



如何防止设计图纸、程序源代码等机密信息
等泄露给竞争对手

如何防止员工离职时擅自拷贝
带走机密资料

如何保护企业机密电子
文档资料的安全

NTA

文档保密解决方案

NTA

目录

现状分析	1
电子文档保密的迫切性.....	1
企业面临的两难处境.....	1
确保电子文档保密、构建安全、高效的文档访问平台.....	1
NTA文档保密解决方案	2
NTA安全应用网关.....	2
NTA文档管理系统.....	3
方案简述.....	3
独立的NTA机密文档中心方案.....	3
以NTA为核心的企业综合信息安全平台.....	4
方案特点	5
高安全性.....	5
高可用性.....	5
易扩展性.....	5
实施简单.....	5
NTA方案相对文件加密方案的优势	6
安全性高.....	6
实施简单、管理容易.....	6
兼容性好.....	6
NTA典型用户案例分析	7
H通信技术公司.....	7
S微电子有限公司.....	8

现状分析

电子文档保密的迫切性

知识经济时代，企业的核心竞争力将更多地来自于技术发明、专利、创新等“软资产”，随着信息系统应用的普及，这些“软资产”体现为大量的电子文档。在日常工作中，需要数十甚至数百位员工协同工作，不可避免地需要涉及机密电子文档，如何很好地保护这些重要资料，成为摆在企业面前的一个难题。

调查结果显示，68%的企业每年发生6起敏感数据丢失事件；20%的企业每年发生22起以上电子文件泄密事件；75%的泄密源自内部雇员故意所为；每次电子文件泄密所造成的损失平均是50万美元。在以往的企业泄密案件中，由于取证困难，以及现有法律的局限，企业的损失往往是巨大而无法挽回的。

在内部人员故意的泄密行为面前，企业网络中的防火墙、入侵检测以及各种文件加密等技术手段均不能起到真正的防范作用。通过寻求更加完善的技术手段保护机密电子文档，是企业必然的选择。

企业面临的两难处境

虽然企业可以通过各种规章制度和一些技术手段对机密电子文档进行管理，但是传统的安全措施和技术手段无法消

除企业机密电子文档泄漏的隐患。与此同时不可避免地因为安全原因，导致工作效率下降以及公司资源浪费，不利于有效利用现有文档和部门间的协同工作。企业在权衡文档保密与有效利用文档这两种相互矛盾的需求时面临两难处境。

- * 一方面，员工需要使用企业的机密文档；
另一方面，企业需要保护这些机密文档的安全
- * 一方面，员工需要通过使用互联网检索资料，获取信息；
另一方面，互联网的使用却严重地威胁着企业机密文档的安全
- * 一方面，企业需要将存储机密文档的设备进行隔离保护；
另一方面，员工需要随时便捷地访问这些文档

确保电子文档保密 构建安全、高效的文档访问平台

由于根本的文档保密问题没有得到有效解决，限制了企业构建安全高效的文档访问平台。员工无法有效利用企业大量的现有资料，造成很多宝贵的文档只能零散保存，无法共享，成为“死档”。

企业一方面需要完善各种保密制度，利用法律、法规保护自己的专有信息，同时一定要利用切实可行的技术手段从根本上防止泄密事件的发生。企业需要一套文档保密的“硬办法”，不仅要避免文件载体丢失导致的泄密事件，更要防范内部人员的恶意泄密行为。

NTA文档保密解决方案

NTA-DS（基于NTA安全应用网关和NTA文档管理系统）是一套为企业提供机密电子文档保密和有效管理的整体解决方案。NTA-DS采用机密电子文档集中存储、统一管理、用户权限控制的方式，将机密文档集中保存在文档中心并与客户端设备完全隔离，使授权用户可以在权限范围内正常使用，但无法以任何形式复制到客户端设备，从根本上杜绝了机密文档的泄漏，保护企业的核心竞争力。

NTA安全应用网关

NTA安全应用网关，作为一个单独的硬件设备，在不修改应用软件的前提下，把各种平台上的应用（MS Office、Lotus Notes、AutoCAD、Acrobat、PDM、EDA……）以web的方式发布给授权用户，无须对企业现有系统进行大规模改造。在使用过程中NTA只传输经过压缩和加密的键盘鼠标操作信息和屏幕的变化信息，不向客户端传输任何机密文档的实际内容，仅“展示”给用户机密文档的屏幕图像，而用户所有的使用及操作均集中于被隔离的文档服务器上，所有的数据交换亦在被隔离的内部网络中，这也就意味着在整个工作流程中，使用者的PC机和文档服务器没有直接的网络连接，也没有任何真实数据被下载到

客户端的设备上，从根本上保证机密电子文档的安全。



NTA采用瘦客户访问技术，对网络带宽占用非常少，客户端仅需要8~10K的带宽即可建立连接，同时所有的数据交换均经过128位SSL加密，我们甚至可以将这些应用系统安全地发布到互联网上。NTA安全应用网关将有效地解决企业对机密文档、敏感信息等的安全性需求。

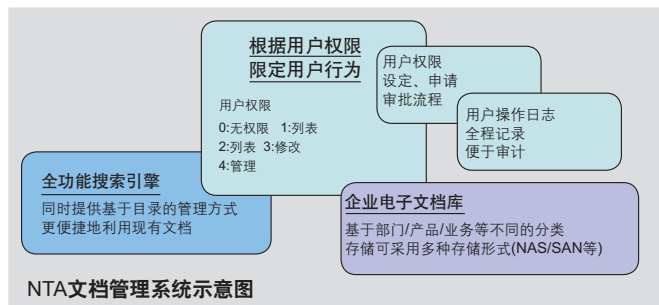
客户端可以被管理或禁止的操作包括：

- * 机密电子文档不会以任何形式（硬盘、内存等）保存在客户端设备上，用户无法以任何形式将机密电子文档复制到客户端的其他存储设备上，包括硬盘存储、软盘存储、光盘存储、U盘存储以及其他客户端存储设备。
- * 可以管理或禁止客户端对机密电子文档的各种输出操作，包括打印、文档编辑中的复制/粘贴、屏幕拷贝等。

NTA安全应用网关支持多种第三方身份认证方式，可以配合企业各种的应用系统，构建安全、灵活、适应性强的应用访问平台，既满足保密需求，同时满足业务需求。

NTA文档管理系统

NTA文档管理系统软件帮助企业建立全面的文档管理与授权机制平台，用户可以对授权的文件与信息进行快速的查找、阅读与编辑，有效解决企业文档版本多、查找不方便甚至丢失等一系列问题，提高工作效率。配合NTA安全应用网关，构建全面的企业机密电子文档中心，在充分保障机密电子文档安全的前提下，提高文档的使用效率。



根据用户权限限定用户行为：系统以文件或文件夹为基本单元向用户分配操作权限，只有拥有相应权限的用户才能执行对应的操作。用户权限细分为：无权限（用户根本无法看到或搜索到该文件）、列表（只能看到或搜索到文件名）、读取（用户可以读取到文件的内容）、修改（用户可以对文件进行修改）、管理（用户可以对文件进行授权），这些权限均可以做出时间期限的规定并随时动态调整。

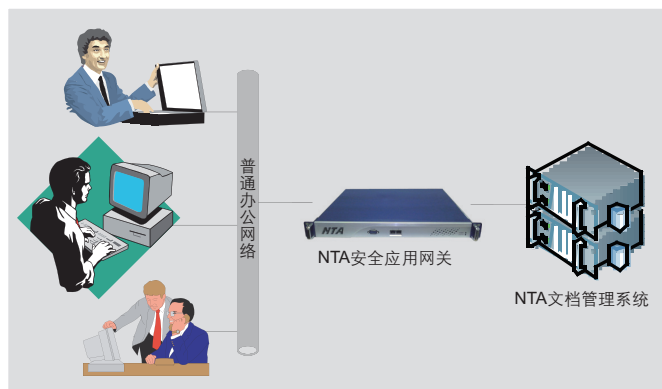
全功能搜索引擎：为用户提供基于目录和搜索引擎的检索方式，提供高效的文档查阅工具，盘活企业现有文档资源，促进内部协作和创新。

用户操作日志：自动记录每个用户的重要操作，包括文档操作，账户操作，权限修改操作等。日志记录可以在线查看。

方案简述

独立的NTA机密文档中心方案

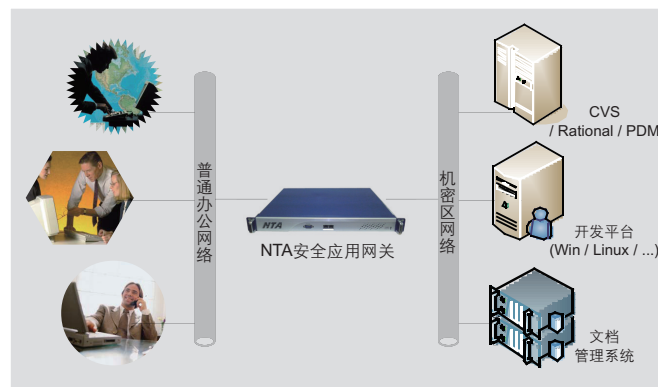
独立的NTA机密文档中心方案采用机密电子文档集中存储、统一管理、用户访问权限控制的方式，将机密电子文档集中保存在机密文件服务器上，通过NTA文档管理系统管理机密文件，用户通过访问NTA设备的方式得到对机密文件的访问授权，得到授权的用户在访问机密文件的全过程中，这些文件不会以任何形式存在于用户使用的PC机的内存或硬盘中，从而彻底防止了机密文件的泄密可能。



以NTA为核心的企业综合信息安全平台

NTA综合信息安全平台以NTA安全应用网关为核心，建立网络机密区，将应用系统集中部署在严密保护的服务器上，通过NTA网关授权用户使用，从根本上杜绝机密信息

的泄漏途径，达到既保护企业机密信息，又不影响工作效率的目的。NTA文档保密解决方案可以配合企业现有应用系统，构建企业的综合信息安全平台。



在本方案中，涉密的应用系统（包括开发工具，PDM、文档阅读和管理工具、版本控制系统等）和机密文件集中部署在机密区网络，机密区的应用系统和文档服务器与外部网络完全隔离，只通过NTA安全应用网关发布应用系统的操作界面。所有授权用户登陆NTA安全应用网关，使用权限范围内的各种系统和工具、根据授权，浏览或修改机密文档，访问应用系统，所有的操作都集中在服务器端，客户端任何对文档的输出、拷贝等行为均被禁止，使用者不能将机密文档本身或者内容复制到客户端的任何设备上。将现在的应用系统纳入统一的NTA信息安全平台，在兼顾高安全性同时又不妨碍员工进行正常的工作。

方案特点

高安全性

NTA文档保密方案是一个综合的文档安全解决方案，能够实现任何终端设备与文档服务器的网络隔离，有效杜绝各种文档泄漏的可能性。它集成了企业内部的安全需求，如集中的文档管理、有效的数据传输控制、客户端不留下任何信息等。它可以灵活地放置在内网、DMZ区，甚至直接与互联网连接。NTA与客户端的连接均通过128位的SSL加密，在整个使用过程中不会在客户端残留任何临时文件。认证系统可以与企业现有认证系统结合，确保信息资料的安全，为企业提供一个整体的文档安全解决方案。

NTA文档保密方案可以完全实现企业实施文档保密的最核心目的（防止内部员工的故意泄密行为），从根本上保证了机密电子文档的安全。NTA文档管理系统，可以定义用户对于机密文档或文件夹的权限，包括无权限（无法看到或搜索到该文件）、列表（只能看到或搜索到文件名）、读取（可以读取到文件的内容）、修改（可以对文件进行修改）、管理（可以对文件进行授权），这些权限均可以做出时间期限的规定并随时动态调整。

高可用性

NTA方案在保证高安全性的同时，不影响授权用户的正常使用，广泛地配合企业现有应用系统，可以最大限度保持原有的使用和操作习惯；可以同时适用于各种软硬件环境，可以同时适用于各种类型的文档，可以同时适用于内部使用和外部使用；NTA安全应用网关支持7x24不间断的工作模式。

易扩展性

NTA方案无论从网络布局还是硬件配置均为企业将来的扩展留有充分的余地，为各种其他应用需求提供了方便的平台；NTA方案同时支持各种服务器操作系统平台和各种客户端设备，确保整个系统的可持续发展。

实施简单

NTA方案能快速实施并投入使用，效果立竿见影。

NTA方案相对文件加密方案的优势

安全性高

NTA方案的应用领域主要是防止内部人员的故意泄密行为，机密电子文档集中存放、统一管理，文档不被下载、保存在客户端PC机上，安全性高。

文件加密技术仅适用于防止载体（U盘、硬盘、光盘等）丢失或文件传送过程中产生的泄密可能。文件虽被加密，但最终仍然被下载、存放在客户端PC机中，不适用于防止内部人员的故意泄密行为（在得到阅读权限的客户端PC机内，被加密的文件一定会被以某种形式解密成明文，故意者就有办法将明文读取出来保存，达到窃密的目的）。

实施简单、管理容易

NTA方案是数据、应用系统大集中方案，对数以百（千）计的客户端没有实施要求，可以做到以点代面，迅速实施和推广。

文件加密技术方案是客户机/服务器模式，实施复杂，需要维护大量的客户端系统，同时，安装的客户端系统容易与客户端的系统、应用软件、杀病毒软件等等发生冲突，需要考虑与各种不同版本软件的兼容性，非常难与实施和维护，不利于项目的推广和应用。

兼容性好

NTA可以配合现有的和未来的任何软件或应用系统（如：CRM /ERP/等系统），文件加密系统只能对一些独立的文件加密，很难配合大型的应用系统。

NTA典型用户案例分析

H通信技术公司

业务类型：通讯、网络设备研发、制造。

主要产品：网络产品（路由器、交换机、EPON、无线局域网）、通信产品、视频会议、存储产品、监控产品、网络安全产品等

公司规模：5000人以上，51%以上为研发人员，年销售额超过60亿人民币

业务范围：全球，产品和解决方案已经覆盖全球90多个国家和地区

1：安全的应用系统发布平台

H公司使用NTA，作为其访问各种应用系统的统一平台，涉及的应用系统有：

办公自动化和工作流：通过NTA，用户可以从包括互联网在内的任何网络，访问并使用OA和工作流(Notes)系统。

用户范围：经常出差的领导和员工、派驻在供应商工作的公司员工等。

产品研发管理系统：通过NTA访问PDM系统，使得部署PDM系统非常容易，同时，防止了使用PDM系统容易产生的泄密问题。

用户范围：需要访问PDM的部门员工，包括：研发、生产、采购、质量控制、维修和售后服务、财务等

2：保密文档访问平台

H公司将需要保密的文档，统一部署在保密文档服务器中，通过NTA发布给需要浏览的员工，定期检查授权，到期取消授权。涉及到的文档类型有：MS Office类PDF文件 各种类型的CAD图纸文件

3：涉密开发访问平台

只有通过NTA，研发人员才可以从办公区访问机密区的开发机进行开发、或从机密区通过NTA访问办公区，使用Notes、访问互联网等系统。

通过NTA在不同的网络之间互相访问，既可以保持原有工作方式不变，同时，NTA做到禁止各种可能产生泄密隐患的行为（如：上传或下载文件、文档的拷贝、粘贴等）

S微电子有限公司

业务类型：集成电路以及半导体微电子相关产品的设计、生产与销售。

主要产品：音响、音效电路；红外遥控发射电路；四位、八位MCU电路；电能表、万用表和其他计量类电路；显示驱动电路；光电模块产品；电源管理电路；IC卡电路；有线、无线局域网类电路；基于CD伺服的SOC电路；应用于数字家电的系统集成芯片；

公司规模：1000人以上，年销售额超过10亿人民币

业务范围：全球

1：保密文档访问平台

S公司将需要保密的设计文档，统一部署在保密文档服务器中，通过NTA发布给需要浏览的员工。涉及到的文档类型有：MS Office类 PDF文件 各种类型的ED IC图纸文件

2：涉密开发访问平台

只有通过NTA，研发人员才可以从办公区访问机密区的开发机进行开发

最主要的开发工具是：ED (Linux)

通过NTA在不同的网络之间互相访问，既可以保持原有工作方式不变，同时，NTA做到禁止各种可能产生泄密隐患的行为（如：上传或下载文件、文档的拷贝、粘贴等）

3：分支机构涉密开发访问平台

S公司在国内不同地区和美国成立了几个研发中心，这些研发中心的研发人员通过互连网登陆NTA访问和使用总部的设计系统。

经理级别的设计人员在出差时也通过互连网登陆NTA访问和使用总部的设计系统。

www.ntaip.cn



美国戴闻信息技术公司 北京办事处

北京市海淀区知春路1号 学院国际大厦1715室

电话：010-82335769 传真：010-82335749

www.ntaip.cn