深信服智安全
SANGFOR SECURITY

深信服下一代防火墙

产品概述

深信服下一代防火墙是面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备。深信服下一代防火墙采取本地与云端联动的安全检测模式，围绕用户业务整个生命周期，提供全过程的安全防护技术，并通过云安全服务提供 7*24 小时安全问题分析和快速响应的技术服务，为用户提供简单有效的安全技术保障。

深信服自 2011 年推出全国首台下一代防火墙，在政府、金融、教育、运营商、大企业等多个行业得到广泛应用，截至到 2017 年底，深信服下一代防火墙的用户高达 4.5 万家以上。深信服作为国内下一代防火墙的第一品牌，主导和推进了公安部第二代防火墙标准的建立与制定，同时连续多年成功入围 Gartner 企业级防火墙魔力象限。

功能特性

全面的安全防护能力

- 采用融合的产品理念，集传统防火墙、WAF、VPN、IPS、防病毒、带宽管理等功能于一体，简化部署，提高管理效率；
- 独特的双向流量检测技术，帮助用户主动发现网络中保护对象存在的安全风险；
- 产品内部多功能联动，拥有主动防御各类威胁攻击的能力，同时与云端服务联动，快速提升用户的应急响应能力；

安全可视化

- 基于用户安全和业务安全视角，将用户网络存在的安全风险直观展示，帮助用户快速看懂风险状况；
- 支持用户资产的自动发现以及资产脆弱性和服务器开放端口的自动识别；
- 可视化综合风险报表对当前网络的安全状态进行评估，并给出相关优化建议，帮助用户直观地了解当前企业网络的安全性，降低网络安全运维难度。

简单快速交付

- 场景化的配置向导，用户选择不同的部署方式以及使用场景，即可实现产品的快速实施；
- 支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，简化用户配置工作；
- 内置安全运营中心，检测用户网络各阶段存在的安全问题，并形成代办列表，帮助用户快速消除安全隐患；

应用场景

● 互联网出口场景

客户痛点：

◆ 互联网出口需要多种安全设备，用户投资大，安全设备难以管理；

◆ 企业员工日常上网办公，由于缺乏安全意识，办公 PC 中毒现象屡见不鲜；

◆ 安全运维人员人手有限，传统安全产品日志经常看不懂，企业安全问题无法快速分析，导致运维工作繁重；

应用价值：

✓ 单台下一代防火墙替代多种传统安全产品，简化管理，提升用户投资性价比。

✓ 专业的僵尸主机检测技术，帮助用户及时发现已中勒索病毒和远控木马的僵尸主机，降低安全事件带来的企业内部数据资产泄露风险。

✓ 可视化的网络安全风险展示，帮助用户快速定位发现安全问题，实现安全简单运维。

● 数据中心场景

客户痛点：

◆ 高级网络攻击手段屡见不鲜，企业数据中心虽然划分了安全区域，但是应用层攻击防护存在短板；

◆ 各种 0 Day、勒索病毒等新型威胁攻击可以轻松绕过数据中心防火墙，安全管理人员担心数据中心存在类似安全风险；

◆ 内部缺乏有效的管理技术手段，有意或无意的高危操作可能导致业务数据泄露；

应用价值：

● 为企业数据中心服务器提供 L2-7 层的完整安全防护，防止黑客非法入侵，保障企业 OA、邮件、销管等应用的安全和稳定运行。

- 实时风险监测，及时发现并弥补业务漏洞，帮助用户快速解决安全隐患。
- 丰富灵活的细粒度安全策略，保障总部员工、分公司员工和运维人员对数据中心的合法访问。

● 对外业务保护场景

客户痛点：

◆ 企业网站直接暴露在互联网中，各种黑客攻击防不胜防；

◆ 企业官网被非法植入色情、赌博、反动言论等内容，导致客户访问量减少，百度排名逐渐下降；

◆ 安全事件发生后，安全管理人员缺乏及时预警检测手段，往往后知后觉；

解决方案：

✓ 保护用户网站在遭受到黑客攻击后的可用性，避免用户网站被劫持、挂马、植入后门、篡改等安全事件的发生。

✓ 基于动态防篡改机制，保障企业网站的 SEO 搜索排名，防止企业形象损害和信誉度降低。

✓ 提供 7*24 小时云端监测和应急处置服务，提升企业用户安全事件快速响应能力。

典型案例

部分客户列表					
央企	招商局集团	宝钢集团	中铁一局	大唐移动	华润电力
互联网行业	巨人网络	联想	浪潮	携程	搜狗
科技集团	京东商城	小米科技	海康威视	北大方正	康佳集团
房地产	链家地产	碧桂园	万科	广大企业集团	海印集团
知名制造业	比亚迪	安踏	广汽丰田	国美电器集团	奥康国际