

DPtech Scanner1000 漏洞扫描系统



产品概述

信息技术飞速发展，网络应用日益复杂和多元化，利用漏洞攻击的网络安全事件日趋严重，权威机构统计 95%以上的攻击事件都利用了未及时修补的漏洞，让用户蒙受巨大的社会、经济损失，漏洞俨然已经成为危害互联网安全的罪魁祸首之一。

因受应用层技术复杂、更新快等因素限制，传统产品主要针对操作系统漏洞进行扫描，针对应用级漏洞，如Web 应用、SSL 加密等漏洞管理效果不佳，并且在漏洞管理上过于单一，不具备漏洞预先通告、定期评估、漏洞自动修补等重要功能，无法从根本上避免攻击产生。因此，只有从技术本源入手，采用完整、有效和持续的漏洞扫描管理系统才能有效地避免攻击威胁。

DPtech Scanner1000 系列产品是业界性能卓越、漏洞检测全面、功能丰富的漏洞扫描系统，能够满足各种应用环境的部署与管理需求，目前已成为漏洞管理的首选产品。

产品特点

■ 闭环管理流程，提供全方位漏洞管理

DPtech Scanner1000 可提供漏洞通告、关联检测、自动修复、资产风险管理、漏洞审计多维度闭环管理功能，通过高性能的多核硬件平台，可实现对网络中各种资产进行全方位、高效的漏洞管理。

■ 全面精确的Web 安全分析，确保应用层漏洞防护

DPtech Scanner1000 支持针对Web 应用系统进行代码级检测，消除跨站脚本攻击、SQL 注入、网页挂马等漏洞威胁，且支持对SSL 加密应用的漏洞管理。

■ 自动补丁管理，及时解决潜在风险

DPtech Scanner1000 能有效的和微软的WSUS 服务进行联动，当检测到相关漏洞后，可以通知管理员在指定主机上启用相应的WSUS 联动配置，当有漏洞补丁发布时，该主机就会主动到指定的 WSUS 更新服务器获取最新的漏洞修复补丁。

■ 漏洞库自动更新，持续安全防护

DPtech Scanner1000 漏洞扫描系统采用迪普科技应用识别与威胁特征库APP-ID，该特征库可进行自动、及时、准确的升级，从而确保漏洞判断准确无误。

产品系列



Scanner1000-Blade













Scanner1000-GS



Scanner1000-MS

功能价值

技术优势	功能价值
 支持多种网络资产	支持终端设备、服务器、路由/交换设备等网络资产 支持多种操作系统 (Windows/Linux/Unix) 、应用服务、数据库
 深度Web 漏洞扫描	Web 服务器检测、插件检测、配置检测、注入攻击漏洞检测、注射攻击漏洞检测、远程文件检索漏洞检测、文件上传检测、FORM 弱口令检测、数据窃取检测、GOOGLE-HACK 检测、中间人攻击检测、Web2.0 AJAX 注入检测、Cookies 注入检测、弱口令扫描
 网页木马检测	支持各种类型木马检测、木马分析、木马溯源
 应用漏洞扫描	SMTP/POP3、FTP、SNMP、端口扫描、弱口令扫描
 多种扫描方式	支持定时扫描、手动扫描等多种扫描方式
 支持网络爬虫方式	可自定义扫描深度、预定义用户登录参数、提供交互式用户登录参数设置、支持并发扫描
 自动漏洞修复能力	自动补丁管理，可与微软WSUS 联动
 ICP 备案提醒功能	可支持ICP 备案提醒功能，能够扫描网站的ICP 备案是否到期，并可提供告警
 丰富的报表功能	可提供扫描结果对比、漏洞报告、统计分析等多种报表类型
 全面的特征库	漏洞库兼容 cve 、cncve、cnnvd, bugtraq, 包含危险特征超过 22000 个

杭州迪普科技有限公司

地址：浙江省杭州市滨江区通和路68号中财大厦6层

邮编：310051

官方网站：www.dptechnology.net

售前咨询热线：800-9900-598

技术支持热线：400-6100-598

Copyright©2011 杭州迪普科技有限公司 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。