安贤科技
NUBOSH TECHNOLOGY

基于OpenStack云基础架构的安全实践

传统的数据中心安全方案

忽略了数据中心内部“东西向”的安全威胁

很难防御新的威胁

安贤科技 NUBOSH TECHNOLOGY

层出不穷的“未知威胁”

由于数据中心的数据集中存放，成为黑客“高价值”的猎物。攻击者为了获取数据，针对数据中心的安全漏洞，不断变换攻击方法，现有的“基于特征库”的安全软件对此失效。

数据中心安全防护盲点

在虚拟化的环境中，同一主机上的虚拟网络数据无法被传统的网络安全设备侦测，造成安全防护的盲点。

价格昂贵

手动加固和配置安全不仅昂贵，而且通常缺失补丁、网络防火墙和用户目录配置等关键特征，无法满足安全需求

我们的反思

安贤科技
NUBOSH TECHNOLOGY

“特征库防护”投资巨大，却无法有效应对威胁。

云服务器工作负载通常只限于一套专门的运行功能

Gartner的Cloud Workload Protection Platforms

新的白名单安全模型： 通过工作负载的可视化、行为管控的方法，保障安全

CWPP模型的核心能力（I）

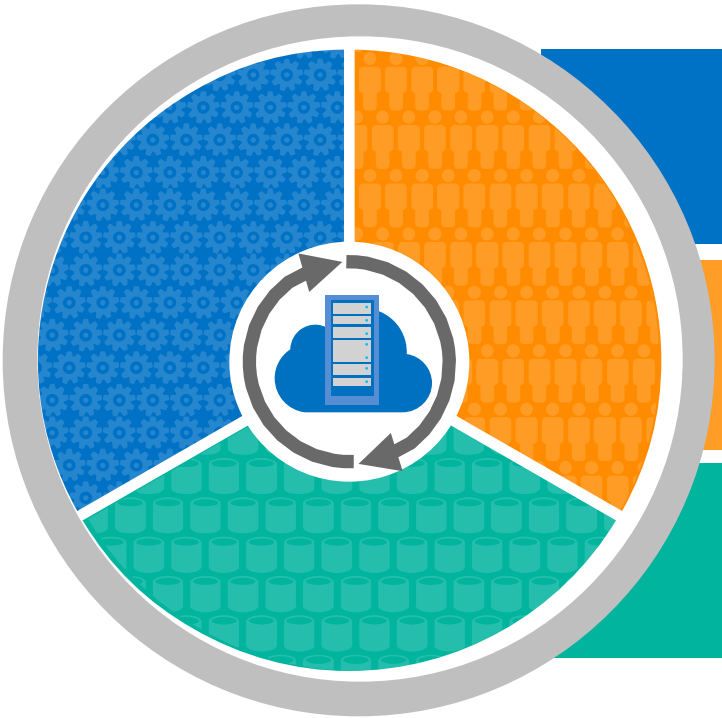
配置和漏洞管理

根据公司标准方针确保加固、配置系统。再根据公司的补丁政策，完成系统补丁，定期持续更新系统

工作负载分割和网络流量可视化

应该支持数据中心东西流量的微型分割需求。另外，一些解决方案提供可视化和监控通信流量，可视化工具让运维和安全管理员可以了解流量类型、设置策略、监控偏差

CWPP模型的核心能力（II）



系统完整性监控和管理

管理程序和虚拟机系统镜像加载前进行评估，一般会通过物理系统中硬件层面的可信任措施实现评估。第二个是在工作负载自启后，实时的监控核心系统文件完整性。

应用程序控制（白名单）

使用白名单以控制在服务器运行什么文件，阻止恶意软件的运行。

渗透阻止和内存保护

应用控制解决方案不会一直可靠，应该跟预防漏洞利用和内存保护功能相结合。

我们的实践

安贤科技
NUBOSH TECHNOLOGY

采用“无代理安全”技术，在计算节点部署安全软件，提供：

- 虚拟机病毒、恶意代码防护
- 分布式防火墙
- 分布式入侵检测
- 应用控制
- 可视化安全数据分析

系统架构

安贤科技 NUBOSH TECHNOLOGY

控制节点

支持服务

Maria DB

Rabbit Message MQ

基本服务

Keystone

Glance

Nova Manage

Neutron Server

Horizon

可选的服务

Cinder

Swift

Heat

Centimeter

网络接口

管理网络

网络节点

网络基本服务

ML2 Plugin

Layer2 Agent (OVS)

Laye3 Agent

DHCP Agent

网络接口

外部网络

管理网络

私有网络

计算节点

APP OS | APP OS | APP OS | APP OS

安全

文件安全组件

管理组件

网络安全组件

计算

QEMU

安全设备

网络

Layer2 Agent (OVS)

网络安全插件

网络接口

管理网络

私有网络

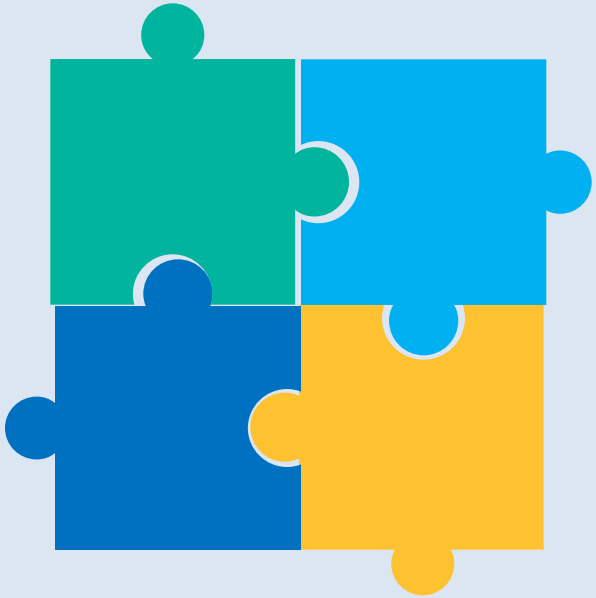
安全特征库

安全信誉服务

管理中心

单点登录

虚拟补丁



- ✓ 根据虚拟机系统及软件，自动调整入侵检测规则，及时对利用系统漏洞的入侵行为进行阻止。
- ✓ 主要应对
  - 01 无法及时更新补丁
  - 02 服务无法停止，进行补丁更新
  - 03 已经停止维护的软件

工作负载分割和网络流量可视化

01 支持海量的访问日志、文件安全、防火墙、入侵检测日志数据的处理。

02 以虚拟机、操作系统、应用程序、攻击类型、恶意代码类型、时间等多个维度对文件、网络的海量安全数据进行关联性分析；并辅以多种图表形式，对同一数据进行描述，便于用户理解。

03 支持安全事件的数据挖掘，便于管理人员及时准确的找到攻击源，阻断安全威胁。

04 通过对行为数据的分析，快速定位未知威胁。

应用程序白名单

安贤科技
NUBOSH TECHNOLOGY

避免未授权的程序运行

对虚拟内部可以运行的应用程序设置“白名单”，避免未授权的应用运行。

应用程序白名单

安贤科技
NUBOSH TECHNOLOGY