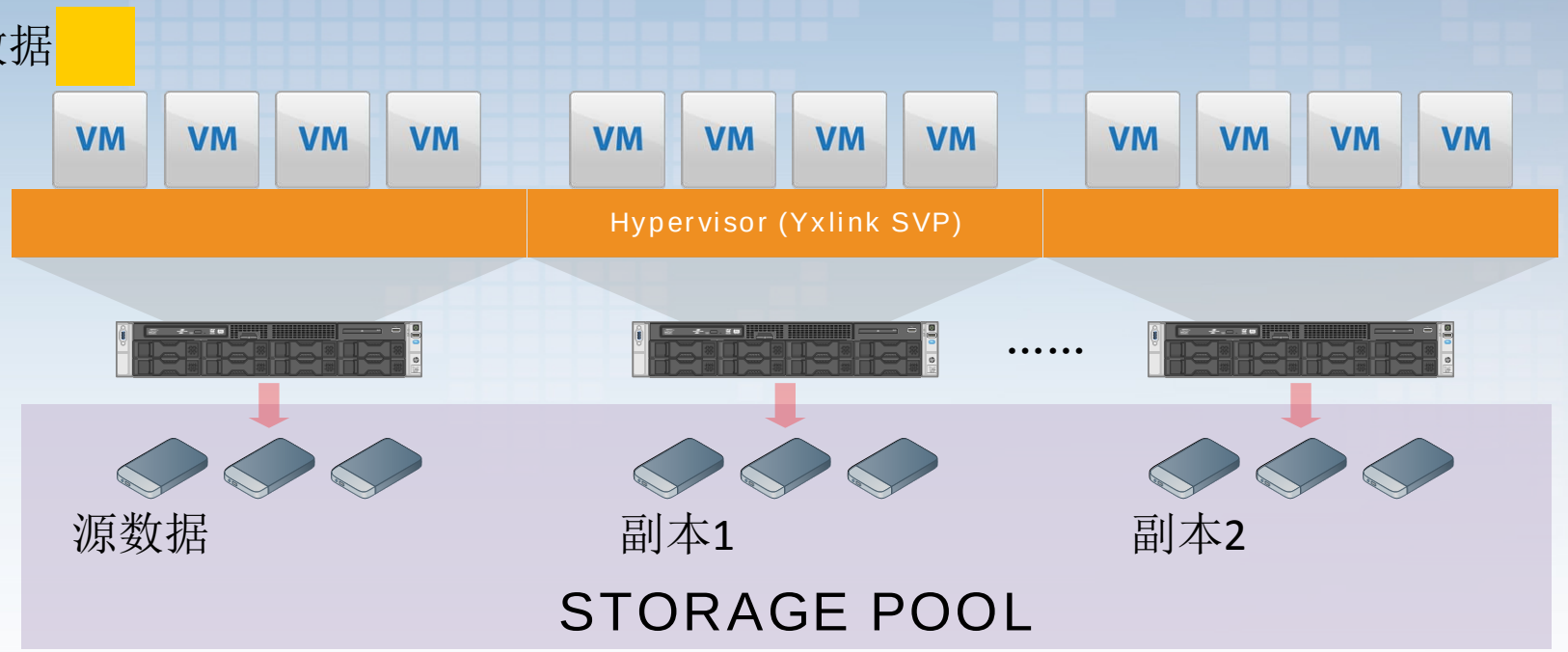
Rsync，它使用所谓的“Rsync演算法”来使本地和远程两个主机之间的文件达到同步，这个算法只传送两个文件的不同部分，而不是每次都整份传送，因此速度相当快。

超融合的多副本快照和实时备份技术

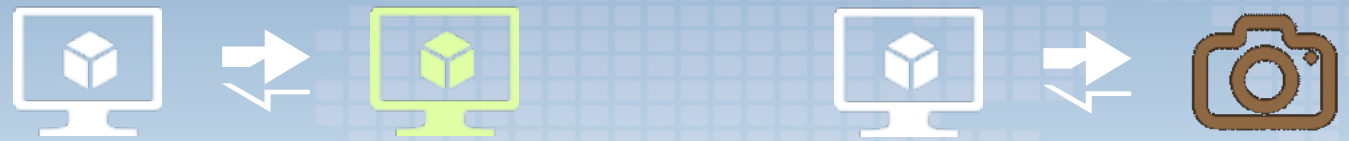
超融合的多副本分布式文件系统

多副本技术

- 当数据（虚拟机、快照、文件等等）写入磁盘时，根据用户设置的副本数量，会被自动“同步”写入到另1个或者多个的节点之中。
- 1：X副本比例，X≥5。



超融合的磁盘及内存快照技术



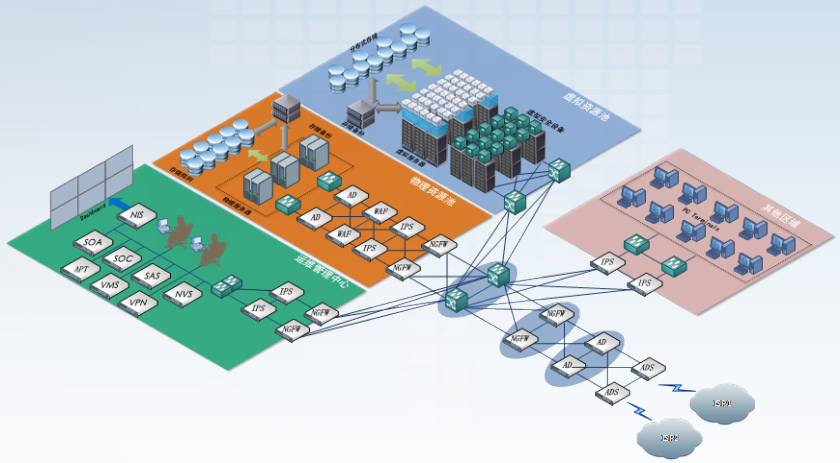
增量快照
（天）

无需
备份软件
备份主机

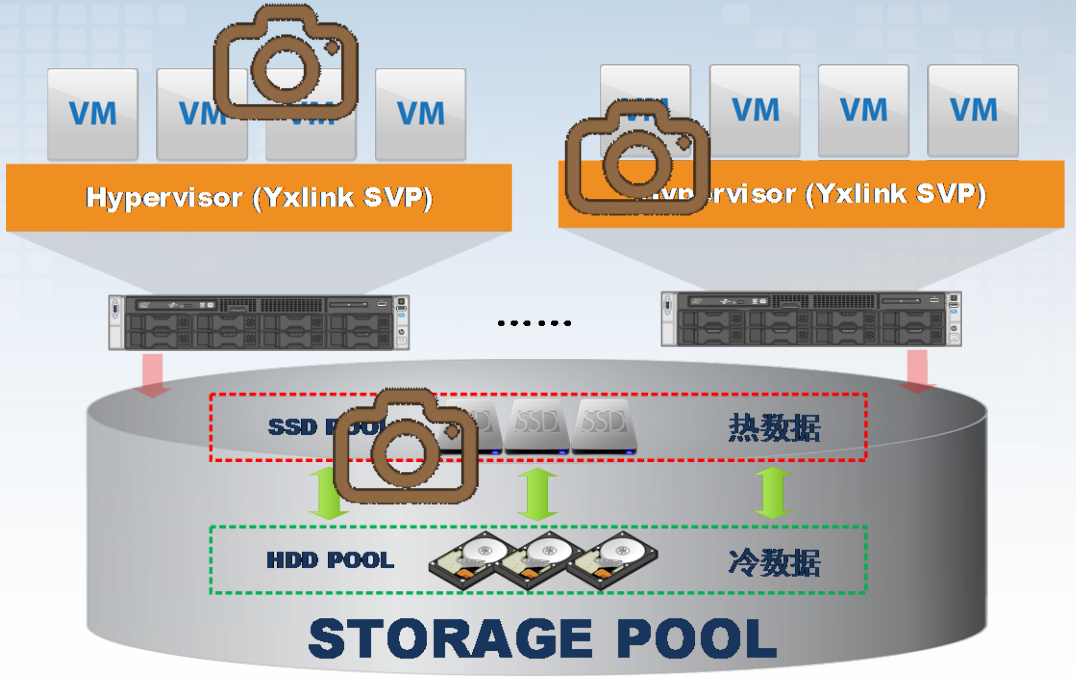
快照备份
（小时）

HCI

超融合的磁盘及内存快照技术



文件/数据库同步



总结

铱迅信息技术股份有限公司

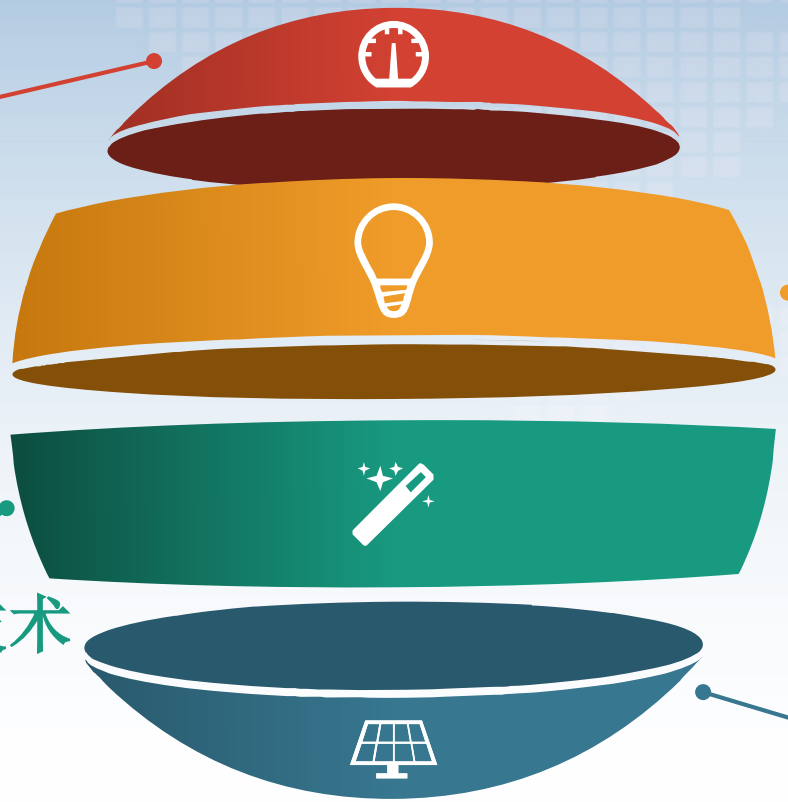
总结

安全可知

资产及漏洞识别
资产关系图绘制
蜜罐技术+态势感知，侦测内网跳板
安全日志实时留存与实时分析告警

安全管控-物理网络下高强度的内网东西、南北向访问控制技术

根据应用划分VLAN
所有东西向流量经过汇聚
根据资产关系图设置访问控制策略



安全管控-虚拟化安全管控技术

VXLAN技术
SDN软件定义网络技术
SDS软件定义安全技术
无代理防病毒技术

安全应急与恢复

利用超融合技术构建备份系统
超融合的多副本快照和实时备份技术

OWASP
Open Web Application Security Project

THE END

汇报人：杨谦
QQ：568623
电话：18021500396