【产品彩页】

DPtech XDR终端检测与响应系统

杭州迪普科技股份有限公司

产品概述

随着 IT 技术的飞速发展以及互联网的广泛普及，各级政府机构、组织、企事业单位都分别建立了网络信息系统。互联网中，终端计算机是源头，也是终点。随着信息网络建设的发展，终端计算机安全防护越来越重要。如何推进终端计算机安全建设，夯筑底层安全体系，是当今企业面临的问题。虽然防火墙、入侵检测系统等常规的网络安全产品可以解决信息系统一部分安全问题，但计算机终端的信息安全一直是整个网络信息系统安全的一个薄弱环节。据权威机构调查，超过 85%的安全威胁来自企事业单位内部。在国内，高达 80%的计算机终端应用单位未部署有效的终端安全管理系统和完善的管理制度，造成内部网络木马、病毒、恶意软件肆虐，各种 0day 漏洞、APT 攻击层出不穷。同时系统与应用软件的安全漏洞使得黑客入侵有机可乘；自主知识产权操作系统的缺乏，使得国内广大终端用户面临前所未有的挑战。除此之外，企事业单位内部网络与终端安全问题还包括：

- 终端病毒、木马问题严重，不能高效有序查杀；
- 全网被动防御病毒、木马的传播与破坏，无法应对未知威胁；
- 不能及时发现系统漏洞并进行补丁分发与自动修复；
- 资产不能精确统计，资产变动情况掌握滞后；
- 终端单点维护依靠大量人工现场处理；
- 未经认证的U盘、移动硬盘等移动存储介质成为病毒传播的载体；
- 光驱、网卡、蓝牙、USB 接口、无线等设备成为风险引入的新途径；
- 终端随意接入网络，入网后未经授权访问核心资源；
- 非法外联不能及时报警并阻断，导致重要资料数据外传流失；
- 终端随意私装软件，恶意进程持续消耗有限网络带宽资源。

针对以上问题，迪普科技推出了领先行业的产品解决方案——DPtech XDR 终端检测与响应系统。

DPtech XDR 终端检测与响应系统是集恶意代码防护、桌面管理、终端威胁检测与响应（EDR）于一体的全新一代终端安全管理系统，系统建立统一管理的终端安全整体防护体系，有组织有计划地监测和分析终端安全状态，统一配置终端安全策略，提供终端的安全保障能力，确保终端系统正常、高效的运行，提供彻底解决终端安全威胁的全生命周期的管理，包括事前预警防范、事中应急处置、事后追责溯源，完成终端安全威胁闭环。

产品特点

■ 先进的体系结构

终端安全管理系统采用了先进的分布式的体系结构，使用了 B/S（浏览器/服务器）和 C/S（客户端/服务器）两种模式进行通讯和管理，B/S 模式用于控制和管理方面，使用该模式控制中心进行全网控制和管理更加方便、快捷；C/S 模式用于通讯方面，该模式使客户端和主控中心在通讯方面更加稳定。实现对整个网络上所有计算机的集中管理，清楚地掌握整个网络环境中各个节点的安全状态，既方便管理员管理，又能在最大程度的减少整个网络中的安全漏洞，为用户的网络系统提供安全可靠的解决方案。

■ 顶尖的杀毒引擎

防病毒系统的杀毒引擎采用了智能广谱技术、内存杀毒技术和比特动态滤毒技术等多项全球顶尖的杀毒技术，可以安全地清除引导区病毒、邮件病毒、恶意网页、木马程序、黑客程序、VBS 病毒生产机、宏病毒、蠕虫以及其他类型的病毒，查杀病毒数量超过60000种。

■ 联动智能主动防御体系

增强智能主动防御体系，对未知病毒实施多行为联动主动防御，更准确、更全面地防御未知病毒。系统级行为监控，从注册表、系统进程、内存、网络等多方面对病毒行为进行主动防御，全方位保护系统安全。

■ 内核级自防御体系

大部分主流病毒技术都进入了驱动级，病毒已经不再一味逃避杀毒软件追杀，而是开始与杀毒软件争抢系统驱动的控制权，使杀毒软件功能失效。防病毒系统拥有强大的自防御体系，阻止了病毒目前所有已知的破坏手段，从系统底层保护自身安全，为保障系统安全打下了坚实的基础和前提。

■ 反病毒Rootkit、Hook技术

越来越多的病毒开始利用 Rootkit 技术隐藏自身，利用 Hook 技术破坏系统文件，防止被安全软件所查杀。防病毒系统反病毒 Rootkit、反病毒 Hook 技术能够检测出深藏的病毒文件、进程、注册表键值，并能够阻止病毒利用 Hook 技术破坏系统文件，接管病毒钩子，防御病毒于系统之外。

■ 全方位的病毒监控体系

防病毒系统的病毒监控功能非常强大，监控的对象包括软盘、光盘、硬盘、内存、网络邻居、文件夹、OFFICE、文档、邮件、网页、注册表、各类脚本等，帮助您构筑起全方位的安全壁垒，让您的计算机远离病毒侵袭。

■ 强大自我保护能力

防病毒系统对终端使用的进程进行保护，防止病毒程序恶意关闭杀毒软件进程。对自身的安装程序和安装目录进行保护，防止中病毒计算机安装杀毒软件被病毒关闭，有效防止病毒镜像劫持，关闭杀毒软件的情况发生，即使中病毒后也可安装杀毒软件终端安全管理系统防病毒，高效的处理病毒问题。

■ 全方位系统性能监控

可以对网络中各级控制中心的系统性能，CPU 使用率、磁盘使用率、服务状态等指标进行监控，让管理员一目了然的掌握整个系统的工作情况。

■ **自动化智能管控终端**

通过计划任务管理、智能升级、系统补丁管理等多元化功能，制定针对终端的安全策略，控制中心会自动进行杀毒、漏洞修复、自动升级等安全操作，确保终端安全。

■ **简洁易用，缩短学习曲线**

桌面管理系统配置简单，操作直观、便捷，易于使用和维护；提供全中文的、统一规范的图形接口界面。让 IT 管理员无须任何培训就可以进行系统管理。

■ **自动化合规基线**

桌面管理系统从驱动层接管操作系统，终端如违反了控制中心配置的合规基线项，控制中心会根据自动检测的结果对终端的不合规项进行强制矫正，做到终端合规基线统一化。

■ **行为安全管控**

通过终端行为策略的下发，最终实现对终端用户的上网行为、机密信息传输、网络应用行为、各种操作行为的统一管控和统计分析，降低终端用户行为访问的安全风险。

■ **安全审计管理**

通过对终端行为的管理与综合审计，最终实现对终端操作行为、远程访问行为的集中记录与审计，便于对各种事件信息的统计分析和事后跟踪、追查。

■ **提高机密文件的安全性**

桌面管理系统中的文件操作审计及违法外联功能能够能有效的防止单位重要档案、文件及数据遭内部或外部人员非法拷贝，例如使用 USB 盘(Flash Disk)等存储设备将数据外泄，构筑监督机制，避免造成重大损失。

■ **灵活的系统可扩展性**

桌面管理系统架构合理，采用多层架构和线程池技术，保证系统高性能和海量吞吐能力和很强的伸缩性。

■ **高效率的网络通信**

由于有大量的代理和服务器的交换信息，数据存储过程，网络通信的效率也至关重要。如由于数据交换的信息占用了正常的用户带宽，影响网络运行，会对系统应用的实际效果造成影响。桌面管理系统通过高效率的压缩算法，使得远程桌面控制时的网络通信也降到最低。对于单位的局域网更加不成问题。平时的网络通信更是只有几K的带宽占用。

■ **良好的设备兼容性**

由于桌面管理系统更多的是和操作系统层和网络通信层进行编程，和硬件设备层的相对隔离使得桌面管理系统具有良好的设备兼容性，不同的硬件条件都可以使用桌面管理系统进行管理。

■ **全面的终端行为数据采集**

通过在终端安置的“探针”，持续性的对终端的主机、进程、网络连接、终端行为等信息进行采集， 并实时将采集到的数据上报至威胁信息平台进行统一的管理和分析。

■ **智能检测，精准识别攻击**

通过人工智能持续学习、行为能力分析、大数据分析引擎、智能沙箱引擎，真正洞察威胁本质，能够更有效的检测鉴定未知病毒，实现对未知病毒的精准锁定。

主要功能

终端安全管理系统防病毒主要功能:

终端安全管理系统防病毒的控制中心采取了多项先进的技术，功能强大，简单易用。丰富的网络管理功能，能够实现全面集中分组管理全网查杀毒、全网远程设置、远程杀毒、集中式授权管理、全面监控邮件客户端、统一的管理界面、直接操纵客户端等多种复杂的管理功能，让往常繁重的日常管理工作变得轻松自如。

■ 全方位的资产管理

全面展示全网终端软硬件资产、操作系统、病毒库日期、进程等详细信息，实时记录资产信息变更，做到终端安全管理一目了然。

■ 实时全面的病毒防护体系

可通过控制中心对网络内的服务器、客户机进行远程策略设置、病毒查杀、远程升级等各种管理操作；病毒检测处理主要包括：

- **实时和定时检测/清除病毒**：实时检测和清除来自各种途径的各类恶意代码和特洛伊木马等黑客程序。对来自 Internet、E-mail 或是光盘、软盘、移动存储、网络等各种入口渠道的宏病毒、特洛伊木马、黑客程序和有害程序等全面进行实时监控。

- **多重压缩格式文件查杀**：支持查杀 DOS、Windows 等系统的 ZIP、GZIP、ARJ、CAB、RAR、LZH、UPX、ASPACK、FSG 等多种压缩包格式的文件。

- **内存监控**：能够直接对运行程序的进程和线程进行扫描，并直接在内存中对正在运行的染毒文件进行清除病毒的工作。

- **网页监控**：查杀含有未知恶意代码网页的能力，确保用户在浏览网页时不被恶意网页病毒干扰和破坏。

- **引导区监控**：可查杀引导区的病毒，确保用户在用户系统固定扇区固定磁道不被病毒所感染。

- **注册表监控**：全面监控注册表，确保注册表不被恶意病毒所修改。

- **邮件病毒检测**：支持邮件接收、发送检测；邮件文件静态检测、清毒；邮箱静态检测、清毒。至少同时支持Foxmail、Outlook、Outlook Express、Notes 和 Netscape 等客户端邮件系统的防（杀）病毒。

- **可移动设备防护**：可通过设置密码限制可移动设备的使用，实现网络防毒系统实施统一管理和监控。

■ 防毒策略的定制与分发

防毒策略的定制和分发对全网的病毒预防起着至关重要的作用。网络管理员通过控制中心对全网或某个分组设置统一的防毒策略也可对特定的客户端设置防毒策略以保证防病毒策略的有效实施。具体的防毒策略包括设置客户端的实时监控的选项设置客户端定时扫描病毒设置保护密码防止客户端用户关闭实时监控或卸载杀毒软件等。

■ 病毒报警

终端安全管理系统防病毒具有自动报警功能，无论网络中的哪一台计算机感染了病毒，都会马上通知控制中心。让管理员在第一时间做出反应，将病毒带来的风险和损失减小到最低的程度。在管理控制中心服务器或整个能登录控制中心的网络上方便地查看全部范围（或组范围）的病毒报警和报告，包括感染节点的主机名、IP 地址、病毒名称、清除情况、被感染文件的路径等。

■ **系统补丁管理**

伴随着网络的飞速发展，利用操作系统漏洞的攻击和恶意程序也层出不穷，为了尽可能减少用户的操作系统感染病毒的几率，减少通过已知漏洞入侵造成不可预料的损失，终端安全管理系统防病毒特设全网操作系统补丁检查。该功能可以在安装了客户端的机器上主动的扫描出系统需要的补丁，并实现自动下载安装的全自动化操作，可避免由于机器数目过多而造成的每台机器都单独下载补丁的麻烦。只需管理员在控制中心进行补丁的下发操作，即可完成补丁的分发部署，为网络环境的安全再筑壁垒。

■ **完善的日志报告**

终端安全管理系统防病毒的日志报告功能把网内每一台计算机的升级、查毒、杀毒等事件都详尽记入日志文件中，以备管理员随时查看。同时，还可以根据日志对一段时间内网络中病毒的流行、发作的情况进行统计分析，生成图表形式的报告，帮助管理员有针对性的制定适合本网络的安全策略。

■ **远程管理及增强密码保护**

管理员通过管理员口令登录控制台以后，可以对安装了终端安全管理系统防病毒客户端的计算机进行杀毒、查毒、设置、升级和客户端的安装卸载工作。通过管理员权限设置保护密码，对客户端的卸载、修改、退出、关闭监控、进行密码管理，增强客户端的防病毒能力。

■ **远程文件下发**

可对远程客户端下发文档，远程执行程序等操作。当有重大的病毒爆发时，控制中心可以通过此功能将工具及时的下发下去进行扫描操作。该功能也增加了网络内传输文件的安全性，避免了当网络内的计算机通过共享文件夹进行文件互换时而被病毒侵入的情况发生。

■ **白名单免检设置**

管理员可以通过控制台设置不扫描的文件或者文件夹，客户端在扫描和监控时，会跳过所设置的文件或者文件夹。

■ **统一智能升级**

终端安全管理系统防病毒的智能升级功能可以定时检查病毒库的最新版本，发现最新版本后首先升级控制中心的病毒库，然后自动将升级包分发至局域网内的各个客户端，实现全网络的病毒库版本同步更新。

■ **计划任务管理**

通过计划任务管理功能，可以实现对控制中心进行定时同步升级、补丁库更新、定时执行病毒扫描计划、设置定时清除长期离线客户端、设置客户端自动的开机和关机。

■ **智能安装与卸载**

终端安全管理系统防病毒提供了远程安装功能，用户登录终端安全管理系统防病毒的控制中心后，网络中的其它计算机上可在控制中心首页进行终端安全管理系统防病毒客户端安装，安装过程中自动识别将要安装的计算机、操作系统类型，针对不同的操作系统安装不同版本的客户端，减轻了管理员的工作负担，也提高了管理员的工作效率。同样，也可以通过控制中心对已经安装好的终端安全管理系统防病毒客户端进行远程卸载。

终端安全管理系统桌面管理主要功能:

■ **资产管理**

自动识别全网的软硬件资产，当资产发生变更时，终端则将主机信息及变更情况上报至控制中心，防止由于资产的丢失造成经济损失和数据泄露。

■ **杀毒软件管理**

实时检测终端是否安装杀毒软件，确保每台终端都安装了杀毒软件，能够及时查杀病毒。

■ **报表管理功能**

桌面管理系统支持对全网资产，软件使用情况，违规事件等信息进行报表统计。能够对终端名称、IP 地址、IP段、策略下发执行结果、时间等信息进行报表日志的精准查询，帮助管理员对日常安全防护、安全运维工作进行分析评估。

■ **文件访问管理**

桌面管理系统可对指定文件进行限制文件操作权限或记录特定文档/网络盘文件的操作行为，包括能够对终端系统上所有机密文件读写、复制、改名、移动、拷贝、删除等操作进行实时监控，详细记录机密文件/网络盘文件的操作行为，为企业的审计工作提供帮助。

■ **实时应用程序管理**

桌面管理系统允许对进程设置黑白名单策略管理。白名单策略终端只能运行指定的软件，黑名单策略禁止非法程序的运行，加强应用程序运行管理，保证 PC 软件环境的一致性和可控性。实时记录非法程序的应用程序运行状况的详细信息，让管理人员了解终端用户非法程序的运行情况。

■ **违法外联管理**

能够实时检测内部网络中出现的私自联到外部网络的行为（即“非法外联”行为），对私自联到外部网络的用户阻断网络连接，并将违规行为上报至报警控制中心。

■ **移动介质存储设备管理**

通过桌面管理系统的移动介质管理功能，可以设置禁止或允许移动介质存储设备的接入，帮助用户全面落实 USB存储的使用和控制，实现“非法的进不来，合法的出不去”，保障信息网络与数据的安全。

■ **网络访问管理**

网络访问管理可以部署内部 PC 的网络访问规则，只允许或禁止某些 PC 访问特定的资源。例如禁止访问某网站、禁止收发 Email、禁止使用某程序、禁止访问网络共享等，还可以控制 PC 禁止开放哪些网络端口等等，从而有效规范内部 PC 的网络访问行为。

■ **共享访问控制**

管理员在此页面中可以设置哪些 PC 能够设置系统共享服务，被禁止的终端将无法进行文件共享服务。阻断了黑客通过 445 端口进行入侵的行为，不让黑客有机可乘。

■ **邮件监控及控制**

邮件收发控制——管理员可以设置哪些内网 PC 能够收发邮件，被禁止的计算机将不能收发邮件。敏感字邮件审计记录——管理员可对邮件进行敏感词设置，对邮件内容含有敏感字的邮件进行审计，记录邮件主题、收发地址、抄送地址、IP、等信息。

■ **应用系统采集**

支持对终端系统的主机破坏行为，用户权限操作，应用程序使用进行日志的采集与上报。

■ **打印行为审计**

管理员可设置审计终端打印行为，记录终端打印路径、打印时间，企业可做到对全网终端打印行为的审计查询。

■ **合规基线检测**

桌面管理系统从驱动层接管操作系统，终端如违反了控制中心配置的合规基线项，控制中心会根据自动检测的结果对终端的不合规项进行强制矫正，做到终端合规基线统一化。

■ **分组策略配置**

桌面管理系统能根据用户需求单独对分组或个人进行策略配置，满足不同部门的安全管控要求。

终端安全管理系统 EDR 主要功能:

■ **终端信息采集**

终端联动响应主机信息Host name、操作系统类型、网卡名称、network address（ipv4/ipv6 地址）、主机 MAC 地址、CPU 利用率、网络利用率、磁盘空间、端口、已登录用户名。

■ **进程信息**

进程名称、进程 ID、父进程 ID、进程文件路径、进程文件名称、文件 MD5、CPU 利用率、内存利用率、进程状态、开始时间、终端类型、启动进程的命令字、进程 owner 的信息（用户名、终端信息、登录时间、到期时间）。

■ **网络连接**

连接时间、进程 ID、进程名称、进程对应的文件名称、进程对应文件的 MD5、协议、本地 IP 地址、本地端口、远程 IP 地址、远程端口、发送/接收字节数、网络连接协议（TCP、UDP、HTTP、HTTPS）。

■ **终端行为**

所有系统进程和所有应用进程行为进程信息：进程 ID、进程名称、父进程 ID、进程用户名、进程路径、进程对应的文件名称（含路径）、启动进程的命令字、进程状态、进程开始时间、进程结束时间。

■ **进程使用的模块信息**

进程内加载的模块名称（含路径）及其文件 MD5、文件大小、模块文件的最后修改时间、模块操作时间。

■ **进程所含的子进程信息**

子进程的进程 ID、子进程的进程名称、父进程 ID、子进程的用户名、子进程对应的文件名称（含路径）、启动子进程的命令字、子进程的开始时间、子进程的结束时间。

进程行为：包括进程创建、修改或终止其他进程的行为，注入远程线程的行为。例如：时间、启动注入的进程/发起进程、目标进程、操作行为、成功与否。

■ **文件行为**

包括创建、打开、修改、删除、关闭文件的行为。例如：时间、文件路径、操作行为、文件大小、文件 MD5、成功与否。

■ **注册表行为**

包括创建、读取、修改、删除注册表的行为。例如：时间、注册表项名称、注册表键名称、操作行为、前值、终值、成功与否。

■ **网络行为**

包括时间、源 IP 及端口、目的 IP 及端口、端口协议、访问的 URL/域名、成功与否，其中，端口协议支持 TCP、UDP、HTTP、HTTPS。

■ **DNS行为信息**

包括时间、域名、DNS 解析结果。

文件检测功能:

■ **响应终端可疑文件提取**

发现可疑文件或行为后，管理中心下发文件提取策略，终端检索可疑文件并将文件及其依赖的非系统的动态库提交管理中心。

■ **可疑终端关联文件检测**

管理中心进行大数据关联分析时，对可疑终端下发的文件 MD5 检测策略； 终端响应该策略，检索信息并反馈检测结果，包括：检测时间、检测的终端 IP、匹配的进程名、进程 ID、父进程 ID、进程文件路径、启动进程的命令字、进程文件 MD5、检测文件对象 MD5、检测文件对象本地路径。

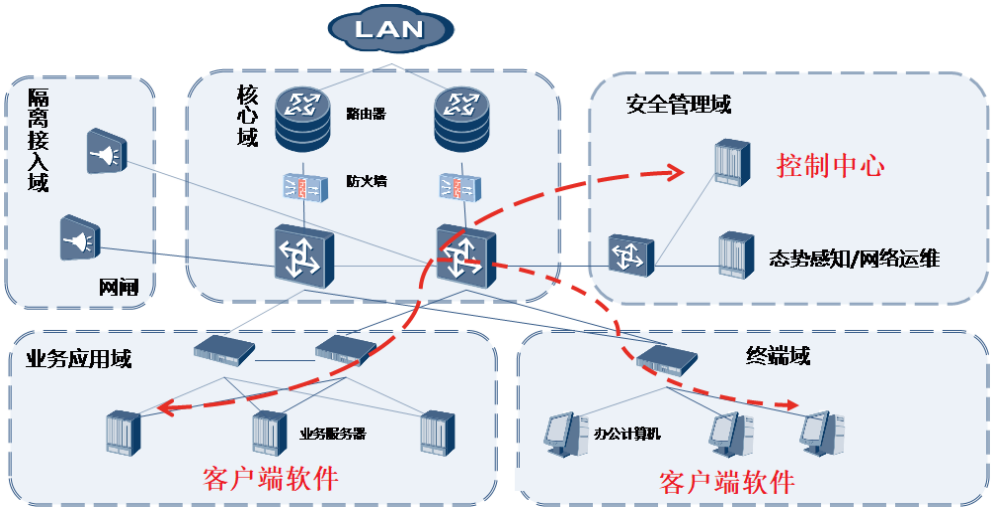
■ **终端联动规则执行**

终端响应管理中心下发的策略，执行配置动作，并反馈结果，包括：执行时间、执行动作的终端 IP、联动响应规则、响应对象名称、执行的动作、执行结果。

部署方式

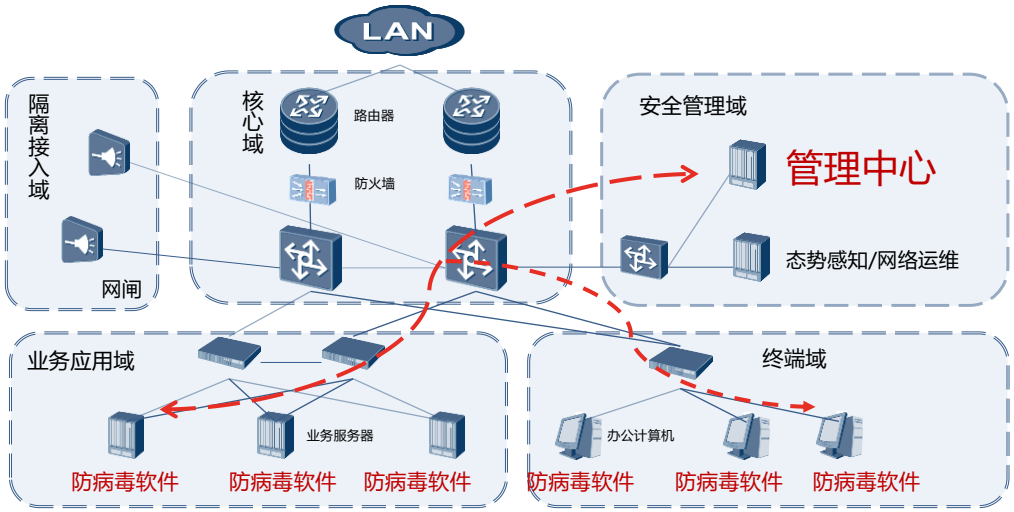
企业网络中，除边界网络安全外，终端安全也是整体安全的关键组成部分。网络设备终端主要涵盖业务服务器及办公计算机。通过控制中心可以对安装DPtech XDR 终端检测与响应系统的终端设备实现统一杀毒、特征库升级、安全策略下发、系统修复、补丁更新和联动响应等功能。

标准部署：



在终端设备安装控制中心后，客户端可以自动连接到控制中心。管理员可直接通过控制中心主机或者任意一台客户端上通过 WEB 浏览器进行登录管理。

云部署：



当企业使用私有云场景时，终端以虚拟机形式出现，XDR终端检测与响应系统在部署好控制台后，可将客户端批量下发给虚拟机与服务器，以对虚拟机终端和服务器进行统一安全管理，保证业务稳定运行。

杭州迪普科技股份有限公司
地址：浙江省杭州市滨江区月明路 595 号迪普科技
邮编：310051
服务热线：400-6100-598