ManageEngine 卓豪

Endpoint DLP Plus

ManageEngine 卓豪

卓豪（集团）旗下的企业IT运维管理软件提供商

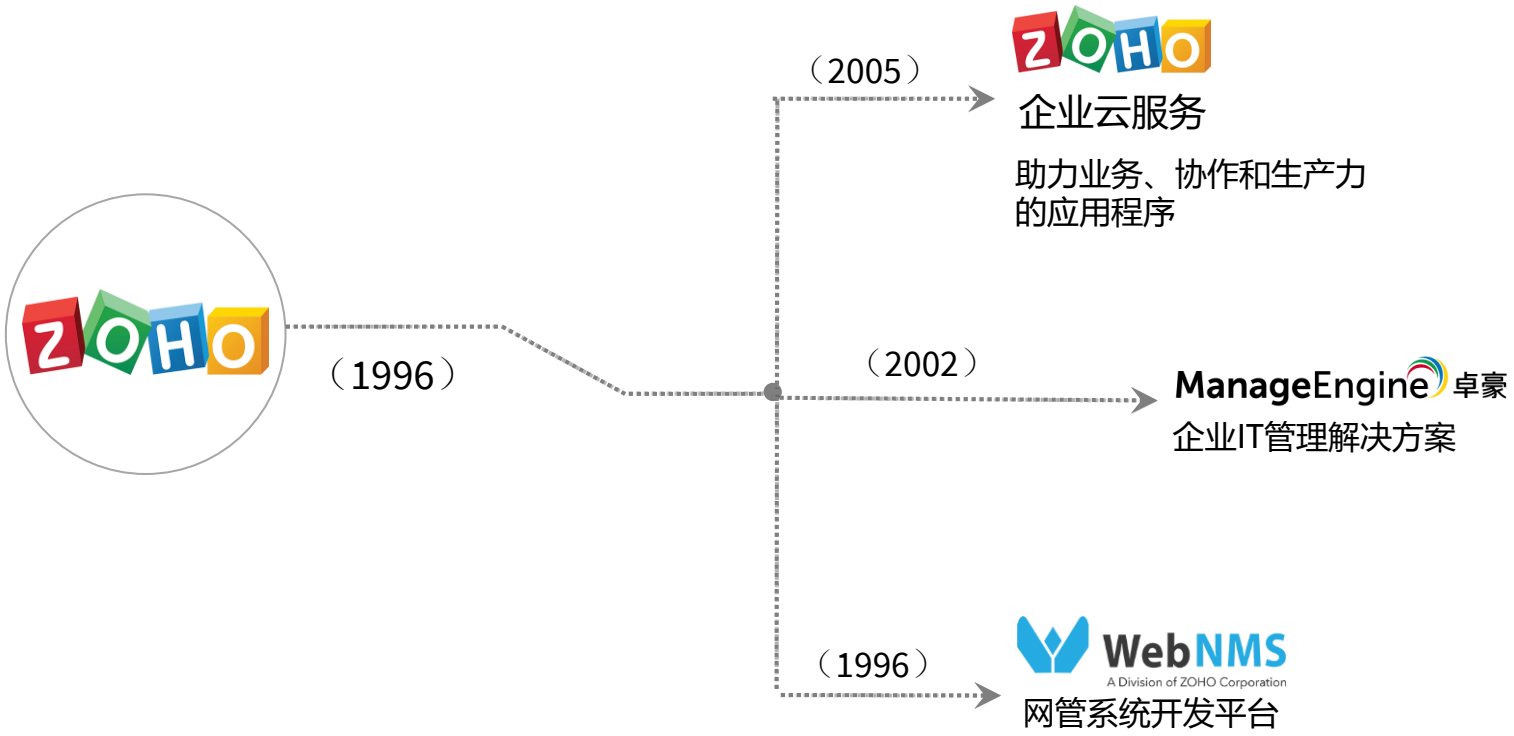
创建于1996年，原名为Advent Net（艾德威特）

值得信赖的国际提供商和合作伙伴

分布全球的分公司

全球百万企业用户的选择

ManageEngine: 卓豪（集团）旗下的企业IT运维管理软件提供商



ManageEngine卓豪解决方案

活动目录管理

活动目录
Exchange服务器
自助服务门户
恢复与备份

IT服务管理 (ITSM)

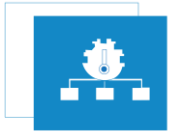
服务台
资产生命周期
CMDB 和 ITIL
客户支持

终端管理

桌面管理
移动设备管理
操作系统部署
补丁管理
浏览器管理

云

应用程序性能
服务台软件
活动目录恢复与备份
移动设备管理
补丁管理
日志管理



IT 运维管理 (ITOM)

网络性能
应用程序性能
终端用户体验
网络配置与变更
融合的基础设施
存储基础设施
带宽和流量

IT 安全

日志管理
防火墙分析
漏洞分析
应用程序控制
特权密码管理
网络异常检测

200万个用户

《财富》500强企业中

每5家就有3家

是ManageEngine卓豪的客户

ManageEngine

Endpoint DLP Plus

一个集成的终端数据丢失防护软件，
专注于保护敏感数据，降低内部风险。

为什么需要数据丢失防护解决方案?

- 数据是组织中极具价值的无形资产，也因此成为了网络安全攻击的首要目标。
- 如果不了解数据的存储和使用情况，可能会导致数据意外丢失或增加内部风险。
- 数据泄漏可能会影响企业信誉，造成声誉和财务损失，而补救工作又耗时费力。

为什么需要一个终端 DLP 解决方案?

大多数终端位于企业网络内部，因为其动态性，面临的风险最高。原因如下：

- 在组织内部，终端通常是员工的首选工作方式，但由于其易于访问而成为了内部攻击的主要途径，员工安全意识薄弱或安全措施防护不当将会导致意外数据泄漏。

- 终端存储着有价值的数据，但往往被企业忽略，而更倾向于保护专业的数据库（即文件服务器），从而增加了终端数据泄露的风险。

高效终端数据丢失防护面临的挑战

- 针对终端上敏感数据的网络安全攻击呈指数级增长，很难对这些攻击进行持续防御。
- 全面管理数据安全信息和每台计算机的用户访问权限，需要耗费大量的时间成本和人力成本。
- 缺少一个综合的终端安全解决方案，能同时满足所有组织的数据丢失防护需求。
- 尤其在终端敏感内容保护方面，用户安全意识薄弱。

ManageEngine卓豪Endpoint DLP Plus是什么?

ManageEngine卓豪Endpoint DLP Plus是一个专业的网络安全解决方案，旨在为用户提供高效的终端数据保护。主动发现内外部风险，阻止敏感数据泄漏。Endpoint DLP Plus提供了丰富而强大的功能，使IT管理员能够即时发现结构化和非结构化形式的敏感数据并对其进行分类，还可以定义组织边界，防止有意或无意的数据泄漏。

功能一览

- 数据发现
- 数据分类
- 数据容器化
- 电子邮件安全
- 云保护
- 设备控制
- 剪贴板保护
- 误报修复
- 工作超控
- 报表

终端数据发现

敏感数据分散存储于大量终端，难以追踪，这导致敏感数据非常容易被篡改或窃取。

有了Endpoint DLP Plus，就可以快速定位存储中、传输中和使用中的数据，包括新生成和已存档的敏感数据。

优点：

- 降低因数据分散而造成的安全保护遗漏。
- 实时检测新生成和已存档的敏感数据，全面掌握所有有价值的数字资产。

使用模板进行数据分类

- 终端包含了大量的非结构化信息。为了助力数据驱动的决策，Endpoint DLP Plus允许IT管理员创建规则，自动检测并分类特定类型的敏感文档。
- 大量的预定义模板对应了常见的敏感文档类型。Endpoint DLP Plus会在终端搜索匹配模板属性的文档，然后将找到的文档合并并标记。
- 为了找到组织特定格式的敏感文件，Endpoint DLP Plus为管理员提供了高级机制，如关键词搜索、指纹识别和正则表达式（RegEx）。

敏感数据容器化

简化数据流有利于改善安全态势，为此，管理员可以利用数据容器化功能：

- 将特定的工作友好和安全的应用程序指定为受信任的应用。
- 将敏感数据限制在这些受信任的应用中，确保数据只在授权的空间中传输。
- 所有来自企业应用的数据都可以自动标记为敏感数据。
- 审计并阻止任何试图从受信任的应用向未经授权的应用传输数据的行为。

强大的云保护

随着远程办公的普及，云服务已经成为一种流行的数据存储传输方式。而为了防止云端数据泄漏，Endpoint DLP Plus为您提供了以下功能：

- 只允许员工使用经过验证的浏览器。
- 禁止将工作内容上传到未经验证的Web域。
- 阻止向第三方云存储和应用程序传输敏感内容。

电子邮件安全

很多员工都喜欢使用电子邮件来实现快速协作，虽然电子邮件很方便，但是如果控制不当就可能带来风险。使用Endpoint DLP Plus，管理员可以：

- 确保敏感内容不会通过电子邮件非法泄漏。
- 通过将受信任的电子邮件域列入白名单，禁止通过个人电子邮件发送工作信息，实现授权信息交换。
- 将经过验证的Outlook电子邮件域添加到受信任的列表中。

设备控制和剪贴板管理

- 用户可以尝试利用硬件工具（如外围设备）来传输数据。Endpoint DLP Plus可控制USB驱动和其他设备的使用。
- 允许特定打印机处理敏感文件并在文件上添加水印。
- 为防止敏感文件的图像被拍摄或传输，对用于屏幕捕获的剪贴板工具进行限制。

误报修复和工作超控

- 从开始使用到长期实施，轻松满足不断变化的用户需求。
- 用户可以通过自助服务门户反馈错误，IT管理员在审核原因后，可以根据需要轻松修改相关策略。
- 允许受信任的用户在说明传输敏感数据的合理原因后超控已有策略。

丰富的报表和深入的分析

- Endpoint DLP Plus仪表板提供了多种信息图表，网络健康状况一目了然。
- 海量的数据安全分析，帮助管理员及时了解已应用策略的效果，迅速掌握数据保护框架。
- 可操作性的见解，支持管理员决策，强化终端DLP策略。

版本

免费版	专业版
管理多达25台计算机	适用于局域网和广域网计算机
• 适合中小型企业 • 全功能 • 可管理25台计算机	• 发现并分类敏感数据 • 利用预定义和自定义模板 • 将数据容器化到受信任的应用中 • 保证电子邮件安全 • 监视云上传 • 限制剪贴板操作 • 控制外围设备 • 误报修复 • 授权工作超控 • 降低内部风险 • 访问智能审计报表

Endpoint DLP Plus能为您的组织带来哪些好处?

- 简化设置，集中部署策略
- 对数据传输的主要途径进行限制
- 有效检测并降低内部风险
- 全面掌握组织数据，支持数据驱动决策
- 减少时间成本，节约数字空间等资源
- 保证数据安全，获得显著的长期投资回报

文档资源

- 获取报价
- 系统要求
- 架构
- 用户手册
- 常见问答
- 免费试用

了解更多

https://www.manageengine.cn/endpoint-dlp/