C:\Users\humaosheng.ESG\Desktop\奇安信公司logo.png

**云安全管理平台**

**产品白皮书**

**新 一 代 网 络 安 全**

**版本信息**

|  |  |  |
| --- | --- | --- |
| 文档名称 | 密级 | 创建人 |
| **云安全管理平台产品技术白皮书V4.0** | **公开** | **云安全产品部** |

**修订记录**

|  |  |  |
| --- | --- | --- |
| 修订日期 | 修订内容 | 修订人 |
| **2017.11** | **创建 云安全管理平台产品技术白皮书V1.0，适用于云安全管理平台V2.0.2P001（2.0.2SP1）** | **云安全产品部** |
| **2018.3** | **更新，适用于云安全管理平台V2.0.2P002（2.0.2SP2）,文档版本V2.0** | **云安全产品部** |
| **2018.10** | **更新，适用于 云安全管理平台V2.0R2P003(2.0.2SP3)，文档版本V2.1** | **云安全产品部** |
| **2019.3** | **更新，适用于 云安全管理平台V2.0R2P003B1(2.0.2SP4)，文档版本V3.0** | **云安全产品部** |
| **2019.5** | **更新，适用于 云安全管理平台v2.0.2SP5，文档版本V4.0** | **云安全产品部** |

版权声明：

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

**免责声明**

**奇安信集团，是专注于为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，包括但不限于以下主体：北京奇安信科技有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及上述主体直接或者间接控制的法律实体。奇安信集团在此特别声明，对如下事宜不承担任何法律责任：**

1、本产品经过详细的测试，但不能保证与所有的软硬件系统或产品完全兼容，不能保证本产品完全没有错误。如果出现不兼容或错误的情况，用户可拨打技术支持电话将情况报告奇安信集团，获得技术支持。

2、在适用法律允许的最大范围内，对因使用或不能使用本产品所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、贸易中断、商业信息的丢失或任何其它经济损失，奇安信集团不承担任何责任。

3、对于因电信系统或互联网网络故障、计算机故障或病毒、信息损坏或丢失、计算机系统问题或其它任何不可抗力原因而产生的损失，奇安信集团不承担任何责任，但将尽力减少因此而给用户造成的损失和影响。

4、对于用户违反本协议规定，给奇安信集团造成损害的，奇安信集团将有权采取包括但不限于中断使用许可、停止提供服务、限制使用、法律追究等措施。

5、对于从非奇安信集团指定站点下载的本产品以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证该产品是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件，使用此类软件，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。

6、无论在任何原因下（包括但不限于疏忽原因），对任何人通过使用本产品上的信息或由本产品链接的信息，或其他与本产品链接的网站信息所导致的损失或损害（包括直接、间接、特别或后果性的损失或损害，如收入或利润之损失，电脑系统之损坏或数据丢失等后果），奇安信集团不承担任何由此产生的一切法律责任。

以上声明最终解释权归奇安信集团所有。

目录

[1. 引言 1](#_Toc9534988)

[2. 产品介绍 2](#_Toc9534989)

[2.1. 产品概述 2](#_Toc9534990)

[2.2. 产品架构 2](#_Toc9534991)

[2.3. 部署模式 4](#_Toc9534992)

[2.4. 产品模块 4](#_Toc9534993)

[3. 技术特点 6](#_Toc9534994)

[3.1. 平台稳定可靠 6](#_Toc9534995)

[3.2. 丰富的安全服务组件 7](#_Toc9534996)

[3.3. 分布部署，统一管理 9](#_Toc9534997)

[3.4. 用户与资产结构 10](#_Toc9534998)

[3.5. 安全服务链编排 12](#_Toc9534999)

[3.6. 用户自助服务 13](#_Toc9535000)

[3.7. 计量计费账单 14](#_Toc9535001)

[3.8. 云安全态势感知 14](#_Toc9535002)

[3.9. 在线/离线升级服务 15](#_Toc9535003)

[4. 产品简述 16](#_Toc9535004)

[4.1. 安全市场 16](#_Toc9535005)

[4.1.1. 自主安全组件 16](#_Toc9535006)

[4.1.2. 第三方安全组件 18](#_Toc9535007)

[4.2. 组件管理 19](#_Toc9535008)

[4.3. 资产管理 21](#_Toc9535009)

[4.4. 租户信息同步 21](#_Toc9535010)

[4.5. 监控告警 22](#_Toc9535011)

[4.6. 订单管理 24](#_Toc9535012)

[4.7. 计量计费 25](#_Toc9535013)

[4.8. 报表管理 26](#_Toc9535014)

[4.9. 云安全态势 26](#_Toc9535015)

[4.10. 日志审计 28](#_Toc9535016)

[5. 产品价值 30](#_Toc9535017)

# 引言

随着云计算的普及，大量分散数据集中到私有云和公有云内，这些数据中包含的巨大信息和潜在价值也吸引了更多的攻击者，根据国家计算机网络应急技术处理协调中心（简称CNCERT/CC）报告，网络安全事件依然持续不断爆发，而针对云上安全防护的需求也将与日俱增。《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》等云计算标准对云环境中的安全防护的标准和范围做出了明确的要求，云上的安全责任将由云服务提供商与租户共担，需要充分保证租户业务安全的同时还要求云服务提供商能持续运营安全服务。

传统单纯依靠部署虚拟化安全设备的方式，部署周期长，使用不便利，配置复杂已经无法满足云环境下安全的需求。用户希望能够构建一套使用便利，可持续运营，覆盖从边界到主机、应用的立体化云安全防护体系。

# 产品介绍

## 产品概述

传统业务开始往各种云上迁移后，云内承载的业务越来越多，而云内业务安全建设却远远落后于业务迁移的进度，构建的云上业务安全体系不仅要从边界入侵防范、主机恶意代码防范、数据库审计等传统安全防护能力着手，更要让各种安全服务能力与云计算按需交付的特点进行深度的结合，并通过各种云端、大数据的能力，构建一个全方位的云安全解决方案。

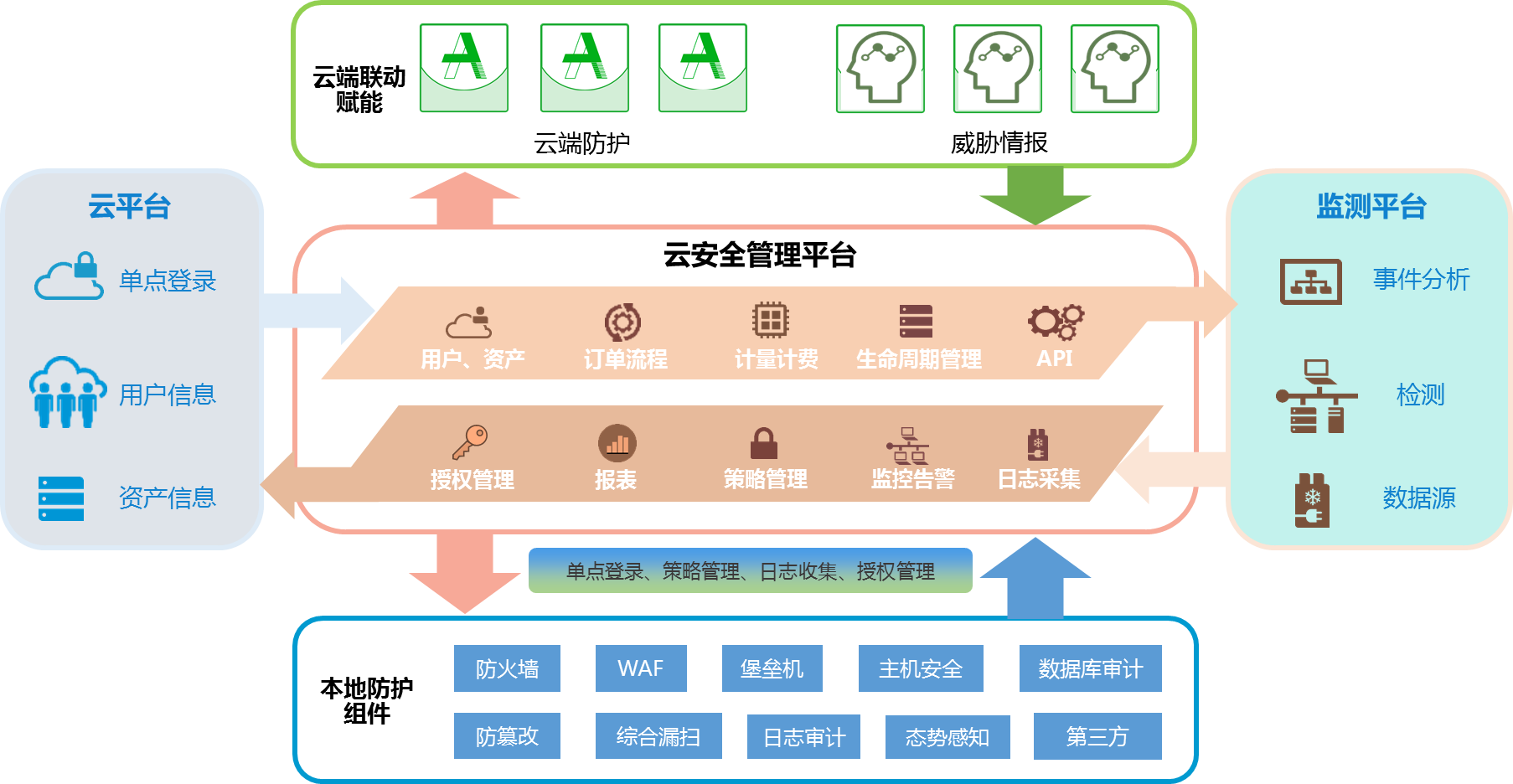
云安全管理平台一个架构先进、适用范围广的云计算安全管理产品，能广泛兼容多种云计算环境，为云服务提供商搭建安全服务能力供给平台，实现安全服务的可运营、可持续产出。平台提供的整体安全能力覆盖了云外南北向访问安全、云内主机东西向访问安全、到主机安全、漏洞管理、web应用层面完整的安全防护体系和多种审计手段。同时，云安全管理平台结合了奇安信优势的云端防护能力和大数据未知威胁检测能力，能够为各种公有云、行业云、私有云构建一套真正属于云时代的安全防护框架。

本文档为您介绍云安全管理平台以及其所用到的关键技术。

## 产品架构

云安全管理平台提供了一个可持续运营的安全服务平台，并面向云计算的租户和管理员提供租户管理、自服务、统一策略管理、计量计费等功能。平台内集成了丰富的安全组件，包括智慧防火墙、主机安全等等组件从网络、主机、应用等多个层面保障云租户的业务安全。

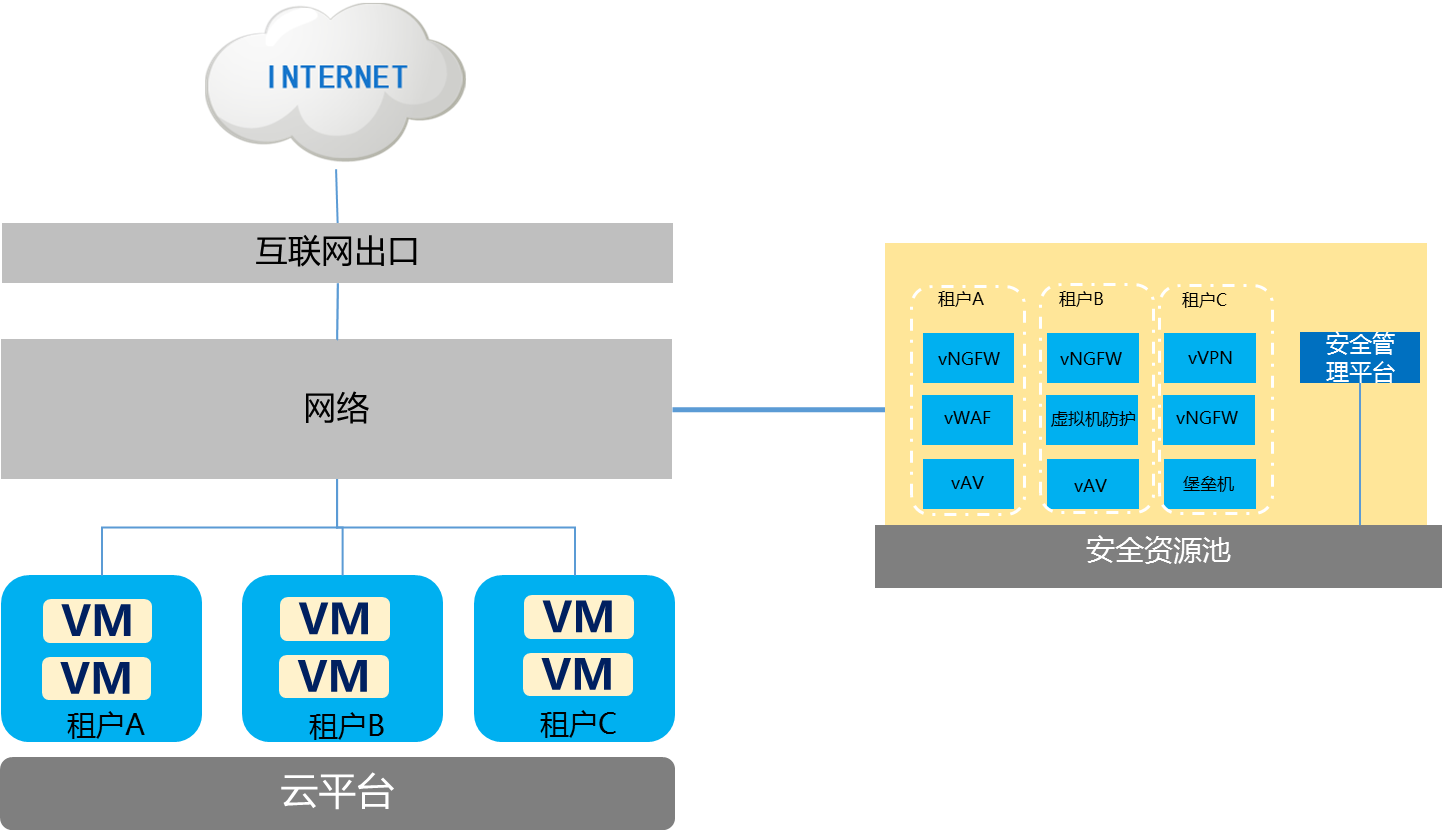
安全管理平台架构如下图所示：



主要组件及其功能：

* 本地防护组件：在本地安全资源池内提供具体安全功能和防护能力的安全实例，包括主机安全控制中心、智慧防火墙、web应用防火墙、堡垒机等，各种安全组件运行在奇安信安全云上。奇安信安全云，是奇安信自主知识产权的私有云平台，基于标准x86服务器实现计算、存储、网络能力的虚拟化，为安全管理平台和租户的虚拟化安全设备提供计算、存储、网络环境。奇安信云安全资源池是国内首个完整支持多资源池部署、多区域网络引流、统一管理的安全资源池。
* 云安全管理平台：核心管理平台，负责本地安全组件的生命周期管理、授权激活、日志收集、安全策略。并为系统用户提供诸如租户管理、订单审批、自服务、计量计费等功能。云安全管理平台提供对租户的自助门户和系统管理门户，根据不同的登录角色进行区分。
* 云平台：云安全管理平台保持开放、兼容的策略，可以与第三方的云管理平台对接。实现统一的用户认证，租户、账号数据同步。通过统一的用户登录和数据同步，优化用户使用流程。
* 大数据平台：云安全管理平台能够将各种安全日志以标准格式提供给用户大数据分析平台，并且提供了大量的接口给数据分析平台进行联动。

## 部署模式



云安全资源池支持多区域部署，在需要安全服务的数据中心内部署一套云安全资源池，可以为该数据中心内的业务提供的完整的安全服务。云安全资源池建立在独立硬件环境上与已有的云平台完全解耦，可以与多种云平台实现共存。租户申请的安全服务以虚拟化NFV设备的形式运行在安全资源池内，不同的租户之间的安全设备通过虚拟网络实现逻辑的隔离。安全资源池集成丰富的安全组件供租户购买和选择。

## 产品模块

云安全管理平台的主要组件及其功能：

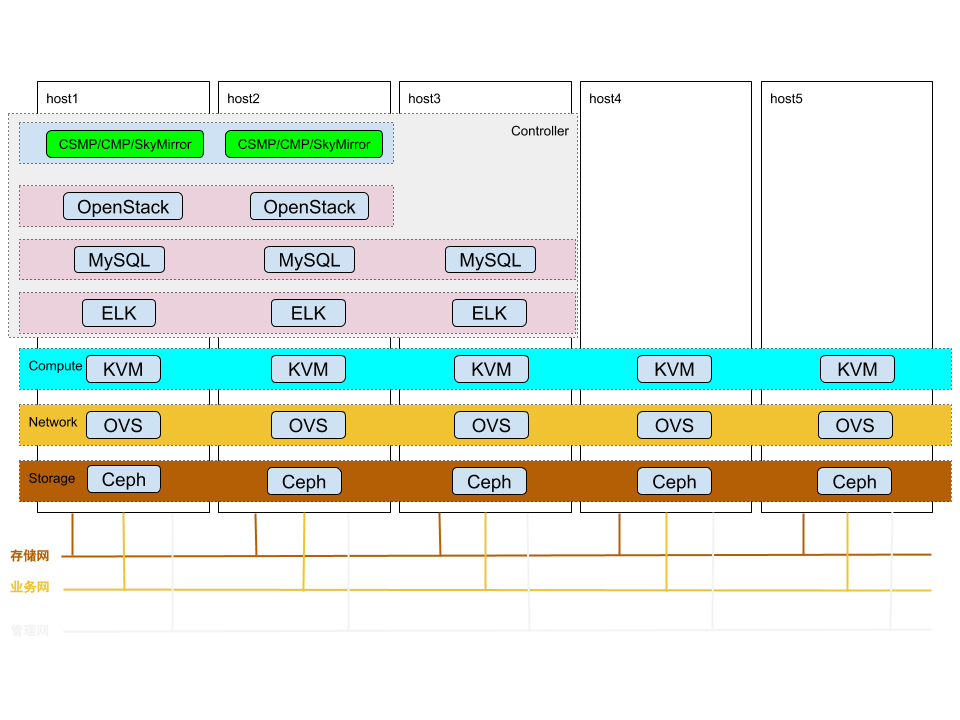
|  |  |
| --- | --- |
| 模块 | 功能 |
| 云安全管理平台软件 | 通过集成多种安全组件，实现以下的功能：  安全市场：允许云计算租户按需在云安全管理平台的门户上申请安全防护资源，实现安全资源的在线申请、自动化开通。  安全组件管理：对安全实例全生命周期的统一管理。  资产管理：关联用户资产与安全服务。  监控告警：安全组件资源、状态监控统一告警。  服务编排：对安全组件的可视化编排部署  报表管理：集合多维报表。  计量计费：支持对云租户使用的安全资源计量和计费，实现资源使用情况可量化。  多租户：支持多租户模式，云平台租户同步。 |
| 云安全资源池 | 基于软件定义安全的架构设计理念， 在奇安信安全云平台基础上以云安全需求的角度设计的安全资源池化平台，与云平台架构松耦合设计，支撑丰富多样、快速上线的安全组件，确保可扩展性、灵活性和稳定性的云安全防护。 |

# 技术特点

云安全管理平台的安全资源池技术具备以下的特点：

## 平台稳定可靠

云安全管理平台整体设计上支持高可靠性架构，采用的高可靠技术包括网络层面、应用层面、数据层面、日志数据层面。



云安全管理平台支持的高可靠性措施包括：

1. 管理平台主备：管理平台采用主备模式，并支持心跳检测，管理平台故障后，可以在秒级切换到备份平台。
2. 数据备份：数据库支持多活互备模式，通过负载均衡进行访问，任意一个数据库都保存完整数据。
3. 日志数据多副本：日志采用主备模式，日志数据写入时保存多副本，任意副本数据丢失都可以恢复。
4. 客户端接入：客户端直接访问高可靠部署的浮动IP地址，浮动IP地址保证故障切换前后对用户IP地址不变，减少用户对故障切换的感知。

多种高可靠技术保障了从用户访问到数据备份、日志存储层面的全面冗余，支撑系统的稳定可靠运行。

## 丰富的安全服务组件

云安全管理平台集成了种类丰富的安全组件，覆盖从远程接入、边界防护、入侵防护、病毒过滤、终端防护、堡垒机、数据库审计等全面的安全能力。不仅能够提供立体化的安全防护能力，还能充分满足各种合规标准中信息安全防护的要求。

租户可以通过安全资源池内对各个安全组件的介绍详细了解安全组件的特点、功能、性能、部署拓扑等信息。

|  |  |
| --- | --- |
| 名称 | 描述 |
| 主机安全 | 主机安全管理系统是集主机防病毒、主机防火墙、主机入侵防御、Hypervisor层防护、主机加固、webshell检测于一体的虚拟化安全解决方案，旨在解决虚拟化环境下虚拟主机的病毒风险、攻击风险、管理风险及宿主主机的安全等一系列的安全问题。 |
| 无代理主机安全 | 无代理主机安全是集成了实时数据分析、防恶意软件、进程管控、防火墙、应用程序控制、入侵防御等模块的主机安全系统，通过无代理的安全防护模式，在虚拟机外部进行文件及网络的安全检测，极大的提高系统的安全防护效率，提升虚拟化、云计算的投资回报率。 |
| 智慧防火墙 | 新一代智慧防火墙（下面简称“智慧防火墙”），在提供复杂环境组网、扫描攻击防护和虚拟系统等功能的基础上，深度集成了漏洞防护、间谍软件防护、失陷服务器检测等高级安全防护功能，快速构建基于威胁情报、态势感知、智能协同、安全可视化等新一代技术的安全防护解决方案。 |
| 网站防护 | 提供业界领先的Web应用攻击防护能力，通过多种机制的分析检测，能够有效的阻断攻击，保证Web应用合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。同时，针对当前的热点问题，如SQL注入攻击、网页篡改、网页挂马等，能够按照安全事件发生的时序考虑问题，优化最佳安全-成本平衡点，有效降低安全风险。 |
| 数据库审计系统 | 基于云平台的数据库审计技术，实现数据库操作行为审计、事件追踪、威胁分析、实时告警等多种功能，保障云环境下核心数据的安全，以高性能的产品，为云用户提供稳定可靠的云数据库审计服务。 |
| 堡垒机 | 堡垒机系统是租户连接云资源的安全管理工具，帮助云租户更加安全、精细的管理云上的虚拟机、数据库等资源。结合多年的运维和安全实践，将云上的运维和安全有机结合。对运维过程事前规划、事中控制和事后审计。事前规划即用户身份管理，可自定义用户访问资源的权限，托管设备密码并定期改密；事中控制即只需要记住堡垒机系统的用户名和密码就可实现单点登录，操作过程中可对特殊命令精准管控，防止越权操作，操作过程实时监控；事后审计即历史会话记录精确查询、操作指令精准定位、操作视频回放，还集成了多维度的综合审计报表。在此之上，将自动化运维、资产拓扑发现、账号安全等完美集成在系统之中。 |
| 综合漏洞扫描 | 综合漏洞扫描，是一套完整的、全方位的漏洞管理与等级保护检查评估系统。 该系统包括资产管理、系统漏扫、网站漏扫、数据库漏扫、基线配置核查、木马病毒扫描、弱口令扫描、网站恶意代码扫描、实时在线的网站监控预警 （含可用性、安全漏洞、篡改、敏感内容、网马、暗链、钓鱼等）、等级保护检查评估等功能，一揽子解决了用户信息化环境下， 所有应用设备及信息系统的漏洞管理、监测预警、定级评估等问题，实现了等保合规化与扫描结果的综合分析与可视化展示。 |
| 网页防篡改 | Web防篡改是专门针对网站篡改攻击精心研发的一款防护产品，系统主要功能是通过文件底层驱动技术对Web站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片等任何类型的文件进行非法篡改和破坏。防篡改系统保护网站安全运行，维护政府和企业形象，保障互联网业务的正常运营，彻底解决了网站被非法修改的问题，是高效、安全、易用的新一代的网页防篡改系统。 |
| 态势感知 | 态势感知在集中管理所有安全组件日志数据的基础上，综合运用攻击地图炮、安全拓扑等可视化技术手段，对云中资产的安全风险、攻击威胁的分布、趋势、来源进行综合的感知呈现，为总体把握安全态势提供有力支撑。 |
| 日志审计 | 日志审计通过对安全组件的安全事件和系统日志进行集中收集、标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保业务运营安全；支持对事件进行追溯，为客户提供真正可信赖的事件追责依据和安全分析数据源。 |
| Web云防护 | Web云防护提供综合的安全防护、资源加速、安全管理配置服务，包括安全能力：Web攻击防护能力、DDoS/CC防护能力、网站缓存加速、网站永久在线、统一的安全配置管理；无需在客户数据中心部署任何软硬件，2T+的防护带宽储备、简捷的接入方式、统一的运维支持、小时级以内完成重大安全漏洞的防护，让使用者足不出户即可享受最全的安全价值、最优的安全运维服务、最快的响应支持。 |

安全组件的对接主要分为两大类，一类是设备类组件，一类是服务类（SaaS）组件。

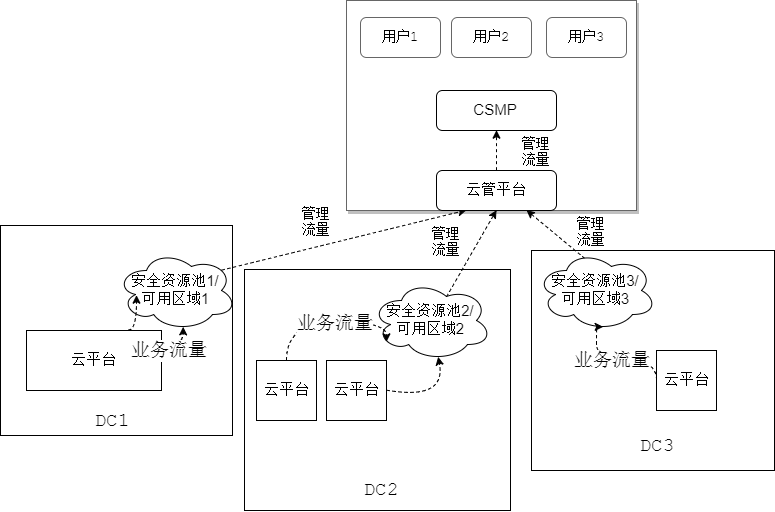
设备类组件是指用户在申请开通安全组件时，为用户从安全资源池创建一台安全设备，并将授权信息同步到设备中，创建完成后，此安全设备的全生命周期均可由用户进行管理。

服务类组件是指在安全资源池已经部署好了安全设备，用户通过申请使用其中的部分资源对业务进行防护，相当于开通了安全服务，这台安全设备的生命周期无需用户负责。其中也包括像Web云防护这类在线的SaaS安全服务，即设备也不在安全资源池中部署，Web云防护的底层是分布在公司全国IDC内的。

## 分布部署，统一管理

* **支持多可用区域**

相比其他安全资源池解决方案，云安全管理平台领先支持多资源池的部署模式，当用户有多个数据中心或多个机房时，业务系统可能分布在多个不同的可用区域。安全资源池支持多区域、多资源池部署的模式，可以与业务的可用区域一一对应，并且能够通过云安全管理平台进行统一的管理。

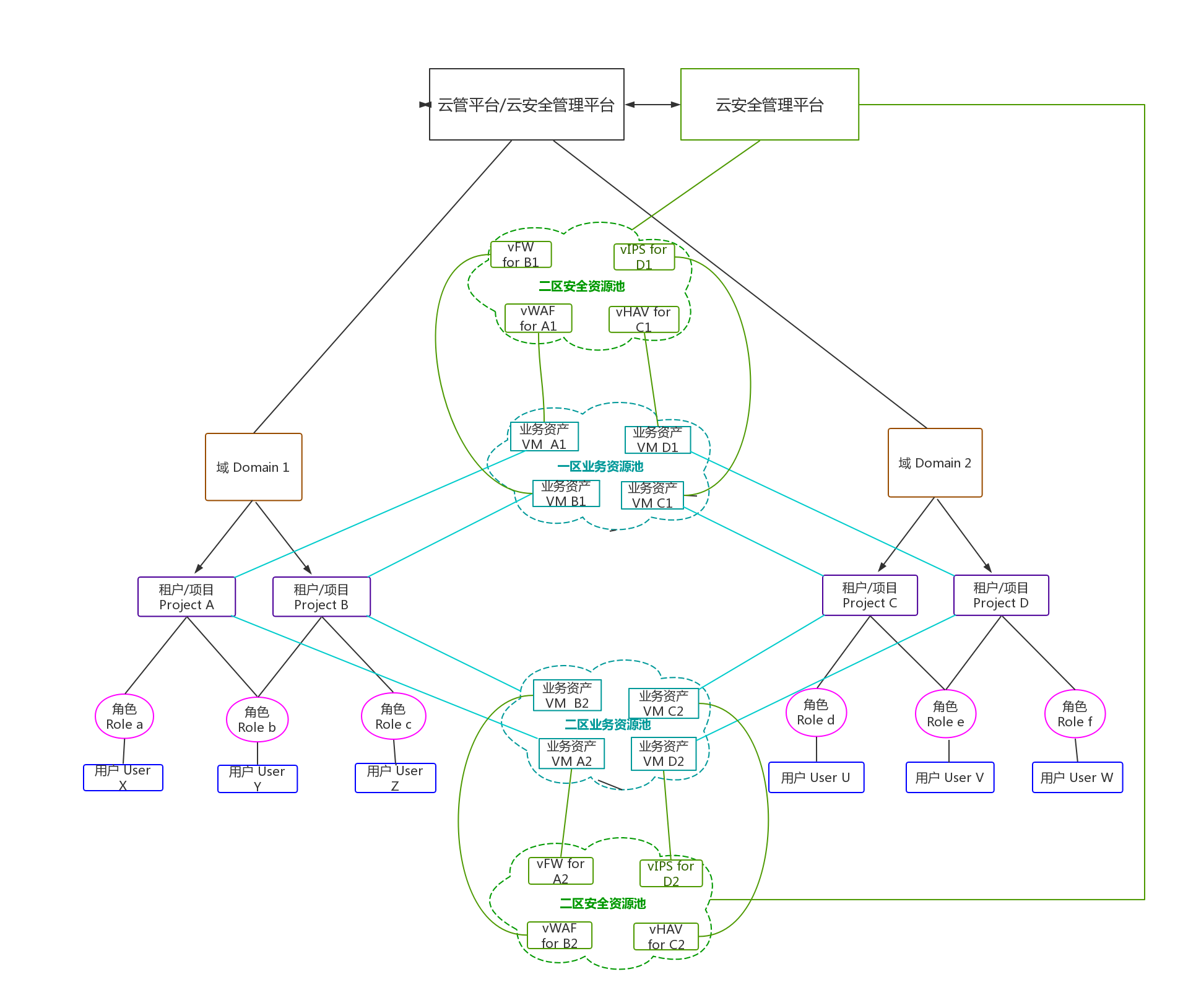


## 用户与资产结构

云安全管理平台适用于云平台的安全防护，也适用于非云平台、混合云中的安全防护的，针对不同场景，均支持灵活的用户管理和资产管理，实现从云业务到安全的无缝过渡。

云安全管理平台针对以上场景设计了一套用户和资产体系，适用于市面上主流的云管平台多租户系统，同样也支持混合云场景的多租和非多租共存的场景。

云安全管理平台用户和资产架构：



在上图中，若同步云平台，则云安全管理平台与云管平台均使用同一套用户体系；若未同步，则由云安全管理平台独立的用户系统支撑。

用户体系有不同的级别：域（Domain）、租户/项目（Project）、用户（User），支持一套系统下多个域，有一个默认域Default Domain，域下可以有多个项目，每个项目下有多个用户，而用户可以关联多个项目，每个用户在会有一种角色（对应了一套操作权限）。

云平台在每个项目下会有对应云虚拟机业务资产，这些资产可分布在不同的资源池之中，项目下的用户可对业务资产进行管理，而云安全资源池也可对不同资源池的业务资产分项目进行防护。

目前已经适配的云平台包括Openstack、曙光云（Easystack定制版）、南网鼎信云、咪咕云（苏研云定制版）、浪潮云等云平台，具体的云平台在上述概念和结构中有微小差异，适配情况请联系供应商确认。

## 安全服务链编排

* **自动化网络引流**

租户可以通过网络引流功能，将需要保护资产的网络访问流量引流到部署在安全资源池内的虚拟化防火墙实例上，通过智慧防火墙对流量进行过滤，保证访问数据的安全。

用户在云安全管理平台上对虚拟机进行引流时，仅需填写被保护资产的IP地址，云安全管理平台自动完成引流配置的生成、配置下发等操作，大大减少人工干预的过程，缩短业务上线时间。

安全资源池

网络流量

下发策略路由



云安全管理平台

被保护资产

网络引流功能也同样支持多资源池部署，云安全管理平台根据被保护资产所属的区域自动在对应的网络设备上下发引流路由。

* 服务链编排

当用户的业务同时购买了防火墙和网站防护两种组件时，需要同时采用两种组件对业务进行防护，则需要防火墙和网站防护的服务链功能。

服务链结合了自动引流、安全组件网络配置等功能，通过对交换机、安全组件转发规则的修改，实现防火墙和WAF组件的服务编排。编排后的流量走向为：

1. 客户端访问受保护的网站，DNS解析到的地址为网站防护的地址。客户端访问网站防护，源地址为客户端地址，目的地址为网站防护地址。
2. 网络设备收到目的地址为网站防护的数据包后，通过策略路由将数据包转发到防火墙上。
3. 防火墙对流量进行过滤后转发给网站防护。
4. 网站防护收到流量后，寻找域名的对应的源服务器，经静态路由发送到源服务器上。源地址为网站防护地址，目的地址为源服务器地址。
5. 源服务器收到客户端的访问请求。

安全资源池

网络流量

下发策略路由



云安全管理平台

被保护资产



## 用户自助服务

* **支持自动审批**

订单能够自动完成审批，租户的申请的安全组件创建完成之后将出现在用户的组件列表内。

* **支持多级审批，自定义审批角色**

订单审批功能支持自定义多级审批流程，并可以根据需求添加审批节点和审批角色。满足业务开展的需求。

## 计量计费账单

云安全管理平台创新地提供了大型云服务提供商按量购买安全组件授权的模式，大型云服务提供商可以按需采购安全服务的许可，许可不足后再以充值的方式增加平台内的许可数。满足大型云服务提供商合作运营的需求。

* **计量计费功能**

云安全平台内各种的安全服务的费率可以由运营商自主设置，同时支持关闭计费功能。关闭计费功能后不再计算安全组件的使用费用。

* **丰富的账单和报表**

平台支持提供丰富的每月账单和报表信息，协助用户更好地分析服务的使用成本，优化服务配置。

## 云安全态势感知

* **丰富的可视化视图**

云安全管理平台内提供了丰富的态势感知视图，运营商和租户可以查看整体威胁态势、威胁类型、受攻击的主机和域名、攻击记录等数据，各种威胁的数据通过可视化的方式呈现在大屏上。

* **高可靠的海量日志存储**

日志管理功能保证了日志存储的安全性与完整性。日志数据通过多副本的方式存储在硬盘内，保证数据存储的高可靠性。由于日志服务器的存储系统可以按需扩展，容量仅受限于硬盘大小与数量，因此可以实现用户日志的长时间保存，为日志分析与法律遵从提供完整的数据。

* **高性能日志在线查询**

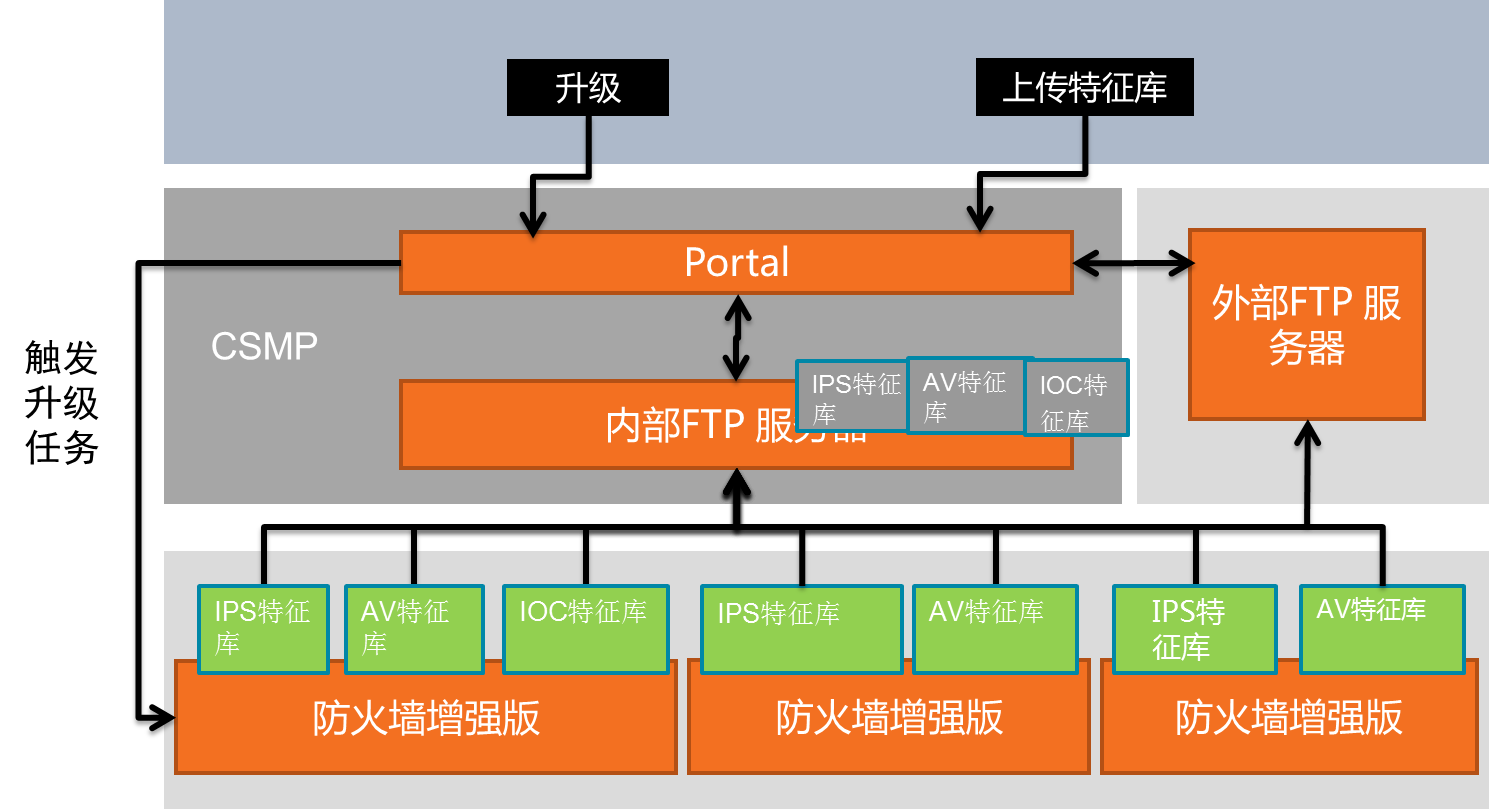
在线日志查看提供强大的日志查询与分析能力，可以对租户所有安全组件的数据进行统一在线展示。由于数据查询可以在线进行，不仅提高了日志查询统计的效率，而且能够实时查看安全时间和攻击记录。

## 在线/离线升级服务

* 本地特征库升级服务器

云安全管理平台内部提供了本地升级服务器功能。默认情况下，防火墙连接公网上的IPS特征库升级服务器，当防火墙无法访问公网时需要云安全管理平台作为升级服务器，供防火墙升级特征库。

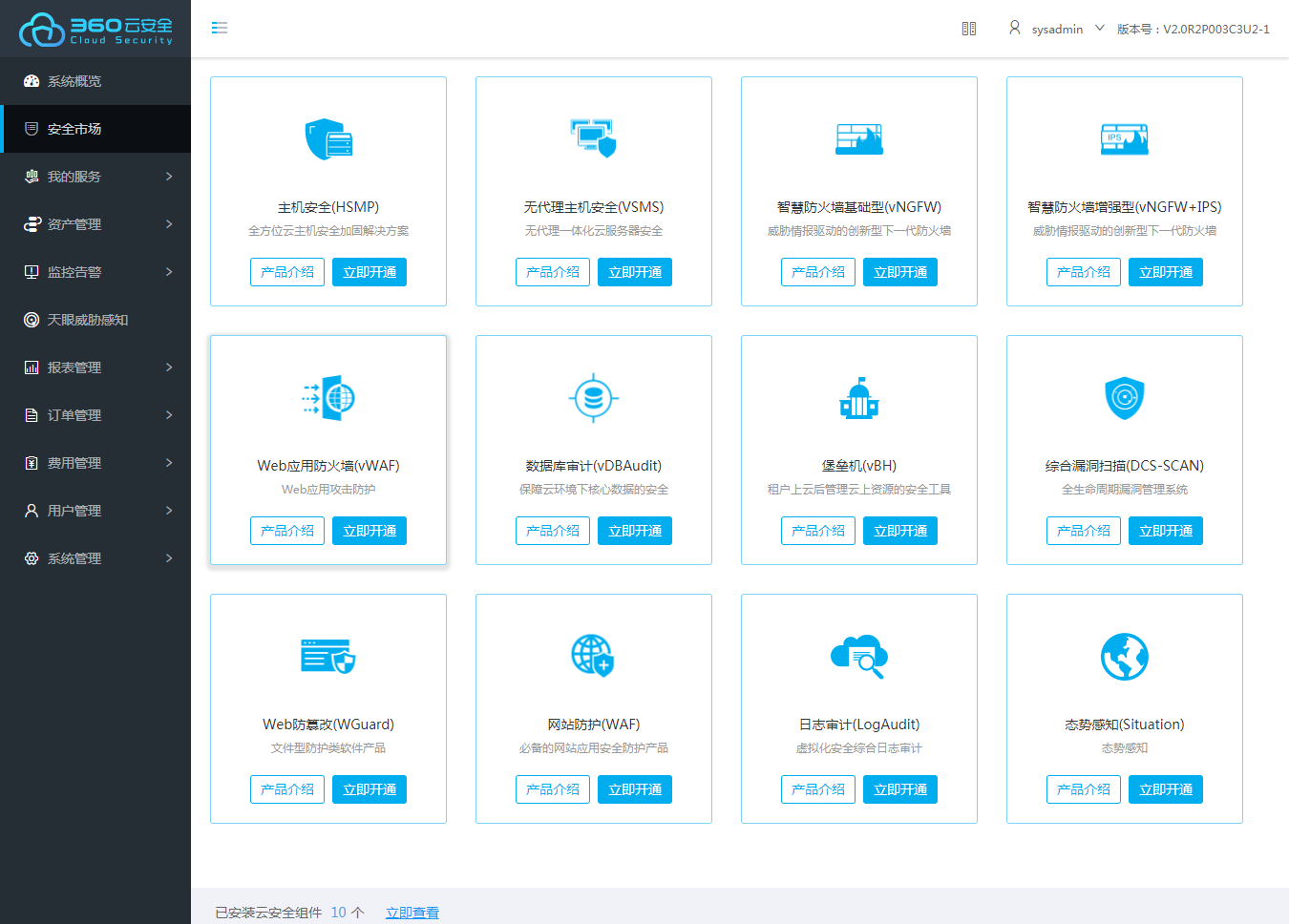
本地FTP服务开通成功后，即可上传特征库文件到FTP服务器上，点击“上传”按钮，选择本地的特征库文件后上传到服务器上。同时支持用户使用外部的FTP服务器。



# 产品简述

## 安全市场

### 自主安全组件



云上业务的安全涉及终端安全、网络安全、应用安全、审计等各个层面，对应的安全防护技术包括防病毒、防火墙、WAF、漏洞扫描、堡垒机等不同层次的安全组件。云安全管理平台整合和集成这些安全组件，以虚拟化实例的方式部署在安全资源池内，以供租户使用。



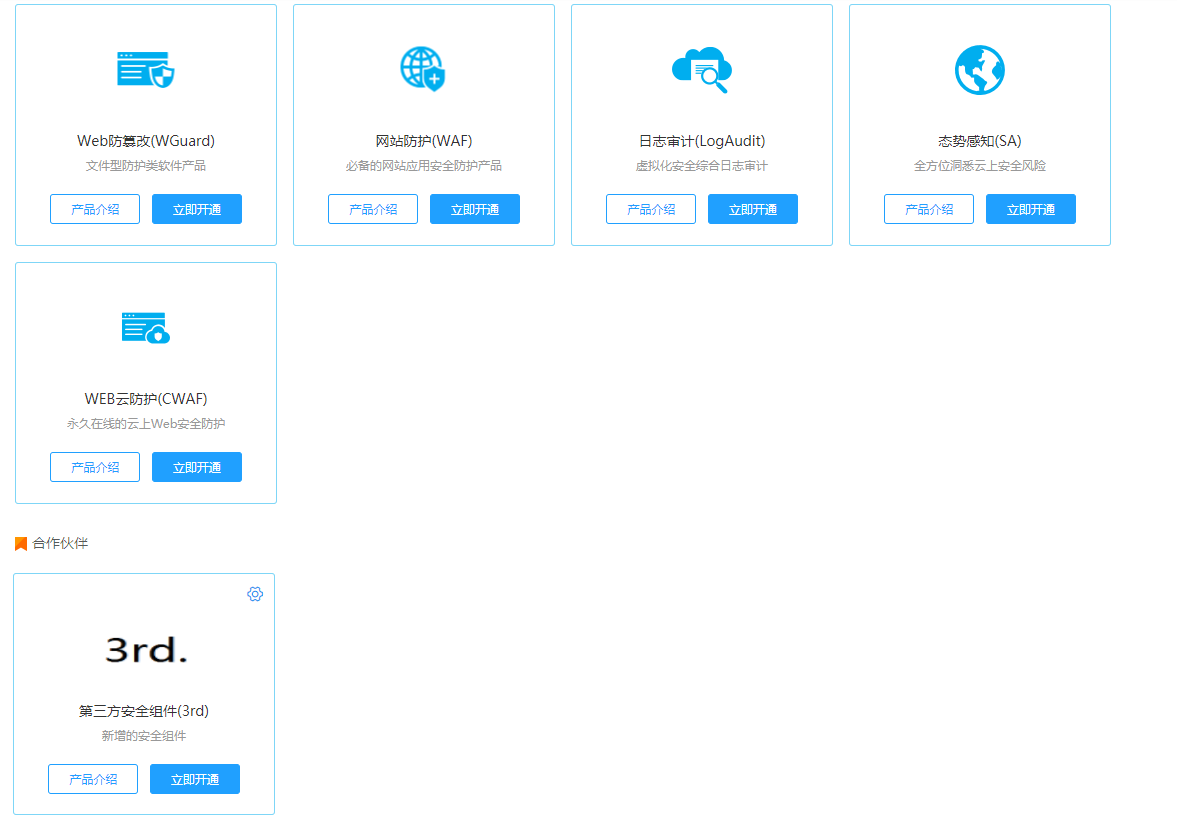
已经集成的安全组件以产品的形式显示在安全资源池内，租户在购买对应的安全组件之前可以查看安全组件的介绍，包括组件的功能亮点、优势、性能参数、部署拓扑等信息。



租户可以根据需要保护资产的属性申请对应的安全组件，并且可以灵活选择安全组件所在的可用区域、网络分区、规格、授权数量、使用时长等配置。组件有效期不足时可以通过续费的方式，增加安全组件的有效期。当组件内部如：域名数、可管理资产数等授权数量不足时可以通过扩容的方式增加安全组件内的授权数。

### 第三方安全组件

系统管理员可以将第三方的安全组件发布到安全市场中。管理员上传第三方安全组件的镜像之后，可以通过安全市场的第三方组件发布功能，将安全组件镜像发布给租户使用。发布的第三方安全组件可以实现全生命周期的管理和运行状态监控。通过第三方组件发布功能，用户可以自行将任意的安全镜像发布给租户使用，让云安全平台有了无限的扩展可能。



## 组件管理

* 生命周期管理

租户的各种安全组件以虚拟化镜像的方式部署在安全资源池内，不同的租户分别对自己的安全组件进行配置。安全组件的创建、初始化、激活等操作都又云安全管理平台自动完成。用户安全订单审批通过后，云安全管理平台将按照用户申请准备好安全组件。

安全资源池

vFW

vWAF

租户1

租户2

vFW

HSMP

云安全管理平台

* 单点登录

单点登录可以实现从云安全管理平台到安全组件之间的免账号密码登录，用户无需填写安全组件的账号密码，即可直接登录到设备的管理界面。当用户有多个安全组件需要管理时，单点登录功能可以免去大量的重复工作，而且可以避免因为遗忘设备管理账号密码带来的烦恼。

云安全管理平台

安全组件1

安全组件2

用户

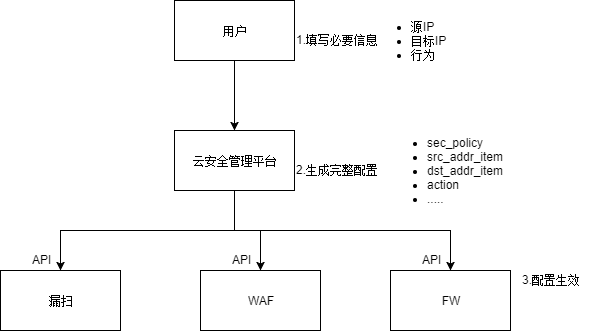
账号密码登录

单点登录

单点登录

* 统一策略管理

云安全管理平台支持对安全组件的安全策略进行统一管理，用户仅需在云安全管理平台输入基础信息，云安全管理平台生成安全策略，并通过安全组件的接口，下发到安全组件内部。简化用户的使用流程。



## 资产管理

* 资产导入管理：支持自动同步与手动创建两种方式添加与同步资产信息。
* 关联安全防护资产：云安全管理平台在对接了云平台后能够同步用户在云平台内的虚拟机资产到本地，并与用户已经开通的安全服务进行关联，用户直观地查看到哪些安全组件防护了哪些资产。以及资产安全事件和漏洞数据的同步。

## 租户信息同步

* **租户同步**

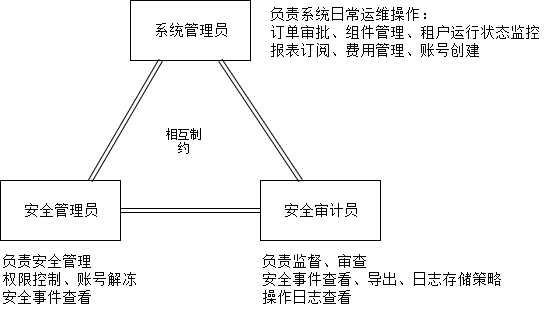
对于多租户的支持是云计算的主要特性，各个云计算租户能够自行登录云安全管理平台进行组件的申请、安全策略的配置。

云安全管理平台原生支持多租户结构，管理员可以在云安全管理平台本地创建多个租户，并添加多个子账号。在实际使用中，为了减少手动创建租户的工作量，云安全管理平台也支持对接云平台，定期同步云平台内的账号信息到本地，用户可以直接使用云平台内的账号登录云安全管理平台。账号同步后，用户所有账号的创建、删除、编辑工作都在云平台内完成。

* **三权分立**

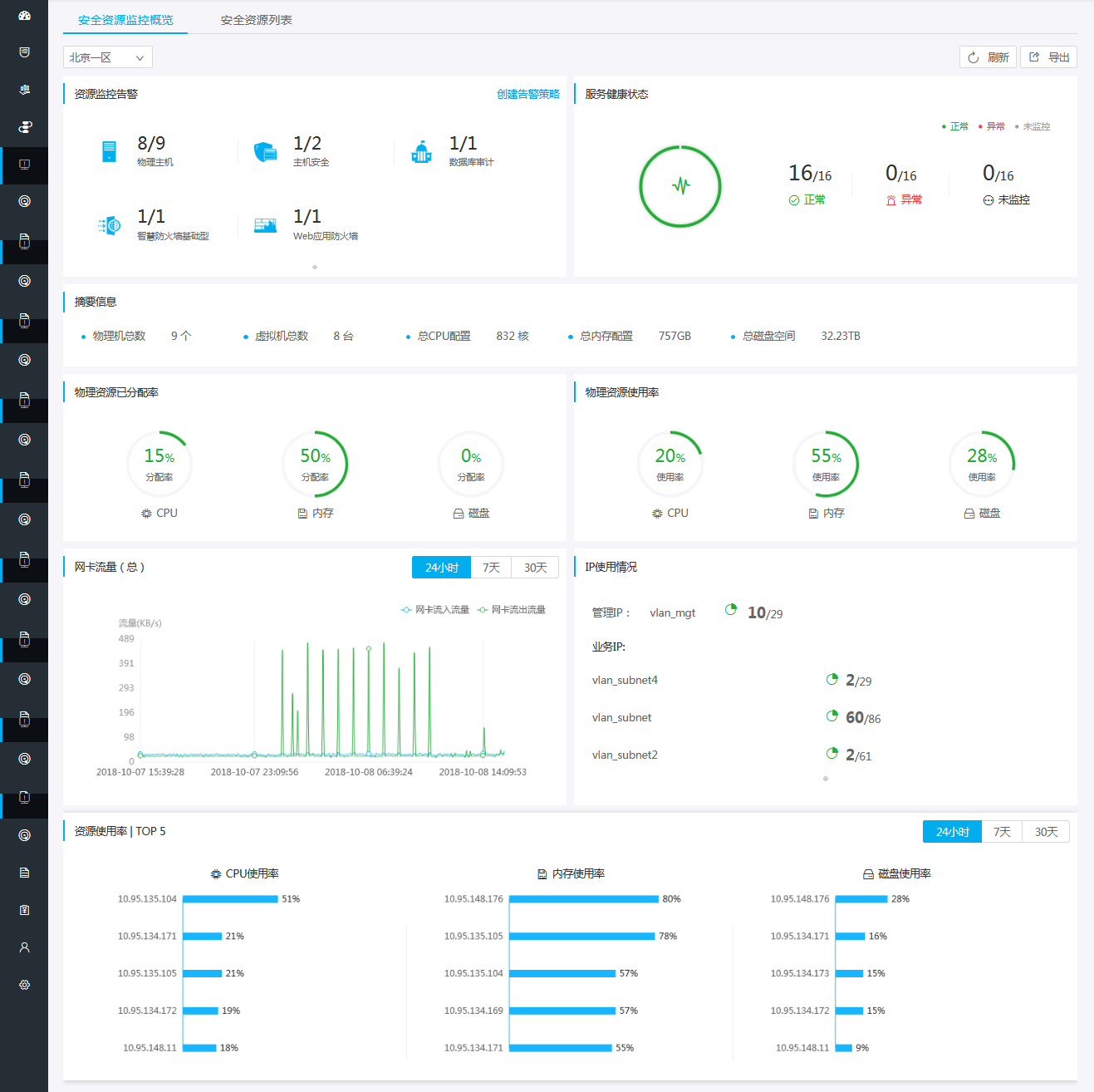
三权分立的管理机制,以最小特权和权值分离为原则,将超级用户特权集进行划分,分别授予系统管理员、安全管理员和审计管理员。在此机制下安全管理软件在实现系统管理、安全管理和审计管理功能的同时,也要保证管理员权限的隔离。

云安全管理平台支持三权分立功能，从普通权限模式切换到三权分立模式后，系统管理员和租户管理员被拆分为三个不同的角色，分别为管理员、安全管理员、审计管理员。三权分立模式满足保密要求高的场景下对于用户权限控制的需求。



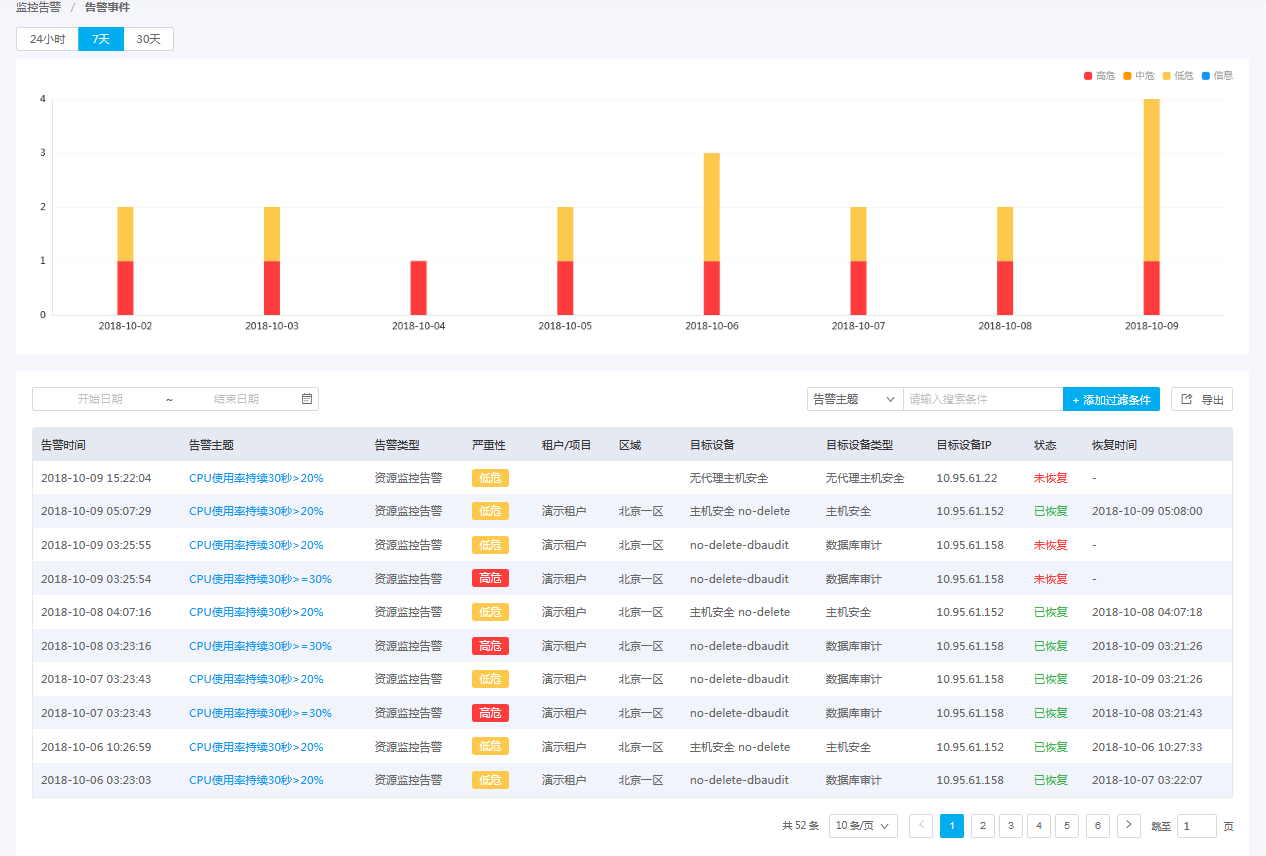
## 监控告警

云安全管理平台在部署后自带资源监控系统，从宿主机层即能对宿主机和上层虚拟安全资源进行实时的全面监控，包括安全资源使用情况和安全服务可用性，便于运维人员第一时间发现问题和采取措施，保障系统的连续可用，降低业务风险。



系统支持统一的告警管理，可配置灵活的告警策略，并根据告警策略及时生成告警。为便于使用，系统自带预定义策略，可直接使用，若用户有个性化需求，也可设置自定义告警策略。告警范围包括对所有安全资源的监控告警、对安全事件的告警、对授权到期或不足的告警、对设备异常操作的告警以及日志存储和存档空间使用告警。支持在线告警事件查看，也支持邮件告警通知。

除可设置告警策略及事件外，还有些系统告警，如高可靠状态切换、订单审批等系统默认通知和告警。



## 订单管理



订单管理实现了订单的在线提交、审批、执行等操作。当租户在线提交安全服务的请求后，租户的管理员或系统的管理员可以对租户申请的内容进行审核。同样也支持无需审核的模式，所有申请直接通过。

云安全管理平台将根据租户订单的内容自动创建对应的安全组件镜像。

## 计量计费

* 服务可衡量



云安全管理平台提供了一个可运营的安全即服务的平台。创新地支持按需充值许可的方式，云服务运营商可以随时自由地扩容各种安全组件的授权数量，并向云租户提供计费的安全服务，协助云运营商将安全服务真正运营起来，一次建设，持续产出。



云安全管理平台提供了丰富的账单和报表数据，对于安全服务的使用情况一目了然，能够持续跟踪云服务使用成本，优化系统结构。用户可以导出每月的账单数据和消费记录。

## 报表管理

云安全管理平台集中汇总了各类报表，既满足平台级统一报表，也可补充各组件的报表信息。报表内容包括安全产品使用情况、安全设备资源监控、告警事件统计、订单记录、消费账单、安全威胁防护事件等。

用户可根据需要自动生成日报、周报、月报、季报等周期性报表，也可自定义选择时间范围生成一次性报表。所有生成的报表可集中展示和管理，支持在线预览和随时下载。同时可配置报表自动发送到邮箱，提高时效。



## 云安全态势

云安全管理平台可提供云安全资源池，其中包括有丰富的云安全防护及检测组件，这些安全组件构成了在云环境中针对南北向、东西向以及租户间的安全能力，在这些具体的安全能力基础上，云安全管理平台还提供了面向集中安全态势把控、综合安全威胁呈现、云资源安全风险展示在内的云安全态势感知功能。

云安全态势感知针对云中的典型角色，分为运营商安全态势和租户安全态势的呈现，分别对应云运营方的针对整个云资源池进行态势感知的需求以及云租户对自己所租用云资源范围内的态势感知。



* 云运营商安全态势

运营商安全态势感知从展示整体云资源池安全态势的角度出发，基于CSMP所能获取的全部安全数据信息，从安全组件的防护效果视角、安全威胁的攻击分布和趋势视角、漏洞分布、近期高风险点、租户等保合规等视角对云资源池所面临的总体安全威胁和利用安全手段的防护效果进行了综合呈现。

CSMP安全态势大屏由若干态势视图组成，分别为安全威胁及防护统计数据，云中受高危攻击监视视图（地图展示），攻击源监视视图（地图展示），三级等保符合租户视图，组件部署及防护量概览，漏洞分布视图，主机失陷监测视图，威胁防护组件趋势视图，近期高危风险点视图，威胁类型排名视图以及威胁源排名视图。

* 云租户安全态势

租户安全态势大屏以各租户所使用云环境中的资源为范围，利用该租户所启用各类安全组件所产生的安全数据，进行整体安全威胁及防护态势的展示。

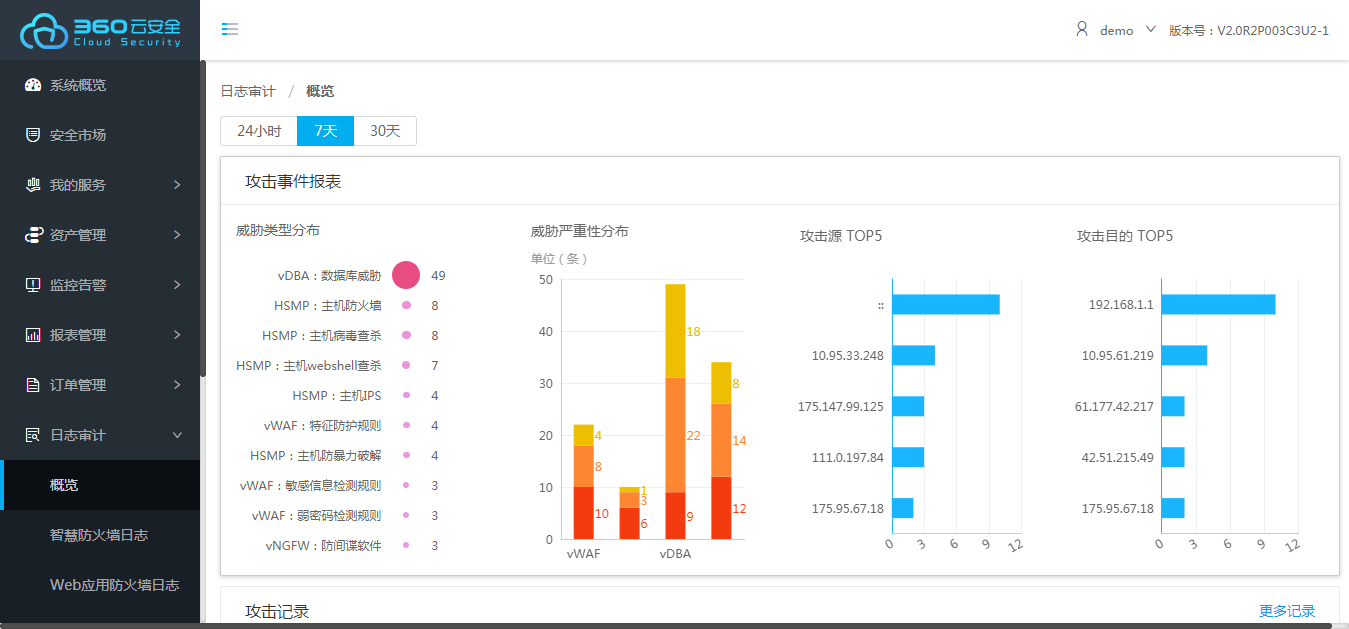
租户安全态势大屏由若干态势视图组成，包括防护拓扑视图、威胁地图视图、主机威胁分布视图、主机威胁类型Top5视图、高风险资产Top10视图、WEB威胁综合监视视图、WEB攻击威胁Top5视图、受攻击WEBTop5视图、安全漏洞监视视图、安全组件威胁防护趋势视图、威胁源Top5视图、最新攻击事件视图组成。

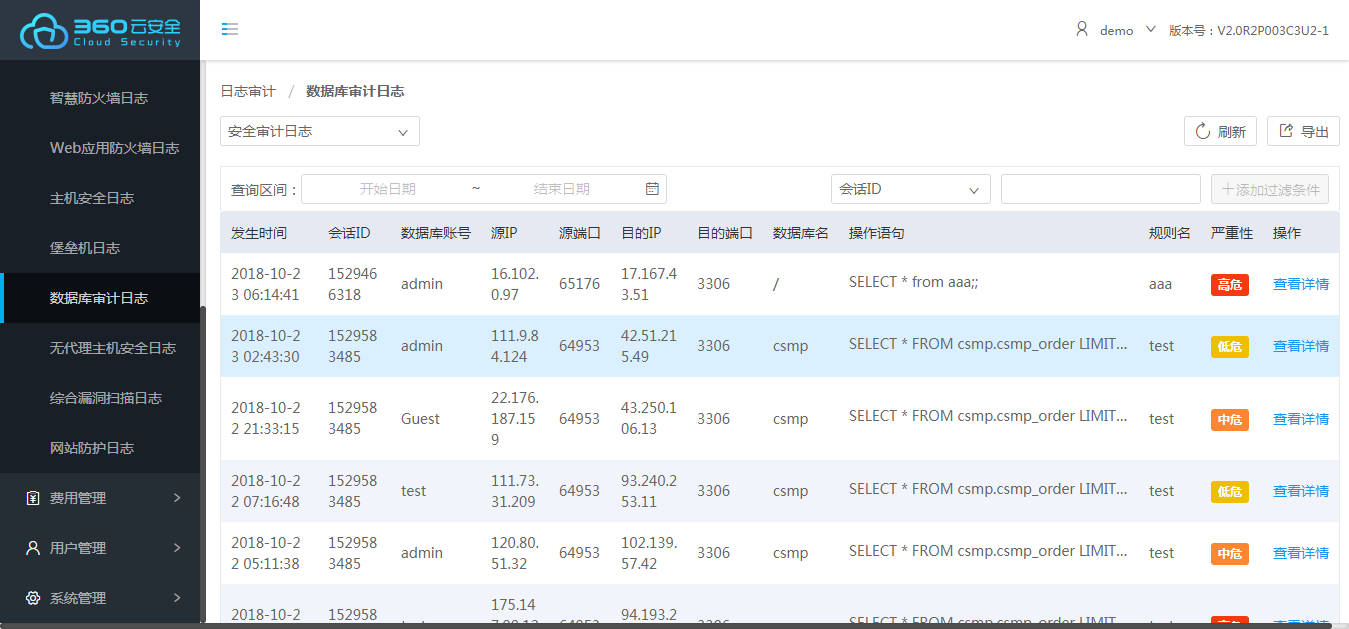
## 日志审计

云安全管理平台集中收集各种安全组件产生的访问流量日志、威胁日志和操作日志，如流量记录、web攻击事件、异常登录事件、漏洞检测事件、病毒攻击事件、异常事件等，用于事后溯源分析。

海量日志多地备份，支持自定义存储时长，可设置存档处理，也支持离线导出，满足审计合规要求。

日志审计对各种安全威胁数据进行了汇总分析，并通过丰富的报表进行可视化展示，帮助管理员及时掌握网络中被防护的安全状态，为进一步的深入分析和决策奠定准确的数据基础。





# 产品价值

云安全管理平台软件为云运营商提供了一个能够持续运营的安全业务平台，每个云平台服务商都可以轻松地在本地快速搭建起一套安全服务平台，向已有的云计算租户提供安全防护能力。云安全管理平台内集成的各种组件能为云租户的提供多个层面上的安全防护能力，同时满足各种合规的要求。

安全资源池底层采用安全云实现计算、存储、网络资源的虚拟化。奇安信安全云为虚拟化安全组件的运行和监控提供了全面的运维管理功能。奇安信安全云是奇安信集团拥有自主知识产权的私有云平台，奇安信在公有云和私有云领域深厚的技术积累保证了底层平台的安全可靠。专用的安全云平台不仅保证了底层的安全，同时也节约了云服务运营商在底层云平台的投资，无需增加额外投入。

另一方面，由于租户在使用云服务时无须了解云中的实际架构和技术实现，从用户感知上其使用的是独立完整的设备或计算资源，而无需关心具体设备的安装、部署等环节。云服务提供商在提供这种服务时可以按照租户使用的情况进行收费。

总结云安全管理平台带给的云服务运营商和租户的价值如下：

1. 可运营、可管理的云安全平台：

* 支持旁接部署模式可以和多方云平台对接，即可以支持Openstack、曙光云（Easystack定制版）、南网鼎信云、咪咕云（苏研云定制版）、浪潮云等云平台的对接，也可以支持第三方私有云平台的对接（需针对项目单独适配）；
* 支持与第三方云平台深度集成，可以通过云平台实现安全服务的编排，提供更为友好的用户体验；
* 统一的自助门户，实现安全服务的自助申请和自动创建、激活，实现云安全服务的按需申请，按量付费；
* 支持云安全服务的计量和计费，并提供了丰富的报表数据，保证云安全服务使用的透明；
* 与各种安全组件的无缝集成，租户在平台上即可完成安全组件的创建和基础的安全策略配置工作，无需复杂安装部署过程，用户体验良好；
* 所有安全事件的统一收集、呈现、威胁态势分析，并可以统一设置告警策略；
* 服务链支持与传统网络设备对接实现自动化的网络引流，减少人工操作，缩短安全服务上线时间。

1. 丰富的安全组件协助云租户构建立体的安全防护体系。云安全管理平台已经集成的安全能力包括：

* 智慧防火墙/IPS/VPN
* 主机安全
* 无代理主机安全
* 网站防护
* 数据库审计
* 堡垒机
* 漏洞扫描
* 网页防篡改
* 日志审计
* 态势感知
* Web云防护