用友云
yonyou cloud

迈向云端 创变未来

2017中国企业互联网大会

用友云
yonyou cloud

企业安全因云而动

数据驱动的自适应安全架构

王亮
360企业安全
解决方案总监

云的边界发生变化

Public Cloud

Application Application

Application Application

Hybrid Cloud

Private Cloud

2017 150亿->2021 451 亿

数据分散->集中

边界动态+虚拟化

360 企业安全 安全第一 ™

云安全覆盖的范围

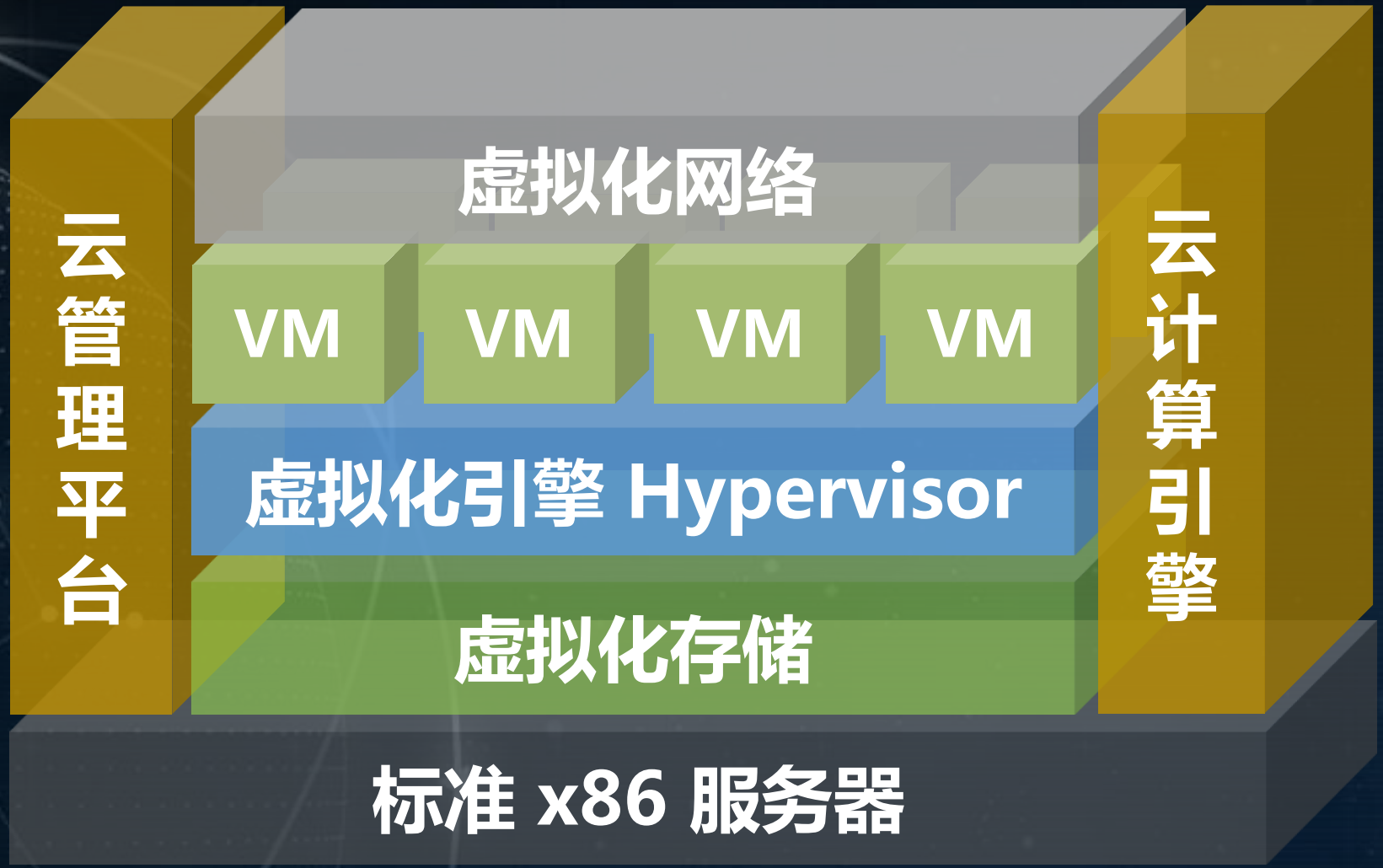
云应用的安全

云基础架构安全

360 企业安全 安全第一™

云计算的核心技术

虚拟化技术
+
管理调度



云安全带来的挑战

360 企业安全 安全第一™

深入思考新的架构

持续监测和分析

进化到积极防御

安全体系的进化论

依赖 → 进化

架构安全	被动防御	积极防御	威胁情报	反制进攻
加强自身 强身健体	构筑工事 纵深防御	全面监测 快速响应	获取情报 准确预警	进攻反制 先发制人

360 企业安全 安全第一™

Source: SANS-2015-积极安全防御体系

自适应的安全架构

预防、预测

Proactive risk analysis
主动风险分析

Predict attacks
预测攻击

Baseline systems
基线系统

阻止、防护

Harden and isolate systems
强化和隔离系统

Divert attackers
转移攻击者

Prevent issues
阻止事件

响应、调查

Remediate/ Make change
修复与进行变更

Design/Model change
设计/模式变更

Investigate/ Forensics
调查与取证

检测、监控

Detect issues
检测事件

Confirm and prioritize risk
确认风险并按优先级排列

Contain issues
抑制事件

360 企业安全 安全第一™

Source: Gartner-2011-自适应安全模型

带来革命性的改进

战法研究

掌握敌情

数据是基础

解我情

作战方案

数据驱动安全

数据驱动安全

驱动是手段

海量数据采

数据建模、业务建模、机器

化分析

安全是目标

360的云安全理念

预测

1、360大数据资源
2、态势感知

主动风险评估

1、态势感知

预测攻击

防御

1、主机防火墙
2、虚拟防火墙
3、云堡垒机

强化和隔离

1、病毒查杀
2、虚拟化层防逃逸

安全防护

1、WAF（web应用防护）
2、防DDOS攻击

阻止事件

数据驱动
自适应
云安全

响应

1、病毒查杀隔离
2、安服响应

修复/完善

1、完善方案
2、安服响应

设计/程式更改

调查取证

检测

1、IPS
2、webshell
3、流行木马库检测
4、漏洞检测

安全基线检测

事件监测

遏制事件

360 企业安全 安全第一™

360自适应云安全

人工智能引擎

弹性边界

云防火墙协同

主流云平台融合

云端查杀

自适应网络边界

态势感知

重建边界

QVM切片学习

360 企业安全 安全第一™

360数据驱动法则

全球文件样本库		最全的样本行为库		最大的存活网址库		全球域名信息库	
每天新增样本	900万	总日志数	18.9万亿条	每天查询	200亿条	90亿	DNS 解析记录
总样本数	145亿+	每天新增	380亿条	每天处理	100亿条	每天新增记录	100万条

数据来源 全球 **6亿** PC 安全客户端，**8亿** 移动端安全客户端；360 浏览器、搜索终端等。

数据来源 互联网基础设施 DNS，猎网、补天等各类举报与相应平台，以及 **100+ 第三方** 数据源。

大数据服务器规模超过 **60000台**，总存储数据接近 **1.3EB** 每天新增超过 **1.5PB**。

每天各种数据计算任务 **10万个**，每天处理数据量 **10PB**。

- 大数据病毒样本库
- 威胁情报
- 病毒查杀引擎
- 猎网平台
- 中文漏洞库
- IPS规则库
- WebShell库
- 主动防御库
- 补天平台

360 企业安全 安全第一™

数据驱动 的 自适应 云安全架构

用友云 yonyou cloud | 企业服务都在这