ESET Endpoint 企业版产品更多功能详解

ESET Endpoint Antivirus（EEA）		
功能模块	**Endpoint 安全产品从企业经营角度分析所具备的优势**	**Endpoint 安全产品从 IT 管理角度分析所具备的优势**
防病毒/反垃圾邮件模块	确保企业数据安全，保护终端设备免受恶意软件感染，适用于跨平台网络防护。采用云端文件声誉数据库技术，大大提高扫描速度，将误报值保持在绝对最低水平，从而有效保护企业数据安全以免外泄。	终端设备免受恶意软件侵袭，是企业高效、稳定工作的前提。企业终端设备部署了 ESET 安全软件后，即能得到全天候防护，时刻保证数据的安全。向云端上传的信息只限于可执行文件和存档文件，不涉及保密信息。上传的信息也无法追溯到个人。ESET 云扫描技术不但提高了扫描速度和检测率，同时也将误报降至最低水平。
可移动存储设备的自动扫描功能	当插入 USB 盘、CD、DVD 和其他可移动存储设备时，实现恶意软件自动查杀，清除 autorun 一类的病毒。	自动查杀 USB 盘、CD、DVD 等移动媒介中的恶意软件，当可移动存储设备中作为病毒载体时，有效保护系统免受感染。
HIPS 主机入侵防御系统	HIPS 主机防御系统行为检测技术的运用，有效保证 ESET 安全产品免遭恶意篡改，从而确保企业终端设备的安全。关键系统注册表键值、进程、应用程序和文件都受到有效的保护，禁止非法访问和修改。	对整个系统和各个组件的行为，均能够通过自定义规则的方式阻止非法操作。自动生成详细的 HIPS 日志，便于违规记录的审核和汇报。软件内置了自身防御功能，保护 ESET 安全软件免遭恶意篡改，从而为系统持续发挥最大的防护效力。
客户端反垃圾邮件模块	自动过滤陌生垃圾邮件，提高员工工作效率，降低钓鱼攻击带来的风险。可根据用户类别设定过滤级别，以符合您企业的电子邮件通讯策略。	提供强大的发垃圾邮件模块，含黑白名单功能和自我学习模式，可以根据不同客户端和工作组区分设定。原生支援 Microsoft Outlook 邮件客户端，无需更多操作，即能针对各类通讯协议（POP3、IMAP、MAPI、HTTP）提供强力防护。
系统资源占用少	使企业计算机长期稳定运行，延长硬件使用寿命。Endpoint 安全产品不像其他庞大臃肿的防毒软件，绝不会拖慢系统运行速度，从而提升企业整体	Endpoint 解决方案有别于其他庞大臃肿的防毒软件，占用系统资源少，实现企业计算机产出的最大化。可以在较老的计算机系统上部署而不必升

	工作效率。	级硬件,从而延长硬件的使用寿命。在笔记本电脑上使用,更能通过节电模式节省电量,使外出工作时的续航时间更久。
跨平台防护	在分别运行 Windows、Mac 和 Linux 系统的计算机之间传送文件或电子邮件附件变得安全、省心,任何针对这些操作系统的恶意软件都能够实现自动查杀。	ESET 安全解决方案实现了跨平台查杀恶意软件,Windows 版防毒软件同时能够查杀针对 Mac 系统的病毒,反之亦同,从而提供更强的防护性能。
ESET 系统救援功能	在其他方式都不能奏效时,可以通过系统救援 CD 或 USB 盘启动终端计算机进行病毒查杀,帮助恢复系统数据。	使用 CD 和 USB 盘启动染毒系统,清除深层恶意软件,增加恢复数据的几率。
设备控制	避免企业数据在未经授权的前提下,非法复制到 USB 盘、CD、DVD 及其他存储设备上。设备控制策略具有灵活、适宜性强的特点,可以针对个人用户和工作组设定不同的参数,例如序列号、厂商代码、型号等,方便数据访问的分类控制。	通过一系列预设参数,例如序列号、生产厂商或型号等,针对不同存储媒介和设备实现规则和策略的集中化管理。针对不同个人用户和工作组设定只读、读写或阻止访问权限。系统自动生成详细的访问和扫描日志,简化策略的强制实施和跟踪管理。
受信网络检测	当企业出差人员离开受信网络,在咖啡厅、机场或酒店接入公共热点时,有效保护企业机密数据避免外泄。阻止一切监听企业通讯的不法行为。	接入 Wi-Fi 等陌生网络时应用更严格的防护策略。默认设定受信网络后,其余网络连接均应用严格的通讯模式。在外勤人员使用咖啡厅、机场或酒店提供的公共热点时,有效保护用户和笔记本电脑数据避免非法窃取。
支持 Microsoft NAP	按照客户端计算机身份,配合公司管理策略,控制客户端对网络资源的访问。通过 Microsoft 网络访问防护(NAP)插件,与公司管理策略实现完美集成。	帮助控制符合性和实现网络监控(准备性/状态)。SHA 插件收集客户端信息,并通过 NAP 架构与服务器端进行通讯。可按照以下项目设定客户端的符合条件:病毒库时间、防毒产品版本、防护状态、防毒功能适用性和防火墙状态。通过强制数据库更新的方式,令终端计算机符合运行条件。
更新回溯	只需点击几次按钮,即可返回应用之前的病毒库和模块更新版本,以便解决不兼容或系	解决不兼容或其他系统异常的情形,只需点击几次按钮,返回到已知良好状态的之前

	统异常的情形。	病毒库和模块更新版本即可。能够根据需要冻结更新,选择临时回溯至之前版本或直到人工调整设定为止。
延时更新	保障公司在线系统每周 7 天每天 24 小时稳定运行，避免由于防毒软件更新或其他事件,造成重要系统暂时无法使用,从而影响公司正常工作的情形。	确保更新顺利,侧重公司正常工作的延续性:先在非关键系统应用防毒软件更新,之后再在关键系统上应用,可选择同时清除更新缓存。
ESET Remote Administrator Console/Server		
功能模块	**Endpoint 安全产品从企业经营角度分析所具备的优势**	**Endpoint 安全产品从 IT 管理角度分析所具备的优势**
集中管理功能	运用 ESET 远程管理工具，实现对原有、当前和未来 ESET 安全软件的统一集中化管理，从而有效控制 IT 预算。通过单一中央控制台,轻松实现所有终端设备、服务器、智能手机以及虚拟机的集中管理,适用于运行 Windows、Mac 或 Linux 等多系统的混合网络环境。	ESET 远程管理工具允许用户通过单一中央控制台,集中管理 Windows、Mac 和 Linux 交互平台上所有的 ESET 安全软件。本解决方案支援 IPv6 架构,甚至智能手机和虚拟机也能实现集中化管理。
角色管理功能	角色管理功能能够根据不同个人和工作组的职责，为 IT 管理团队划分相应的权限。系统生成详细的审核日志,方便权限的跟踪与管理。	在不同个人和工作组之间,为管理员分配各自的权限。详细的审核日志便于角色的跟踪管理,内置的密码检查机制保证管理员口令强度和口令的安全性。
动态客户端工作组	轻松调整适用于不同员工组别的安全规则。动态工作组可以基于身份识别条件和终端设备安全事件所采取的应对措施实时进行自动调整。	根据操作系统、客户端名称掩码、IP 掩码、最新检测到的病毒等参数,创建不同的用户组。设定各用户组的专属策略,并在参数发生变化时自动调整到相应的用户组中。
事件通知/报告生成	设定通知优先级、重要通知类别、通知内容详细度以及通知时间间隔，节约 IT 团队管理时间,使其得到关键信息并做出及时应对的同时,不会造成网络负荷。	有助于快速查找潜在的问题,使需要关注的事件一目了然,令网络管理更加简单和轻松。设定通知的优先级和报告时间,可以选择立即发送或按照预设时间批量汇报。创建通知规则、通知详尽度并可以设定通过电子邮件、系统日志、SNMP 告警方式或文本文档转

		发。
远程管理功能	IT 管理人员只需要简单点击几次鼠标,即能从一个地点实现所有终端设备上 ESET 安全软件的远程安装。	通过一次性集中安装方式,实现ESET Endpoint 安全软件和任何 msi 安装程序的远程安装。ESET 远程管理工具可以向 Windows 平台推送安装 ESET Endpoint 安全软件，新一代 Endpoint 安全产品更能实现Mac 和Linux 系统的远程集中安装。
导入和导出策略	通过一次性设定配置信息并导出设定档,集中应用于终端设备和用户组的方式,有效节约管理人员工作时间,避免忙中出错。	一次性设定配置信息、导出设定档并集中应用于目标终端设备和工作组上，以此节约 IT 管理人员工作时间并降低出错的几率。
远程模块切换功能	通过远程启用和禁用防护模块,减少系统维护时的停用时间。	通过远程启用和禁用已安装的防护模块,简化系统维护和调试工作。可以设定恢复先前设置的等待时间,以免系统长时间失去防护。除了反隐藏之外的所有模块,均在终端设备重启后自动启用。
实时网络状态表（WEB 页面形式）	显示服务器负载和安全状况的实时信息,帮助总览整个网络的安全状况。通过网页状态表,可以从企业网络之外的任意地点访问并掌握企业网络的关键信息。	通过中央控制台或任意网络节点访问基于网页的状态表,令企业网络整体信息一目了然。可以通过 ESET 远程管理工具的报告页面,设定状态表中显示的信息。能够通过数据流实时传送方式,监管网络安全状况和服务器负荷统计信息。
支持多种日志格式	利用数据采集功能,使得安全事件之间的关系分析变得异常轻松和快捷。所采集的数据,可以使用第三方安全信息和事件管理工具(SIEM)查看。	采用兼容数据格式,方便数据分析,令数据处理和采集变得异常简单。ESET 软件支持多种日志格式,可以通过第三方安全信息和事件管理工具（SIEM）查看。
设备控制报告	监控企业中可移动存储媒介和设备的使用情况,将所有重要信息集中在一处保存。	对可移动存储媒介和设备创建详细的使用日志,集中报告追踪记录,使报告变得异常简单。报告内容包括时间戳、用户名、计算机名、工作组名称、设备类别、事件详细信息和触发行为的记录。
支持 RSA enVision 远程信令	支持 RSA enVision 远程信令警报工具，与这一常见的第三方	

警报工具	SIEM 工具实现轻松集成。	
ESET SysInspector 系统分析工具	为 IT 管理员提供了找出潜在安全风险的必要工具,以便预先采取防范措施。	识别终端系统中运行的所有进程、安装的软件以及硬件的配置信息。通过对照终端系统的前后两次镜像,帮助查找潜在的安全风险。
随机任务执行	避免由于虚拟终端计算机上的杀毒风暴或服务器响应延迟，导致系统运行变慢的情形。此项功能保障同时排程的安全任务不会导致网络减慢或数据流受到负面影响。	设定执行任务的随机时间偏移量,尽量减少虚拟终端上的杀毒风暴,以及在同时进行系统扫描时网络驱动器上的资源冲突,以避免终端用户感受性能变慢的情形。
本地更新服务器	将防毒软件更新所占用的流量降低到最小程度,从而为与工作相关的网络服务预留更多的带宽资源。	将 ESET 远程管理员工具用做您公司中终端计算机更新的镜像服务器,最大程度减少互联网带宽的占用。能够为移动办公群体,指定第二更新设定档,以便当终端设备无法访问公司内部镜像时，直接从 ESET 服务器获取更新。支持 HTTPS 通讯协议。
更快访问数据库	数据库的迅速响应意味着加快终端计算机上报告和数据汇总速度，从而全面提高 IT 管理收益。	优化数据库性能,能够更快地收集终端计算机数据和生成报告,从而提高您工作的产出率。
数据库清理	通过设定,可选择仅保存关键性和近期安全日志,从而使数据库整洁和一目了然,避免服务器运行减慢的情形。	保持数据库工作正常、相应迅速并控制数据库大小。