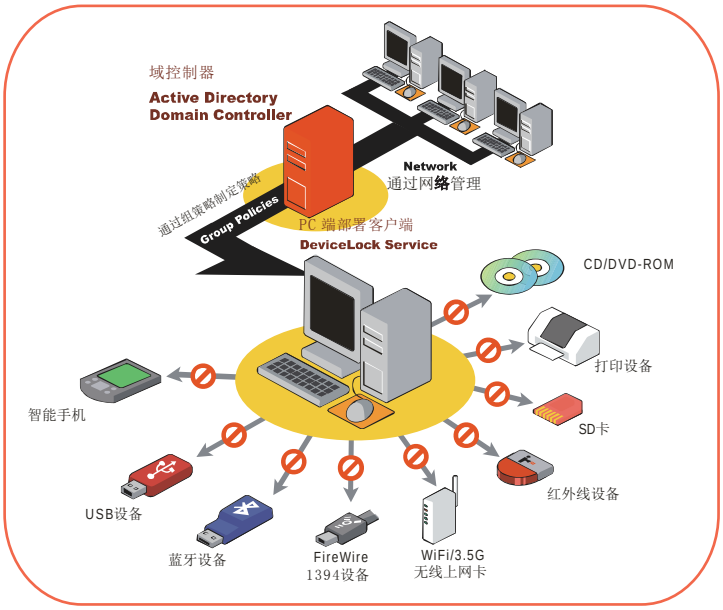
DeviceLock®

Proactive Network Security

便携式储存设备是資料外洩防護上最大的安全漏洞？使用DeviceLock®立即關閉它！

DeviceLock®是定位与终端资料外泄防护(Endpoint DLP)的简单好用工具。它可以阻止非授权用户存取USB、蓝牙、WiFi，以及其他随插即用（Plug and Play）的设备，以保护企业网络安全与无形资产。通过策略指派可以完全地控管哪些用户（Users）、何时（When）以及如何（How）才能在企业网内使用便携式存放设备。



▲ DeviceLock®支援多种设备管理

DeviceLock®為系統管理者提供以下功能：

- 通过中央管理平台，依用户、用户组、时段，控管外设与连接端口的存取策略。
- 根据类别（例如：便携式存储外设、光驱）或连接端口（例如：USB、蓝牙、红外线）设定存取权限，不影响如键盘、鼠标等合法设备使用。
- 针对存储设备，通过只读(Read Only)的策略設定，可以让U盘、外接硬盘或刻录机变成只读，禁止电脑的資料复制出去。
- 对外接的使用进行记录并集中储存。亦可针对允许使用的人员，将其外存的文档留档到服务器，以利审计。

为什么需要建置端点数据外泄防护?

组织若不对资料外泄的风险加以控管，可能面临的是名誉损失甚至于法律责任与经济赔偿。而资料以外泄事件中(包含无心的过失及恶意的外泄)超过80%是由于组织内部的员工导致。因此除了针对恶意软件的防护措施之外，针对电脑的各种便携式存放设备也应当实施适度的管控，以降低资料外泄的风险。

如同研究机构Gartner在其「如何解决便携式存储设备的安全威胁」研究报告中指出：「漠视便携式存放设备的非授权与不受控管的滥用，正促使企业逐渐将本身暴露在安全风险之中」。目前新的外設不断推出，包括智能手机3.5G/WiMax网卡、大容量U盘、硬盘、存储卡、刻录机等都很容易获得，且存储容量不断创造高峰，也对企业的资料外泄防护上带来莫大的挑战。

DeviceLock

与AD&组策略无缝整合

DeviceLock应用于使用AD域环境中，可以通过组策略(Group Policy)集中配置、存储与同步策略内容。与企业中暨有的网域采用相同的管理方法，可以大幅减少管理时间与降低学习成本。

灵活且细致的存取控管策略

存取策略可按用户、用户组来配置，亦可对特定的计算机中所有用户(Everyone)，或者本机的账号配置对应的权限。可按相应设备类型制定策略，并对USB设备进行分类，实现USB 设备的分类控管。策略的内容支持除按时段、每周工作日区别之外，还可针对存储设备配置只读的策略，使企业数据无法写出至非授权的设备中。

真实文件格式管控

支持依据档案的真正格式制定允许或禁止传输的策略，使用户不能通过篡改文件后缀名来规避策略。您可以禁止如CAD、PSD等设计图文件，输出到计算机外部DeviceLock目前支持超过3000种格式特征数据库。

iPhone等智能手机的数据外泄防护

通过DeviceLock，您可控管个人的智能手机(iPhone、Blackberry、Windows Mobile)接到计算机时，日历、邮件、工作、记事本还是图片或其他文件，哪些内容可以传输或同步或哪些行为是禁止的。DeviceLock可以识别通过USB、蓝牙、串口或红外线连接的设备。

USB设备白名单

可以针对特定的设备型号、设备序号(DeviceID)进行允许或禁止。USB设备的生产厂商会按照其取得DeviceID。常见的应用是单位内仅允许经过申请的特定设备才能存取，其它设备一律禁止。制定时可针对产品编号整批开放，或者是针对唯一设备序号进行放行。

媒体白名单Media White List

可针对特定的DVD/CD-ROM光盘片建立特定的媒体指纹，并且设定仅有特定的指纹才能使用。一旦光盘中的内容变更，则其指纹就会不同。常见的应用是在一些开放的数据查询计算机上，如图书馆、公共展示机等，要锁定仅能使用特定数据的光盘，甚至锁住光盘弹出按钮，避免被未经授权的用户更换。

暂时白名单Temporary White List

针对出差在外又临时需要使用外部存储设备，可以通过电话/电子邮件向相关管理员申请临时性的权限。操作时须由用户先回报计算机上显示的设备序号，管理员据此产生一个临时性开放码。该开放码可以指定放行的分钟数，或直到设备拔除。中间的沟通可通过电话完成，而开放期间的使用行为也可留下审计纪录。

完整设备使用审计纪录Audit Log

提供设备使用情况的完整审计记录。记录内容包含事件时间、设备类别、执行动作、执行人身分、当时的程序(Process)。审计记录以操作系统日志(Event Log)格式存于客户端计算机，也可配置自动传回到服务器，以便后面做报表与审计。

提供外存文件留档(Shadowing)

文件留档功能可以针对允许使用外接设备的人员，将其外存的所有文件复制、存档一份到服务器中，以方便审计外存文件的所有内容。当设备不在内部网络时，文件留档的数据会暂存于客户端，待回到内网后在后台将隐藏于客户端的留档文件移动到服务器中。

防破坏机制的设计

客户端程序设计了一系列防破坏措施保护本身不被用户破坏。保护措施包含服务无法被用户任意停用，后台程序无法被暴力停止，即使拥有本机管理员权限也无法破坏。系统可以指定特定DeviceLock管理员账号，只有管理员才能进行相关的维护与管理操作。

加密软件整合应用

DeviceLock可以识别经过加密的PGP、TrueCrypt与DriveCrypt磁盘(含U盘等各种便携式存储设备)。可以在策略指定唯有外接设备是加密的情况下，才准许写出文件，如果接入的是未加密的U盘，则仅能只读，以符合企业的安全策略。

内、外网的策略差异化

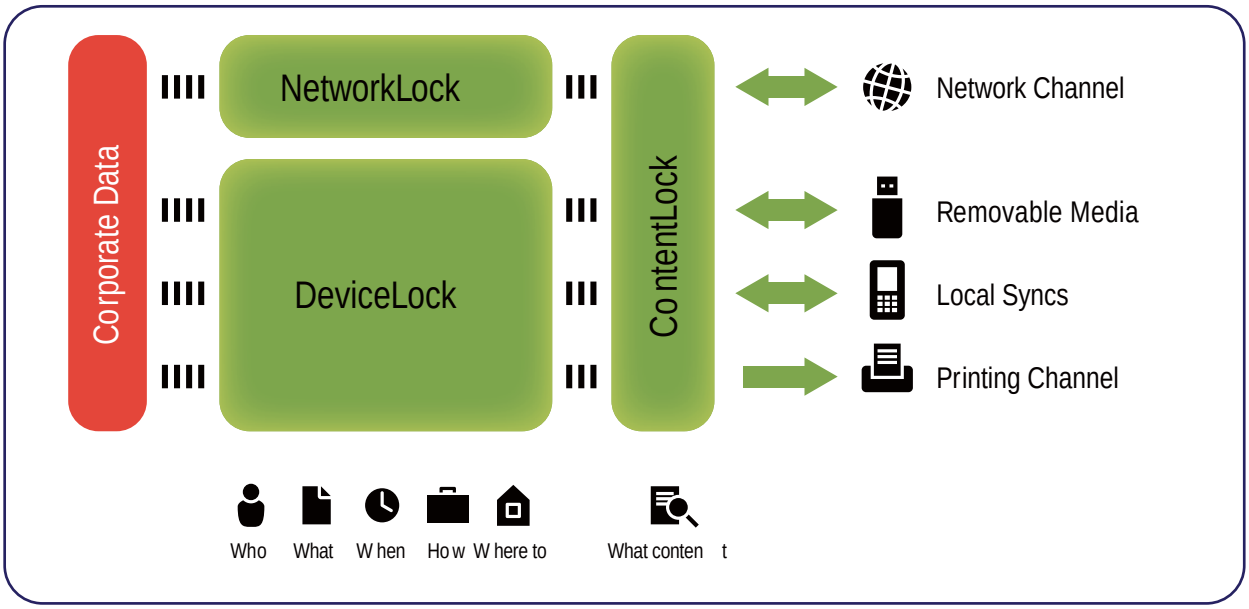
DeviceLock提供内外网感知能力，以制定当终端位于内部网络或外部网络时可以分别适用不同的策略。例如，当终端的有线网络接到内网时就禁止使用WiFi无线网络机，以避免有线、无线桥接带来的风险。

DeviceLock

更多延伸功能

防键盘记录Anti-keylogger功能

可以侦测用户的计算机键盘是否被偷偷串接硬件式键盘记录设备。DeviceLock侦测到有这些设备存在时，会通过特有技术欺骗PS/2接口的键盘输入信号，使得其记录到的指是一串无意义的乱码。



Network-Lock 功能 （选购）

针对终端的网络传输通讯进行检查，并执行策略。该功能可以识别HTTP、 FTP、IM (ICQ/AOL、 MSN Messenger、 Jabber、 IRC、Yahoo! Messenge...)、加密的HTTPS、 FTP-SSL 等通讯协议，可以依据这些协议中传送的内容、文件格式实施放行或阻挡的策略。也可对这些信道传送的信息，进行信息重组与记录。

Content-Lock 功能 （选购）

Content-Lock模块可以设定内容感知相关的策略，以杜绝个人资料与敏感信息的外泄。「内容感知规则」的设定，不仅预设提供的真实文件格式识别，还可以依据关键词、正则表达式(Regular Expression)等，以识别出诸如身份证号码、地址、手机号码、固定电话等个人资料信息。

DeviceLock服务监控

通过布署DeviceLock Enterprise Server，可以监控分散在个人计算机端客户端程序的运作状况，并进行集中记录与统计。

权限报表功能

协助您可以对内部各计算机的DeviceLock权限进行盘点与报表功能，以达到审计目的。

回传数据流量优化与压缩

针对审计纪录与文件留档的数据收集操作，可以制定带宽使用限制，并可对收集的数据流自动压缩，以降低网络负载，减少大量数据回传时所造成的网络冲击。当布署多部数据回收主机的情况下，可自动选择优化的回传路径。

Search Server模块

Search Server模块提供针对DeviceLock Enterprise Server收回的留档文件，进行「全文检索」方式的审计。它可以对常用的文件格式中文字内容进行检索查询。这些格式包含：Adobe Acrobat (PDF)、Ami Pro、压缩文件案(GZIP、RAR、 ZIP)、Lotus 1-2-3、 Microsoft Access、Microsoft Excel、Microsoft PowerPoint、 Microsoft Word、Microsoft Works、OpenOffice (documents、 spreadsheets and presentations)， 以及其他常用格式。

报表模块(选购)

网页式DeviceLock记录报表，让管理员可以通过网页界面，查询与调阅这些外围与文件的存取记录。提供依计算机、用户账号、存取动作、事件种类、日期时间等进行不同角度进行报表审计。管理员除了直接用浏览器浏览报表之外，还可以自定义周期性报表，自动通过电子邮件寄送报表内容。

DeviceLock®可以为企业与组织提供完善的外设安全控管解决方案，具备完整的外设支持、可灵活制定权限策略，同时具备大企业与小网络均适用的管理架构，并且可以支持AD与Group Policy的管理策略指派，授权模式灵活。

提供灵活多种部署方式

部署DeviceLock®时，可以通过以下不同的方式来进行：

- 通过管理接口针对内网的计算机单一或批次进行推送
- 通过AD Group Policy(组策略)进行软件推送
- 支持微软 SMS 集中布署(提供 msi 安装程序)
- 通过域 Logon Script 自动化安装
- 单机通过安装程序逐一安装

完整外接外设管控支持

凭借DeviceLock®，管理者可以制定策略阻挡非授权用户使用各种外设。DeviceLock®支持针对「设备接口(Ports)」、「设备类别(Device Types)」以及「设备序号(Device ID)」进行三个层级的管控。

设备類別 Device Types

- 软驱 Floppies
- 光驱 CD-ROMs/DVDs
- 硬盘 Hard Drives
- 磁带机 Tape Devices
- 蓝牙Bluetooth
- 无线网卡 WiFi Adapters
- 便携式存储设备
  例如：U盘、外接硬盘、记忆卡、MO光盘…等
- 智能手机
  例如：iPhone, Windows Mobile, BlackBerry & Palm OS设备
- 打印设备 包含：本地，网络，虚拟打印机

Ports

- USB
- FireWire (1394)
- 红外线 Infrared
- 串口(COM) & 并口(LPT)

加密设备的整合

- PGP Whole Disk
- TrueCrypt
- BitLocker To Go (BL2G)
- DriveCrypt(BL2G)
- Lexar® JumpDrive SAFE
- Lexar® SAFE

如需试用 DeviceLock或是更多的详细信息，请登录 www.docutek.com.cn

布署环境需求

DeviceLock 可以布署于下列环境：

安装NT/2000/XP/2003/Vista/2008/7支持32-bit以及64-bit的平台上。

内存需求：64MB (含)以上

硬盘空间需求：25MB

Designed for Microsoft® Windows®XP Windows®2000 Windows NT®

代理商

内网安控信·息·安·全·管·理·的·极·致·延·伸
Own Your IT Governance From Managing Insder Security Threats.
docutek达友科技

上海公司. Shanghai Office.
上海市徐汇区漕宝路80号803室
TEL : 86-21-6440-3373 FAX : 86-21-6440-3372
http://www.docutek.com.cn

经销商