Zeus DLP System（宙斯数据防泄露系统）产品介绍

概念和术语：

- *敏感文件*，根据策略设置哪些文件是需要被保护的文件，一旦设置，只有**可信进程**可以正常查看和修改文件内容
- *敏感区域*，指在同一个系统内部，**敏感文件**可以在哪些计算机系统之间流转
- *可信进程* ，被选定为可以打开和访问敏感文件的进程
- *非可信进程*，与可信进程相反
- *明文外泄*，即当可信进程打开敏感文件之后，通过另存为，剪贴板，临时文件，静默复制等方式直接泄露明文内容的方式
- *密级*，衡量用户保密等级的高低，一般情况下，等级高的用户创建的文件在被等级较低的用户访问时会应用不同的访问策略
- **文件加敏**，指的是将原本是明文内容的文件加密，成为保密系统的一部分，可信进程可以查看和修改该文件
- **文件脱敏**，指的是将原本加密的敏感文件解密，使其脱离保密系统，成为任意进程可访问和修改的文件

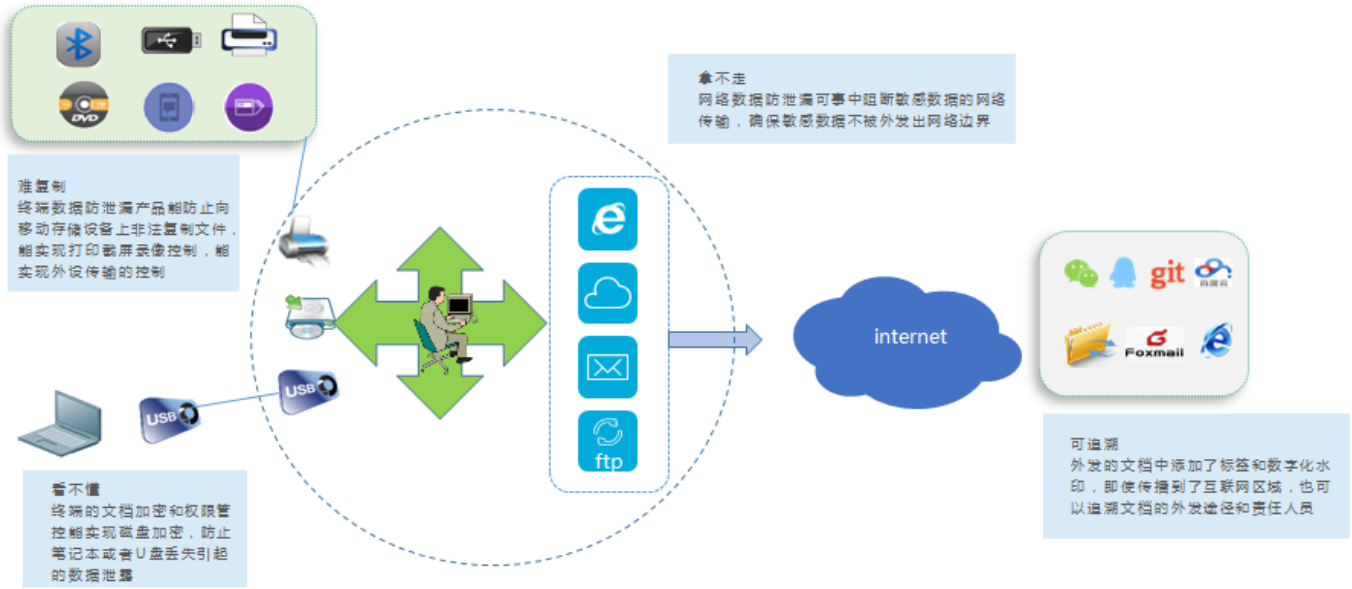
本产品适用场景:

- 有保密需求的企业或者个人终端计算机
- 有保密需求的政府职能部门
- 其它有保密需求的场景

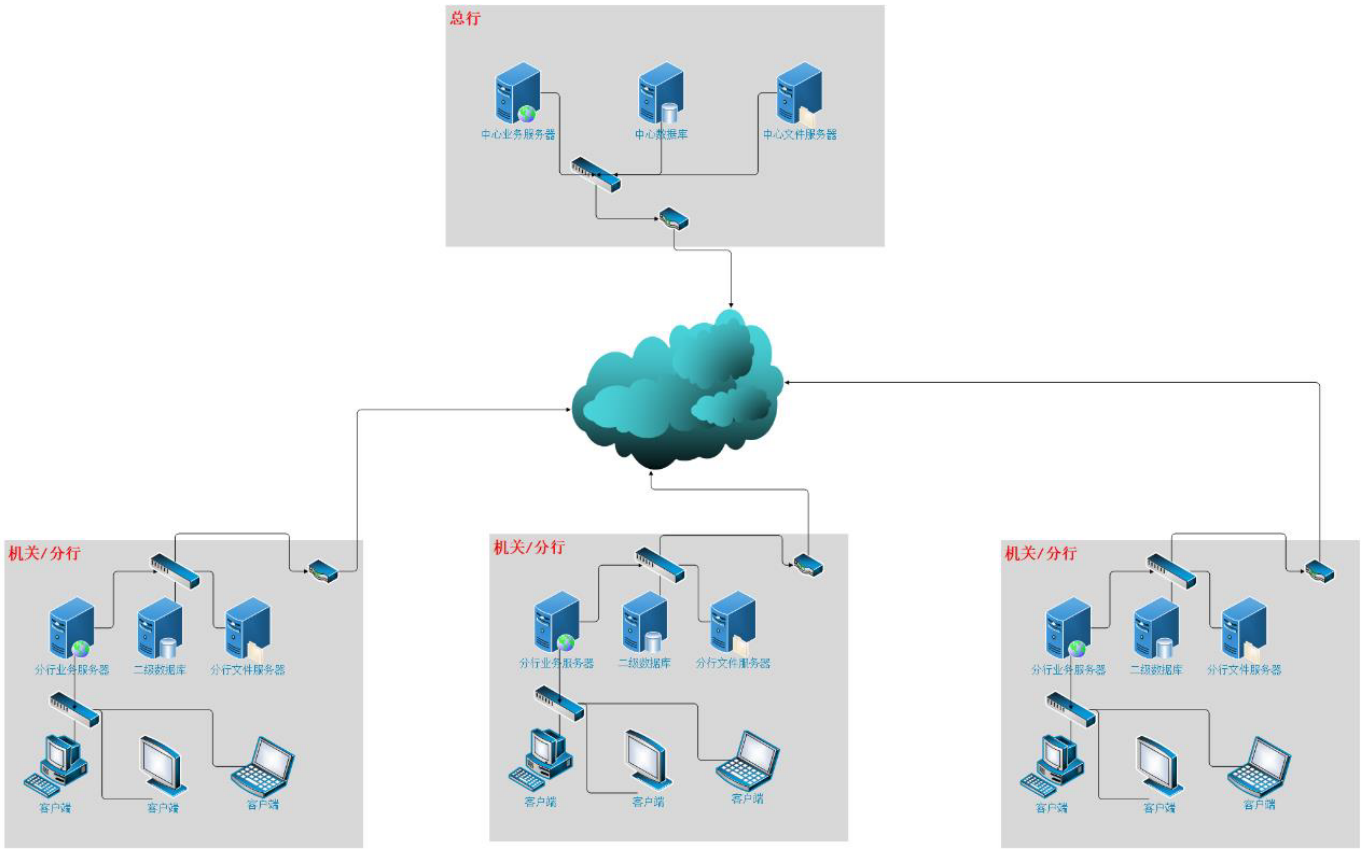
产品价值

终端数据防泄漏产品 主要解决通过移动存储设备非法复制数据、通过外设违 规传输数据，通过截屏拍照录像打印泄露敏感数据的问题。终端 DLP 还能对文档 权限进行控制从而解决磁盘加密和明文外带等问题。 终端数据防泄漏产品主要实 现对终端电脑上的敏感数据的发现、管控和外发保护，主要包括外设管控、移动 存储管理、全盘扫描、数据操作审计、水印管理和资产审计等功能

终端数据防泄漏产品效果示意图



终端数据防泄漏产品架构示意图



产品功能

策略控制

针对计算机上不同的程序访问不同的文件定制权限控制策略，灵活多变，*亦可针对不同的用户控制相关的文件访问权*(可定制)

优势：

- 可以设置不允许微软的Word应用程序打开敏感文件(如: "绝密.docx")，但是允许国产应用WPS打开
- 可以设置微软的Office套件禁止访问某些敏感文件(如："D:\保密资料\绝密.docx")
- 可以阻止本地计算机运行某些程序
- 可以禁止某些用户或者进程删除某些文件(文件防删除)
- 可以对某些进程或者用户隐藏某些文件或者文件夹
- 可以重定向对某些文件的访问，例如用户访问文件A，实则看到的是文件B的内容
- 可以禁止某些用户或者进程对某些文件的访问，当访问发生时，将提示用户一个错误信息
- 可以控制敏感文件向非敏感区域的转移
- ....

策略设置可灵活多变，根据不同的应用场景自行选择，也可以将策略服务器部署在内网(可定制)

特点：

- 支持持久化存储，即当策略应用之后，所有的涉密计算机在下次重启会自动应用上次设定的策略
- 支持在运行时修改，例如可以按需求在系统运行时进行策略的增加，删除，修改，查询

- 支持热加载，即客户端程序在接受管理员新下发的策略之后可以立即应用到当前系统中而无需重启电脑，即时生效

视图隔离

可信进程与非可信的进程采用不同的文件视图，可信进程打开和访问敏感文件时展示明文视图，非可信进程打开文件时展示密文视图

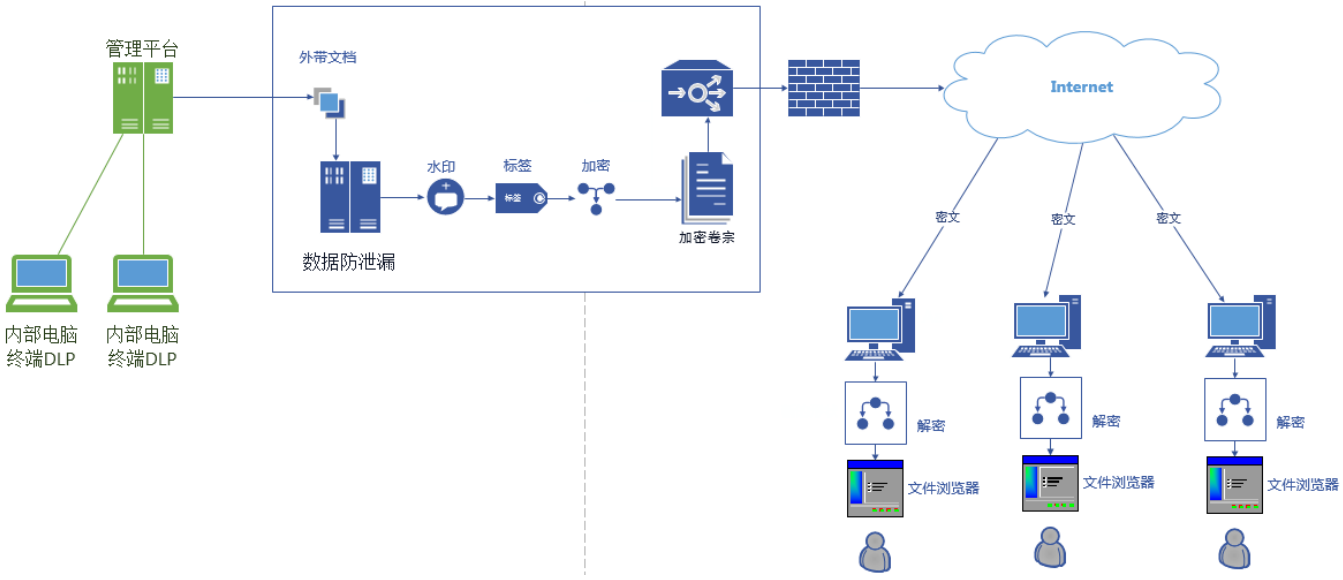
此外：亦可根据用户需求设定访问同一个文件时不同的用户看到的是不同的文件内容或者文件版本(可定制)

透明加解密

- 该过程对用户完全透明，在涉密计算机上，敏感文件可以从受信区域向外部(网盘或者其它形式的共享服务器)转移，转移之后的文件依然是加密状态，敏感文件亦可以完全相反的方向转移，并自动加密(可设置策略)
- 明文外泄阻止，当可信进程打开敏感文件之后，通过另存为保存到一个非敏感区域(或者非敏感文件形式)，目标文件将会根据策略自动加密
- 支持CIFS文件系统的文件透明加解密，即用户可以打开一个远程文件，或查看或编辑，文件内容在远程服务器上会自动加密
- 支持USB可移动设备外泄管理，当敏感文件从内部敏感区域转移到可移动USB外设(或移动硬盘)上时，可以根据策略自行选择是否允许该操作，另外：非可信进程转移文件时文件永远是密文状态，如果是可信进程可以根据策略选择自动加密
- 可信USB设备管理，即授权在敏感区域内，哪些USB设备是可以被用来转移内部敏感文件的(可定制)
- 支持文件密级，即拥有完全不同的密级的用户创建的文件，密级等级高的用户创建的文件将不能正常被密级较低的用户查看或者修改

明文外泄示意图:

USB设备外发管控示意图：



敏感文件加固

对于涉密的敏感文件进行加固

- 防止外部人员通过技术手段将密文数据暴破或者解密
- 防止外部人员通过技术手段攻破文件密级控制，从而绕过安全检查访问密级较高用户创建的敏感文件

插件

插件功能主要用于当核心功能管控不到的范围，例如剪贴板明文外泄 当配置插件之后，在默认情况下，用户将无法通过剪贴板将保密文件的明文内容直接复制到外部

插件支持热加载，当管理员通过配置不同的插件版本或者新增插件的功能时，可通过下发策略的方式将插件下发到涉密计算机，当下次用户重新打开相应的程序时，新版本的插件将自动应用到系统中，即时生效

说明：

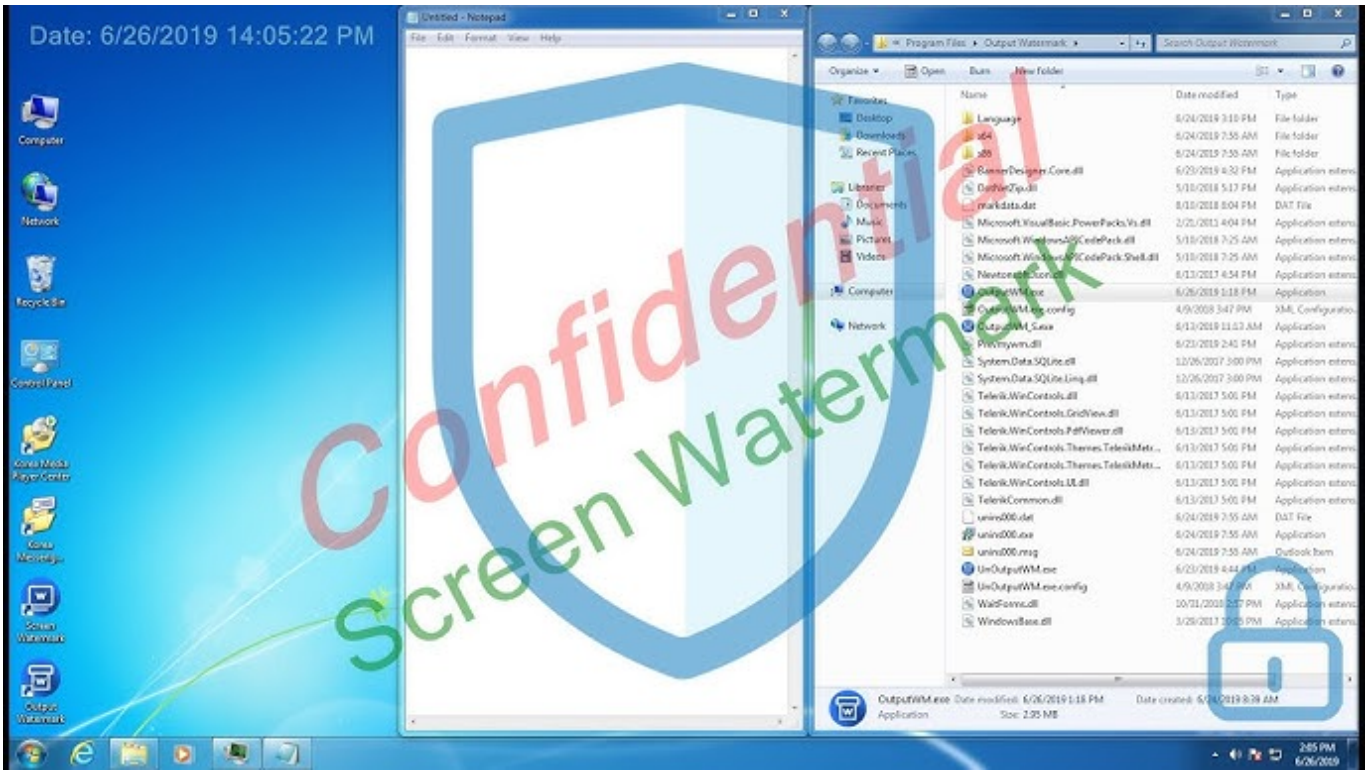
- 插件可用于配置灵活多变的定制需求场景，本产品的演示视频中权对剪贴板明文外泄做了演示
- 插件的很多功能需要根据企业需求定制开发，但是本产品的插件设计十分完备，能应对大多数系统需求

屏幕水印

屏幕水印功能用于涉密计算机上，可将水印(文字或者图片形式)叠加到屏幕的任意区域上，标明该涉密计算机的立场的同时也能防止用户通过手机拍照等摄像摄影的方式外泄敏感数据

说明： 如需其它水印功能，则可以根据需求定制

屏幕水印效果图



文件加敏和脱敏

- 文件加敏，可以使用客户端对某些非敏感文件进行加密保护，成为保密系统中的一部分，只能在保密系统内部流转和使用s

- 文件脱敏，将文件解密，文件不再拥有敏感属性，可以供外部非敏感区域使用

审计

对敏感文件的访问以及操作(读，写，外发，由于策略设置造成的访问失败等)，转移，明文外泄等事件进行记录

通过**插件**也能实现更多的审计功能

产品优势

灵活弹性的策略控制

策略控制是DLP系统中非常重要的一环，因此策略是否够灵活以及弹性空间是否充足是衡量一个策略系统是否能应对多变的需求环境的重要指标

传统的DLP系统策略权能够应对有限的策略控制，即只能控制有限范围内的可信进程访问敏感文件的场景

而本产品则能支持非常灵活多变的文件访问控制策略(详见**策略控制**章节)，可以控制任意进程(用户)访问任意文件时的权限控制，权限控制单元则非常灵活，通过配置策略规则可以满足非常多的需求场景，真正实现一套策略，单侧部署，多处使用

内核态的明文外泄控制

一般来说市面上很多产品采用的是用户层的明文外泄管控，这类产品通常需要采用目标注入的方式挂接模块到目标进程中实现相关功能

由于目标软件可能经常性更新，这导致产品的功能模块也需要经常性更新，无形之中也增加了系统维护成本，而且故障率也相对较高

本产品采用的是内核级的明文外泄管控措施，可以完美解决文件另存为，可信进程复制文件到其它非敏感区域的明文外泄问题，此功能不需要任何其它外部措施就可以正常工作

事实上该功能也是通过策略配置的，所以很多看似复杂的功能全部通过策略去做成可配置化，大大减轻了产品端和维护端的压力

同时内核级的防护也提升了对抗难度，有效缓解了"有经验的技术人员"通过常规技术手段试图绕过明文外泄安全检查的窘境

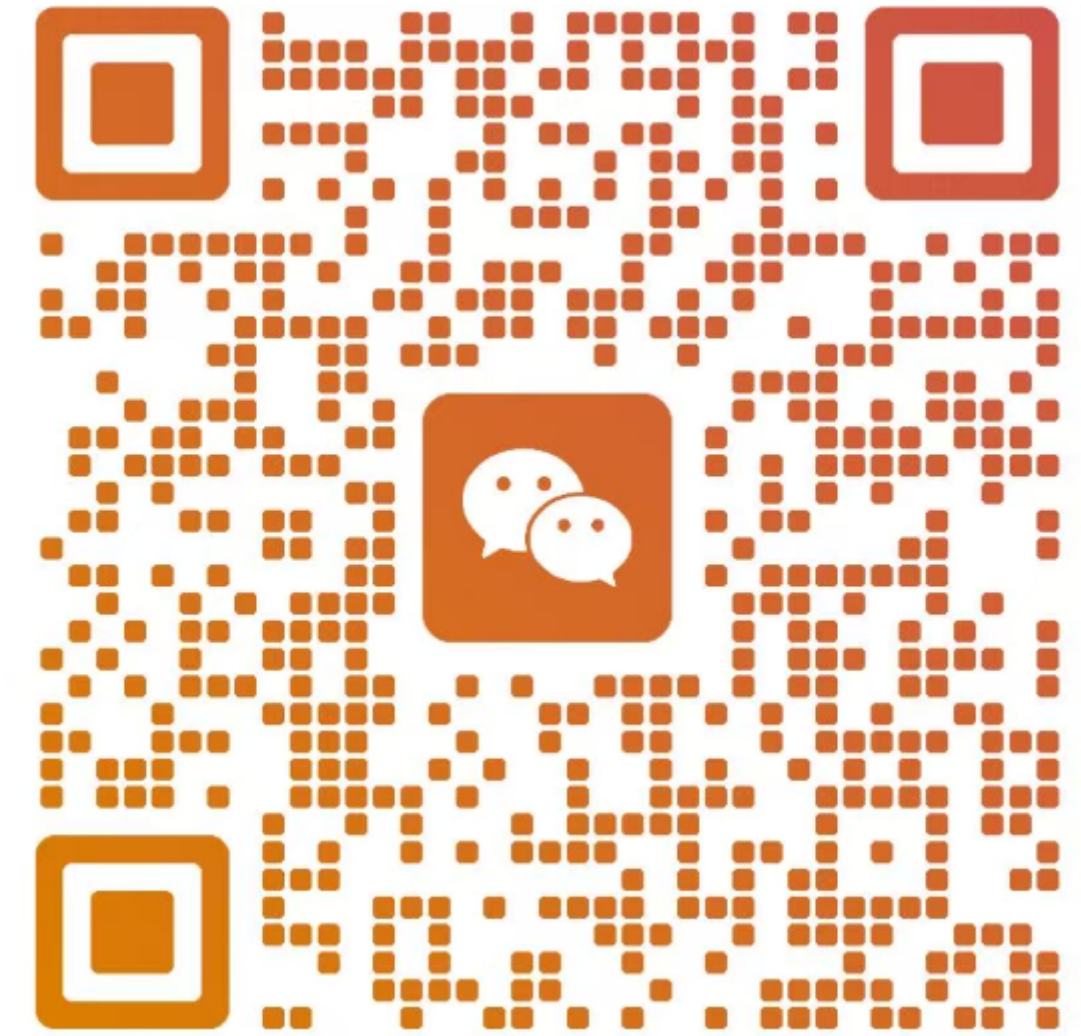
由于很多软件都会创建一些临时文件，传统DLP系统往往会直接忽视这些文件，从而造成临时文件的**明文外泄**，基于这个因素的考量，该功能也会对一些软件创建的临时文件进行检测和加密(如果有必要)，以防止该形式的**明文外泄**

演示视频

→ 观看链接(点击链接观看)

商务合作

WX: @bigcat9668 Email: microcoolibm@163.com



其它

- 本产品截止目前，本产品具备上述所有功能，其中标有“可定制”的部分具备基本功能框架，需要根据企业需求定制