

# 迪普科技 CSSMP 云安全管理平台



## 产品概述

CSSMP 云安全管理平台是一款架构先进、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边界出口南北向访问安全、云内主机东西向访问安全、终端安全、漏洞管理及 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迪普在云端防护能力上的优势与大数据未知威胁检测能力，能够有效的为各种公有云、行业云、私有云用户构建一套真正属于云时代的安全防护框架。迪普云安全管理平台实现了云技术平台中的运营能力、安全能力、运维能力，解决云上的运营与安全问题。

## 产品特性

### ■ 单点登录 统一门户

迪普云安全管理平台提供整个云内外安全的统一门户管理。用户不必记忆多套用户名和密码，也不必逐一记录、收藏不同安全产品的登录地址信息。只需要登录云安全管理平台，即可对该用户名下的所有安全设备进行登录与管理。

### ■ 多租户 多权限管理

每个用户、角色都具备不同的权限，管理员可以自由设定角色权限，实现不同用户所具备的权限不同，展示的管理平台界面不同。达到多租户同时登录云安全管理平台管理其名下的安全设备，且租户之间互不影响。

### ■ 产品自由发布

管理员可以自由发布各种安全产品、按需设置发布的产品、产品规格及性能，并支持将第三方的安全产品发布在迪普云安全管理平台系统中。发布的产品可供租户自由选择开通，满足租户不同的业务安全需求。

### ■ 产品一键式开通部署

云安全管理平台提供安全产品的一键式开通、自动部署。租户在一键式开通产品时，可以自由选择安全产品的种类、性能规格、有效周期等信息。产品开通后实现自动化部署与云安全资源池内的自动流量牵引，降低运维难度。

### ■ 统一策略配置下发

云安全管理平台集成各类安全产品的策略配置功能，可以通过云安全管理平台对安全产品进行策略的下发，解决传统安全设备运维管理成本高和难度大的痛点，实现安全产品的简单化运维服务。

### ■ 安全态势 可视化

云安全管理平台可基于各类安全产品提供的攻击日志与检测结果进行聚合分析，并通过可视化大屏的方式进行展示。展示内容包含安全组件的开通情况、受到各类攻击情况、攻击类型 top、攻击源 top、攻击目的 top 等有代表性的信息，并根据受到的攻击与检测到的漏洞情况对用户的安全态势进行打分。

## ■ 能力资源弹性扩容

云安全管理平台提供动态的弹性扩容能力。当资源池设备的资源不足时，可以通过横向增加服务器的方式进行扩容。当单一安全能力性能不足时，可通过另起一个安全虚机的方式来提升单个产品的安全能力。

## ■ 组件流量编排

迪普云安全管理平台通过自主研发的安全资源池分流器进行精准流量编排，基于租户网络创建分流策略组，在租户开通原子能力的同时同步创建引流策略。租户只需根据实际业务场景配置网络策略即可完成不同安全原子能力的流量编排。

## ■ 安全原子裂变

通过安全原子裂变技术可实现安全原子能力的共享，在同等资源条件下，可为租户提供更多逻辑独立的安全能力原子。区别于传统仅基于租户数据进行的表层隔离，安全原子裂变技术真正做到了不同租户间的流量转发、策略表项、产品管理等多维度的安全隔离。

## 产品功能

产品功能	功能描述
 云安全管理平台 CSMP	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。
 下一代防火墙	除具备传统防火墙的访问控制功能，还具备应用层入侵防御功能和恶意代码防范（防病毒）功能。通过单路径并行处理的安全检测引擎和应用识别，实现对用户、应用和内容的深入分析。
 WEB 应用防火墙	针对 Web 应用提供全方位的安全防护，对事前扫描、事中攻击及事后的网页篡改及信息窃取都能提供相应的防护策略。
 入侵防护系统	为用户操作系统、中间件、数据库、邮件服务器、DNS 服务器和 FTP 服务器等核心资产提供专业的应用层防护。
 上网行为管理及流控	提供专业的应用控制、带宽管理、上网行为审计、关键字过滤、用户行为分析等功能。
 VPN	提供资源访问控制，隧道加密功能。
 零信任	集成动态策略引擎，根据终端环境、用户行为、业务访问等多个维度实现动态策略实时调整，在威胁事件发生时，系统可以自动调整安全策略，评估用户信用等级，降低威胁事件响应成本。
 综合日志审计	实时进行安全事件的分析、溯源，协助用户进行安全分析及合规审计，及时有效的发现异常行为和安全事件。
 数据库审计	为云计算环境下的用户提供完整的数据库审计分析、泄密轨迹分析、数据库攻击威胁分析等安全能力。
 堡垒机	集中账号管理、集中访问控制、集中安全审计。

 慧眼安全监测	快速资产盘点、精准定位风险隐患，及时响应通报。检测操作系统漏洞、应用系统漏洞、弱口令、配置问题、Web 服务器漏洞安全及风险评估等功能。
 智能安全网关	集成 IPSec、SSL、L2TP、GRE 等多种 VPN 技术，支持国密算法，实现分支机构、移动办公人员的统一安全接入，提供内部业务跨互联网的安全访问。同时提供攻击防护、用户认证、行为审计、带宽管理、链路负载均衡等多种安全功能。
 网页防篡改	通过攻击拦截、文件监控、页面锁定等方法对网站的动态及静态文件进行多层次，多维度的全面保护。
 主机安全及管理	提供内网防入侵、终端集中管理审计、数据防泄漏、终端防病毒、远程安全接入等终端主机安全功能。
 网络审计	提供完整的数据库审计分析、泄密轨迹分析、数据库攻击威胁分析等安全能力。实现事件追根溯源，全面保护数据资产安全。
 物联网应用安全控制	对整个物联网前端 IP 设备和传输的流量进行精确管控，通过设备认证与应用认证防范非法 私接、设备仿冒、非法扫描、DDoS 攻击等问题。

杭州迪普科技股份有限公司

地址：杭州市滨江区月明路 595 号迪普科技

邮编：310051

官方网站：www.dpotech.com

服务热线：400-6100-598

杭州迪普科技股份有限公司 保留一切权利

免责声明：虽然 DPtech 试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，为此，DPtech 对本资料中信息的准确性不承担任何责任。DPtech 保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。