Cloud Security Platform
云安全平台

SecurityOne™

可视、可控、可审计的云计算系统安全管理平台

基本介绍

SecurityOne 以云计算数据中心为核心，为客户提供专业的安全产品和安全服务，降低客户面临的安全风险，实现云计算系统的安全连续性与合规性。

功能特点

SecurityOne 帮助用户确保包括身份联合认证、记录管理、用户管理、Web 访问管理与配置等云服务安全，为管理人员提供全局视角，确保用户业务的不间断运营安全，并提供可靠、安全的云内外环境。

SecurityOne 主要功能特点如下：

- **基础架构安全**

提供网络、主机、终端、虚拟化等核心 IT 基础设施的安全：

网络层面的安全控制包括网络访问控制（如防火墙），传输数据加密（如 SSL、IPSec），安全事件日志，基于网络的入侵检测系统 / 入侵防御系统 (IDS/IPS) 等。

主机（服务器和存储）层面的安全控制包括主机防火墙、访问控制、安装补丁、系统巩固、强认证、安全事件日志，基于主机的入侵检测系统、入侵防御系统等。

终端安全控制包括 BYOD 设备分类、数据安全分级、访问控制策略和设备管理策略，保证任何时间和地点的安全接入和威胁防护。

虚拟化层面的安全控制提供包括虚拟机的安全隔离、虚拟机镜像安全管理、虚拟化环境下的通信安全、虚拟化和物理安全设备的统一管理和可视化等技术。

- **应用安全**

应用程序的安全控制手段包括软件开发生命周期内嵌安全开发流程、“最小特权”配置、及时安装应用程序补丁、用户认证、访问控制、帐户管理、浏览器用最新的补丁加固。

WEB 终端安全措施包括 WEB 入侵异常检测引擎，能够有效分析和识别各类已知和变形的应用攻击，为防御准确性和高效性提供了基础，具备防御能力强、易用性好、安全态势实时告知、审计日志完善、部署灵活并支持虚拟补丁、虚拟主机等特性。

- **数据安全**

数据安全技术包括事前扫描和事后审计：事前扫描评估，可以建立安全数据库，保障用户信息的可用性、保密性和完整性；审计作为事后追溯的最有效依据，不仅是合规的要求，也是内部自身安全运维管理的要求，在满足合规的同时，能够弥补组织安全策略的不足，快速提升审计能力和安全水平。

- **身份 / 访问安全**

身份和访问管理包括：身份供应、取消供应、认证、联盟、授权和用户配置文件管理，以及能满足各种用户和访问流程自动化需求的开放式应用程序接口等。支持在组织内构建一套强大的目录和身份联合管理功能—如体系架构和系统、用户和访问生命周期管理流程、审计和合规功能。

平台优势

- 一站式的云安全解决方案
- 网络设备、安全主机和应用系统日志全面标准化
- 国际标准化的关联分析引擎，为用户提供全维度、跨设备、细粒度的关联分析
- 提供集中化的统一管理平台，实现信息资产的统一管理
- 集中审计系统
- 安全日志的全生命周期管理
- 全面的智能收集功能
- 创新的日志解析能力
- 先进的关联算法
- 可维护性及可扩展性

INTPLE 引跑科技 | 服务热线：400 669 9289
公司网站：www.intple.com