



挑战

黑客发动网络安全攻击的首要目标是敏感数据。因此，制定有效的数据防御策略是保证业务正常开展的关键。然而，大量未经过滤的新信息使得我们很难辨别哪些信息是重要的、需要保护的。如果不对关键信息进行追踪，就可能导致滥用或未经授权的数据泄露，从而给组织带来重大损失。要解决这个问题，您需要一个高效的数据泄露防护工具，用于敏感数据检测和保护。

解决方案

ManageEngine卓豪的Endpoint DLP Plus（终端数据丢失防护）是一款集成软件，可以对网络中的数据移动进行自动定位、标记和控制，识别并保护终端中的敏感数据，减少意外数据泄漏，并抵御内外部网络攻击。

利用Endpoint DLP Plus预防内部风险

Endpoint DLP Plus的工作机制可以有效控制内部风险。首先，它会扫描所有敏感的数字资产，发现组织的机密数据，并按来源和特性分类。然后，帮助IT管理员创建规则，作为虚拟边界，防止敏感数据由于疏忽被泄露，防止被恶意攻击者劫持。最后，还提供了详细的报表，标记可疑的用户行为，并主动阻止未经授权的文件操作。

发现数据

- ◆ 持续追踪含有敏感信息的存储文件和新增文件，实时掌控海量数据。
- ◆ 部署策略，检测所有结构化和非结构化的敏感项。
- ◆ 根据部门、职能、项目或角色创建目标计算机组，提高搜索效率，找到特定类型的敏感文件。
- ◆ 接收实时指标，紧跟不断发展的数据趋势，适应安全态势的变化。

使用预定义模板进行数据分类

- ◆ 根据相似的属性对敏感数据进行分组。
- ◆ 利用大量预定义模板，对常见形式的敏感内容(如个人身份信息PII)进行分类。
- ◆ 使用特定于国家的预定义模板对各种类型的PII进行分类，例如各个国家的财务和医疗信息。

使用自定义模板进行数据分类

- ◆ 创建自定义模板，准确找出预定义模板没有涵盖的复杂多样的敏感项。
- ◆ 利用指纹技术，找到公司特有的或经常使用格式的敏感文件。
- ◆ 利用正则表达式（**RegEx**），识别具有特定长度或字符组合的字符串的文件。
- ◆ 启动关键词搜索，找到包含独特文本的内容。

云上传保护

- ◆ 加强网络保护，只允许使用选定的浏览器来处理敏感数据。
- ◆ 禁止将含有敏感项的文件导出到各种云存储软件。
- ◆ 禁止通过第三方文件共享应用程序传输敏感内容。

设备控制

- ◆ 将授权的**USB**设备和外围设备标记为受信任的设备，同时默认阻止所有其他设备。
- ◆ 阻止机密信息下载，确保打印机安全。
- ◆ 允许在可以打印的敏感文件上添加水印。

误报处理

- ◆ 允许受信任的用户超控限制性策略。
- ◆ 允许员工通过自助服务门户申请超控权限。
- ◆ 直接从控制台查看申请超控权限的原因。
- ◆ 必要时调整策略以满足用户需求。

服务器硬件要求

被管设备数量	处理器	内存	硬盘空间
1 - 250	英特尔酷睿 i3 (2 核/4 线程) 2.0 GHz 3MB缓存	2GB	5GB
251 - 500	英特尔酷睿 i3 (2 核/4 线程) 2.4 GHz 3MB缓存	4GB	10GB
501 - 1000	英特尔酷睿 i3 (2 核/4 线程) 2.9 GHz 3MB缓存	4GB	20GB
1001 - 3000	英特尔酷睿 i5 (4 核/4 线程) 2.3 GHz 6MB缓存	8GB	30GB
3001 - 5000	英特尔酷睿 i7 (6 核/12 线程) 3.2 GHz 12MB缓存	8GB	40GB
5001 - 10000	Intel Xeon E5 (8 核/16 线程) 2.6 GHz 20MB缓存	16GB	60GB
10001 - 20000	Intel Xeon E5 (8 核/16 线程) 2.6 GHZ 40MB缓存	32GB	120GB

如果被管计算机数量在1000台以上，建议在Windows服务器版中安装Endpoint DLA Plus。

如果被管计算机数量在3000台以上，建议使用一个微软SQL Server数据库。

软件要求

服务器支持的操作系统
Windows 7/ 8/ 8.1/ 10/ Servers 2003/2003 R2/2008/2008 R2/2012/2012 R2/2016/2019/20

代理支持的操作系统

Windows OS*	Windows Server OS*
Windows 10/11	Windows Server 2016/19/20
Windows 8.1	Windows Server 2012 R2
Windows 8	Windows Server 2012
Windows 7	Windows Server 2008 R2

数据容器化

- ◆ 将受信任或高度安全的应用程序标记为 "企业应用"，以确保敏感信息只在这些选定的软件应用程序中处理。
- ◆ 确保所有来自企业应用的数据默认都被自动标记为敏感。
- ◆ 限制数据从企业应用向非企业应用的传输，以防止未经验证和易受攻击的软件访问机密内容。

剪贴板工具管理

- ◆ 执行剪贴板监视，防止敏感内容被截屏。
- ◆ 禁止用户将工作内容粘贴到非工作空间和应用。

电子邮件安全

- ◆ 选择用于传输敏感内容的受信任的组织域。
- ◆ 授权发送信息到合法的**Outlook**邮箱。
- ◆ 阻止通过个人邮件上传工作内容。

报表和告警

- ◆ 简洁清晰的仪表板界面设计，快速了解网络健康状况。
- ◆ 进行诊断分析，评估每个终端的安全状况。
- ◆ 接收传输数据尝试被阻止的告警。