绿盟云安全集中管理系统

NCSS

产品白皮书

【绿盟科技】

■ 文档编号	■ 密级 完全公开
■ 版本编号	■ 日期
■ 撰 写 人	■ 批准人

© 2020 绿盟科技

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 版本变更记录

时间	版本	说明	修改人

目 录

一. 产品概述 3
1.1 背景需求 3
1.2 产品介绍 5
二. 产品组成 6
2.1 产品架构说明 6
2.2 产品模块介绍 7
三. 安全能力支持 9
3.1 虚拟化资源池能力 9
3.2 终端防护能力 9
3.3 网站安全能力 10
四. 产品应用场景 10
4.1 私有云平台防护场景（无租户） 10
4.1.1 场景描述 10
4.1.2 典型部署 11
4.1.3 客户收益 11
4.2 云租户防护场景 11
4.2.1 场景描述 11
4.2.2 典型部署 12
4.2.3 客户收益 12
4.3 云等保防护场景 12
4.3.1 场景描述 12
4.3.2 典型部署 13
4.3.3 客户收益 13
4.4 安全增值场景 13
4.4.1 场景描述 13
4.4.2 典型部署 14
4.4.3 客户收益 14
五. 产品优势 14
5.1 丰富的安全能力 14
5.2 开放式架构设计 15
5.3 弹性扩容 15
5.4 软件定义安全 15
5.5 多层级高可用性 15
5.6 安全服务组合包设计 16

5.7 自身系统安全设计 16
5.8 网站安全运营服务 16
六. 总结 17

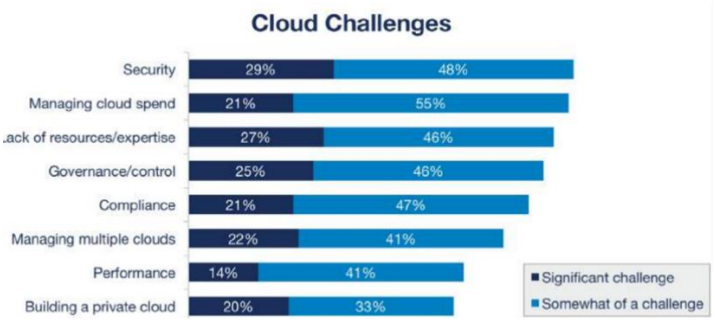
一. 产品概述

1.1 背景需求

1.1.1 云安全需求

云计算，通过网络将 IT 以抽象化的方式交付给客户，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，带来了便捷、弹性、按需的服务模式，给企业、运营商等机构降低了使用、运维成本，同时，通过集约化的资源管理，在云运维方面带来了很大的便利；

云计算作为 IT 基础设施建设的首选已经毋庸置疑，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，自 2017 年以来发生的安全事件来看，无论是公有云还是私有云，安全事件不断，如亚马逊 AWS S3 存储服务器一直存在泄漏数据，其中包括 NSA，美国陆军，分析提供商等的泄密事件；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。



注：来源于RightScale:2018年云状况云调查报告

因此对于安全管理来说，云计算既是挑战，也是机遇。首先，云计算引入了新的威胁和风险，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。

1.1.2 合规需求

随着云计算技术在国内的大力发展和推广，传统的安全法律和法规已经显的力不从心，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； 这些政策里面大家关注对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做了明确说明，《网络安全法》第二十一条明确要求“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。

《网络安全等级保护技术》2.0 版本已于 2019 年 5 月 13 日发布，并在 2019 年 12 月 1 日正式实施，这一举措也标志这我国网络安全正式跨入 2.0 时代，将在未来发挥重要作用。新的等保 2.0 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；针对云计算使用环境单独制定了云计算安全扩展要求，同时基于云服务交付模式的不同，对云上用户和云管理方的安全责权进行了重点划分。

1.1.3 安全增值需求

1.1.3.1 云安全增值需求

云计算其中一个特点就是服务按需付费，租户根据自己业务情况购买对应的云服务资源：计算、存储、应用等，根据资源使用情况进行付费，这就是云服务提供商的收入方式；理论上云安全也是其中一种云上服务，所以云服务提供商也想把安全投入转变为安全收益。

同时对于购买云计算的用户，安全方面越来越受到重视；而且云租户在云环境下对于安全的了解和认识也有了新的变化，对于安全的需求和细粒度划分都有了自己的想法；传统的

安全模式以及云上安全整合不再是用户所需的；租户需要的是按照自己业务情况定制对应的安全能力，并可以查看自己业务运行的安全态势、漏洞信息、攻击事件、报表信息等信息。此安全模式也成为了云服务提供商另一个对云安全增值方案需求的一大动力。

1.1.3.2 传统 IDC 业务增值需求

近年来，随着信息化的发展，越来越多的企业开始依赖互联网开展业务，这主要体现在1）越来越多的开始租用专线接入互联网；2）更多的客户购买 IDC 托管服务。这给运营商带来了巨大的市场空间和机会，但也面临的巨大的挑战。一方面是行业内其它运营商的竞争压力，二是越来越严峻的外部安全威胁和层次不穷的安全事件，网络威胁大量涌现，IDC 用户的 IT 系统遭受拒绝服务攻击、感染病毒、网页被篡改、用户账号被窃取、信息被盗取、业务被中断，甚至遭到黑客勒索的安全事件也时常见诸报端。网络安全问题已经成为影响 IDC 提升服务水平和竞争力的主要障碍。

由于国家对安全合规和重大安全保障的重视，最终用户提出了越来越多的安全需求，这也是一个较好的市场机会。运营商具有优质的客户资源和大量的线路带宽资源，具备做安全增值业务的客观优势。利用优势资源，开展安全增值业务，不仅可以提升客户粘度，增加业务收益，同时也是工信部合规的加分项。因此新的安全增值能力以及更贴近其业务的安全增值解决方案也成为了运营商的需求点；

1.2 产品介绍

绿盟云安全集中管理系统（NCSS）是为了解决私有云和行业云安全问题以及解决安全增值场景实现而提供的一整套平台级产品。采用“软件定义安全 SDS”架构，将虚拟化安全设备和传统硬件安全设备进行资源池化的整合。通过该平台实现安全设备服务化和管理的集中化，以及安全能力的“按需分配、弹性扩展”， 满足客户的合规性需求，提高云上安全运维效率。

1.2.1 安全资源池化

在云计算环境下，计算、存储、网络都变成一个大的资源池，并可以根据用户需要对外提供服务能力。那么我们也可以将安全变成一个资源池，利用这些池化能力，为客户提供安

全服务；在云中心的出口部署一个安全资源池处理需要防护和检测的流量，这些流量进入安全资源池并对这些流量进行如抗拒绝服务攻击、访问控制和 Web 防护等处理；

1.2.2 云平台安全管理

绿盟云安全集中管理系统通过统一的运维门户对安全资源池的资源进行管理、分配、服务编排；还可以掌握安全资源池的运行状态，使用率；配合虚拟化技术形成安全能力弹性扩展；可对资源池内物理安全设备、虚拟化安全设备提供丰富的拓扑、设备配置、故障告警、性能、安全、报表等网络管理功能，从而实现了对云内所有分布的安全资源进行统一的管理，统一的运行监控。

该系统还具备了对接其他平台的能力；可通过对接云资源管理平台实现云租户账号以及资产同步；对接计费系统为提供用户可选的安全服务运营提供支撑；另外，还可以结合全流量分析、漏洞威胁预警、态势感知等平台，实现对云平台安全态势的统计监控分析和预警处理，并可以通过自身展示某一阶段内安全运行状态和报告输出。

1.2.3 合规性原则

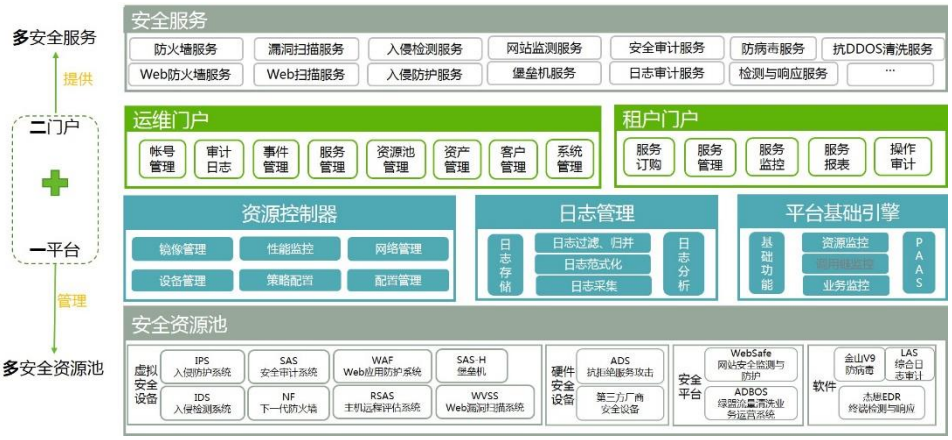
云计算除了提供 IaaS、PaaS、SaaS 服务的基础平台外，还有配套的云管理平台、运维管理平台等。要保障云的安全，必须从整体出发，保障云承载的各种业务、服务的安全。绿盟云安全集中管理系统（NCSS）借鉴等级保护的思想，依据公安部、工信部关于等级保护的要求，对云平台和云租户等不同的保护对象实行不同级别的安全保护，满足安全等级保护要求。

二. 产品组成

2.1 产品架构说明

绿盟云安全集中管理系统（NCSS）遵循以业务为中心，风险为导向的，基于安全域的纵深主动防护思想，综合考虑云平台安全威胁、需求特点和相关要求，对安全防护体系架构、

内容、实现机制及相关产品组件进行了优化设计。平台的实现主要分为三个层面，最底层：安全资源池；中间层：平台控制层；最上层：平台应用层；



2.2 产品模块介绍

2.2.1 安全资源池

支持虚拟化安全产品、软件类安全产品以及硬件安全产品等不同类型的的安全能力的纳入，并接受安全资源池的统一管理，对外提供相应的安全能力。目前该方案提供的安全资源池包含了虚拟化类型安全能力有：vNF、vIPS、vWAF、vIDS、vSAS、vRSAS、vWVSS、vSAS-H、vLAS、vDAS；软件类型安全能力有：EDR 和金山 V9 防病毒、主机防篡改；硬件类型安全能力有：硬件 ADS；

安全资源池还支持提供和对接平台类安全能力，可以提供 websafe（网站安全监测）能力，同时还提供了标准接口可以直接对接 ADBOS（流量清洗业务运营系统）标品版本，实现云清洗增值服务。

2.2.2 平台控制层

2.2.2.1 资源池控制器

资源池控制器可对安全资源池中所有安全能力进行集中调度管控，实现对安全能力的策略管理、配置管理、性能监控、服务编排、网络管理等功能，还可根据应用场景的不同灵活配置和扩展。

运维门户可通过控制器实现安全服务的开通，针对虚拟化的安全设备可以控制设备的生命周期管理，实现启动、关闭、重启和删除等操作。资源池控制器还可以对接云内网络设备，实现引流的全自动化流程，当租户下发了防护策略后把云内流量自动按需牵引到安全资源池内做检测和防护。

2.2.2.2 日志分析模块

日志分析模块可以收集安全资源池中各类安全设备日志，通过采集、范式化、过滤和归并等一系列处理流程，实现各种安全设备日志的统一管理和存储。在日志管理的基础上，进行一些分析规则的配置，对标准化事件进行分析，符合规则的进行告警，并区分不同租户或者业务系统推送到门户进行呈现。

2.2.2.3 平台基础引擎

平台基础引擎采用 WEB 前端与后端业务逻辑分离设计，为门户提供基础功能支持。为平台基础提供 PAAS 功能层服务包括消息中间件、数据服务等；平台基础引擎采用微服务设计，借助容器化实现各个功能组件，利用容器管理系统可快速实现对资源、业务、调用链的监控。

2.2.3 平台应用层

2.2.3.1 租户门户

以满足用户细粒度的安全需求和自主可控、可管理的安全目标；用户可根据自己的业务情况，在租户界面服务市场中自行按需选择满足自己安全需求的安全能力，实现安全的自主可控；同时在租户安全服务界面自主实现安全服务细粒度的策略配置和下发；用户还可以通过服务监控、服务报表了解自己购买服务的运行情况和业务系统的安全风险。

2.2.3.2 运维门户

通过运维门户对安全资源池的资源进行统一管理，对资源池中安全能力抽象形成安全服务并进行组合和发布；能通过运维门户对安全资源池进行统一的监控、对事件告警进行统一的查看，也可以查看整个安全资源池的运行状态、服务使用率，实时掌握安全资源池动态。在运维门户上也可以实现对整个 NCSS 各个组件模块运行稳定性的整体监控，保障整个系统的正常运行。

三. 安全能力支持

3.1 虚拟化资源池能力

分类	安全产品	功能简述
虚拟化资源池能力	虚拟化下一代防火墙（vNF）	基础防火墙功能、应用识别控制、应用层防护、资产风险识别等
	虚拟化 WEB 应用防火墙（vWAF）	防护各类 Web 安全威胁和拒绝服务攻击
	虚拟化入侵防护（vIPS）	敏感数据保护、高级威胁防御、僵尸网络防护、客户端防护等
	虚拟化入侵检测（vIDS）	敏感数据外发检测、客户端攻击检测、非法外联检测、僵尸网络检测等
	虚拟化网络安全审计（vSAS）	内容审计、行为审计、数据库审计、流量审计等
	虚拟化漏洞扫描（vRSAS）	操作系统漏洞、应用系统漏洞、弱口令、配置问题、风险分析等
	虚拟化 WEB 应用漏洞扫描(vWVSS)	Web 服务器漏洞安全检测、风险安全评估
	虚拟化堡垒机（vSAS -H）	集中账号管理、集中访问控制、集中安全审计等
	综合日志审计（vLAS）	对客户资产日志进行采集、统一管理、集中存储、统计分析
	虚拟数据库审计（DAS）	对数据库所有访问行为进行监控和审计、对危险操作进行告警、对数据库访问行为进行统计并图形化展现。

3.2 终端防护能力

分类	安全产品	功能简述
终端防护能力	防病毒 AV	提供终端查杀病毒、软件管理、漏洞补丁、统一升级管理等功能；
	终端检测与响应 EDR	支持主机网络访问隔离、攻击与威胁防护、终端环境强控、安全基线检查以及沙箱防护等功能
	主机防篡改 HWAF	提供操作系统层面防篡改双引擎防护、统一管理、实时监控

3.3 网站安全能力

分类	安全产品	功能简述
网站安全能力	网站安全监测 Websafe	提供网站漏洞检测和篡改监测、挂马监测、敏感词监测、黑链监测等功能。
	流量清洗业务运营系统 ADBOS	NCSS 提供标准接口，可直接对接绿盟流量清洗业务运营系统 ADBOS 标品，实现业务流量清洗功能；

四. 产品应用场景

4.1 私有云平台防护场景（无租户）

4.1.1 场景描述

- **描述：**

  企、事业单位内部私有云，无租户概念，主要是通过云环境做统一业务的承载，整体规模较小，防护流量不大；

- **行业：**

  小型企业、地方金融、教育、医疗、地方政府（少量）；

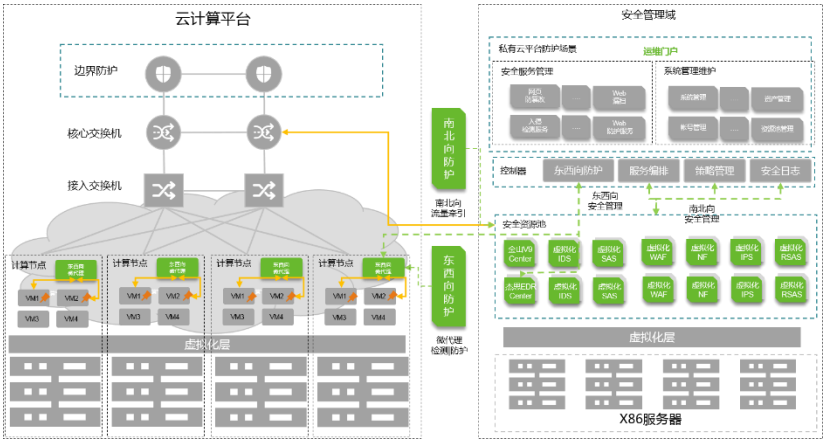
- **需求：**

  1）整体云环境的统一防护；

  2）保证云平台满足等保合规；

  3）缺乏专业安全运维人员，有安全能力集中管理和方便运维的迫切需求；

4.1.2 典型部署



4.1.3 客户收益

- 多样化的安全组件，丰富的管理能力；
- 安全设备集中运维管理，且提供简易的 Web 管理界面，减少运维人员工作量；
- 升级扩容、日常维护便利，减少对专业安全知识的依赖

4.2 云租户防护场景

4.2.1 场景描述

- **描述：**

  在一些行业云环境，例如：政务云、金融云，以及一些大型企业集团内建设的私有云，往往都有租户的概念。云平台为不同的租户划分云资源供其搭建自己的业务系统，对应的也要给租户提供对应的安全能力。

- **行业：**

  运营商、金融、政务、大型企业；

- **需求：**

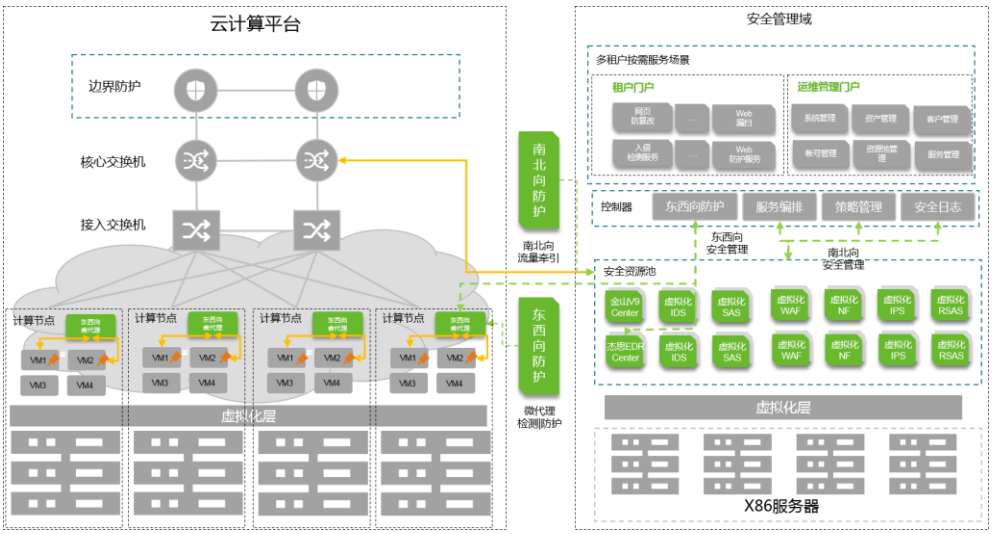
  1）局限于传统的基础设施安全防护，云内租户业务系统防护日益迫切，缺少租户安全防护措施；

  2）租户服务自主化需求；

  3）安全能力多样化、安全合规需求；

  3）统一运维管理需求；

4.2.2 典型部署



4.2.3 客户收益

- 清晰的责任边界，云平台与云租户安全职责共担；
- 安全即服务快速开通交付，无需改变云租户现有网络；
- 多租户安全设备共享，设备复用降低运维成本，提高利用率；
- 云租户基于自身安全需求选择安全服务，按需选取，按量使用；
- 安全统一管理，运维简单方便；

4.3 云等保防护场景

4.3.1 场景描述

- **描述：**

  随着等保 2.0 的发布，云上租户的信息系统需要单独测评，和云平台的责权一分为二，云上租户的等保需求成为新的诉求点；

- **行业：**

  运营商、金融、政府、企业以及其他等级保护要求的行业领域；

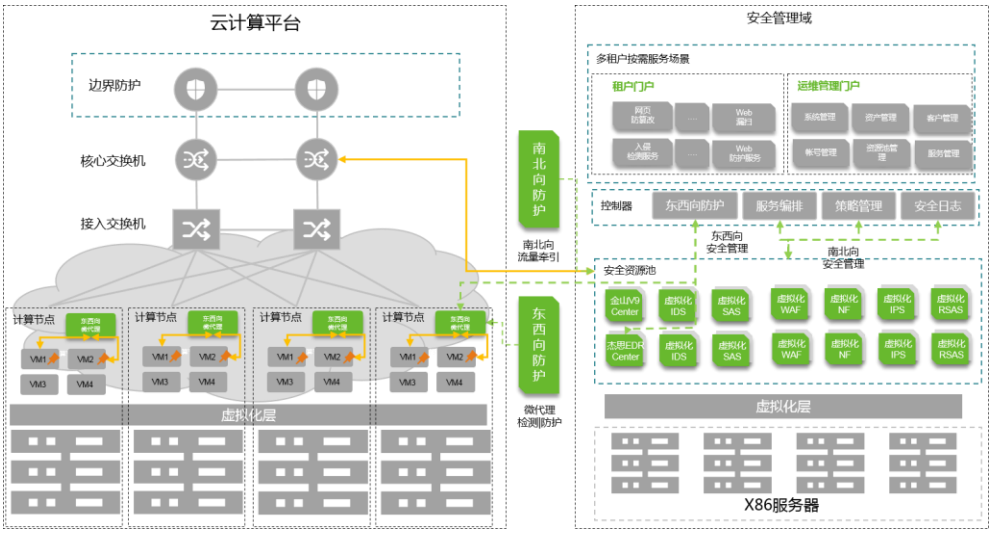
- **需求：**

  1）采用什么手段能够提供满足其云上租户等保合规的安全能力；

  2）通过什么方案把云平台安全责权和云内租户安全责权的划分；

3）需要为客户提供服务化的安全能力；

4.3.2 典型部署



4.3.3 客户收益

- 丰富的安全能力覆盖等保合规要求；
- 安全服务快速交付，安全服务化，提供等保服务包组合配置，一键选择即可开通服务，减少租户对云服务商的咨询，快速满足安全合规需求；
- 集中化管理及时响应安全变化，

4.4 安全增值场景

4.4.1 场景描述

- **描述：**
  - 部分由云服务商提供的行业云，在提供云服务的同时，把安全也作为一种增值手段一起提供给租户；
  - 一些传统的城域网 IDC、省级电信运营商具有增值服务的能力，例如云清洗；在此基础上他们需要加入更多的安全能力来丰富他们的业务，来获得更多的收益；
- **行业：**

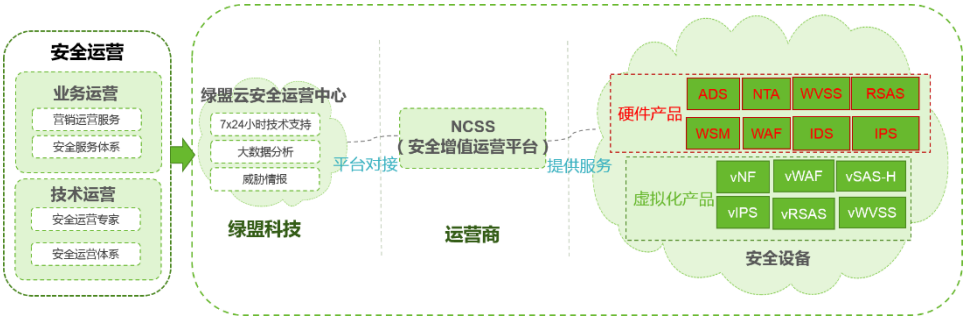
  运营商、金融、政务；
- **需求：**

1）随着国家合规和重保的重视，最终用户安全需求逐渐增多；

2）运营商传统增值业务遇到天花板，需要新的业务增长点体现业绩和政绩，充分利用优势资源；

3）云服务商需要借助提供云平台提供云服务的机会，为租户提供更多云上安全服务，满足客户的合规以及防护需求；

4.4.2 典型部署



4.4.3 客户收益

- 兼容传统和云环境，不但适应传统 IDC 数据中心为专线用户提供服务，还可以为云环境下租户提供服务
- 安全能力满足网站集约化防护要求，具备 WEB 安全监测、防护、扫描、清洗能力
- 安全成为 IDC“增值”服务的一环，依托此成为新的业务增长点

五. 产品优势

5.1 丰富的安全能力

绿盟云安全集中管理系统可以提供从预防→检测→防护→响应等多种类型安全服务，构建纵深安全防护，形成安全能力闭环，保障信息安全。同时绿盟作为老牌网络安全厂商，在安全的积累上有着丰富的经验，例如：安全策略、规则、信誉库等方面十分丰富，虚拟化安全能力也可媲美硬件安全设备，为客户提供优质的安全服务。

5.2 开放式架构设计

开放式结构主要体现在两个方面。第一方面，绿盟云安全集中管理系统可以实现与主流的云平台对接，实现云平台上资产同步与防护流量的灵活调度，保证云平台上业务的安全；另一方面，安全资源池提供统一接口，第三方厂商通过提供符合安全资源池的接口文件、日志信息后可接入安全资源池进行统一管理。绿盟云安全集中管理系统的开放式架构设计，给云平台和租户提供了更好的服务和更多的选择。

5.3 弹性扩容

云平台需要掌握目前云平台安全能力的使用情况，随着云用户的不断接入，租户的业务系统也越来越多、越来越大，安全所需要的资源和能力也越来越高；通过绿盟云安全集中管理系统可以实时掌握安全资源池的运行状态，在安全资源池能力不足时进行扩容；

安全资源池具备云计算特征，可以通过增加承载安全组件的计算节点，实现快速的横向和纵向扩容，横向是指自动增加虚拟机集群，提升安全防护能力，纵向是指通过调整虚拟安全组件的单台虚拟机的 CPU、内存等能力，快速提供单台虚拟设备的安全防护能力；

5.4 软件定义安全

软件定义安全 SDS 通过软件编程的方式调配安全设备资源，实现了一种灵活的网络安全防护框架。将 NFV 形态或硬件形态的服务资源池抽象为统一的服务资源池，实现服务链的自定义和统一编排。云上租户选择安全能力后一键下发配置策略，底层通过软件自动化的完成策略、流量牵引和服务编排等一系列动作，大大减少了运维人员的工作量。

5.5 多层级高可用性

绿盟云安全集中管理系统在设计上考虑了多个层面的高可用设计，保障客户业务稳定的运行。平台应用层和平台控制层的组件均可支持热备切换，保障上层安全管理平台的正常运行。安全资源池，防护组件双服务链备份，策略实时自动同步；资源池服务器故障，快速在

其它服务器中启用备用安全服务链；链路层，数通高可用设计，确保无单故障点；链路层多点故障，还有 bypass 设计，保障业务连续性；

5.6 安全服务组合包设计

安全资源池覆盖了几乎所有层面的安全能力，从应用层、主机、网络、数据层；除了提供每个层次的安全防护能力外，还可以通过服务组合，自定义安全服务内容；安全资源池一方面通过平台自身进行模版组合，对用户发布不同的服务包，例如：等级保护二级服务包、等级保护三级服务包、网站防护服务包等，方便用户一键选择，达到防护目的，带来便利的同时也大大降低了用户的使用门槛；另一方面，当客户厌倦或者觉得现有的组合不满足要求时，可通过服务自定进行组合，选择自己需要的，提高了安全服务方式的灵活性。

5.7 自身系统安全设计

绿盟云安全集中管理系统，产品自身在开发过程中经过多轮安全性测试。研发从接入安全、接口安全、web 安全、代码安全、数据安全等多个方面进行内部安全测试，保障该系统交付后不会对客户环境引入新的安全风险。

5.8 网站安全运营服务

在提供网安防护能力的基础上，为客户提供“7*24”的运营服务，专注于为客户实时响应流量或者业务异常告警、评估网站安全状况、监测网站安全事件。运营人员经过专业的数据分析对攻击事件进行处置，闭环管理威胁事件，直到问题解决，能够最大程度的保证防护效果；会对扫描发现的中高危漏洞进行自动验证和专家人工验证，提供专家级修复建议，并对漏洞的整个生命周期进行管理，直至漏洞修复。

六. 总结

目前，云计算技术也在快速发展和演进，云计算平台的体系结构也在不断变化，绿盟科技也在持续跟踪、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，对安全保障体系不断地改进和完善。