ManageEngine 卓豪

ManageEngine DataSecurity Plus

运维文档

目录

产品介绍

概述

DataSecurity Plus 是数据可见性和安全性的一站式解决方案。本文档简要概述了 DataSecurity Plus 的功能、优点等。

DataSecurity Plus 是什么?

DataSecurity Plus 是一个实时文件服务器审计、数据风险评估和数据泄漏预防解决方案。他审计文件变更及违规策略，识别不符合合规性问题，告警至管理员，并响应事件以减轻对数据存储的潜在损害。

为什么喜欢它

ManageEngine DataSecurity Plus 让您更易了解:

- **获得文件访问的可见性** 变更，以及共享和 NTFS 的权限。
- **监视文件完整性** 并提醒管理员异常活动。
- **检测敏感数据** 从内容和上下文分析。
- **提高存储效率** 简化垃圾文件管理.
- **防止数据泄漏** 通过 USB 设备和工作站。

系统要求

以下是使 DataSecurity Plus 平稳运行所需的硬件和软件规格。

硬件	最低要求	推荐配置
处理器	2.4GHz	3GHZ
核心	4	6 及更高
内存	8GB	16GB 及更高
磁盘空间	50GB	100GB*

*可能会有所不同，具体取决于为审核和数据风险评估配置的服务器数量。

软件需求

支持的浏览器： Internet Explorer 9 及更高版本，Mozilla Firefox，Google Chrome（推荐）和 Microsoft Edge。

Windows 支持的版本： Windows Vista，7、8、8.1 和 10; Windows Server 2008、2008 R2、2012、2012 R2 和 2016

首选屏幕分辨率：1280 x 800 像素或更高

支持平台： Windows File Server 2003 及以上

最佳实践: 我们建议您有一台专用的计算机来安装 DataSecurity Plus。

权限指南

授予 Domain Admin 凭据后，DataSecurity Plus 会立即开始在许可的模块中进行检测，审核，分析和响应活动。 如果您不想提供 Domain Admin 凭据，请按照本指南中的步骤设置所需权限最少的服务帐户。

1. 每个模块所需的特权

以下步骤列出了 DataSecurity Plus 的每个版本和每个模块所需的特权。 在提供每个模块的特定权限之前，应首先授予这些权限。

- **向用户授予对产品安装文件夹的完全控制权。**

  DataSecurity Plus 需要完全控制产品安装文件夹才能写入数据库。

  - 使用 Domain Admin 特权登录到安装了 DataSecurity Plus 的计算机。
  - 找到产品安装文件夹； 右键点击**属性 > 安全 > 编辑;** 添加 **DataSecurity Plus 用户 r**，并提供完全控制权。

- **授予用户对 DataSecurity Plus 的存档文件夹的完全控制权。**

DataSecurity Plus 要求**完全控制** 在存档文件夹上，用于存储和检索数据库中的存档数据。

要查找存档文件夹的位置，请打开 **DataSecurity Plus > 文件审核 > 配置 > 归档配置**

使用 Domain Admin 特权登录到目标计算机。 找到文件夹；右击 **属性 > 安全 > 编辑；** 添加 **DataSecurity Plus 用户，** 并提供完全控制权限。

- **授予用户对所有 DataSecurity Plus 的计划报表文件夹的完全控制权。**

  DataSecurity Plus 要求**完全控制**在“计划报表”文件夹中，以将计划报表保存在指定位置。

  - 要查找“计划报表”文件夹的位置，请打开 **DataSecurity Plus > 文件审核 > 配置 > 计划报表 > 修改计划报表。执行后**您可以在下面看到位置。
  - 使用 Domain Admin 特权登录到目标计算机。 找到文件夹；右击，跳转到**属性 > 安全 > 编辑；** 添加 **DataSecurity Plus 用户，** 并提供完全控制权限。

  对所有目标文件夹重复计划报表的步骤。

- **向用户授予对所有 DataSecurity Plus 的告警脚本文件夹的读取和执行权限**

  产品要求 **读取 & 执行** 触发告警后，每个告警脚本文件夹上的权限即可执行脚本

  - 要查找告警脚本文件夹的位置，**打开 DataSecurity Plus > 文件审核 > 告警 > 修改告警配置文件。** 您可以在动作下面看到位置 。

- 使用 Domain Admin 特权登录到目标计算机。 找到该文件夹，右键点击，转到 **属性 > 安全 > 编辑；** 添加 **DataSecurity Plus 用户，** 并提供读取 & 执行权限。

- **向用户授予对配置了“移动/删除”响应的文件的“修改”权限**
    - 使用域管理员权限登录到**目标计算机**，找到为其配置了“移动/删除”响应的文件。
    - 右击 **文件**，跳转到 **属性 > 安全 > 编辑，** 添加 **DataSecurity Plu 用户，** 并提供 **修改** 权限。
    - 对配置了指定响应的所有文件重复这些步骤。

2.文件审核模块所需的特权

以下步骤详细说明了分配 DataSecurity Plus 的“文件审核”模块所需的最低特权的过程。

- **使用户成为高级用户组的成员**
    - 使用“域管理员”权限登录到域控制器。 打开组策略管理控制台，右键点击 **DataSecurity Plus 权限 GPO > 编辑**
    - 在组策略管理编辑器中，选择 **电脑配置 > 首选项 > 控制面板设置。** 右击 **本地用户和组 > 添加本地组。**
    - 在“新建本地组属性”向导中，选择 **根据操作进行更新。** 选择 **用户组** 在“组名”下，添加 DataSecurity Plus 用户。

3. 数据风险评估模块所需的特权

DataSecurity Plus 需要读取权限才能在文件共享中定位敏感数据（例如 PII，ePHI，信用卡详细信息等）。

在需要审计的文件夹授予用户 **读取权限**有两种方法：

- **使用户成为本地管理员组的成员。**
    - 使用 Domain Admin 特权登录到任何计算机。 打开 **MMC 控制台 > 文件 > 添加/删除管理单元。** 选择 **本地用户和组 > 添加 > 另一台电脑 > 添加目标计算机。**
    - 选择目标计算机，然后打开 **本地用户和组。** 选择 **组**右击 **管理员 > 属性 > 添加 DataSecurity Plus 用户。**
    - 对要审核的每个 Windows 文件服务器或群集重复上述步骤。
- **授予用户对共享的读取权限以及对每个审核共享的 NTFS 权限。**
    - 使用 Domain Admin 特权登录到任何计算机。 打开 **MMC 控制台 > 文件 > 添加/删除管理单元。** 选择 **共享文件夹 > 添加 > 另一台电脑 > 添加目标计算机。**
    - 选择目标计算机，选择**共享**右击 **属性 > 安全 > 编辑 > 添加 DataSecurity Plus 用户**然后提供 **读取权限**用于共享和 NTFS。
    - 对要审核的每个共享重复上述步骤。

4.终端 DLP 模块所需的特权

DataSecurity Plus 需要本地管理员凭据才能监视所有终端。 若要使用户成为本地管理员组的成员，请执行以下操作：

- 使用 Domain Admin 特权登录到任何计算机。 打开 **MMC 控制台 > 文件 > 添加/删除管理单元。** 选择 **本地用户和组 > 添加 > 另一台电脑 > 添加目标计算机。**
- 选择 **目标计算机**然后打开**本地用户和组**。选择**组**右击 **管理员 > 属性 > 添加 DataSecurity Plus 用户**
- 对要审核的每个终端重复上述步骤。

> **注意:**如果您要监视大量终端，那么让 DataSecurity Plus 用户成为每个终端的本地管理员是一项繁琐的任务。 为了简化过程，请向 DataSecurity Plus 用户提供 Domain Administrator 凭据。

5.文件分析模块所需的特权

本节详细介绍了 DataSecurity Plus 的“文件分析”模块所需的最低特权。

- **确保本地系统用户具有对所有受监控文件的读取权限。**

  默认情况下，**本地系统用户** 具有 **完全控制**权限。但是，对于文件分析，仅需要**读取权限**。如果您想更改默认权限，请确保 **本地系统用户** 具有 **读取权限** 在文件服务器中监控所有文件。

端口配置指南

以下是有关为 DataSecurity Plus 的正常运行需要打开的端口的详细信息。

- 产品端口

  下表列出了 DataSecurity Plus 使用的默认端口。这些可以在安装期间或安装后进行更改。

端口	协议	作用
8800	HTTP	产品 Web 服务器/代理通信
9163	HTTPS	产品 Web 服务器/代理通信

> **注意：**要在安装后更改默认端口，请打开 **DataSecurity Plus 控制台 >"管理"选项卡**在**常规设置下,**转到**连接 >更改端口**

- 系统端口

  下表列出了 DataSecurity Plus 使用的目标计算机上的端口。这些端口可以在 Windows 或第三方防火墙上打开。

端口	协议	目的地址	服务	作用	方向
135	TCP	受监视的计算机	RPC	代理通信	出站
137	TCP 和 UDP	受监视的计算机	RPC	代理通信	出站
138	UDP	受监视的计算机	RPC	代理通信	出站
139	TCP	受监视的计算机	RPC	代理通信	出站
445	TCP 和 UDP	受监视的计算机	RPC	用于列出文件共享	出站

389	TCP 和 UDP	域控制器	LDAP	用于将 AD 对象与 DataSecurity Plus 同步	出站
636	TCP	域控制器	通过 SSL 连接的 LDAP	用于将 AD 对象与 DataSecurity Plus 同步	出站
3268	TCP	域控制器	全局目录	用于将 AD 对象与 DataSecurity Plus 同步	出站
3269	TCP	域控制器	通过 SSL 连接的全局目录	用于将 AD 对象与 DataSecurity Plus 同步	出站
88	TCP	域控制器	Kerberos	用于将 AD 对象与 DataSecurity Plus 同步	出站
25	TCP	SMTP 服务器	SMTP	发送电子邮件	出站

465	TCP	SMTP 服务器	SSL	发送电子邮件	出站
587	TCP	SMTP 服务器	TLS	发送电子邮件	出站
49152 - 65535	TCP	受监控的计算机	RPC 随机分配的高端 TCP 口	用于代理通信和集群配置	出站

注意：

1. 远程注册表服务必须在安装了 DataSecurity Plus 代理的所有计算机上运行， 以监视代理状态
2. 如果您使用的是 Windows 防火墙，则可以通过启用以下列出的出站规则，在受监视的计算机上打开动态端口 49152 至 65535。
    - 远程事件日志管理（NP-In）
    - 远程事件日志管理（RPC）
    - 远程事件日志管理（RPC-EPMAP）

要启用上述规则：打开 **Windows 防火墙 > 高级设置 > 入站规则，**右键点击相应规则，然后选择**启用规则。**

安装 DataSecurity Plus

您可以将 DataSecurity Plus 安装到任意符合条件的机器。

点击如下链接下载 DataSecurity Plus。

Download

将 DataSecurity Plus 安装为应用

默认 DataSecurity Plus 会被安装为应用。下载完成后，请按照如下步骤进行安装：

1. 打开**安装向导**打开后，点击**下一步**。
2. 阅读**许可**，并点击**是**。
3. 选择安装位置，并点击**下一步**。默认 DataSecurity Plus 会被安装到 **C:\Program Files (x86)\ManageEngine\DataSecurity Plus**。

   故障排查：指定目录已存在安装文件。请指定一个新的安装位置。

   如果目标文件夹中存在来自先前 DataSecurity Plus 的文件，则会发生此错误。 您可以手动删除 DataSecurity Plus 文件夹，或在 **C:\Program Files (x86)\ManageEngine** 创建一个名为 "DataSecurity Plus <构建号>"的文件夹，并使其成为目标文件夹。
4. 输入您想要用于 DataSecurity Plus 的端口号，然后点击**下一步**。

> **注意:**DataSecurity Plus 使用的默认端口是 8800。

5. 注册以获得技术支持。 所有您需要做的就是输入 您的企业电子邮件 ID，然后点击**下一步**。

> **注意:** 防病毒扫描程序干扰数据库文件可能会影响数据库的正常运行。 确保 DataSecurity Plus 安装文件夹不受防病毒扫描程序的影响。

6. 点击**下一步**允许 DataSecurity Plus 开始将文件复制到安装目录。 此过程将需要几分钟。
7. 选择**启动 DataSecurity Plus** 然后点击**完成。**

将 DataSecurity Plus 安装为 Windows 服务（推荐）

要将 DataSecurity Plus 作为 Windows 服务运行：

1. 跳转到 **Windows > DataSecurity Plus。**
2. 点击**安装为服务**

或者，您也可以

1. 打开**命令提示符。**
2. 浏览到**<installation dir>\ManageEngine\DataSecurity Plus\bin 文件夹。**

3. 输入“*InstallNTService.bat*”.

> **最佳实践:** 安装 *DataSecurity Plus* 作为服务，以确保即使在用户注销后事件收集也不会停止。

卸载 ManageEngine DataSecurity Plus

要卸载 *DataSecurity Plus*：

1. 停止 *DataSecurity Plus*。跳转到 **Windows > DataSecurity Plus > 停止 DataSecurity Plus 服务器**。
2. 跳转到 **Windows > DataSecurity Plus > 卸载 DataSecurity Plus**。
3. 在**安装向导**中确认您想要卸载 *DataSecurity Plus*。
4. 在**反馈表**填写适当的详细信息。
5. 点击**确认**退出向导。

启动 DataSecurity Plus

有两种方法可以启动 *DataSecurity Plus*：

1. 作为服务（使用系统帐户）。
2. 作为应用程序（使用登录的用户帐户）。

启动 DataSecurity Plus 为服务

1. 将 DataSecurity Plus 安装为服务。
2. 跳转到 **Windows > 控制面板 > 系统和安全 > 管理工具 > 服务 > ManageEngine DataSecurity Plus > 起送服务。**

注意: 要使用具有以下功能的其他帐户将 DataSecurity Plus 作为服务运行：所需的最低特权，跳转到 **Windows > 服务** 右击 **ManageEngine DataSecurity Plus**。选择 **属性 > 登录** 并提供您要用于将 DataSecurity Plus 作为服务运行的帐户的凭据。

作为应用程序启动 DataSecurity Plus

1. 将 DataSecurity Plus 安装为应用程序。
2. 跳转到 **Windows > DataSecurity Plus > 启动 DataSecurity Plus 服务器。**

故障排除: “Windows 安全告警：Windows 防火墙已阻止此程序的某些功能。”

要启动 DataSecurity Plus，请解除阻止以下程序：

1. 数据库服务器
2. JavaTM 2 Platform Standard Edition binary

访问 DataSecurity Plus

1. 打开网络浏览器并输入**"http://<hostname>:<port number>"**在地址栏。

   hostname 是已安装 DataSecurity Plus 的计算机的名称，port number 是在 DataSecurity Plus 安装期间指定的 Web 服务器端口号。

   DataSecurity Plus 使用的默认端口是 8800。

> **注意:** 要验证 DataSecurity Plus 与您的计算机之间的通信，请转到 **Windows > 命令提示符** 并输入命令 **"Ping <hostname>".</hostname>**

2. 对于首次登录的用户，输入 **admin** 作为用户名和 **密码**，然后点击 **登录**。

> **提示:** 设置 DataSecurity Plus 后，通过导航到**> 管理 > 通用设置 > 个性化 > 更改密码**更改其默认密码。
>
> **提示:** Google Chrome 是运行 DataSecurity Plus 的推荐网络浏览器。

许可详细信息

DataSecurity Plus 有三个版本（免费版，试用版和专业版），所有版本都打包在一个下载中。

要下载 DataSecurity Plus，请点击下面的链接。

免费下载

关于试用版

首次下载 DataSecurity Plus 时，用户将拥有 30 天的功能齐全的试用版。 在这段时间内，他们可以评估产品提供的每个模块和功能。 此版本的用户将获得 24x5 的免费技术支持。

以下是 DataSecurity Plus 试用版的限制：

- 在“数据风险评估”模块中，只能配置 500GB 的数据用于数据发现。
- 在 Endpoint DLP 模块中，只能配置 300 个工作站进行审核。
- 在文件审核模块中，只能配置五台服务器进行审核。
- 在文件分析模块中，只能配置五台服务器进行分析。

关于免费版

30 天后，试用版将自动转换为**免费版**， 除非购买并申请了许可。 此版本的用户将继续获得 24x5 的免费技术支持。

以下是对 DataSecurity Plus 免费版的限制：

- 在“数据风险评估”模块中，只能为数据发现配置 100GB 的数据。
- 在 Endpoint DLP 模块中，只能配置 50 个工作站进行审核。
- 试用期过后，不会在文件审核和文件分析模块中获取新的事件数据。

关于专业版

DataSecurity Plus 专业版可以：

- 在 Windows 文件服务器和故障转移群集环境中，对所有文件访问，修改，移动和权限更改进行审核，报告和告警。
- 分析历史和实时审核数据，并提供文件访问趋势的洞察力。
- 在勒索软件攻击中检测并自动处理事件响应。
- 分析文件存储并提供有关文件所有权，文件安全性，磁盘使用情况等的可视化分析。
- 跟踪工作站和可移动存储介质中的文件活动。
- 通过 USB 和 Outlook 电子邮件检测并破坏敏感文件的泄漏。
- 使用存储在 Windows 文件服务器，故障转移群集和 Microsoft OneDrive 环境中的个人数据（PII / ePHI）查找文件并对其分类。
- 创建并维护存储的敏感数据的清单。

有关 DataSecurity Plus 的三种解决方案的各项功能的更多详细信息，请访问 版本对比页面。

许可和购买

专业版的许可模式因每个解决方案而异：

解决方案	许可依据

解决方案	许可依据
文件审核	文件服务器数量
文件分析	数据大小（TB）
终端 DLP	工作站数
数据风险评估	数据大小（TB）

这些可以单独购买或一起安装。 有关专业版许可证的定价详细信息，请查看询价页面。

要购买 DataSecurity Plus 许可证，请访问 ManageEngine store.

有关与许可或购买有关的任何问题的答案，或者要延长您的试用许可，请联系 china-sales@zohocorp.com

应用 DataSecurity Plus 许可

购买 DataSecurity Plus 之后，您的邮箱将会收到我们发送给您的.XML 许可文件。请按照如下步骤应用许可文件，将试用版或免费版升级到专业版。

1. 打开 DataSecurity Plus 产品界面。

2. 点击右上方的**许可** 链接。
3. 在弹出的许可明细对话框，点击“浏览”，并选择 ***License.xml*** 许可文件，然后点击**升级**。

文件审核

关于文件审核

DataSecurity Plus 的文件审核是 *Windows* 文件服务器实时审核和分析软件，可监视，审核，告警和报告在文件服务器环境中进行的所有文件访问和修改。借助 *DataSecurity Plus* 的文件审核解决方案，您可以

审核文件访问

审核文件访问和修改，以跟踪谁访问了什么文件，何时何地访问何处。

监视文件更改

跟踪并触发即时告警，以了解对敏感文件进行的异常更改。

审核复制并粘贴

跟踪文件服务器之间以及工作站之间的文件复制和粘贴操作。

审核访问权限

审核 *NTFS* 和文件共享权限，以了解谁有权访问哪些文件以及它们可以执行哪些操作。

打击勒索软件

通过自动威胁响应机制立即检测并关闭勒索软件攻击。

监视文件完整性

通过实时监控来检测关键文件的未经授权的更改并发出告警。

设置文件审核

域设置

请按照以下步骤配置所需的域。

1. 点击 **配置** > **管理** > **域设置**。点击 + **新增域**。
2. 输入域名称。
3. 点击 **身份验证**，并提供域用户的凭据。

> **注意:**如果未选中“身份验证”选项，则 DataSecurity Plus 将使用登录到本地系统的用户的凭据作为域用户凭据。

> **小贴士:**使用具有域管理员凭据的帐户来确保产品具有足够的权限来收集日志。 如果您不想提供域管理员凭据，请按照 此指南 以设置服务帐户的最小权限。

4. 点击 + **添加域控制器**并选择需要配置的域控。
5. 点击**保存**。

小贴士:配置多个域时，请根据所需的默认视图选择一个默认域。

文件服务器配置

文件服务器配置：

1. 配置您要配置的文件服务器所在的域。
2. 点击**文件审核**选项卡。转到**配置 > 源 > Windows 文件服务器。**
3. 点击右上角的 **+添加文件服务器**
4. 从下拉列表中选择您的域。
5. 点击“ **选择服务器**” 字段旁边的+。您将看到该域中可用服务器的列表。
6. 选择要审核的服务器。
7. 选择要监视的对象

   审核共享：选择一个或多个要审核的共享。

   要审核子文件夹，本地文件夹或本地文件：输入它们各自的路径。

8. 最后，点击**安装代理并结束**.

集群配置

请按照以下步骤配置集群服务器以进行文件审核：

1. 添加您要配置的集群所在的域。

2. 点击 **文件审核**标签，跳转到**配置 > 来源 > Windows 文件集群**。

3. 点击 **+ 添加集群**。

4. 输入集群名称，然后点击 **下一步**。

5. 选择要监视的集群节点。 点击 **下一步**。

6. 选择集群客户端访问点（CAP）。点击 **下一步**。

7. 选择所有要审核的共享。 点击 **查看**。

8. 查看完配置的设置后，请点击 **配置**。

9. 成功配置集群后，其状态将显示在集群配置窗口中。

工作组配置

通过执行以下步骤在“文件审核”中配置工作组服务器。

1. 添加要配置的工作组所在的域。

2. 点击 **文件审核**选项卡。转到**“配置” > “源” > “工作组服务器”**。

3. 点击右上角的**+添加工作组** 。

4. 点击**“选择服务器”**字段旁边的+，然后选择要审核的服务器。

5. 选择要监视的对象。

   要审核的共享：选择一个或多个要审核的共享。

   要审核子文件夹，本地文件夹或本地文件：输入它们各自的路径。

6. 点击**“安装代理并完成”**。

仪表板

全局概览

快速获取选定域内所有已配置服务器的基本审核数据的快照。 您可以使用 **选择域** 选项。

默认情况下，您将获得以下数据：

- 服务器摘要报表
- 基于服务器的报表
- 服务器安全更改
- 服务器失败事件
- 服务器移动或重命名事件
- 服务器删除事件

小贴士: 您可以在 **最近 24 小时**和 **最近 7 天**之间切换以查看异常变化和偏差的视图。

服务器概述

快速获取所选服务器的基本审核数据的快照。

您可以使用**“选择服务器”**选项来查看所有审核的服务器上的数据。

默认情况下，您将概览以下数据：

- 访问量最高的文件
- 访问次数最多的流程
- 访问量最高的用户
- 访问量最高的共享文件夹

- 访问量最高的主机

注意：需要使用刷新图标来获取最新数据。

报表

访问审核报表

DataSecurity Plus 文件审核解决方案提供了多种默认报表类别。 请按照以下步骤查看它们：

1. 点击 **文件审核** 标签，跳转到**访问审核 > 审核报表**
2. 选择**服务器名称** 查看该特定服务器的审核数据。
3. 使用**期间**下拉列表框来选择所需的时间范围
4. 选择“审核报表”下的任何默认报表，然后查看相关数据。

所有文件/文件夹更改

报告所有进行的访问，包括创建，修改，删除，移动，重命名，权限更改和所有者更改事件。

文件创建

创建的所有文件的列表。

重命名/移动的文件

列出所有已配置文件的所有移动，重命名和文件扩展名更改。

被删除/覆盖的文件

所有已删除和覆盖文件的列表。

安全权限更改

所有安全性更改的列表，包括权限更改，所有者更改和 SACL 更改。

所有失败的尝试

所有失败的读取，写入和删除尝试的列表。

文件读取

所有文件读取事件的列表。

文件复制

本地或远程访问期间复制的所有文件的列表。

小贴士: 您可以使用图形右上角的可用编辑选项来刷新数据，更改视图或将特定视图添加到仪表板。

FAQ: 如何创建新的文件审核报表？

访问分析报表

请按照以下步骤查看有关您环境中已分析的访问事件的报告：

1. 点击 **文件审核**标签。跳转到 **访问审核 > 汇总报表**。
2. 选择 **服务器名称**查看该特定服务器的访问分析。
3. 使用 **时间段**下拉列表框来选择所需的时间范围。
4. 选择下面的 **汇总报表** 查看和分析相关数据:
    - 访问最多的文件
    - 修改最多的文件
    - 进程访问最多的文件

- 用户访问最多的文件
- *N* 天后访问的文件
- *N* 天后修改的文件

> **注意:** 您可以在以上报表中更改 *N* 的值。

5. 使用 **基于用户的报表** 根据执行操作的用户来分析成功事件，失败事件或所有事件。
6. 使用 **基于主机的报表** 根据执行操作的主机分析成功事件，失败事件或所有事件。
7. 使用 **基于共享的报表** 根据执行操作的共享来分析成功事件，失败事件或所有事件。
8. 使用 **基于地点的报表** 分析成功事件，失败事件或所有事件的位置。

默认告警

默认告警

在 *DataSecurity Plus* 中，基于告警配置文件配置触发电子邮件通知。设置文件服务器后，将立即开始事件收集和处理，对使用默认告警配置生成的事件进行交叉验证。

“告警”选项卡显示有关在定义的**期间内**在选定的**服务器**上触发的告警的详细信息。

您可以查看告警的分类和概要分析明细，告警源的报告，触发它们的人，位置以及是否违反阈值。

以下是 DataSecurity Plus 的文件审核解决方案中的默认告警：

文件/文件夹移动或重命名告警

在关键文件被移动，重命名或覆盖时发出告警。

文件/文件夹安全性更改告警

在安全性更改（即权限更改，SACL 更改和所有者更改）发生时通知。

文件/文件夹已删除告警

在敏感文件被覆盖或删除时发出告警。

媒体文件告警

通知数据所有者或管理员有关环境中存在的媒体文件实例的信息。

勒索文件告警

在潜在的勒索软件攻击时通知。

基于阈值的告警

在突然出现异常更改或文件访问事件激增时通知。

配置

预定义的审核策略

默认的审核策略是配置文件，基于该配置文件，一旦设置了文件服务器，就会开始进行事件收集和处理。

预定义的配置根据以下过滤器收集审核数据：

用户：全部

动作全部

创建	修改	删除	移动
所有者变更	覆盖	权限变更	重命名
SACL 变更	文件复制	访问失败	还原
写入失败	删除失败	文件扩展名更改	读取
文本复制	文件属性变更	文件粘贴	

监视对象:全部

请按照以下步骤修改默认审核策略：

1. 单击**文件审核**选项卡。转到**“配置”>“设置”> “审核配置”**。
2. 选择任何服务器，因为所有配置的服务器的预定义配置都相同。
3. 在表中，您将找到默认访问审核配置。选择编辑。
4. 在**“条件”**选项处，添加新的过滤器或编辑预定义的过滤器。
5. 点击**保存**。

要创建新的审核策略，请执行以下步骤：

1. 单击**文件审核**选项卡。跳转到设置 > 审核配置。
2. 点击右上角的**+添加报告**。
3. 为新策略提供合适的名称和描述。
4. 通过使用**包括**和**排除**选项来修改审核条件。
5. 点击**保存**。

自定义报告

请按照以下步骤配置自定义审核报告：

1. 单击**文件审核**选项课。转到**“配置” > “设置” >“自定义报告”**。
2. 选择要为其配置报告的服务器。
3. 点击右上角的**+创建自定义报告** 。
4. 为新报告提供合适的名称和描述。
5. 通过使用**包括**和**排除** 选项来修改报告条件。
6. 单击**保存**.

警报

请按照以下步骤查看或修改默认警报：

1. 单击**文件审核**选项卡。转到**“配置”> “设置”> “警报配置”**.
2. 您可以选择任何服务器，因为所有配置的服务器的默认配置都相同。
3. 现在，您可以查看已配置的预定义警报的列表。

4. 如果需要，您可以选择使用**“编辑”**选项来修改预定义的警报。
5. 单击**“编辑”**后，添加或修改警报详细信息，包括**“ 条件”**部分下的警报详细信息。
6. 单击**保存**。

要创建新的警报配置文件，请按照以下步骤操作：

1. 单击 **文件审核** 选项卡。转到**“配置” > “设置” > “警报配置”**。
2. 单击页面右上方的;**+添加警报**。
3. 为新警报提供合适的名称和描述。
4. 根据警报的严重性对警报进行分类。
5. 如果要配置基于阈值的警报，请选中**“阈值限制”**复选框。
6. 要对任何事件执行定制响应，请提供脚本文件路径。

> **提示：**脚本是迄今为止最被低估的响应策略。您可以运行脚本来关闭服务器，停止用户会话，禁用帐户等等。您要请求自定义回复吗？ 联系我们的支持团队。

7. 要将电子邮件通知发送给管理用户，请选中**“电子邮件通知 ”**旁边的框，然后单击**“编辑”**.
8. 在**“电子邮件设置”**弹出窗口上，提供要将通知发送到的电子邮件 ID，优先级，主题和警报消息。
9. 设置指定时间内发送电子邮件的最大数量。这将限制要发送给警报的电子邮件数量。点击**保存**.

10. 选择触发警报的**条件**点击**保存**.

计划报表

请按照以下步骤安排将报告发送到管理员的邮箱。

1. 单击**文件审核**选项卡。转到**配置 >设置 > 配置计划。**.
2. 点击右上角的**+安排新报告**。
3. 为时间表提供合适的名称
4. 选择计划的频率以及计划开始的日期。
5. 指定要用于接收报告的格式（*PDF*，*HTML*，*CSV*，*XLSX*）以及报告的存储位置。
6. 指定要将报告发送到的电子邮件 *ID*。
7. 然后，点击右下角的 **+添加新报告**。
8. 选择服务器。然后选择您希望接收的审核和分析报告。选择报告时，请选择审核数据的时间范围。
9. 单击**保存报告**。
10. 单击**保存**以在配置的时间运行计划，或单击**“保存并运行”**以立即运行一次计划，然后在配置的时间再次运行。

排除

请按照以下步骤从文件审核解决方案内或全局范围的报表和告警中排除管理员组和其他受信任实体：

1. 点击**文件审核**标签。跳转到 **配置 > *Settings* > 排除配置**。

2. 选择是要全局排除实体还是基于服务器排除实体。
3. 根据用户操作，文件类型，用户等选择所需条件。
4. 点击 **保存**。

存储配置

保留策略

请按照以下步骤启用保留设置：

1. 点击 **文件审核**标签。跳转到 **配置** > ***Storage*** > **保留配置**。
2. 选择您希望保留告警的天数。

> **注意**：保留设置适用于所有类别的告警。

3. 选择您希望保留计划报表的天数。
4. 点击 **保存**。

归档

请按照以下步骤启用存档：

1. 单击**文件审核**选项卡。转到 **配置** > **存储** > **存档配置**。
2. 选中**启用归档**旁边的框。

3. 输入您希望将数据归档之后的天数。

4. 选择用于保存归档日志的目标文件夹。

5. 点击**保存**。

注意： 默认情况下，存档计划每天在本地时间凌晨 2 点运行。您也可以通过单击**运行**运行选择立即运行它。

注意： 存档数据的默认目标文件夹是 *C:\Program Files x86)\ManageEngine\DataSecurity Plus\bin\Backup.*

恢复归档事件

要查看，加载和卸载存档的日志，请执行以下步骤：

1. 单击**文件审核**选项卡。转到**“配置” >“存储”> “还原存档事件”**。

2. 这里将列出所有存档文件。

3. 选择您要管理的文件。

4. 根据需要单击**“加载选定的文件”或 “卸载选定的文件”**。

文件分析

关于文件分析

基于 Windows 环境的 DataSecurity Plus 的文件分析功能可分析文件元数据并提供可视化分析。 使用该解决方案，您可以：

查找重复文件:

发现并管理存储中文件的冗余副本，并确保最佳利用磁盘空间。

分析文件存储:

查找陈旧和非商业文件，分析文件存储模式，查看有关文件类型分布的报表，等等。

发现文件安全性问题:

检查有效权限； 识别具有开放访问权限，权限不一致等问题的文件和文件夹。

检测和管理事件:

分析存储并接收有关磁盘空间严重不足的告警。

本指南旨在帮助用户安装和设置 DataSecurity Plus File Analysis 模块，并在其 Windows 环境中接收有关文件和文件夹的分析。

设置文件分析

配置域

按照以下步骤配置所需的域

1. 进入 **配置 > 管理 > 域设置**，点击页面右上角的 **+ 添加域**
2. 输入域名
3. 选中**认证**旁边的复选框，并提供域用户凭据

> **注意:**如果未选中认证选项，DataSecurity Plus 将使用登录到本地系统的用户的凭据作为域用户凭据

> **提示:**使用具有域管理凭员据的帐户，以确保产品有足够的权限来收集日志。
>
> 如果您不想提供域管理员凭据，请参考此 指南 以最少的权限建立服务帐户。

4. 点击**添加域控** 旁的 + 符号，选择域控
5. 点击 **保存**

> **提示:**配置多个域时，请根据您需要的默认视图选择默认域。

添加文件服务器

按照以下步骤添加您希望使用文件分析模块监视的服务器。

1. 进入**文件分析 > 配置 > 来源 > Windows 文件服务器**

2. 点击右上角**添加服务器**

3. 点击 **选择服务器**右侧的**+**

4. 在**选择服务器**弹出框中，添加 **服务器** ，点击“选择”后弹出框关闭。

5. 选择要监视所有驱动器还是只监视特定的驱动器。

6. 点击 **安装代理并关闭**

工作组配置

通过执行以下步骤配置工作组服务器：

1. 跳转到 **文件分析> 配置 > 资源 > 工作组服务器。**

2. 点击右上角的**+ 添加工作组** 标签。

3. 点击**选择服务器**旁的**+**按钮，并选择要审核的服务器。

4. 通过执行以下操作来配置工作组服务器选择要分析的驱动器。

5. 点击**更新。**

仪表板

存储概述

设置解决方案后，几分钟后即可开始在仪表板上查看数据。 存储概述显示了对域中已配置磁盘上的存储模式的分析。

在这里，您可以细化查看所有旧文件，旧文件和非业务文件的垃圾文件分布。 该表还显示了每台服务器的所有垃圾文件的总大小以及该服务器所用总空间的百分比。

在“存储概述”的右半部分中，有一个名为“已分析的总大小”的面板。 它显示了“文件分析”模块分析的数据总大小，以及有关文件和文件夹的总数和密度的有用细分。

在这些下方，有一个表格显示所有已配置的磁盘，它们的大小，每个驱动器中使用的空间以及进度条以显示可用的存储空间。

安全概述

“安全概述”显示了对整个域中已分析文件和文件夹的权限状况的分析。

默认情况下，“安全概述”具有以下模块：

休眠用户拥有的文件：显示不活动，已禁用，已删除和已过期用户拥有的文件数的图形分类。

权限不一致：显示继承中断的文件和文件夹的数量和百分比。

开放式访问：显示在您的域中共享的文件数量和百分比，这些文件提供对用户或组的完全控制访问权限。

开放式访问（基于用户）：显示拥有最多文件数量（允许无限制访问）的前五用户的列表。

休眠用户拥有的活动文件：显示休眠用户拥有的活动文件总数。

注意:活动文件是最近已访问或修改的文件。

报表

报表概述

在 报表概述下，您可以看到显示选定服务器的存储和安全概述的图形和图表。 服务器视图下有两个选项卡：

存储视图: 显示有关文件创建，垃圾文件，文件类型分布，用户的存储消耗以及磁盘空间不足的分析。

安全视图: 显示对休眠用户拥有的文件，权限不一致，打开访问文件和文件夹，休眠用户拥有的活动文件以及用户和组的文件和文件夹计数的分析

存储报表

可用的存储报表如下：

- **文件类型摘要**: 显示每种文件类型中的文件数及其大小。
- **文件所有者摘要**: 提供有关每个用户拥有的文件总数和全部大小的信息。
- **文件类别摘要**: 提供有关每个文件类别中文件数量和大小的信息。
- **旧文件（基于创建时间）**：列出早于 *N* 天的文件。*N* 可以在报表页面上更改。
- **旧文件（基于访问时间）**：列出 *N* 天未访问的文件。可以在报告页面上更改 *N*。
- **重复文件**: 列出分析的驱动器中检测到的重复文件副本。
- **未修改的文件**: 列出在 *N* 天内未被修改的文件。可以在报表页面上更改 *N*。
- **大文件**: 列出大于配置大小的文件。

- **隐藏文件**: 列出具有“hidden”属性的文件。
- **非业务文件**: 列出已配置为非业务的文件类型的文件。

注意: 您可以在服务器上报表配置页面选择要配置为非业务的文件类型。

安全报表

可用的安全报表为：

- **具有开放访问权限的文件**: 列出允许用户完全控制访问的文件。
- **完全控制**: 列出选定用户具有完全控制访问权限的文件。
- **权限不一致**: 列出继承中断的文件。

按需报表

按需报表的列表为：

- **有效权限**: 显示所选服务器，共享/和子级别中用户的有效权限。
- **所有共享**: 列出选定服务器中的所有共享文件和文件夹，以及有关共享名称，类型，共享路径和本地路径的详细信息。
- **开启的会话**: 列出选定服务器中的所有打开的用户会话，以及有关主机 IP，用户名，连接时间，空闲时间和打开文件数的详细信息。
- **打开的文件**: 列出在生成报表时打开的文件。

- **连接点**: 列出选定服务器，文件夹和子级别中的连接点以及目标位置。
- **特权用户**: 列出具有特权的用户。
- **孤立文件**: 列出与由于计算机错误而被卸载或分离的程序关联的所有文件。
- ***NTFS* 权限**: 向用户显示所选文件共享的安全权限。

触发告警

在 **文件分析 > 告警**下，您可以找到在所选时间范围内触发的所有告警的列表。

由于文件分析模块不提供实时信息，只在运行扫描计划时会触发告警。默认设置下，提供以下告警:

勒索文件类型: 当发现已知的勒索软件文件类型时，将触发告警。

磁盘容量低: 当可用磁盘空间低于 *25%*时，将触发告警。

> **注意:** 关于配置新告警的步骤，点击这里

配置

报表

DataSecurity Plus 文件分析模块为所有报表预定义了配置。要查看或编辑报表的功能级别:

1. 进入 **文件分析页签 > 配置**
2. 在左侧目录，进入 **设置 > 报表配置**
3. 在你需要修改或查看的报表旁点击 **修改** 图标

> **注意:** 默认报表配置如下:
>
> **公开文件权限报表**: 文件对“Everyone“ 配置任意权限或对任意用户配置"完全控制" 权限
>
> **不活跃用户报表**: 已停用超过 90 天或已过期/禁用的用户帐户
>
> **重复文件报表**: 具有相同大小、相同名称和/或相同最后修改时间的文件
>
> **非企业文件报表**: 已知的勒索软件文件类型和视频文件
>
> **过期文件报表**: 最后一次访问和最后一次修改的时间超过五年的文件

告警

要在文件分析模块中配置告警:

1. 进入 **文件分析 > 配置**
2. 在左侧菜单,点击 **设置 > 告警配置**.
3. 点击右上角 **+ 创建告警**
4. 在下一页，填入新的告警的名称及简介
5. 在**严重性**下拉框中对告警级别进行分类
6. 在**条件**框中，在**包含**种配置触发告警的详细信息

7. 为了缩小报告范围，减少误报，您可以在**排除**中
   配置相关信息

8. 您可以在 ***Response*** 中配置告警的适当响应

> **提示:** 脚本是迄今为止最被低估的响应策略。您可以运行脚本关闭服务器， 停止 用户会话，禁用账户，以及更多操作。您想要自定义响应吗? 联系我们

9. 完成一个或多个响应后，点击 **保存**

扫描

文件分析工具会定期扫描文件服务器，以使报告保持最新状态。 要查看或编辑这些计划的扫描：

1. 跳转到**文件分析** ***tab*** **> 配置**。
2. 在左侧菜单上，转到 **设置 > 扫描配置**
3. 在您要查看或编辑的扫描计划上点击 **编辑**图标。

> **推荐配置:** 默认情况下，将设置以下推荐的扫描计划：
>
> ***Metadata scan***: 每 30 天一次。

元数据增量扫描：每 24 小时一次。

安全扫描：每 24 小时一次。

磁盘空间扫描：每 24 小时一次。

计划

请按照以下步骤将计划报表发送到管理员的邮箱。

1. 点击**文件分析**标签。 点击 **配置> 设置 > 计划配置**。
2. 点击**+ 新建计划报表**
3. 为计划提供一个合适的 **名称**
4. 选择计划的**频率**和**时间**。
5. 指定您要接收的报表**格式 (PDF, HTML, CSV, XLSX)**以及报表的存储位置。
6. 指定接收报表**邮件地址**。
7. 然后点击右下角的**+ 新建报表**。
8. 选择**服务器**。然后选择**审计和分析报表**。在选择报表时，选择审计数据的**时间范围**。
9. 点击**保存报表**。
10. 点击**保存**以在配置的时间运行计划，或单击**保存并运行**立即运行计划，然后在配置的时间再次运行。

数据风险访问

数据风险访问

DataSecurity Plus 的数据风险评估会检查文件内容，以发现关键数据，并根据敏感度和漏洞对其进行分类。有了它，你就可以:

发现敏感数据

查找、分析和跟踪存储在文件服务器、OneDrive 等中的敏感个人数据(也称为 PII 或 EPHI)。

对风险最高的数据进行分类

使用内容和上下文参数确定最易受攻击的数据。

标记敏感文件

使用自动和手动文件标记可以更快地对文件进行分类，并减轻 IT 管理员的负担。

扫描分类的文件类型

扫描超过 50 种文件类型的敏感内容，包括电子邮件、文本和压缩文件。

设置数据风险访问

域配置

按照以下步骤配置所需的域。

1. 点击进入**配置 > 管理 > 域配置**。点击**+ 添加域**。
2. 输入域名称。
3. 勾选**认证**，并提供一个域用户的凭证。

> **注意:**如果未选中身份验证选项，DataSecurity Plus 将使用登录到本地系统的用户的凭据作为域用户凭据。

> **提示:**使用具有域管理员凭据的帐户以确保产品有足够的权限收集日志。如果您不想提供域管理员凭据，请参考指导文档设置所需的最少权限设置服务帐户。

4. 点击**添加域控制器**字段中的 + 符号，然后选择需要的域控。
5. 点击**保存**。

> **提示:**配置多个域时，请根据您需要的默认视图选择默认域。

文件服务器配置

按照以下步骤配置所需的文件服务器:

1. 配置要配置的文件服务器所在的域。
2. 点击**文件审核**标签。进入**配置 > 源 > Windows 文件服务器**。
3. 点击 **+ 添加文件服务器**。
4. 从下拉列表中选择您的域。
5. 点击**选择服务器**字段的+图标，您将会看到域中可用的服务器列表。
6. 选择要审核的服务器。
7. 选择要监控的对象

   审核共享: 选择一个或多个要审核的共享。

   审核子文件夹，本地文件夹或本地文件：输入它们各自的路径。

8. 最终，点击**安装代理并完成**。

仪表板

使用详细的仪表板快速获得风险最大的文件类型、用户和文件服务器的快照。默认情况下，仪表板显示以下关键信息:

- 规则命中排行
- 策略命中排行
- 包含敏感数据的文件类型排行
- 敏感数据源排行
- 存储敏感数据的用户排行
- 包含敏感数据的服务器排行

提示:您可以使用右上角的**时间**下拉列表查看不同时段的数据。

报表

所有记录

DataSecurity Plus 的数据风险评估模块报表发现的敏感数据的每个实例，以及其位置、扫描时间、违反策略等。

您可以使用 **过滤**选项根据风险评分、位置、数据源等有选择地查看数据。

文件服务器报表

查看所选文件服务器中扫描的文件总数、有违规的文件、触发警报的文件和风险文件的图形摘要。

您可以使用**时间**下拉框，查看在特定时间范围内发现的敏感数据的详细报表。

OneDrive 报表

查看选定 OneDrive 帐户中扫描的文件总数、违规文件、触发告警的文件和危险文件的图形概览。

您可以使用 **期间**下拉列表，查看在特定时间范围内发现的敏感数据的详细报表。

触发的告警

要查看由策略违例触发的告警列表：

1. 跳转到 **风险分析 > 报表 > 告警记录 > 告警 s**。
2. 使用 **期间** 下拉菜单以查看在特定时间范围内触发的所有告警。

配置

预定义风险访问策略

按照以下步骤查看 *DataSecurity Plus* 的数据风险评估解决方案中的默认策略:

1. 点击 **风险分析**标签。进入 **配置 > 发现策略配置 > 策略**。
2. 选择要查看的策略并点击 **编辑**选项查看更多。
3. 通过点击表上方的 **+ 添加规则**按钮向现有策略添加规则。
4. 选择您想要应用的规则。
5. 点击 **保存**。

提供的预定义策略:

***GDPR* 策略**: 确定一般数据保护法规(*GDPR*)强制适用的个人数据(*PII* 或 *EPHI*)实例。

创建新的风险访问策略

按照以下步骤配置新策略:

- 点击**风险分析**标签，进入**配置 > *Discovery* 策略配置 > 策略**。
- 点击 **+ 添加策略**。
- 命名策略并包括适当的描述。

- 点击表上面的**+ 添加规则**，将规则添加到新建的策略。
- 选择要添加的规则。

  例如：如果您想要发现您文件中存在的 *Visa* 卡详细信息实例，请选择 ***Credit card - Visa card*** 规则。

- 点击添加规则表下面的**+ 添加排除规则**，将排除规则添加到新建的策略。

  例如：如果要查找财务部门拥有的文件之外的 *Visa* 卡详细信息实例，请选择 ***Credit card - Finance Department*** 规则。

- 选择要添加的排除规则。
- 点击**保存**。

预定义数据发现规则

按照以下步骤查看或编辑 *DataSecurity Plus* 的数据风险评估解决方案中的预定义规则：

- 点击 **风险分析**标签。进入 **配置 > 发现策略配置 > 规则**。
- 选择您想要查看的规则并点击 **编辑**选项查看更多。
- 检查用于定义规则的关键字集或正则表达式。

> **注意：** *DataSecurity Plus* 提供超过 *50* 个预先配置的数据发现规则。

创建新的数据发现规则

按照以下步骤配置新的数据发现规则:

- 点击 **风险分析**标签。进入**配置 > 发现策略配置 > 规则**。
- 点击右上角的 **+ 添加规则**。
- 命名规则，并包含适当的描述。
- 选择规则的 **匹配类型**，例如关键字集或正则表达式。

> **提示:** 使用关键字集时，一个确切的短语可以用来定位敏感信息。在搜索文本或数字模式时使用正则表达式。

- 输入关键字集或正则表达式模式。
- 在 **发生次数**字段中，设置个人数据所需的阈值。
- 点击**保存。**

计划扫描

按照以下步骤计划数据发现扫描:

1. 点击 **风险分析**标签。进入 **配置 > 扫描配置 > 计划**。
2. 点击右上角的 **+ 新添计划**。
3. 列出计划并包括适当的描述。
4. 选择要扫描的策略。

5. 选择要扫描的共享。

6. 选择要扫描的 *OneDrive* 文件夹。

7. 启用 **增量文件扫描**。

> **最佳实践**: 总是选择增量文件扫描选项，除非是一次性扫描。通过只扫描新文件或修改后的文件，可以减少运行时间。

8. 输入**计划持续时间**。

9. 选择 **开始日期**。

10. 指定 **排除时间**。

> **提示:**数据发现本身就是一个 *CPU* 密集型任务。将最关键的业务时间添加到排除时间中，以最小化对生产力的干扰。

11. 点击 **添加**。

12. 点击 **保存**。

终端 DLP

关于终端 DLP

DataSecurity Plus' 终端 DLP 解决方案保护敏感数据不受传统和虚拟终端的暴露或窃取。使用它，您可以：

审核终端使用

通过实时监视，审核和监视打印机、传真、剪贴板和 USB 的使用。

防止数据泄漏

阻止敏感的个人数据如 PII 和 ePHI 通过 USB 或电子邮件泄露。

响应事件

设置未经授权的 USB 使用警告，阻止通过电子邮件产生的数据泄漏(Outlook)，并立即纠正问题。

本指南旨在帮助用户安装和设置 DataSecurity Plus' 终端 DLP 解决方案 并收集其环境中终端使用情况的分析。

设置终端 DLP

配置域

按照以下步骤配置所需的域。

1. 进入 **配置** > **管理** > **域设置**. 单击页面右上角 **添加域**

2. 输入域名。

3. 选中 **认证** 旁边的复选框，并提供域用户的凭据。

> **注意:**如果未选择认证选项，DataSecurity Plus 将使用登陆本地系统的账户作为域用户验证。

> **提示:**使用具有域管理权限的账户，以确保产品有足够的权限来收集日志. 如果不希望提供域管理账户，请根据 此向导的步骤以最少的权限建立服务账户。

4. 单击**添加域控制器**字段中的+符号，并选择所需的一个。

5. 单击 **保存**

> **提示:**在配置多个域时，根据需要的默认视图选择默认域。

工作站配置

要为终端 DLP 配置工作站，请遵循以下步骤:

1. 进入**终端 > 配置**

2. 选择左侧菜单**来源**下的**设备**。

3. 在 **已配置的工作站** 页面中，选择右上角 **添加工作站** 。

4. 选择您的域名。

> **注意:** 若要添加未列出的域，点击 **添加新域** 并遵循此页的步骤。

5. 点击**选择工作站** 右侧的 + 符号，添加你需要审核的工作站。

6. 然后，为已选择的工作站选定**安全策略**。

7. 点击 **安装代理并完成**。

报表

基于数据源报表

要查看基于数据源报表

1. 单击 **终端** 页签， 进入 **报表 > 基于数据源报表**.

2. 选择一个 **终端名称** 以查看特定终端的审核数据。

3. 使用 **周期**下拉框来选择你想要的时间范围。

可以查看以下报表:

文件完整性报表

使用实时监视终端获取本地文件系统中的变更报表。

文件复制报表

在本地或远程访问期间复制的所有文件的列表。

邮件审核报表

在选定的终端列出 *OutLook* 电子邮件使用。

打印机审核报表

所选终端的打印机使用情况报表。

网络审核报表

列出文件上传和下载活动。

文件共享报表

列出对共享文件的访问和修改。

可移动存储文件活动

USB 设备上文件活动报表。

文件分类报表

要查看文件分类报表:

1. 单击 **终端** 页签. 进入 **报表 > 文件分类报表**.
2. 选择一个 **终端名称** 以查看特定终端的审核数据。
3. 使用 **周期**下拉框来选择你想要的时间范围。

   数据分类报表
   此报表列出手动分类的文件。

注意: 文件根据其敏感性可分为四类。

受限: 最机密的数据

机密: 中等机密

私有:低等机密

公共: 非机密数据

触发告警

要查看在已配置的终端中触发的警报列表:

1. 点击 **终端** 页签，并点击**告警**。
2. 选择一个 **终端名称** 以查看在该终端中触发的告警。
3. 使用 **周期**下拉框来选择你想要的时间范围。

配置

策略

DataSecurity Plus 使用预定义的策略实时识别端点安全漏洞。

您可以使用终端 *DLP* 解决方案监视以下安全策略:

预防数据泄露

阻止包含业务关键数据的文件通过 *USB* 和电子邮件离开网络。

文件活动监视

对工作站中的文件进行审计访问和更改。

文件复制审核

审核用户在工作站内以及外部存储设备上的文件复制操作。

文件完整性监视

检测并响应用户对敏感文件所做的未经授权的更改。

潜在的恶意软件入侵

当安全阈值限制被打破时，通过接收告警来检测潜在的恶意软件。

可移动设备审核

审核 *USB* 和其他可移动存储设备的使用情况。

敏感文件活动监视和响应

接收包含 *PII* 和 *ePHI* 等敏感数据的文件中的用户活动报告。

按照以下步骤修改预定义的策略:

1. 单击 **终端**页签，进入 **配置 > 设置 > 策略**。
2. 选择在预定义策略旁边的图标 **修改**来修改策略。
3. 在**审核配置文件** 和 **告警配置文件**下添加或删除策略。
4. 点击 **保存**.

要创建新的审核或告警策略，请遵循以下步骤:

1. 单击 **终端**页签，进入 **配置 > 设置 > 策略**。
2. 单击右上角 **+ 添加策略** 。
3. 命名策略并包含适当的描述。
4. 选择策略要应用的终端。
5. 选择你需要添加的 **审核配置文件** 及 **Alert Profiles 告警配置文件**

   例如: 如果你想阻止敏感文件移动到 *USB* 设备，选择 **数据泄露防护 – *USB*** 告警配置文件。

6. 点击 **保存**。

审核

按照以下步骤查看 *DataSecurity Plus'* 终端 *DLP* 解决方案中的默认审计配置文件:

1. 单击 **终端**页签。进入 **配置 > 设置 > 审核配置**.
2. 选择你需要查看的 **审核配置文件** 然后单击修改选项查看配置文件的配置方式。
3. 检查配置文件细节及 用于定义规则的**条件**。
4. 您还可以为告警配置响应操作。

告警

按照以下步骤查看 *DataSecurity Plus* 中终端 *DLP* 解决方案中的默认告警配置文件:

1. 单击 **终端** 页签。 进入 **配置 > 设置 > 告警配置**。
2. 选择你需要查看的 **告警配置文件** ，再点击 **修改** 选项，以查看如何修改配置文件。
3. 检查配置文件细节及 用于定义规则的**条件**。
4. 您还可以为告警配置响应操作。

常规配置

连接

在 **配置 > 常规设置 > 连接**中，您可以编辑用于 HTTP/HTTPS 通信的端口号。

默认情况下，将使用以下端口:

HTTP: 8800

HTTPS: 9163

编辑完成后，点击 **保存**。

个性化

在 **配置 > 常规设置 > 个性化**中，您可以看到以下选项:

- 更新显示设置:设置日期和时间格式。
- 更改密码: 更改用于登录 DataSecurity Plus 的密码
- 更新登录页设置：选择默认域以及是否在登录页中查看横幅。

DataSecurity Plus 服务器

在 **配置 > 常规设置 > DataSecurity Plus 服务器**中，您可以:

- 选择在 Windows 启动时自动启动产品。
- 选择成功启动后，启动 DataSecurity Plus 客户端。
- 选择工作模式。DataSecurity Plus 的默认工作模式为"正常"，并且调试信息最少。

隐私设置

在 **配置 > 常规设置 > 隐私设置**中，您可以找到以下选项:

- 密码保护的归档和计划报表，以保持符合 GDPR。
- 发送有关产品质量、稳定性和可用性的使用统计数据。

管理配置

技术员配置

DataSecurity Plus 允许委派两个角色:

1. 管理员—具有完全的权限，可以进行 DataSecurity Plus 的设置和配置。
2. 操作员—具有仅查看报表、告警和图表的权限。

要添加新的技术人员，请遵循以下步骤:

1. 进入 **配置 > 管理 > 技术员**。
2. 点击右上角的 **+ 添加技术员**。
3. 选择域。然后，点击**选择技术员** + 图标，添加所需的用户。
4. 选择角色(管理员或操作员)。
5. 点击 **保存**。

列出、管理和查看配置的技术人员的审核日志:

1. 进入 **配置 > 管理 > 技术员**。

2. 使用不同的**动作**可用来启用/禁用技术人员、更改角色、更改密码或删除技术人员。
3. 要查看技术员所进行活动的审核日志，请点击 **查看**。

邮件设置

请按照以下步骤在 *DataSecurity Plus* 中配置邮件设置:

1. 进入 **配置 > 管理 > 邮件设置**。
2. 指定邮件服务器和端口。
3. 勾选 **身份验证**复选框，提供必要的凭证。
4. 选择连接方式:*SSL/TLS/*无。
5. 提供用于接收邮件通知和报表的邮件 *ID* 以及管理员的邮件 *ID*。
6. 点击 **保存**。

筛选通知

要筛选 *DataSecurity Plus* 触发的通知量，请执行以下步骤:

1. 进入 **配置 > 管理 > 通知**。
2. 选中您希望从可用列表中接收的通知。

> **注意:**为了确保连续、实时的分析，我们建议在代理和服务器之间没有通信超过 6 小时时始终启用告警。

3. 提供发送通知的邮件 ID 和计划邮件的时间。

4. 点击 **保存**。

管理代理

在**管理代理**页面上，可以检查和管理代理服务、驱动程序服务、配置同步和代理属性的状态。

在 **配置** > **管理** > **管理代理**中，您可以找到以下信息:

- 检查代理是否已安装并正在运行的代理服务表。可以使用这个表上的按钮来安装/卸载和启动/停止代理。
- 驱动程序服务表，检查驱动程序服务是否已安装并正在运行。
- 配置同步表，用于检查最后的同步时间和各个配置的同步状态。每个配置都可以使用相应的按钮进行同步。
- 代理属性表，用于比较代理本身和服务器中的代理属性的值。如果属性匹配，则状态将用绿色复选框标记。
- RPC 和 HTTP 通信的状态。
- 手动下载代理并将其安装在所需文件服务器中的选项。

如果出现 HTTP 通信故障，请查看 故障排除。

更多 DataSecurity Plus 代理的详细信息，请查看 代理文档。

SIEM 集成

凭借其 SIEM 集成功能，DataSecurity Plus 允许您将所有文件服务器审核数据转发到您的 syslog 服务器或 Splunk。

要配置 SIEM 解决方案，请遵循以下步骤:

1. 进入 **配置 > 管理 > SIEM 集成**。
2. 点击右上角的 **+ 添加配置**。
3. 选择是要配置 Syslog 还是 Splunk。
4. 如果您需要配置 syslog 服务器:
    - 提供名称、端口号和协议(UDP/TCP)。
    - 选择您希望转发数据的 Syslog 标准和数据格式。
    - 点击 **保存**。
5. 如果您需要配置 Splunk:
    - 输入 Splunk 服务器名称和端口号。
    - 提供发布 URL 和认证令牌。
    - 点击 **保存**。

业务时间

在审核数据时，可以选择查看在业务/非业务时间生成的数据，从而缩小最重要事件的范围。要配置此时间范围，请执行以下步骤:

- 进入 **配置 > 管理 > 业务时间**。
- 勾选 **配置业务时间**的复选框。
- 选择在您的组织中进行常规业务的时间和工作日。
- 点击 **保存**。

联系我们

联系我们

我们很乐意收到你的来信。请使用下面提供的详细信息与我们联系。

与销售团队沟通

要购买 ManageEngine DataSecurity Plus，请填写销售请求表，我们的销售主管将很快与您联系。您也可以通过 china-sales@zohocorp.com 向我们发送电子邮件。

为了最快的反应，你可以给我们一个电话，每天 9 小时，每周 5 天。电话: 400 -660 -8680

与技术支持沟通

如需技术支持，请通过 mes@zohocorp.com.cn 联系我们。

请在您的电子邮件中包含以下细节，以使我们可以更好地帮助您:

- 产品版本(免费版、试用版、标准版)
- 产品构建号

- 问题的简要描述

您也可以和我们的技术支持团队联系，我们的技术支持团队每周 5 天，每天 9 小时，电话:400 -660 -8680。

联系产品内部的技术支持

DataSecurity Plus 支持标签中提供了联系我们的方式，包括:

- **请求支持:** 在线提交您的技术问题。
- **需求功能:** 请求 DataSecurity Plus 新功能。
- **用户论坛:** 与其他 DataSecurity Plus 用户的讨论。
- **在线聊天:** 及时回答问题。