**业务挑战**

目前，许多组织已经将业务系统迁移到云平台上，云平台已经成为组织重要的IT基础设施。云计算技术给传统的IT基础设施、应用、数据以及运营管理都带来了革命性改变，对于安全管理来说，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；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。

        根据调研数据，云计算安全风险是客户所关注的重点，云计算安全已经成为组织规划、设计、建设和使用云计算系统所急需解决的重大问题之一。

**解决方案**

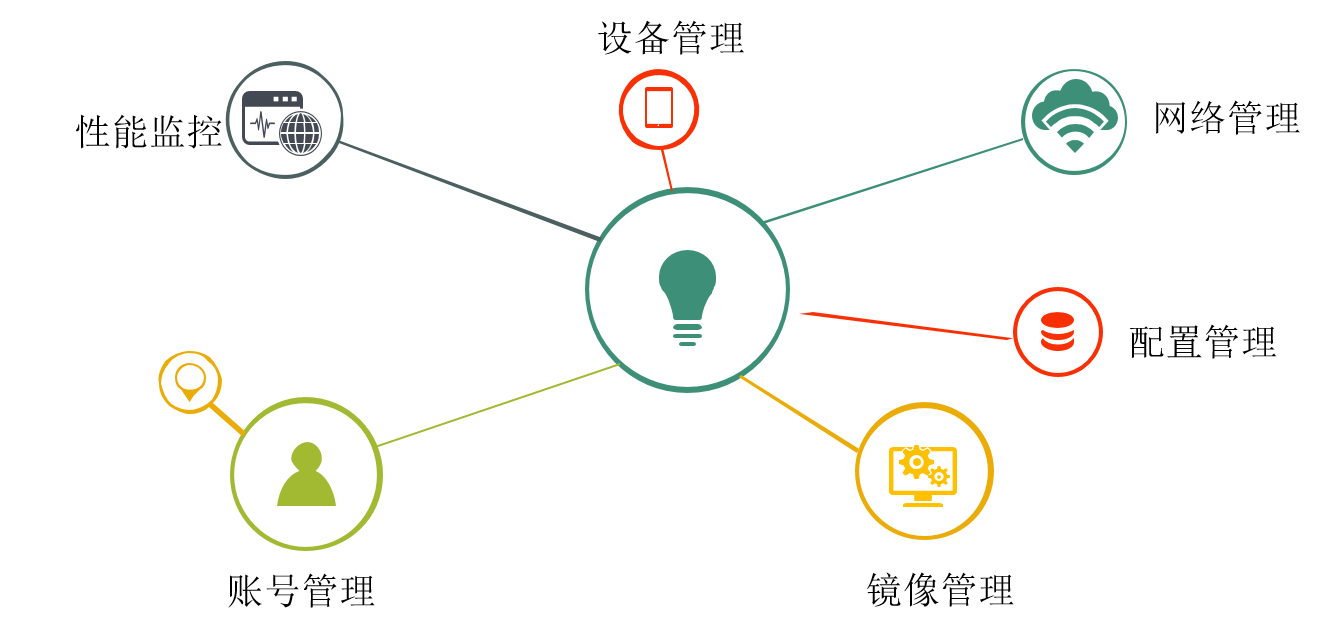
针对云计算带来的安全问题，提出绿盟云安全解决方案，方案遵循以业务为中心，风险为导向，基于安全域的纵深主动防护思想，综合考虑云平台安全威胁、需求特点和相关要求，对安全防护体系架构、内容、实现机制及相关产品组件进行了优化设计。

        基于此方案，我们推出一整套方案型产品——绿盟云安全集中管理系统（NSFOCUS Cloud Security System，简称NCSS），通过提供安全服务和安全运维等功能，为私有云、专有云、行业云等各类用户提供智能、敏捷、可运营的纵深安全防御体系，保障云平台用户的安全。



用户可以选择在绿盟云安全集中管理系统内运行各类虚拟化安全设备，实现对云租户的个性化防护需求。

        系统安全资源池中各类安全产品可提供相应的安全能力。系统可提供安全产品开通、调度、服务编排，以及安全运维功能；提供安全策略管理、配置管理、安全能力管理、安全日志管理等与特定安全应用密切相关的功能。在保障云环境安全的基础上，使安全管理可视化、有效化。



**方案优势**

l  **适应性广，安全功能多**支持VMWare、OpenStack云平台，以及基于KVM、Xen的各种定制化云平台。同时，可以支持物理的、虚拟化、SaaS化的安全资源类型，提供多种安全能力。

l  **模块化架构，可灵活扩展**系统采用模块化架构，根据应用场景和需求的不同，可以选择和部署相应的安全资源、安全应用，满足经济性、合规性要求。

l  **弹性资源，收放自如**通过资源池化技术、负载均衡技术、热迁移技术的能力，可以对外提供安全、弹性的安全功能，自如的进行扩容、缩容。

l  **全程自动化，可快速部署**运用SDN、NFV技术，用户通过系统可以按需、自助的进行安全能力的开通。同时，可以根据业务需要，实现多种安全设备的协同防护，抵御各类安全攻击事件。

l  **基于安全域的纵深防护体系**对于云计算系统安全域边界的动态变化，通过相应的技术手段，可以做到动态边界的安全策略跟随。基于安全域设计相应的边界防护策略、内部防护策略，部署相应的防护措施，从而实现多层、纵深防御，才能有效的保证云平台资源及服务的安全，从而构造纵深防护体系。

**客户价值**

l  **为云环境构建纵深的防护体系**对客户云平台做深入分析，根据其资源和安全需求，从物理基础设施、虚拟化、网络、系统、应用、数据等层面设计、建设和运维一套从点到面的防护体系，为客户的云环境提供持续地安全保障。

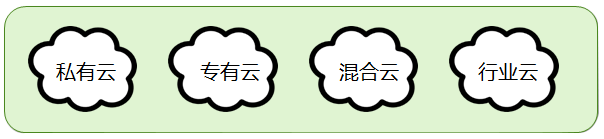
l  **提供可控灵活的安全防护能力**通过安全能力抽象和资源池化，系统可将安全设备抽象为具有不同能力的安全资源池，并根据具体业务规模横向扩展该资源池规模，满足客户安全性能要求。后期还可以随着客户云环境的扩容进行安全资源池的灵活扩展，满足客户对安全服务能力的需求。

l  **内部人员可集中运维**简单、易用的运维平台可对云内虚拟化安全设备进行统一运维管理，可大幅度降低客户运维成本的投入，提高运维管理效率。

l  **向云迁移满足等保合规要求**通过构建安全监测、识别、防护、审计和响应的综合能力，有效抵御相关威胁，保障云计算资源和服务的安全，使客户在向云迁移的过程中满足监管与合规性要求。

**应用场景**

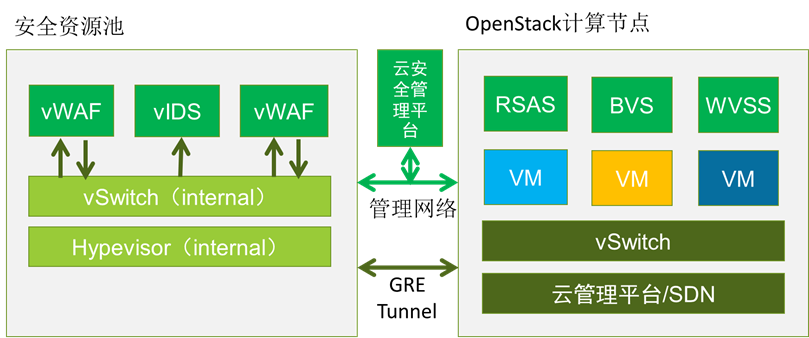
        本方案适用于私有云、混合云、专有云、行业云等各类云平台的安全防护。既适用于原生服务器虚拟化、云平台的场景，也可以使用在SDN和NFV的场景中。



        这里我们重点了解一下基于SDN的安全方案，也就是软件定义安全的应用场景。SDN技术的出现，特别是与网络虚拟化结合，给安全设备的部署模式提供了一种新的思路。软件定义的理念正在改变IT基础设施的方方面面，如计算、存储和网络，最终成为软件定义一切（Software Defined Everything）。这“一切”必然包括安全，软件定义的安全体系将是今后安全防护的一个重要前进方向。

**典型案例**

l  运营商行业典型案例       某运营商作为推动西部信息化建设的重要力量。在混合云平台建设中，面临云平台的安全防御既无成型解决方案，也没有相关产品和技术的问题。为此，引入绿盟云安全解决方案，可及时发现混合云已存在的安全隐患，预警未知的安全隐患；有效降低混合云面临的安全风险，并满足等保合规要求。保障该运营商混合云相关业务顺利上线和顺畅运行。



l  政府行业典型案例        随着某市政务部门信息化建设的大力推进，由此衍生的资源需求，对政务外网云平台性能要求达到了比较高的高度，因此保障业务应用系统安全可靠运行的需求越来越迫切。为了解决信息资源共享率低、业务安全得不到保障等问题，该信息中心引入绿盟云安全集中管理系统。通过部署安全资源池和安全运维管理平台，统一管理云内安全设备，提供云环境内异常流量监测、安全区域划分、漏洞扫描、数据安全防护等安全能力，构建了一个技术先进、安全可靠、服务完备的政务云平台，保障和促进云计算业务的持续发展。