ISC 2017

2017 中国互联网安全大会 China Internet Security Conference

基于云主机安全构建的云安全体系

陈奋

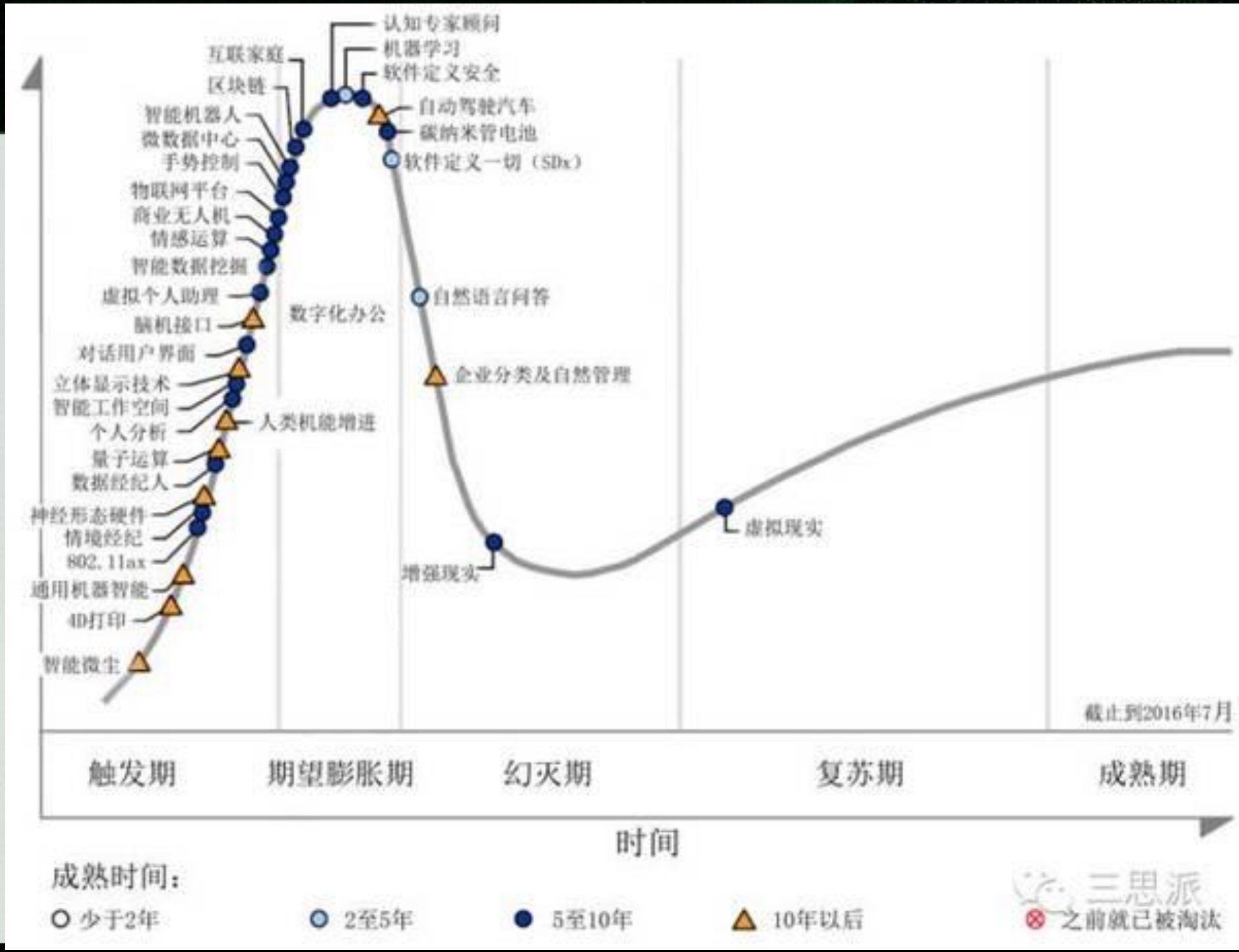
安全狗CEO

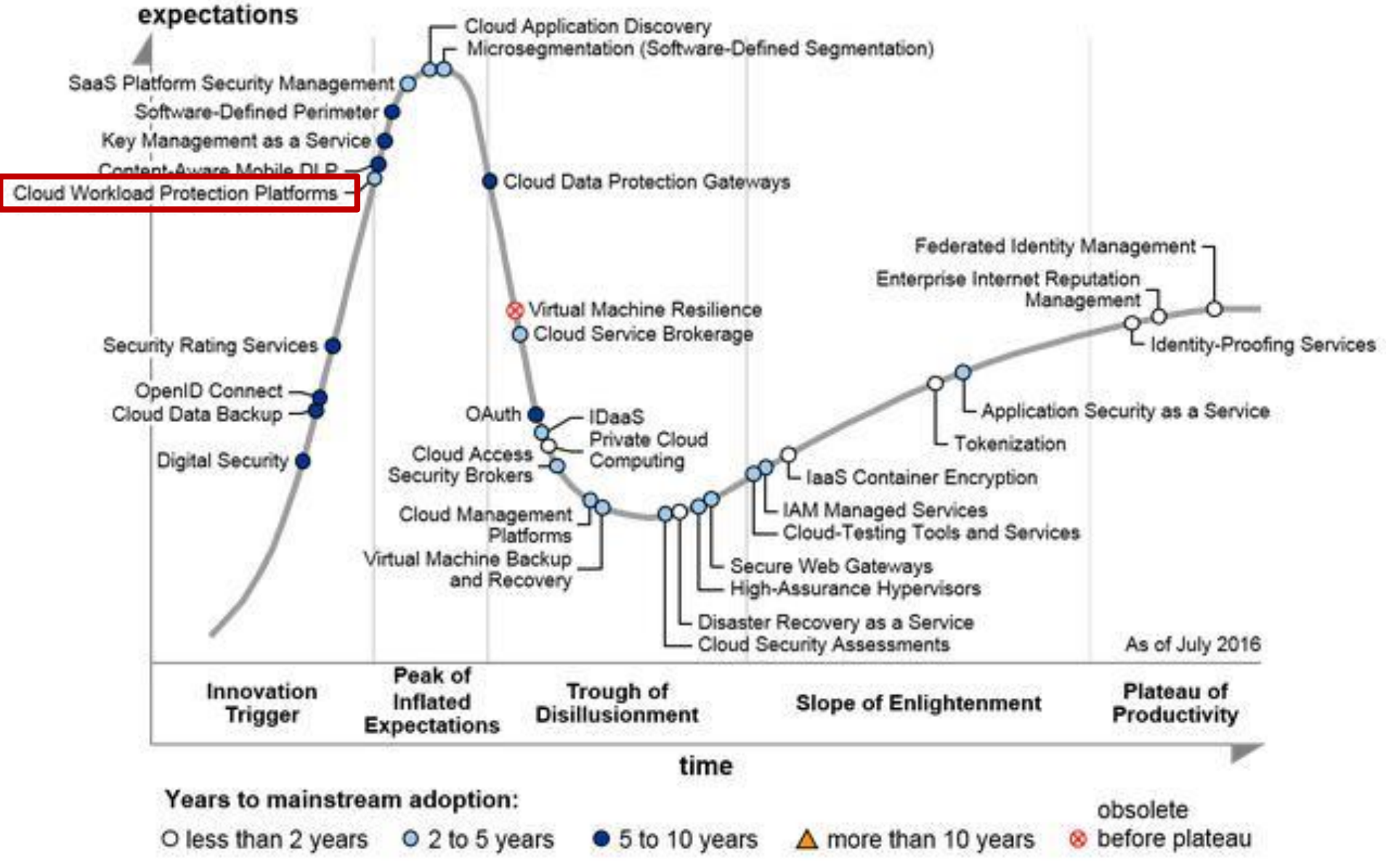
ISC 2017 中国互联网安全大会

360互联网安全中心

目录

一、云计算平台的两种安全架构


认知专家顾问
机器学习
软件定义安全
互联家庭
区块链
智能机器人
微数据中心
手势控制
物联网平台
商业无人机
情感运算
智能数据挖掘
虚拟个人助理
脑机接口
对话用户界面
立体显示技术
智能工作空间
个人分析
量子运算
数据经纪人
神经形态硬件
情境经纪
802.11ax
通用机器智能
4D打印
智能微尘
自动驾驶汽车
碳纳米管电池
软件定义一切（SDx）
自然语言问答
企业分类及自然管理
虚拟现实
增强现实
数字化办公
人类机能增进
截止到2016年7月
触发期
期望膨胀期
幻灭期
复苏期
成熟期
时间
成熟时间：
少于2年
2至5年
5至10年
10年以后
之前就已被淘汰


expectations
Cloud Application Discovery
Microsegmentation (Software-Defined Segmentation)
SaaS Platform Security Management
Software-Defined Perimeter
Key Management as a Service
Content-Aware Mobile DLP
Cloud Workload Protection Platforms
Cloud Data Protection Gateways
Federated Identity Management
Enterprise Internet Reputation Management
Identity-Proofing Services
Virtual Machine Resilience
Cloud Service Brokerage
Security Rating Services
OpenID Connect
Cloud Data Backup
Digital Security
OAuth
IDaaS
Private Cloud Computing
Cloud Access Security Brokers
Application Security as a Service
Tokenization
IaaS Container Encryption
IAM Managed Services
Cloud-Testing Tools and Services
Cloud Management Platforms
Virtual Machine Backup and Recovery
Secure Web Gateways
High-Assurance Hypervisors
Disaster Recovery as a Service
Cloud Security Assessments
As of July 2016
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Years to mainstream adoption:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau

两种解决方案

一种是以虚拟化网络安全设备为核心：主要以传统做硬件防火墙的公司基于SDN方案为代表

备注：图片来自深信服云安全方案

一种是以轻量Agent为核心：主要以Gartner提出的CWPP（Cloud Workload Protection Platforms）云工作负载安全平台方案为代表，国内外都有一些代表产商，如传统安全公司趋势、赛门铁克，新兴安全公司Iiilumio、Varmous等

NATIONAL HARBOR, MD., June 14, 2017 View All Press Releases

Gartner Identifies the Top Technologies for Security in 2017

Gartner, Inc. today highlighted the top technologies for information security and their implications for security organizations in 2017. Analysts presented their findings during the Gartner Security & Risk Management Summit, being held here through Thursday.

"In 2017, the threat level to enterprise IT continues to be at very high levels, with daily accounts in the media of large breaches and attacks. As attackers improve their capabilities, enterprises must also improve their ability to protect access and protect from attacks," said Neil MacDonald, vice president, distinguished analyst and Gartner Fellow Emeritus. "Security and risk leaders must evaluate and engage with the latest technologies to protect against advanced attacks, better enable digital business transformation and embrace new computing styles such as cloud, mobile and DevOps."

The top technologies for information security are:

Cloud Workload Protection Platforms

Modern data centers support workloads that run in physical machines, virtual machines (VMs), containers, private cloud infrastructure and almost always include some workloads running in one or more public cloud infrastructure as a service (IaaS) providers. Hybrid cloud workload protection platforms (CWPP) provide information security leaders with an integrated way to protect these workloads using a single management console and a single way to express security policy, regardless of where the workload runs.

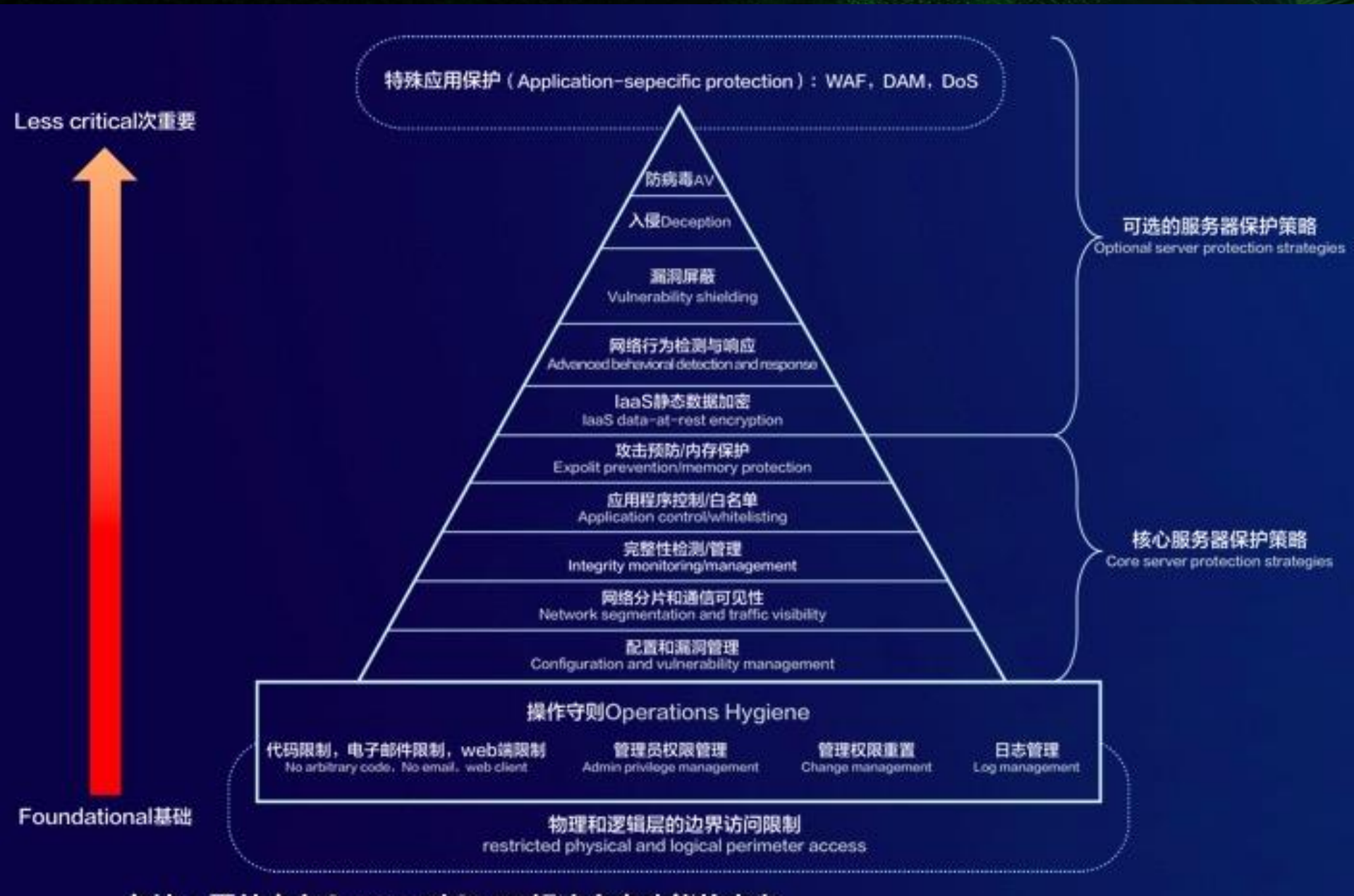
Remote Browser

Almost all successful attacks originate from the public internet, and browser-based attacks are the leading source of attacks on users. Information security architects can't stop attacks, but can contain damage by isolating end-user internet browsing sessions from enterprise endpoints and networks. By isolating the browsing function, malware is kept off of the end-user's system and the enterprise has significantly reduced the surface area for attack by shifting the risk of attack to the server sessions, which can be reset to a known good state on every new browsing session, tab opened or URL accessed.

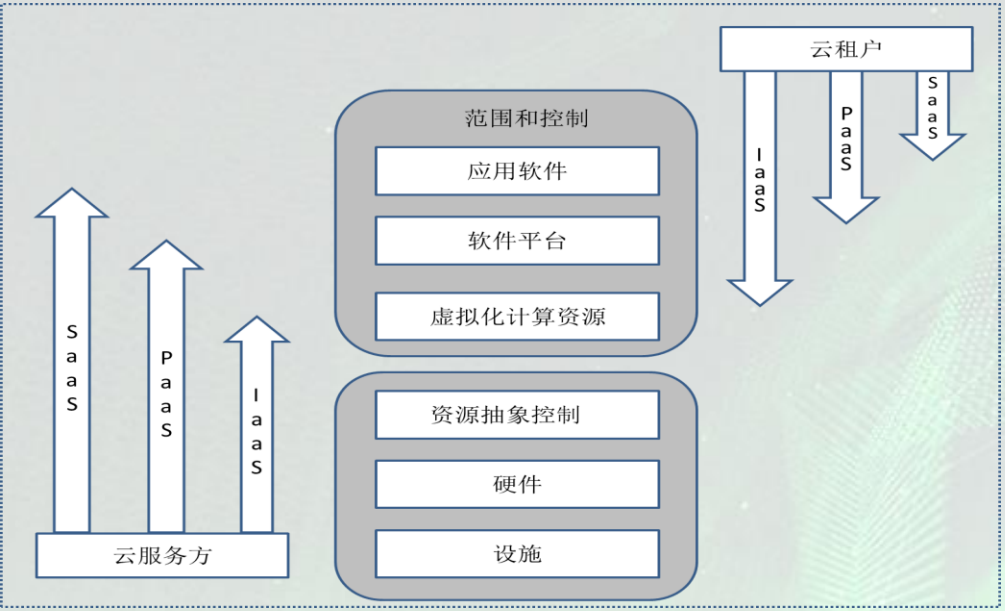
Deception

- Run in physical machines,virtual machines,containers
  支持物理主机、云主机、容器
- Run in one or more public cloud Infrastructure(Hybrid Cloud)
  支持一个或多个公有云等混合云架构
- A single management console and a single way to express securiyt policy
  一个云安全管理中心以及统一的安全策略管理

Gartner对CWPP平台的功能定义



国家等级保护2.0版本中对云计算等级保护的要求



备注：图片来自《网络安全等级保护安全设计技术要求 第2部分：云计算安全要求》

云计算保护环境是云服务方的云计算平台，及云租户在云计算平台之上部署的软件及相关组件的集合。其中，云计算平台的等级保护定级和按照等级的保护工作由云服务方负责，对于大型云计算平台可以将云计算基础设施平台及辅助支撑系统划分为不同的等级对象，各自独立定级。如果云租户在云计算平台上部署的软件及相关组件可以构成等级保护定级对象，则一般称为云租户信息系统，针对其的具体定级和按等级开展的保护工作由云租户负责。

国家等级保护2.0版本中对云计算等级保护的要求

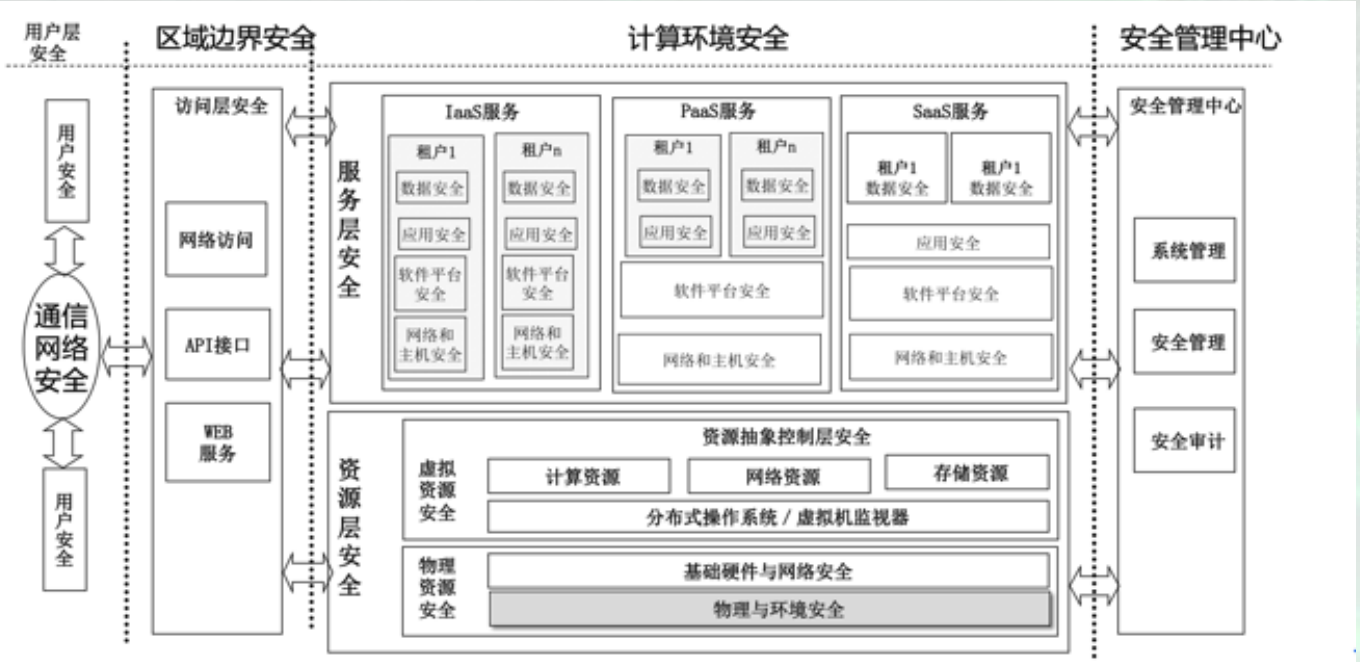


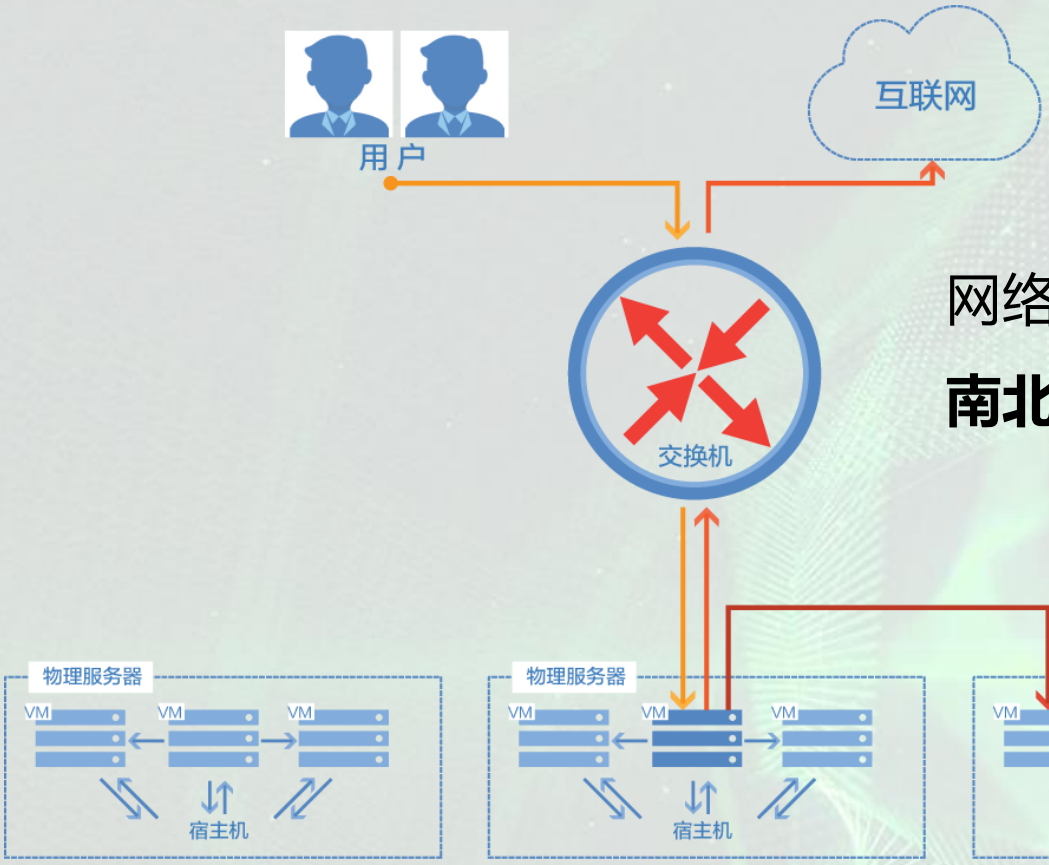
图2　网络安全等级保护云计算安全防护技术框架

备注：图片来自《网络安全等级保护安全设计技术要求 第2部分：云计算安全要求》

依据等级保护**“一个中心三重防护”**的设计思想，结合云计算功能分层框架和云计算安全特点，构建云计算安全设计防护技术框架。其中一个中心指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络

二、从(云)主机角度可以做到的安全

网络边界变迁：(云)主机侧的安全监测成重点



网络流向从原来的南北流向升级为：

南北+东西流向

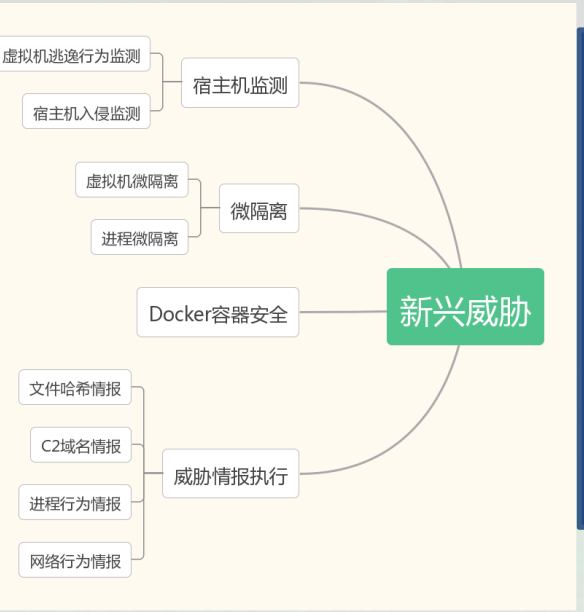
云环境：80%传统威胁 + 20%新兴威胁

网络防护

- 应用层安全威胁
- 系统层安全威胁
- 虚拟化安全威胁

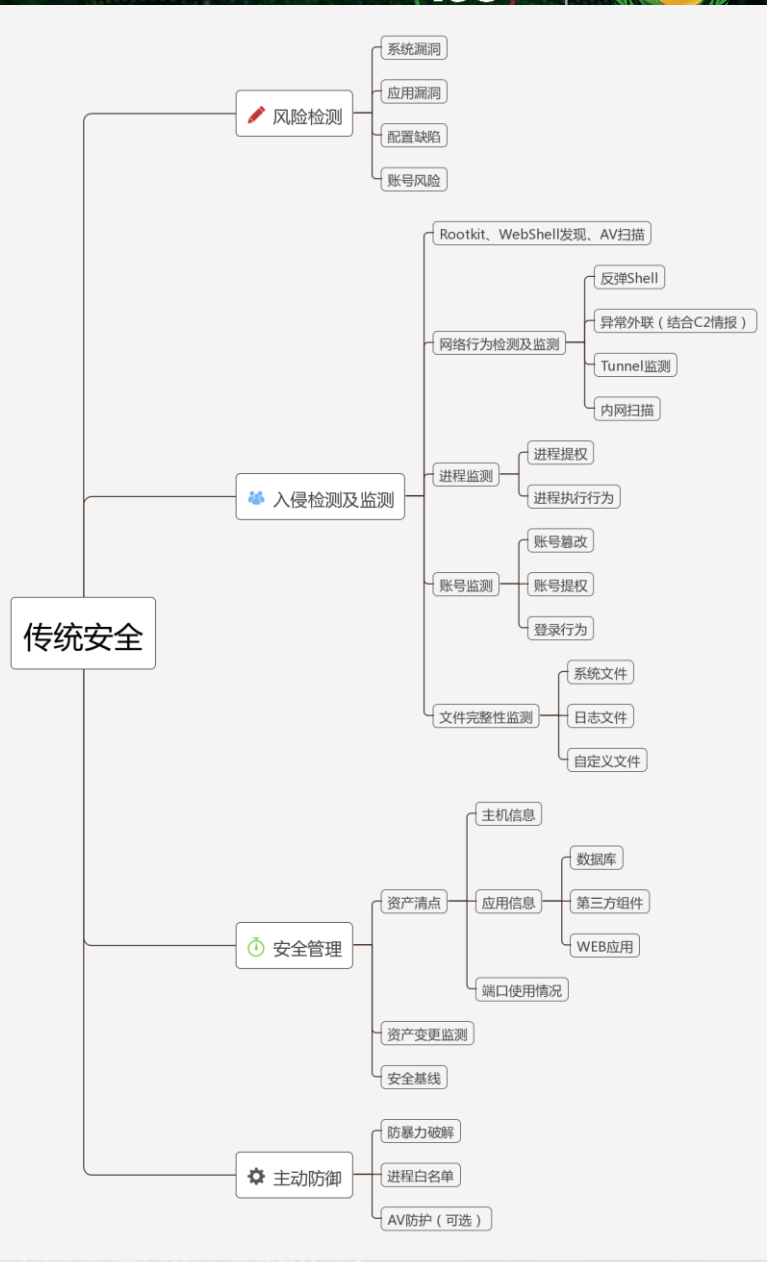
- 传统纯硬件安全模型失效
- 东/西向流量不可见
- 虚拟机间攻击 / 防护盲点
- 虚拟机单独管理复杂
- 虚拟机和宿主机之间的安全威胁

(云)主机侧的安全能力矩阵



新兴安全威胁部分 (20%)

传统安全威胁部分 (80%)



(云)主机侧的安全能力矩阵：资产采集

可以采集了整个云环境中所有云主机采用的WEB应用、数据库应用、第三方组建、端口等更细粒度的资产。

概况 | 资产管理 | 风险管理 | 威胁分析 | 日志分析 | 云监控 | 安全策略 | 告警及报表

资产列表

服务器IP: IP地址 资产信息: 请输入名称或版本号 搜索

网站(9)
端口(147)
web容器(4)
Apache(1)
IIS(2)

主机IP	名称	版本	安装路径
119.29.109.107(10.249.132.211) win2008	MySql	5.5.40	C:\phpStudy4IIS\mysql\in
182.254.228.90(10.104.138.174) CentOS	MySql	5.5.45-log	/usr/local/mysql-5.5.45/
117.28.113.89(192.168.85.129)	MySql	5.5.19	C:\Program Files\MySQL

(云)主机侧的安全能力矩阵：风险监测

无须采用传统的网络漏扫设备即可主动发现云主机的系统漏洞、应用漏洞、配置风险、基线风险、弱口令等安全风险。

(云)主机侧的安全能力矩阵：入侵检测及监测

通过监测云主机的各种异常行为可第一时间发现云主机是否已经被入侵，准确性远高于网络流量设备。

概况 | 资产管理 | 风险管理 | 威胁分析 | 日志分析 | 云监控 | 安全策略 | 告警及报表

当前被入侵主机概览

当前您9台主机中有 3台已被入侵，入侵事件合计 23个，入侵事件概览如下：

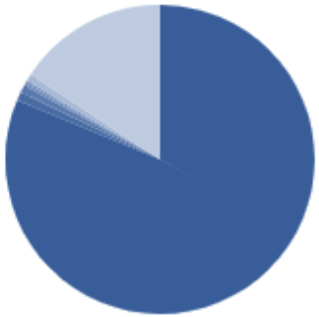
当前被入侵主机列表

全部(3) | 病毒木马(2) | 帐号提权(2) | 敏感行为(0) | 异地登录(2) | 网页后门(1) | 历史记录

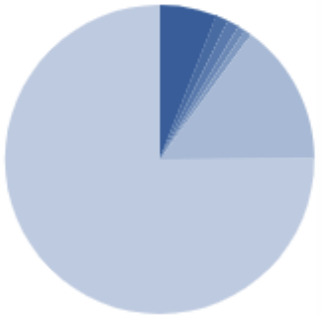
(云)主机侧的安全能力矩阵：进程监测

通过监测云主机详细的进程行为，发现进程异常以及实现进程白名单等功能

概况 | 资产管理 | 风险管理 | 威胁分析 | 日志分析 | 云监控 | 安全策略 | 告警及报表



- svchost.exe 0.91%
- svchost.exe 0.74%
- secbizsrv.exe 0.3%
- lsass.exe 0.27%
- 其他进程 0.75%
- 剩余CPU 15.74%



进程	安全性	CPU使用率↓	内存	内存使用率↓	虚拟内存	线程数
Tasksvr.exe	安全	81.29%	7312k	0.35%	5652k	7
svchost.exe	安全	0.91%	125032k	5.96%	120168k	34
svchost.exe	安全	0.74%	12720k	0.61%	10836k	13
secbizsrv.exe	安全	0.30%	9380k	0.45%	5580k	11
lsass.exe	安全	0.27%	16996k	0.81%	11960k	11
svchost.exe	安全	0.23%	8732k	0.42%	5400k	13

(云)主机侧的安全能力矩阵：宿主机安全监测

在宿主机层进行虚拟机逃逸等新兴威胁的监测，也可以把反病毒等比较占资源的传统安全需求放在宿主机层来实现

(云)主机侧的安全能力矩阵：微隔离技术

Microsegmentation

Once attackers have gained a foothold in enterprise systems, they typically can move unimpeded laterally ("east/west") to other systems. Microsegmentation is the process of implementing isolation and segmentation for security purposes within the virtual data center. Like bulkheads in a submarine, microsegmentation helps to limit the damage from a breach when it occurs. Microsegmentation has been used to describe mostly the east-west or lateral communication between servers in the same tier or zone, but it has evolved to be used now for most of communication in virtual data centers.

为什么不用传统的VLAN或者基于SDN的虚拟网络隔离？

- 当隔离的网络数量增加时投入的硬件成本将大大增加
- 隔离的策略维护困难，规则数会随着隔离网络数量的增加而成倍数的增加
- 无法适配混合云架构

使用基于主机微隔离技术的优势

- 适用于大规模数据中心、云数据中心、混合云架构，无需投入大量的硬件成本
- 让管理员以可视的方式快速进行内部网络隔离及加固，减小攻击面
- 可以隔离到进程、用户层面细粒度
- 可以通过隔离策略识别异常的内网流量

(云)主机侧的安全能力矩阵：威胁情报执行

主机侧是威胁情报IOC落地执行最好最丰富的层面，网络层面往往只能做到C2域名外联发现、异常协议识别，而主机侧可以做到：

- 文件哈希值快速匹配和比对（可实现全网大规模匹配）、实时监测
- 主机网络侧C2域名实时监测
- 主机网络侧反弹Shell监测
- 主机网络侧违规外联行为监测（连接到特定IP地址）
- 主机网络侧特定协议包监测（DNS Tunnel等）
- 进程异常行为监测（函数调用行为、内存行为）

类似于EDR产品的终端威胁捕猎

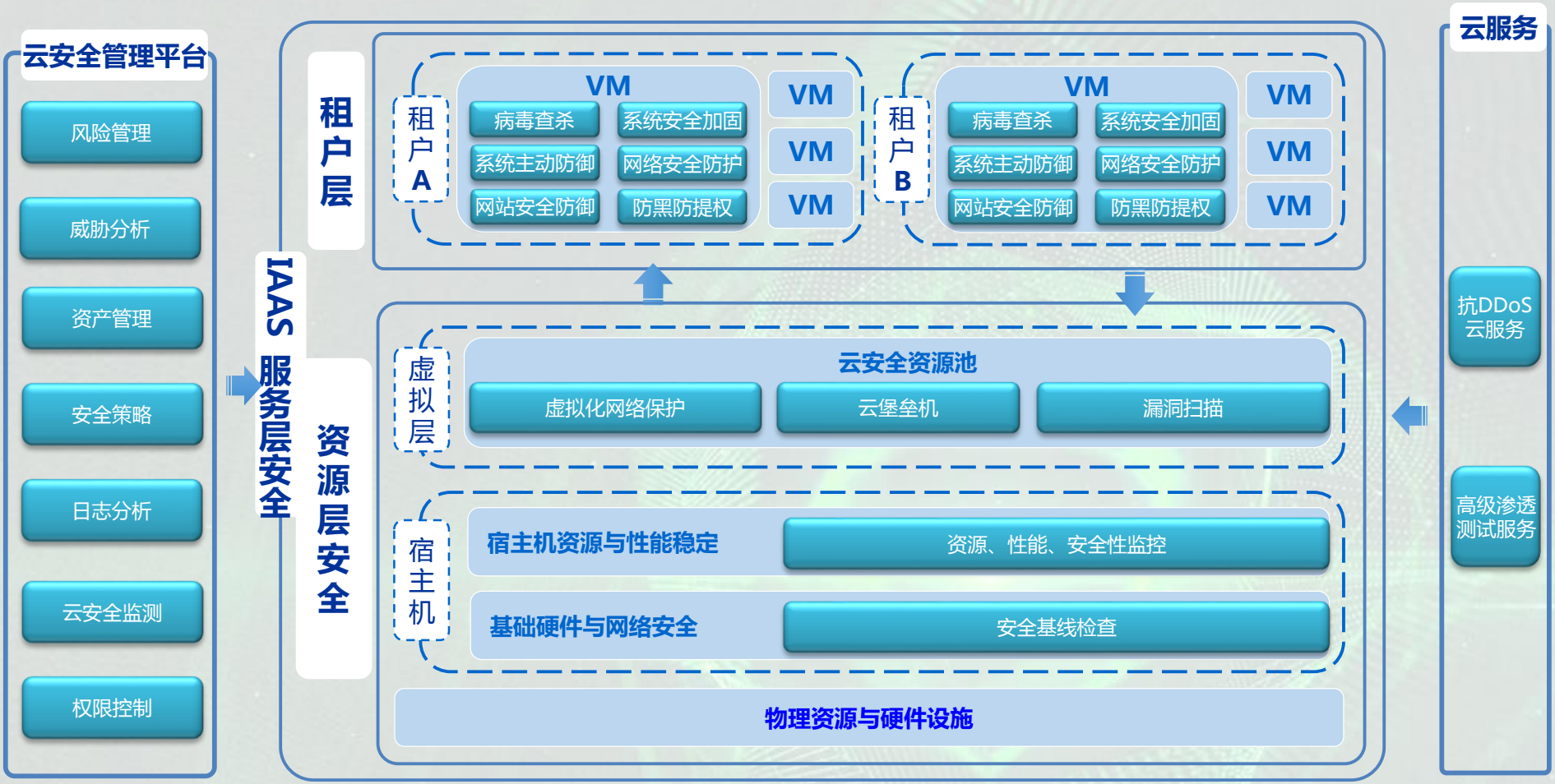
三、统一的云安全管理平台

统一云安全管理平台：满足云等保和管理的要求

统一云安全管理平台：功能范围

让云安全管理变得“主动、可视、可防、可知、可管”

统一云安全管理平台：融合云安全资源池能力



统一云安全管理平台：融合云安全资源池能力

统一云安全管理平台：实例

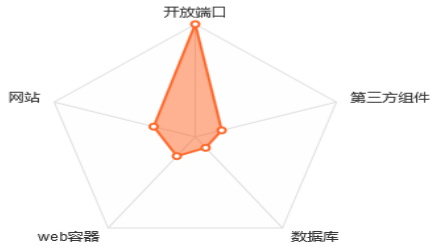
云垒·私有云安全平台

概况 | 资产管理 | 风险管理 | 威胁分析 | 日志分析 | 云监控 | 安全策略 | 告警设置

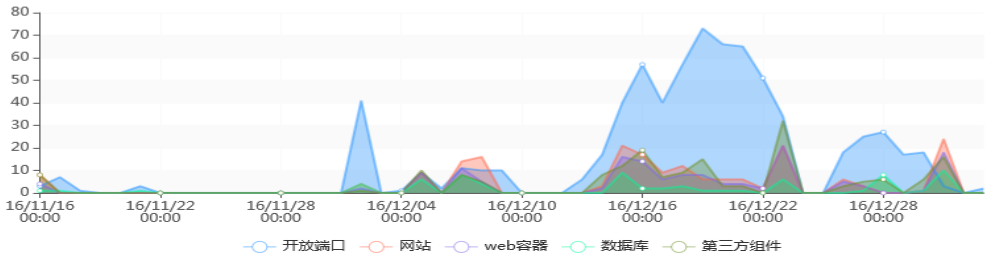
攻击威胁			漏洞风险			运维监控		资产发现		
入侵主机(台)	黑客攻击(次)	攻击来源(IP)	高危主机(台)	高危事件(个)	网站漏洞(个)	异常主机(台)	异常事件(个)	开放端口(个)	网站(个)	服务应用(个)
5	28	0	9	23	0	1	1	251	74	130

当前您的15台主机发现455项，资产概况如下：

资产类型分布



资产变更曲线

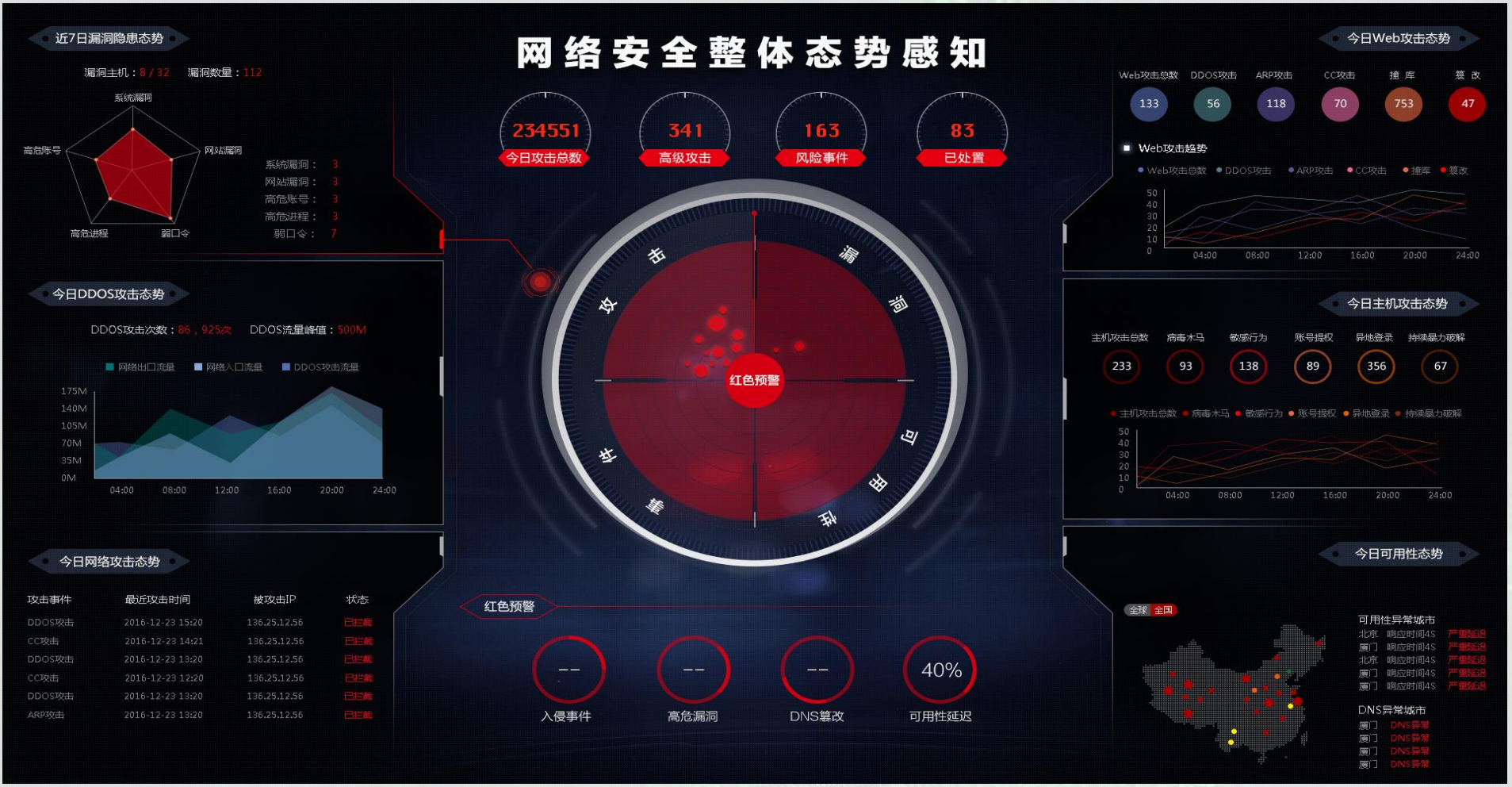


互联网播报

资产变更信息

服务器	变更方式	变更资产	资产类型	变更时间	安装路径
192.168.88.103(192.168.40.166)	新增	443;801;821;8099;49178;54434;	开放端口	2017-01-03 10:32:01	
192.168.88.103(192.168.40.166)	删除	21;49181;49270;3456;56022;	开放端口	2017-01-03 10:32:01	
192.168.88.103(192.168.40.166)	新增	PHPInfo	第三方组件	2017-01-03 10:32:01	C:\APMServ5.2.6\APMServ5.2.6\PHP
192.168.88.230(192.168.31.136)	新增	49156;49157;54385;	开放端口	2017-01-03 09:30:55	
192.168.88.230(192.168.31.136)	删除	49167;49168;123;	开放端口	2017-01-03 09:30:55	
192.168.88.85(192.168.88.85;1...)	新增	49155;49160;49180;49182;54506;55985;55986;55987;55988;63050;63051;	开放端口	2017-01-03 09:01:18	
192.168.88.85(192.168.88.85;1...)	删除	49159;49161;49186;49189;58718;58719;61331;61332;61333;64694;64695;	开放端口	2017-01-03 09:01:18	
192.168.88.230(192.168.31.136)	新增	123;	开放端口	2017-01-02 08:19:43	

统一云安全管理平台：融合态势感知可视化



四、从云主机层面看Docker安全

容器的安全问题

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-9357	264		Exec Code	2014-12-16	2014-12-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Docker 1.3.2 allows remote attackers to execute arbitrary code with root privileges via a crafted (1) image or (2) build in a Dockerfile in an LZMA (.xz) archive, related to the chroot for archive extraction.														
2	CVE-2014-6407	59		Exec Code	2014-12-12	2014-12-15	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Docker before 1.3.2 allows remote attackers to write to arbitrary files and execute arbitrary code via a (1) symlink or (2) hard link attack in an image archive in a (a) pull or (b) load operation.														
3	CVE-2014-3499	264		+Priv	2014-07-11	2014-07-11	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Docker 1.0.0 uses world-readable and world-writable permissions on the management socket, which allows local users to gain privileges via unspecified vectors.														
4	CVE-2015-3627	59		+Priv	2015-05-18	2015-07-02	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.														
5	CVE-2015-3630	264		+Info	2015-05-18	2015-06-25	7.2	None	Local	Low	Not required	Complete	Complete	Complete
Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.														
6	CVE-2014-9358	20			2014-12-16	2014-12-30	6.4	None	Remote	Low	Not required	Partial	Partial	None
Docker before 1.3.3 does not properly validate image IDs, which allows remote attackers to conduct path traversal attacks and spoof repositories via a crafted image in a (1) "docker load" operation or (2) "registry communications."														
7	CVE-2014-5277	17			2014-11-17	2014-11-18	5.0	None	Remote	Low	Not required	Partial	None	None
Docker before 1.3.1 and docker-py before 0.5.3 fall back to HTTP when the HTTPS connection to the registry fails, which allows man-in-the-middle attackers to conduct downgrade attacks and obtain authentication and image data by leveraging a network position between the client and the registry to block HTTPS traffic.														
8	CVE-2014-6408	264		Bypass	2014-12-12	2014-12-15	5.0	None	Remote	Low	Not required	None	Partial	None
Docker 1.3.0 through 1.3.1 allows remote attackers to modify the default run profile of image containers and possibly bypass the container by applying unspecified security options to an image.														
9	CVE-2016-8867	264		Bypass	2016-10-28	2016-10-31	5.0	None	Remote	Low	Not required	Partial	None	None
Docker Engine 1.12.2 enabled ambient capabilities with misconfigured capability policies. This allowed malicious images to bypass user permissions to access files within the container filesystem or mounted volumes.														

容器的安全方案

构建容器平台时去考虑安全问题，主要是从四个方面：

- 基础架构层安全
- 容器调度层安全
- 容器自身的安全
- 应用系统层安全

容器的安全方案：安全基线

容器云平台安全基线（二）

镜像级别

- 创建本地镜像仓库服务器
- 镜像中软件都为最新版本
- 使用可信镜像文件，并通过安全通道下载
- 重新构建镜像而非对容器和镜像打补丁
- 合理管理镜像标签，及时移除不再使用的镜像
- 使用镜像扫描
- 使用镜像签名

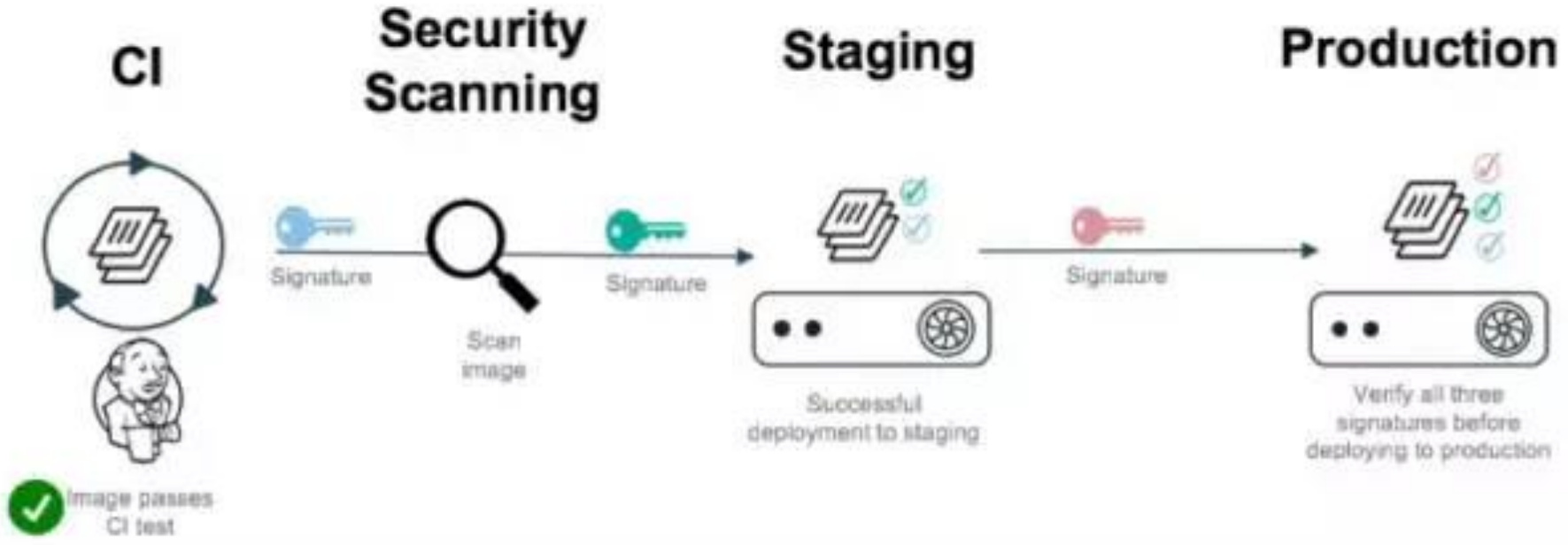
容器级别

- 容器最小化，操作系统镜像最小集
- 容器以单一主进程的方式运行
- 禁止 privileged 标志使用特权容器
- 禁止在容器上运行 ssh 服务器
- 以只读的方式挂载容器的根文件系统
- 属于容器的数据盘符明确定义
- 通过设置on-failure限制容器尝试重启的次数
- 限制在容器中可用的进程数，以防止 fork bombs

其他设置

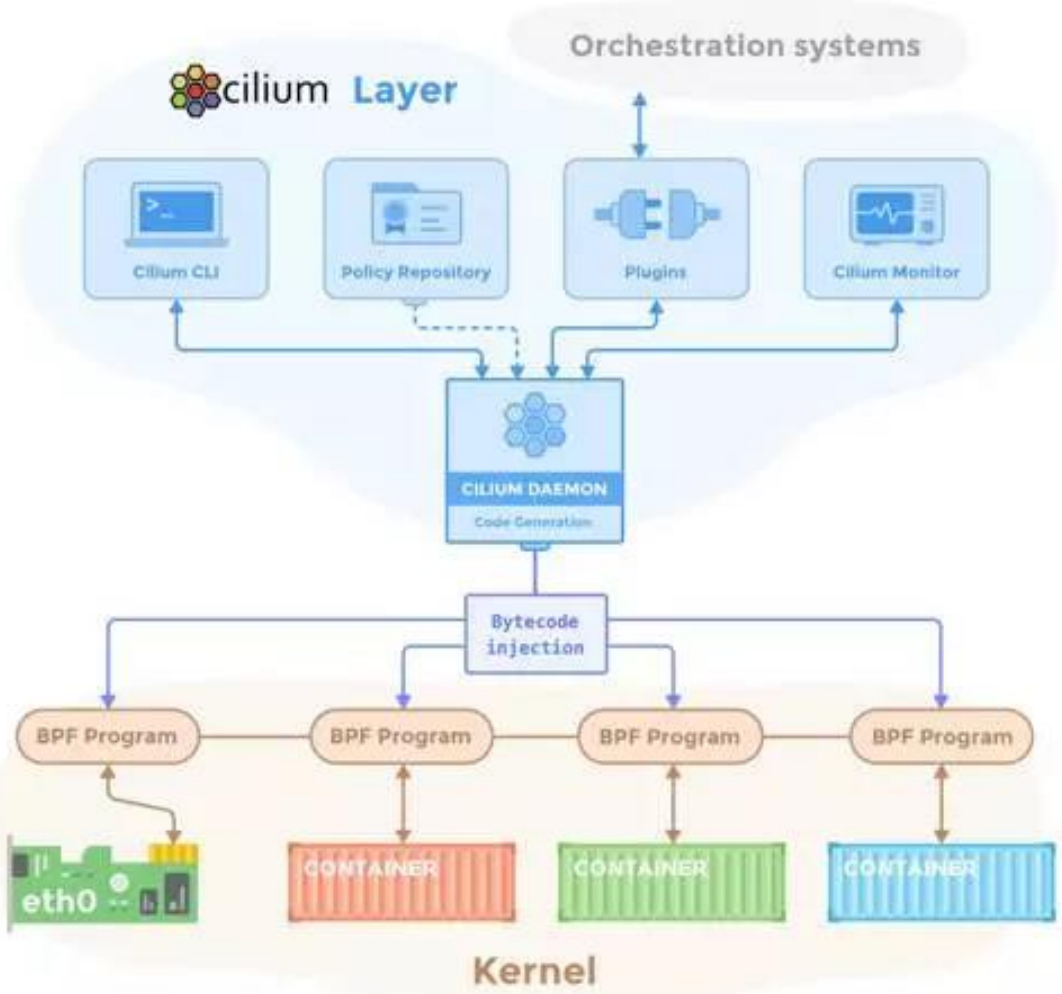
- 定期对宿主机系统及容器进行安全审计
- 使用最少资源和最低权限运行的容器
- 避免在同一宿主机上部署大量容器，维持在一个能够管理的数量
- 周期性检查每个主机的容器清单，并清理不必要的容器
- 监控Docker容器的使用，性能，以及各项指标
- 添置实时威胁检测和事件响应功能
- 使用中心和远程日志收集服务

容器的安全方案：交付过程安全



基于镜像进行交付的，需要对镜像从CI，到部署到生产的过程，每一次的将会都会对它进行签名认证，这样确保镜像最终到生产时是一个安全的，可信的一个资源

容器的安全方案：运行时监测和主动防御

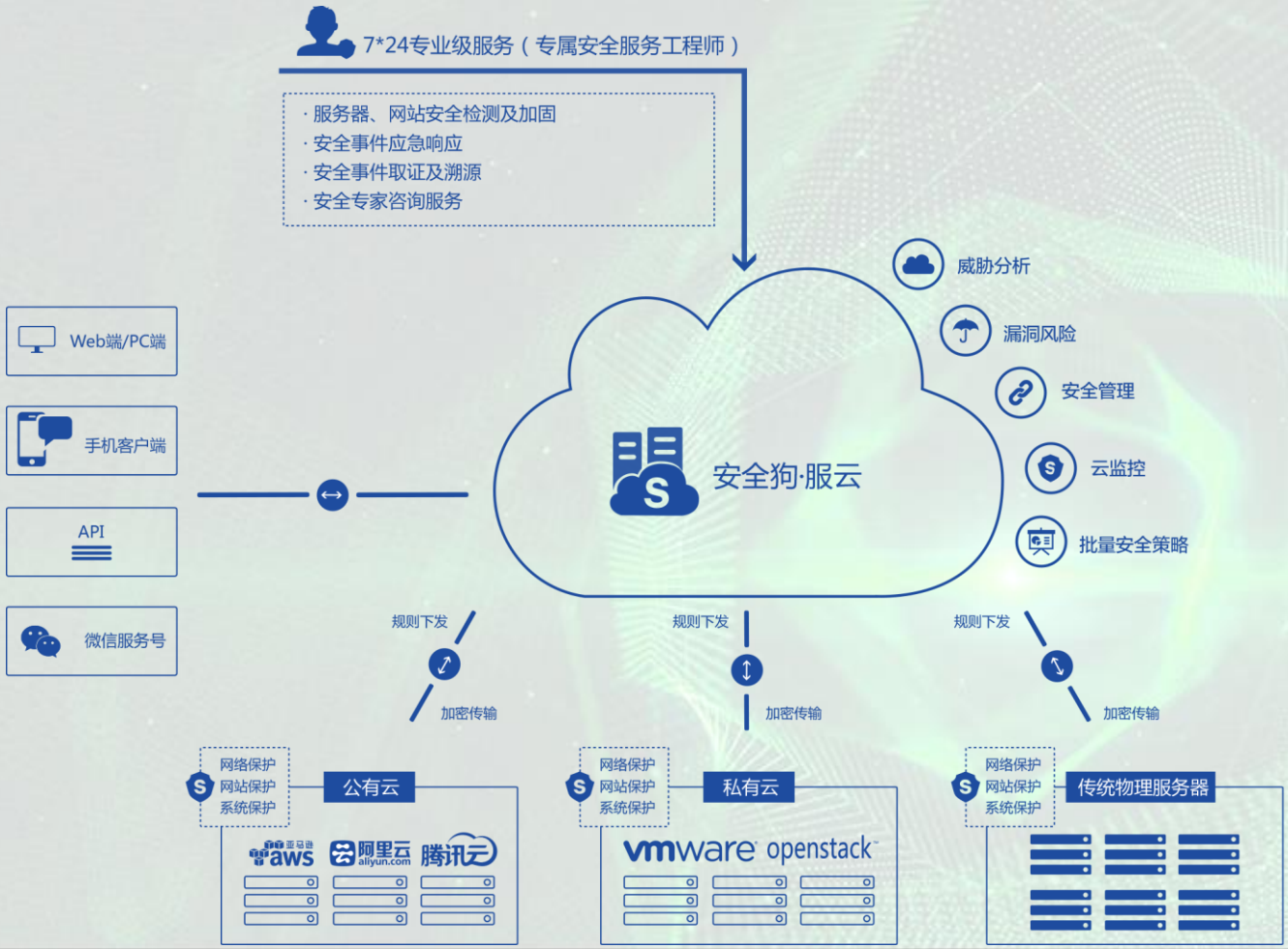


在Docker主机内核层中心对Docker的运行行为、网络行为、文件行为进行统一的监视、访问控制，可以做到对Docker运行时监测和运行时主动保护

五、CWPP平台的最佳实践案例

CWPP平台案例：安全狗云安全平台

安全狗公有云云安全平台用SAAS方式为企业解决(云)数据中心安全问题，提供(云)服务器、应用、业务在内的一站式云安全防护服务。目前用户量超过30W

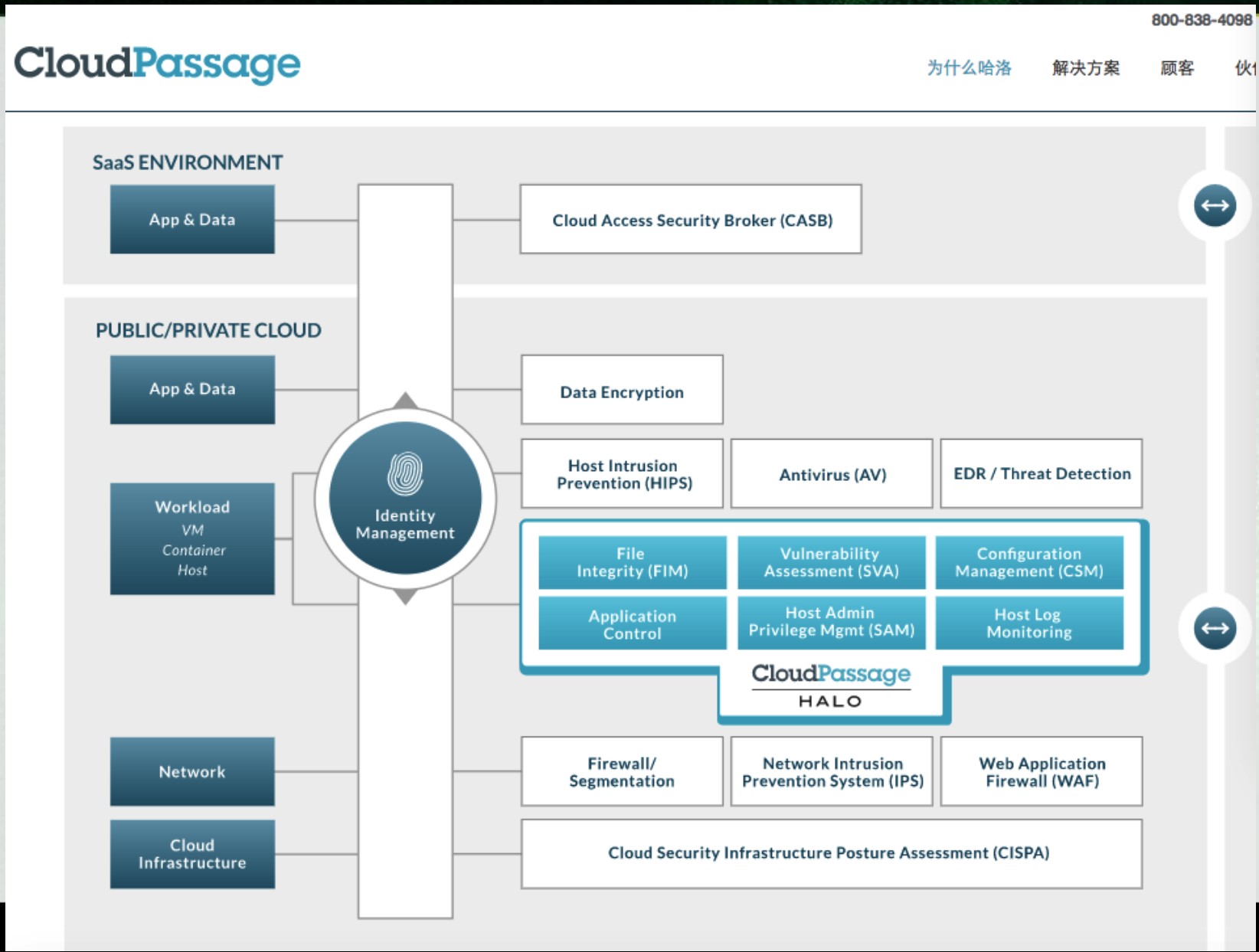


服务

云

端

CWPP平台案例：CloudPassage



CWPP平台案例：illumio

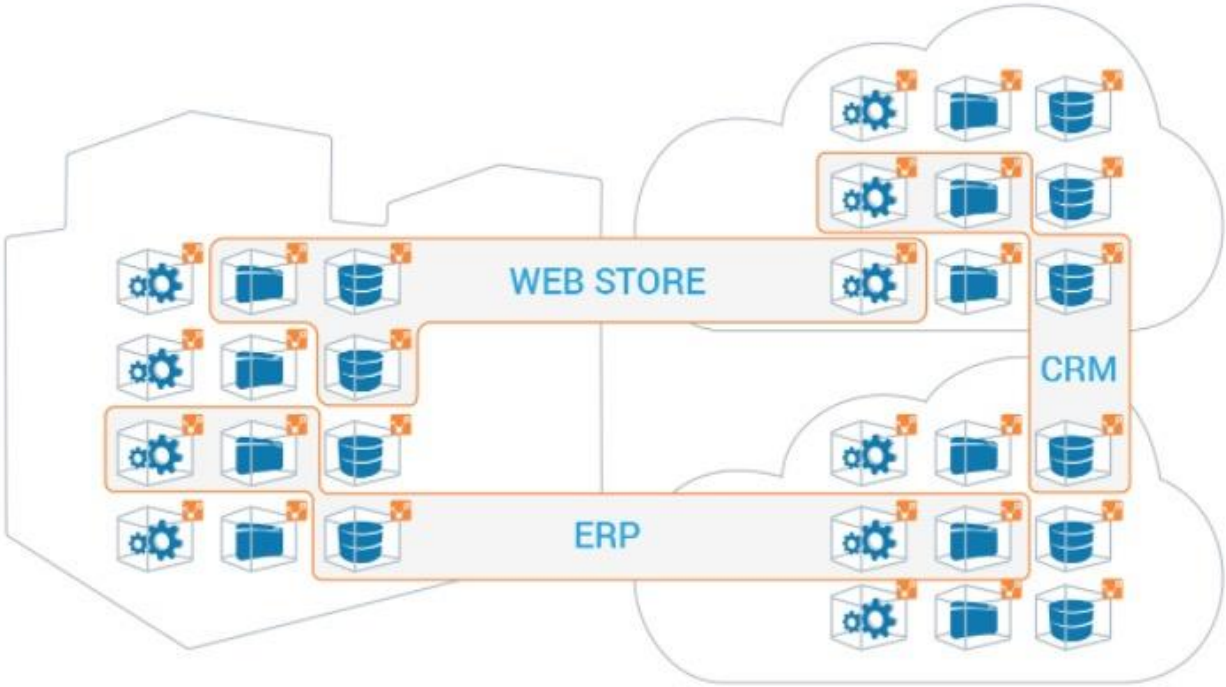
illumio

Blog | Co

SOLUTIONS PRODUCT CUSTOMERS PARTNERS SUPPORT RESOURCES NEWS & EVENTS COMPANY FREE TRIAL

containers on premises, in the cloud, or across hybrid deployments.

- Auto-discovery and automated segmentation policy recommendations or the ability for administrators to define de natural language segmentation policies.
- Modeling of policy to understand policy impact to the application environment without breaking application functio



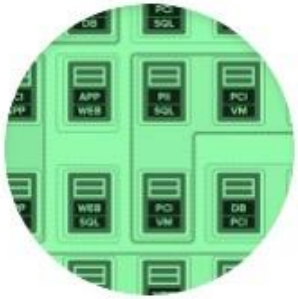
CWPP平台案例：Varmour

vARMOUR
NTER & CLOUD SECURITY

PRODUCT SOLUTIONS RESOURCES PARTNERS COMPANY BLOG

WHAT WE DO

SECURITY POLICY MANAGEMENT



SOFTWARE-BASED SEGMENTATION AND MICROSEGMENTATION

CYBER DECEPTION

HOW WE DO IT

谢　谢