企业数据安全防护

企业数据安全防护

数据安全是降低敏感数据向内、外部泄露风险的最有效层面之一。在该层面，防护的焦点在于数据本身，其目的在于确保数据安然无恙，而不论其传播途径如何。数据的移动性正日益加强，因此数据安全防护至关重要。

数据加密

保存有机密数据的移动设备非常容易丢失或被盗窃，而通过公司网络或互联网传输的数据则有可能会遭到截取。这会给敏感数据带来巨大风险。因而，唯一可以形成阻碍的手段就是：数据加密。数据加密作为一项基本技术是企业数据安全的基石。数据加密过程是由形形色色的加密算法来具体实施，它以很小的代价提供很大的安全保护。在多数情况下，数据加密是保证信息机密性的唯一方法。

- 如何使用 SHA 加密敏感的数据
- 加密密钥管理的一些最佳做法
- FTPS 是在软件上加密数据包的吗?
- BitLocker：Windows 全盘加密数据保护功能

数据备份

像汶川地震这样的自然灾害促使网络管理员加强了企业数据备份和灾难恢复意识。为了保护企业数据安全,备份是必要的。如果要充分地保护企业敏感数据,很明显要考虑到把加密和备份结合起来。

- 全盘加密应该用于数据备份软件吗?
- 备份和灾难恢复失误

数据丢失防护

传统的计算机安全观念以企业为中心，主要关注外部威胁，通常忽略了内部漏洞。然而，Ponemon、Orthus 和 Vontu 最近组织的研究表明，大部分的公司数据丢失（通常叫做“数据泄漏”）往往由公司自身的行为无意中引起。企业数据丢失会带来法律责任、损害商标信誉，这就加大了对数据泄漏防御（DLP）技术的需求。

- 赛门铁克收购 Vontu 拓展数据丢失防护市场
- McAfee 新产品纳入数据丢失防护和加密技术
- 数据丢失防护工具：防止身份窃取新途径？
- 数据丢失防护 防御由内至外

数据保护的其他措施

数据保护名副其实：保护重要的数据不受损害、篡改或丢失。虽然好像很简单，数据保护包含大量的技术、商业过程和最好的实践。除了数据加密和备份，企业数据的安全还依赖于一些其他的因素和策略，例如企业数据的管理和保护策略等。

- 企业数据管理：数据保护的商业过程和架构分析
- 机密数据被删除后还可以访问吗？
- 数据保护策略的要素
- PaaS 环境会置数据于险境吗？
- 数据安全的查漏与补缺

数据存储设备安全

尽管企业和厂商都对通过 Email 或网络造成的数据泄露相当重视，但事实是，敏感的公司数据更有可能通过丢失的手提电脑、CD 盘或 USB 盘落入他人手中。因此，企业数据的安全还应该关注数据存储设备，特别是移动设备的安全。

- **员工私人设备：安全和网络政策的思考**
- **如何锁定移动设备 确保企业数据安全**

如何使用 SHA 加密敏感的数据

问:当处理一个订单的时候，我们必须要进行搜索，把呈报的信用卡号码与第三方提供的热卡(失窃的或者封锁的卡)列表进行对照。根据支付卡行业数据安全标准，即使一个卡在这个列表上，我们也不能把这个卡的号码不进行任何加密处理就放在那里。我们正在考虑使用 SHA-1(安全散列算法-1)把这些号码转换为它们的散列值，然后在我们处理一项支付的时候再进行对比。我们喜欢 SHA-1，因为它不需要任何密钥管理功能。然而，我们担心散列值冲突或者误报问题，所谓误报就是错误地把好卡识别为热卡。像这样使用 SHA-1 是不是一种好方法?

答:使用 SHA-1 创建信用卡号码的散列值以避免用明文形式存储信用卡是一种好方法。此外，由于散列值冲突的机会很少，你不可能得到误报。让我们看一下 SHA-1 和在这种情况下使用它为什么是安全的。

安全散列算法(SHA)家族是由这种算法设计的一套相关的密码散列功能，能够根据任何种类的数据创建一个散列值，这些数据包括文件、口令和本案中的信用卡号码。这个值实际上对于输入的数据来说是独一无二的，因此，由于雪崩效应(avalanche effect)，数据中很小的变化都会导致出现完全不同的散列值。此外，没有切实可行的方法计算一个将导致一个理想的散列值的特定的数据输入，因此使用这个散列值恢复原来的数据是不可能的。这个家族中最常用的功能是 SHA-1。各种流行的安全设备和协议都使用 SHA-1，如 SSL、PGP、S/MIME 和 IPsec 等。

你担心的散列值冲突问题可能是 2005 年 8 月份发生的一次攻击的结果。那种攻击需要低于 2^63(9,223,372,036,854,780,000)的散列值计算以发现在完整版本的 SHA-1 中的冲突。一个冲突意味着两块数据有同样的散列值。这种攻击需要的计算复杂性低于蛮力搜索冲突。蛮力搜索需要 2^80 计算。根据学术密码学，这可以认为是一种安全突破。虽然一些观察人士担心大规模分布式互联网搜索可能发现 SHA-1 的冲突，但是，这并不意味着

这种攻击是实际上可以利用的。不管怎样，有趣的是需要指出，在 2005 年 9 月，微软宣布它在任何功能中都将停止使用 DES、MD4、MD5 和 SHA-1 加密算法。

这样，为什么使用 SHA-1 加密你的信用卡号码仍是安全的呢?因为两个信用卡号码的散列值相同的机会是非常小的，你不可能发现一个好卡和坏卡的散列值是一样的，从而排除了误报的可能性。此外，这种攻击是一种冲突(collision)攻击，而不是 pre-image 攻击。正如我以前指出的那样，冲突攻击是找到拥有同样的散列值的两块数据，但是，攻击者并不知道这个散列值是什么，因此就不能破解使用 SHA-1 检查数据散列值变化的工具。另一方面，pre-image 攻击能够让攻击者找到一个坏的信用卡号码。这个号码能够让散列值功能产生一个非法的信用卡的散列值。然而，因为你在使用一个黑名单，攻击者不能利用这个功能，因为这个对比过程能发现黑名单上的坏卡号码。

如果你仍然感到担心，你可以考虑使用 SHA-224、SHA-256、SHA-384 或者 SHA512。有时候，这些方法统称为 SHA-2。然而，这需要额外的存储空间，因为 SHA-1 创建的散列值的大小的 160 字节，而 SHA-224 创建的散列值是 224 个字节。另外，对比的过程也要慢一些。

(作者：Michael Cobb 来源：TechTarget 中国)

加密密钥管理的一些最佳做法

传输中的数据”密钥管理系统在加密数据“休息”的时候不起作用有两个原因。

第一个原因是传输中的数据加密没有密钥存储的概念。一旦你从一个密钥转移到另一个密钥，旧的密钥就不再需要了。然而，在加密存储的数据时，密钥是正常变化的。旧的密钥必须要保留，否则使用旧的密钥加密的数据就无法读了。第二个原因是如果这个密钥丢失就无法重新建立连接。如果由于损坏或者丢失密钥造成一个虚拟专用网中断，你要做的事情就是重新建立这个连接。然而，如果你丢失了或者损坏了你用来存储一段数据的密钥，那么，那个数据就永远丢失了。这就是好的密钥管理系统必须要跟踪在什么地方使用了什么密钥以及必须要保证没有任何人访问过这些密钥的原因。

目前用来存储加密数据的密钥系统主要有两种类型：单密钥和多密钥系统。单密钥系统使用某种类型的密钥加密数据，简单地拥有这个密钥对于解密数据就全够用了。如果一个黑客获得了那个密钥，他或者她就能够阅读你的加密的数据。这是所有密钥系统中最简单的。

因此，与单密钥系统有关的第一件事情就是创建一个密钥记录，记录系统中使用的密钥以及什么时候使用了这些密钥。这个记录包括当前的密钥和以前创建的目前仍在用来存储数据的磁带的密钥。如果发现一个密钥存在被攻破的可能性，你要立即改变这个密钥并且在密钥记录中登记。

你对单密钥系统做的第二件事情是在存储密钥记录的周围放上你自己的流程。你要尽一切努力保证没有一个单个的人能够访问这个密钥记录。例如，存储密钥记录与你的磁带分开，保证至少必须有两个人在另一个记录中登录才能访问这个密钥记录。

多密钥系统是完全不同的。这些系统使用一套密钥加密数据，使用另一套密钥对管理员进行身份识别。管理员从来不会真正看到用来加密数据的密钥。他们只能看到他们的用

户名和密钥。即使一个管理员能够偷走用来存储加密密钥的数据库，他或者她也不能用这些偷来的密钥阅读你的备份磁带，除非他或者她拥有授权使用这些密钥的系统。

授权系统使用这些密钥的方式每个厂商都不一样。但是，一种方法是使用一种密钥法定人数的概念。这就是要授权一个新的系统，必须要多个人输入用户名和密钥，有时候还需要插入一个物理的密钥卡。完成这个工作之后，这个加密密钥就可以在那个系统上使用了。这种做法可以防止一个恶意的员工窃取你的磁带和加密密钥并且利用这些数据。

(作者：W. Curtis Preston　来源：TechTarget 中国)

FTPS 是在软件上加密数据包的吗?

问：我有一个关于 SSL/TLS，主要是 FTPS 协议方面的问题。在普通环境下，当客户发送或收取数据包时，数据包是在硬件还是软件上加密的？为什么它那么重要？

答：简短的回答是数据包通常是在软件水平上加密的，这可能比在硬件上加密好一些。要解释这一点，我们必须首先弄清楚关于加密技术的基本知识。

SSL 是安全套接字层（Secure Sockets Layer）的缩写，是一种传输层协议，它为所有网络，尤其是因特网提供了端点认证和通信保密技术。TLS 是传输层安全（Transport Layer Security）的缩写，它是基于 SSL 的因特网标准协议。SSL 通用的版本是 SSL3.0 版，TLS 通用的版本是 1.1 版。通常人们使用 SSL/TLS 来统称 SSL 和 TLS。

FTPS 一般是指 FTP/SSL，并且涵盖了大量的方法，通过这些方法，文件传输协议软件能够支持 SSL/TLS 运行安全文件传输。在 FTP 协议标准下，每一种方法使用 SSL/TLS 层来对控件和/或数据信道加密。另外，FTPS 与 SSH 文件传输协议（SFTP）不同，SFTP 是 SSH 基础上的 FTP。

TLS 共有三个基本组成部分：

——算法支持的最初协商，在协商中选择了数据加密过程中使用的对称密码

——通信的两台计算机之间的密钥交换（和认证）技术

——对称密码加密和消息认证

换句话说，对双方交换的数据进行大范围加密之前，TLS 协议发生了很多事情。实际上，交换密钥和认证技术使用了公共密钥加密技术，它们是整个传输过程中计算最为繁琐的部分。这时候就需要使用硬件。

90 年代后期，作为一种安全网络传输协议，SSL 尽力承担所有的公共密钥计算，SSL 应用的迅速增加威胁到了 Web 服务器，大有压倒 Web 服务器之势。像彩虹科技（现在已经并入 SafeNet 公司）之类的硬件加密公司开发出了 SSL 加速器，和应当插入 Web 服务器中的协助处理器主板。这些细心的程序开发者负责 SSL 公共密钥计算，并将传输过程中为数据加密的对称密钥发给服务器。其它加速器的设计实际上也能进行数据加密，充分应用了加密技术，并将明码电文传送给服务器。

FTPS 可以将数据安全的发送到服务器上。如果你需要运行 FTPS，对部分或者全部加密过程中的硬件加速器就值得研究了。然而，有可能需要处理大量的数据——和大量的同步链接——因为加速器的优点是仅仅建立在软件方式基础上的。此外，很难想出为什么这种情况下硬件方法天生就比仅使用软件方法更为安全。切记，要获得 TLS 的所有安全优点，客户机和服务器都应该使用数字认证技术。与其它任何加密系统相比，最可能造成失误的不是加密技术本身，而是运行加密技术的方式。

（作者： Michael Cobb 译者：李娜娜 来源：TechTarget 中国）

BitLocker：Windows 全盘加密数据保护功能

防火墙、或者甚至网络周界之类的物理障碍制约工作人员的工作的时代已经一去不复返了。而今，所有的设备都能够连接到任何地方，包括像笔记本电脑等的基于 Windows 的设备。

在过去几年中，我们一再看到数据泄露的后果。存有成千上万、甚至百万个用户帐户记录的笔记本丢失或者被盗，造成每一位用户个人信息泄漏的潜在危险，更要注意丢失诸如商业秘密或者员工档案等其它形式敏感信息的后果。企业必须要一直保护器件数据。

文件和文件夹的加密可以起到作用，但是它有两个内在的缺点。首先，它依赖用户去加密数据，或者至少要确保所有的敏感和机密数据放在将要加密的合适的文件夹里。其次，黑客如果可以访问加密文件，就能够以某种方法绕开密码保护或者破坏加密。为了保证硬盘数据得到保护，整个驱动器都要加密。

BitLocker 的作用

在 Windows Vista 高级版和 Vista 企业版中，微软引入了一种叫做 BitLocker 的全盘加密机制。有了 BitLocker，用户基本上可以加密硬盘目录（硬盘中的一小部分必须保持非加密，留给启动操作系统时容纳必须的核心系统文件），并且保证未经授权的用户不能访问它。

发挥 BitLocker 的全部功能需要 TPM（受信平台模块）芯片的支持，包括启动前系统完整性认证的附加安全措施。TPM 是集成在主板上的一个特殊的加密处理器，它可以生成独特的绑定在系统硬件结构上的加密密钥。简单地说，加密和解密都被绑定在含有硬盘驱动器的具体硬件上。

当系统中不含 TPM 芯片时，BitLocker 也可以使用存储在 USB 闪存驱动器上的密钥提供加密。在配置没有 TPM 芯片的 BitLocker 时，不论使用组策略还是使用脚本来改变加密钥匙存储到 USB 闪存中的路径，都需要对默认行为做一些修改。

当用这种方式配置时，USB 闪存必须可用，以便打开存储在加密栏中的数据。然而，因为操作系统驱动程序不会被激活，所以正在使用的硬件必须能够保证闪存是基于 BIOS 级别的。

BitLocker 的缺陷

BitLocker 的概念是好的。默认加密整个磁盘卷，并且通过 TPM 芯片把加密钥匙放到当地硬盘里（或者通过 USB 闪存放到验证硬盘里），这种方法比文件和文件夹加密更加无缝地和全面地保护数据。然而，BitLocker 在一些领域仍有缺陷。

BitLocker 在操作系统兼容性上有局限性，仅仅可以在 Vista 和最近发布的 Windows Server 2008 上运行。BitLocker 加密或保护的信息范围较窄。在最初的 Windows Vista 操作系统中，这个版本仅仅加密可启动的系统卷，其余部分未加密，容易受到攻击。有了 Vista Service Pack 1 (SP1)和 Windows Server 2008 中的 BitLocker 版本，微软已经扩大了 BitLocker 的能力，可以对在驱动器上所能发现的任何卷进行加密。但是，BitLocker 仍不能够保护在移动媒介上的数据，比如 USB 闪存驱动器或者刻录的 CD 和 DVD，也不能提供一种与第三方，如销售商或者厂商，安全地共享数据的方法。

在执法部门和政府机构方面，BitLocker 也有一个问题。那就是它没有密匙托管和秘密的解密密钥，这样公安机关或者政府官员就无法解密数据。这就意味着犯罪分子或者恐怖分子的加密数据和 Vista 用户加密的数据同样安全，并且 Big Brother 不能够使制表符保存在任何受 BitLocker 保护的卷上。

BitLocker 的另外一个问题是使用 USB 闪存驱动器作为 TPM 的替代物。许多用户携带 USB 闪存驱动器，所以保留一个 USB 备份的想法似乎很有意义。然而，许多人仅简单地把

笔记本和 USB 闪存驱动器一起携带在包里。这就像锁上你的汽车，但是把钥匙留在车门上一样。

BitLocker 的未来

微软在 BitLocker 的发展方向上采取了明确的措施，但是加密手段需要发展和成熟，以便成为企业数据保护策略中可行的一部分。提供与 BitLocker 相似功能的第三方产品，包括 McAfee 公司（它购买了 SafeBoot）或者 Check Point Software 技术有限公司.（它购买了 Pointsec）的产品。这些产品在 Windows Vista 系统外仍然可以运行，并且提供了保护移动媒介中数据的方法。

许多企业正在考察选择一种数据保护方法作为硬件更新的一部分，或者正在升级桌面操作系统，这些企业应注意到 BitLocker 所提供的功能。已经使用 Windows Vista 操作系统的企业，能从驱动器加密的附加安全措施中受益，而不需要投资和配置第三方产品的附加成本。 Vista SP1 和 Windows Server 2008 上的 BitLocker 的更新消除了仅仅加密可启动卷的限制，使得 BitLocker 成为企业寻求保护客户数据的一种引人注目的可行方案。。

（作者：Tony Bradley 译者：李娜娜 来源：TechTarget 中国）

全盘加密应该用于数据备份软件吗?

问：出于灾难恢复的目的，是不是最好在使用数据备份的同时，也使用全盘数据加密？或者我的企业应该选择其中之一？

答：磁盘加密和数据备份的作用不同，并且应该砸全面系统安全环境中考虑，是在笔记本电脑上还是在企业整体网络上。系统安全涉及到系统和其上存储的数据的机密性，完整性和可用性。

所以，使用加密来保护数据防御窥探者，和保护信息安全不同。如果有人偷走加密的磁盘，你了解了窃取者很难访问其中的内容，就可以得到安慰了。如果这些技术包括大量用户的个人认证信息（PII），加密就可以帮确保你在取得这些数据是对用户许诺的机密性和完整性。

所以这个问题的简单的答案是肯定的。备份是必要的，还应该考虑全盘加密，但是两者之中，备份更加重要。两者结合起来就是加密备份，如果要充分地保护敏感数据，很明显要考虑到加密备份。这种结合的办法使得再把数据写入备份媒体中时加密数据，而备份媒体可以是磁带，移动硬盘或网络服务器。

不管怎样，备份媒体应该单独地、安全地存储。也就是说，在原始的存储位置之外，至少还要有一个不同的安全备份的位置。想象一下，不怕麻烦地进行正常备份，然后把它们和支出原始数据的驱动存放在同一间办公室！如果办公室被窃，所有的一切都可能丢失。知道盗窃者得不到数据，因为它已经加密了，就可以得到一些安慰；如果知道公司在银行的保险储藏盒中有数据的拷贝，那将会极大地减轻痛苦。

（作者：Michael Cobb 来源：TechTarget 中国）

备份和灾难恢复失误

像汶川地震、Hurricane Katrina 这样的自然灾害，促使网络管理员对稳定的数据备份和灾难恢复意识增强，以保证商业的连续性。但是在很多公司都看到了错误的做法，这样策划就到了末日。在本文中，TechTarget 的特约专家 Tony Bradley 将会列出一系列的错误作法，希望可以展示出如果做错了会有什么后果，应该怎么做才对。

1.没有获得管理支持。在任何的 IT 项目中，你可能会做的最遭的状况是没有获得管理支持。没有管理层给你的权威支持和对工作的预算支持，备份和恢复计划注定不能实现。

2.没有提供风险评估。没有某种形式的风险或影响评估，很难清楚哪项资产最重要，那一项可消耗。如果浪费资源而保护可消耗资产，而把重要资产遗留在计划之外，你的计划将会以失败告终。

3.没有书面计划。人们有来有往。可能会出现策划备份和灾难恢复的人员认为足够聪明而没有必要写下来但是，如果不把详细说明和论证充分的计划写下来，供任何人参考，那么当下一场灾难发生时，就不会有恢复。

4.缺乏备份完整性。很多的网络管理员都定期备份，保护企业的重要数据。但是经常出现的错误作法会导致不能验证或核实你可以成功还原，并在灾难发生时及时还原。

5.需要备份和数据恢复时，从网络上把重要数据转移到磁盘或其他的移动媒体上是很好的做法。但是有两种发式，可能会使其弄巧成拙：一种是通过把数据和备份的服务器存储一起，一定会导致同时被破坏；另一种是通过把存储的移动媒体放在在本身就不安全的地方，或者当需要的时候，不能容易并快速地找回的地方.

(作者：Tony Bradley 译者：Tina Guo 来源：TechTarget 中国)

赛门铁克收购 Vontu 拓展数据丢失防护市场

在广泛关注下，赛门铁克周一宣布将收购安全厂商 Vontu，以期进一步拓展和稳固数据丢失防护（DLP）市场。

这项高达 3.5 亿美元的收购计划将在 2007 年第四季度完成，届时还将取决能否通过法规审批和满足其他惯例成交条件。上个月在信息安全圈内有消息传出，加州的安全巨商 Cupertino 将收购 Vontu，并在几周前的季度盈利汇报中宣布。不过，那天并没有宣布任何相关消息。

周一，赛门铁克公司安全与数据管理部门主席 Tom Kendra 表示：“将赛门铁克现有产品同 Vontu 的前沿产品和专业团队相结合，使我们有能力为 Security 2.0 版本用户提供更核心的服务；以信息为中心的安全将不仅保护设备的安全，而且也保护信息自身的安全。”

位于旧金山的 Vontu 以其数据丢失防护（DLP）技术出名，其 DLP 8 产品是一套结合端点和网络技术的整合方案，用来保护存储或使用中的保密数据。

这项收购进一步表明业界对 DLP 技术的日趋关注。不到两周前，赛门铁克的竞争对手趋势科技才刚刚收购另外一家叫 Provilla 的 DLP 厂商。

（作者：SearchSecurity 来源：TechTarget 中国）

McAfee 新产品纳入数据丢失防护和加密技术

McAfee 自去年秋季顺利收购 SafeBoot 公司后，新推出 Total Protection for Data 套件，这是将 SafeBoot 的端点加密和加密 USB 令牌与 McAfee 现有的数据丢失防护产品相结合，重新包装推出市场。

本周一宣布推出的该套件还谈不上是一个集成产品。根据全球解决方案及竞争市场的副总裁 Vimal Solanki 的介绍，McAfee 受欢迎的 ePolicy Orchestrator (ePO)管理控制台将不会管理前 SafeBoot 的两个组件，即 McAfee Endpoint Encryption 和 McAfee Encrypted USB。除非今年下半年发生改变。

Total Protection（完全保护）的主题在 Total Protection for Enterprise 端点安全产品中得以体现，它结合了反病毒、反间谍软件、基于主机的入侵防御、反垃圾邮件以及可选的网络接入控制（NAC）。

端点安全厂商已经非常积极地转向将不同的安全功能特性（如反病毒、反间谍软件、HIPS、防火墙、NAC 等）结合为综合的产品，快速地摆脱传统的只提供单独的反病毒产品的意识。例如，赛门铁克现在推出的 Endpoint Protection 11.0 就是取代了之前的 Antivirus Corporate Edition。其他厂商也采取了类似的措施，通过开发、收购或者合作进行这个转变。

McAfee 强调其产品集成和管理，在快速变化的端点安全和数据保护市场中，是一个主要的卖点。

“客户对太多的代理和控制台感到厌倦，”Solanki 说，“我们已经为现有的产品提供了一个单一的代理。如果客户有 ePO，只需要转换一下就可以了。”

“由于反病毒厂商已经有端点产品，所以将它纳入到同样的管理工具中是非常合理的。”Burton Group 的分析师 Pete Lindstrom 说，“如果 McAfee 有一件事情做得出色并值得称道，那就是它的 ePo。这是企业为什么选择 McAfee 产品的最大原因。”

传统的反病毒公司已经积极向数据丢失防护（DLP）市场迈进。McAfee 开发出了自己的 DLP 产品，其中部分出自于对 Onigma 公司的收购。最近，赛门铁克收购了 Vontu，趋势科技收购了 Provilla。这些被收购的厂商都是专注 DLP。

Solanki 说，采用基于主机和网关的数据丢失防护技术，将磁盘和可移动设备加密相结合，包括了企业必须解决的所有关键数据丢失的方方面面--无论是设备丢失或被窃，或敏感信息的大意误用或恶意使用。并不是只有 McAfee 赞同该观点。加密厂商 Utimaco 最近宣布推出趋势科技的 LeakProof DLP 产品之 OEM 版本。

“数据丢失防护和加密是紧密相关的。”Lindstrom 说，“只要你发现了问题，采用不同的方法去加以解决，是非常合理的。”

(作者：Neil Roiter 来源：TechTarget 中国)

数据丢失防护工具：防止身份窃取新途径？

2006 年，数据盗窃事件在信息安全领域中占据了大半江山； 2007 年，数据盗窃事件的数量只增无减。如果这种态势继续发展下去， 2008 年应该会成为最糟糕的一年。

那些希望防止数据盗窃的企业如果花费了成千上万，而不是数以百万的资金，实施最好的边界安全技术，那么这些努力似乎收效甚微;大量机密信息的泄露继续有增无减，尽管对企业和它们的客户来说后果相当可怕。这激发了安全专业人员对研究新工具的积极性，可以减少他们成为下一个新闻焦点报道的机率。

在过去的几年中，像 McAfee、趋势科技、赛门铁克等众多的信息安全厂商已经在积极研发一套产品，承诺对此将有所帮助。这个产品类别称为数据丢失防护，或 DLP，受到了众多的关注，以至于一些提供反恶意软件和反垃圾邮件的厂商为了进入 DLP 市场，对其业务重点进行调整。举例来说，Clearswift 公司几年前主要的业务重点是反垃圾邮件工具。虽然 Clearswift 公司作为内容安全厂商，其产品线仍包括反垃圾邮件技术，但是它现在将重点放在生产更好的基于网络的数据防护产品。

当软件制造商采用 DLP——过去的安全产品从未采取的方式，努力帮助客户保护数据时，让我们看看这项技术具有怎样的关键特性。

- ✧ 保护信息免受意外泄露——企业允许员工获取其最敏感的信息，但是有些员工根本不知道通过互联网发送数据具有内在危险。例如，财务部门的一个新员工，需要将一份机密文件发送到异地的会计师事务所，他可能会将其以电子邮件附件的形式发送，却没有认识到这份文件通过互联网时是以清晰的文本格式发送。

确保对所有的机密数据采取适当的措施进行标记，这是企业的责任。DLP 产品确保将机密和关键信息贴上合适的标签，避免员工无意中的泄露。标记数据(tagging)是一个将系统的机密数据分类，并贴上合适标签的过程。由于 DLP 的这项标记功能，从而阻止了员

工意外或恶意试图泄露机密信息。举例来说，一个贴有标签的敏感文件会被禁用通过电子邮件和 IM 进行传送。

- ✧ 保护信息免受（来自内部及外部的）恶意窃取——员工的不满情绪仍旧是导致数据窃取的一个重要因素。DLP 的实施可以限制员工传输数据的途径。DLP 也能防止机密数据被复制到 USB 装置、外接式硬盘及 MP3 播放器。
- ✧ 符合法规遵从的要求——许多企业需要遵从某些政府的法规，如《萨班斯-奥克斯利法案》（SOX）、《金融服务现代化法案》（GLBA）、《医疗保险可移植性与可信度法案》（HIPAA）或是这三个都需要遵守。今年，在配合法规遵从的要求这一方面，DLP 技术看来将很有可能扮演一个重要角色。例如，HIPAA 要求医护人员对所有的医疗信息保密，而 DLP 策略不仅是保护这些信息的一种手段，而且也是企业证明其采取符合法规遵从的适当步骤的一种方式。

DLP 产品在大型企业网络的应用实施绝非是一件容易的事。大部分的大型企业都有上百台服务器，存有数以千计的目录和文件。需要对这么多的信息做出清理，并决定哪些信息需要被标记，这对任何一个企业来说，都是一项艰巨的任务。但是，企业不同，需要被标记的数据也不同。这个过程绝对不是一刀切的做法。例如，有的组织会选择标记公司的财务信息、商业秘密等，而另一些公司可能不会这样标记。DLP 实施的成功，需要各管理层人员的配合，从而使得数据被适当归类。这样的团队合作才能确保数据标记策略对整个企业来说是合适而正确的。

评估 DLP 时，对其进行测试的主要功能应该包括系统阻止和监控的功能，以及用户阻止和监控的功能。考虑使用基于主机和基于网络的 DLP 产品也很重要，这可以确保没有运行 DLP 接口的系统也能对数据进行保护。

DLP 技术，将成为安全行业新型的防火墙。毕竟，它应用于下一个逻辑层：而该逻辑层是数据存储的位置。不过，在冒险尝试及购买 DLP 技术之前，最好还是对一些厂商的产品进行评估，确保产品的技术能力不会被花哨的营销活动所掩盖。

（作者：Peter Giannoulis 译者：Eric　来源：TechTarget 中国）

数据丢失防护 防御由内至外

传统的计算机安全观念以企业为中心，主要关注外部威胁，通常忽略了内部漏洞。然而，Ponemon、Orthus 和 Vontu 最近组织的研究表明，大部分的公司数据丢失（通常叫做“数据泄漏”），往往由公司自身的行为无意中引起。

企业数据丢失会带来法律责任、损害商标信誉，这就加大了对数据泄漏防御（DLP）技术的需求。这些技术主要注重数据自动管理的需求。这种“由内而外”的安全模式导致企业努力通过各种产品快速实现数据治理，这些产品往往强调外流内容符合规范（OCC）策略、内部威胁管理和入侵防御体系（EPS）。

然而，在考虑综合的企业数据管理产品或平台之前，信息安全部门必须了解组织的商业流程及其如何保护现有的 IT 资产。这个过程应该包括调查并锁定网络基础设施的关键部分，因为基础设施有可能是数据丢失的来源。在确定数据泄漏的潜在领域时，还要考虑一些重要问题。

- 随着 IT 基础设施变得越来越复杂，要了解数据的保存位置、如何获取数据、由谁获取数据等问题也变得越来越困难。
- 数据管理员和存储管理员的作用开始模糊，很难明确应该由谁负责创建数据排列制度。
- 企业必须努力评价其危险程度。一旦发现了所有的数据内容，就必须制定分类方案，根据敏感度对数据进行分类。
- 那些能访问数据的人通常应该对数据丢失负责。明确哪些用户获得了过度的访问控制权，如高级管理员，他们通常需要高度优先权，但是却没有经过合适的数据安全训练。
- 人们会分析内收邮件，抵御内部威胁，却常常没有注意到外发邮件才是主要的数据丢失源。内部邮件会意外丢失保密信息和专利信息，这是最大的数据丢失领域之一。

- 用个人网上账户、不合适的邮件自动转发功能等行为也会引起威胁，产生严重的法律、经济和监管后果。
- 未经认可使用互联网协议和服务，如 IM、点对点文件共享、博客、社会网址及未经认可将数据上传（FTP）到互联网，这些都是发生数据安全事件的主要原因，应该通过详细的政策加以控制。
- 雇用合同工和外部咨询人员通常需要创建新的用户证书。然而，必须掌握这些用户账户及其责任，因为账户很容易丢失。
- 闪存驱动器、光介质、外部硬盘和个人媒体设备等可移动的存储媒体都是引起数据丢失的便携式设备。
- 移动计算平台（如笔记本电脑、PDA）可从公司环境中移除数据，而使公司所有的监测和控制系统失效。

防御战略规划

企业存储远远不止直连式存储（DAS）、基本的网络文件共享和简单的数据库存储。今天的架构采用 iSCSI 和光线通道、分层和分级存储模型、虚拟存储系统、高端存储阵列以及集群存储，实现储存区域网络（SAN）。由于硬件、软件、及其配置方式的多样性，数据泄漏的修复战略最终应公司而定。

尽管如此，所有的数据损失防御规划（DPL）都应该考虑以下内容：

- 根据员工的数据使用权和信息拥有权，制定基本的公司标准和程序；
- 根据数据丢失和数据暴露引起的企业风险，评价并排列数据；
- 对数据内容进行语句检查，保证监测和分类软件采用有效的识别算法；
- 经常审核企业的关键数据，保证其得到实时防护，同时保证安全协议得到更新；
- 采用有效的数据安全模型，简化基于角色的访问控制（RBAC）以及独立用户的网格控制；
- 根据公司邮件的认可度对员工进行训练，执行此类政策。考虑建立邮件保护平台，自动管理外发邮件；

- 保证员工了解计算机采用的监测系统，阻止其违反政策；
- 经常对具有优先权的用户进行审核，评价并确认每位用户的配置都十分合理；
- 通过采用数字权限管理（DRM）技术，将访问控制直接嵌入敏感数据；
- 采用联邦身份管理，在与商业合作伙伴合作时维护数据安全；
- 形成常规的审计和数据流评价报告，监测数据泄漏威胁，根据时间和用户需求定位数据。

防御数据丢失已经成为一个法律问题，对保护公司的保密性数据、保护客户的私人数据至关重要。今天，数据增长率很高，有效管理新的数据、现有的数据是一项很大的挑战。企业安全策略在解决数据增长问题的同时，必须维持数据的可获取性、企业的生产力、操作的持续性以及数据的可恢复性。最重要的是，要避免终端用户误认为你的 DPL 战略是 IT 法律，就需要全面的通讯和教育，使得企业 DPL 规划的认可度成为一项重要的平行战略。

（作者： Noah Schiffman 来源：TechTarget 中国）

企业数据管理：数据保护的商业过程和架构分析

公司和其他企业都开始理解已经存在和即将来临的数据泄露、隐私和安全规则的含义了。所以安全专家发起了越来越多的技术性项目，完成数据保护的职责。

这些数据保护的执行有很多形式。一些攻击可能使用 e-discovery/或纪录管理项目。其他的可能需要满足 PCI 数据安全标准（Payment Card Industry (PCI) Data Security Standard）的要求或者需要保护用户专有网络信息（customer proprietary network information，CPNI）等电信信息。不同行业中的特别事业的法律法规也不相同，相同的部分是他们都关注数据的保护和恰当的处理。

无论数据和 PCI DSS、CPNI、HIPAA 或其他类型的数据类型或法规相关，在早期都需要回答两个基本问题：

1. 数据存在哪里？
2. 数据如何使用？

当解决法律法规以及国际数据保护标准和用户/商务伙伴的合同时，回答这些问题可以帮助公司弥补他们目前的状态和他们想要的状态之间的缝隙。理解“数据存在哪里”和“数据如何使用”可以帮助企业基本地理解哪里的控制不能生效或者甚至不存在。回答这些关键问题可能可以检测到企业数据泄漏、非授权的访问和处理以及不遵守法律法规和合同义务的问题。

商业过程分析

为回答这些问题，考虑企业中的一下几个数据，并检查在商务过程中数据的存在情况.

需要采用命令管理程序，例如在任何面向消费者的公司。使用采访的问卷调查可以对商务过程的持有者询问更详细的、顺序管理周期的潜过程的问题，例如用户资料的创建和维护。

调查客户资料的过程反映了服务捕获的详细的客户数据。获得一些个人信息包括姓名、家庭住址和电子邮件地址。在详细过程的对话之后，可以创建商业过程图表存储谈话结果。

从可识别的用户数据元素中，可能调查到命令信息是如何被捕获的。还是前面的例子，和用户服务代表的谈话可能反映出他们捕获了购买行为信息，作为他们的命令管理程序的一部分。在这种活动中，架构数据，例如用户的出生日期和非架构数据，例如用户详细购买的原因都添加到了用户资料中。总的来说，这些特殊的数据，可能会提高个人可识别信息（personally identifiable information ，PII）的等级，这取决于合法指导方针。在图表位置就是数据被捕获和存储的地点。

基础架构分析

“数据在哪里”这样的问题还可以通过检查和存储基础架构的各种数据元素，包括资料存储、桌面电脑和数据库等回答。假设领域内的数据元素——例如姓名、地址和社保号码——被识别到了，有两种决定在企业内部存储位置的方法。

第一，采访基础架构的持有者和股东，例如数据库管理员、系统管理员和网络管理人员。这些问答应该反映存储数据元素的数据库和系统，证明信息是如何从一个系统/数据库移动到另一个的，并解释存在什么技术识别和访问管理机制可以保护这些数据元素。和商务过程分析雷西，创建一个数据流表格来存储访问信息。

第二种方法，也是越来越受欢迎的方法要求自动的“数据发现”技术。这些工具扫描网络数据库、文件共享或桌面电脑，寻找用户指定的详细的数据元素。一些产品甚至建立的网络地图，表示数据元素的各个位置。

总结

回答上面提出的这些问题将会寸金企业数据保护策略和程序的开发。了解数据位置和它的处理方式可以允许企业鉴别他们遵守法律法规和/或要求快速战术性回应的合同职责的程度。。

(作者：Russell Jones 译者：Tina Guo 来源：TechTarget 中国)

机密数据被删除后还可以访问吗？

问：为了空间而把文件删除后，这些数据碎片仍然可以访问吗？数据被删除后机密数据仍然可以访问吗？

答：当文件被删除的时候，文件的内容不是从硬盘上移走。例如，当文件从 Windows 的回收站里删除的，只有文件的指向器被删除了。对操作系统文件是不可见的，在目录结构中也不会显示。硬盘上的以前占用的空间也会标志为空闲，而且可以被操作系统再利用。尽管如此，在新的数据写入到这块空间中以前，文件的内容还是存在的。数据的存活不确定，是取决于硬盘是否满了、文件在硬盘上的物理位置以及你使用电脑的频率。有很多工具可以恢复“删除的”文件，是通过搜索硬盘上没有相应的指示器信息的数据实现的。

在删除敏感数据时，写满或删除敏感数据是很好的安全实践。但是应该为你的机密数据设置什么样的删除层级呢？2004 年，美国国家安全局（NSA Advisory LAA-006-2004）发现使用 DoD 5220.22-M-compliant 软件的单独写满就完全可以使电子文件不可恢复。很多数据擦除产品都表明他们满足 DoD 5220.22-M 标准。操作的第二部分是用一个字符、它的不足和一个任意字符擦除所有的可设定的地址，然后再确认。这个过程要执行三次，防止被商业可用的程序恢复。

软件磁盘擦除的一个问题是他不能清洁没有成功删除的硬盘。在这种情况下，你可以通过消磁、融合、焚化、粉粹或者撕裂等方法销毁。物理销毁是最高级别的擦除，但是如果剩余的磁盘碎片大于 512 字节的纪录块，即使如此也还不完全。不管你选择哪一种方法，不管是软件擦除或者是物理损毁，你都必须提供恰当的员工培训，保证你已经采取了“合理的措施”来保护数据。

联邦商务委员会的关于恰当的存储和某些客户信息的处理的 FACTA 规则要求这些信息得到恰当的处理。虽然物理销毁磁盘比用软件擦除成本高得多，而被攻击的数据的潜在成

本可能会占最大的部分。我推荐 NIST Special Publication 800-88, 介质清除指导方针。这些推荐可以用于这种类型的机构中，而且在设计恰当的销毁策略的，而这些策略是基于你信息的机密等级。

(作者：Michael Cobb 译者：Tina Guo 来源：TechTarget 中国)

数据保护策略的要素

数据保护的一个重要的商业驱动因素是近来汹涌的规则要求。很多政府都已经开始要求实行新的电信和数据存储规则。如果不遵守法规就要面临可怕的后果。有的国家已经逮捕了一些违反电信和档案的法律的行政犯罪。这些法规通常都定义了需要保密的信息有哪些、多长时间、在什么情况下。其他的法规也是为了确保文档、文件和数据库中信息的机密性。重要通信信息的丢失就是违反了这些法规，还可能导致企业受罚而经理被采取法律行动……

数据保护名副其实：保护重要的数据不受损害、篡改或丢失。虽然好像很简单，数据保护包含大量的技术、商业过程和最好的实践。不同的技术用语不同的数据保护的方面。例如，保护存储架构对于保证数据不被篡改或恶意破坏是非常必要的。为了保护数据的无意丢失或者永久的破坏，需要良好的备份策略和技术。

企业的规模决定了数据保护所需要的实践、程序或技术。没有理由证明小型商业需要配置昂贵而高端的解决方案来保护重要数据。另一方面，把数据备份到磁带或者磁盘上，当然是每个企业都会做的。大型企业有使用先进技术的资源和动机。

无论企业的规模和构成有何不同，目的都是一样的。因为缺少可核实数据的完整性和可用性，数据保护需要努力减少企业的损失。

配置数据保护策略时要考虑的实践和技术有：

备份和恢复：它为数据作的离线复制，是为在灾难和数据损坏时用以恢复的。

远程数据移动：即时或者准即时的数据移动到目前的存储系统以外的地方或者到另外的设备，来保护系统和建筑的物理损伤。这种技术最常见的两种形式是远程文件复制和文档或域的复制。这些技术把数据从一个系统复制到另一处的系统。

存储系统安全：存储系统要采用最好的实践和安全技术，增强服务器和网络的安全措施。

数据生命周期管理（Data Lifecycle Management，DLM）：关键数据在线和离线存储的自动移动。DLM 的重要方面是把被认为是终态的数据设置到最终状态，这样数据就不能改动，而把数据以不同的类型存储时也取决于它的年龄。

信息周期管理（Information Lifecycle Management，ILM）：它是信息资产的评估、编目和保护的全面策略。它还是和法规的遵守相关的。ILM，和 DLM 有些类似，它是在信息而不是原始数据上操作的。结果取决于信息的内容，而且需要考虑信息的关系的策略。

所有的这些方法都应该配置在一起，形成一个合适的数据保护策略。

（作者：Tom Petrocelli　译者：Tina Guo 来源：TechTarget 中国）

PaaS 环境会置数据于险境吗？

问：实施平台即服务（platform-as-a-service，PaaS）环境有什么样的数据保护风险？

答：一次又一次地，令人兴奋的网络技术的开发在恰当地解决安全和数据保护上失败。在我考虑 PaaS 的数据保护问题之前，我们在给它之前的 SaaS 或者软件即服务一些时间。

SaaS 已经取代了早期的 acronym, ASP 或应用服务提供商。软件及服务是基于 Web 的应用程序，它是软件提供商在网络上保存和提供的。尽管如此，它和通常的软件的关键去别在于 SaaS 用户为应用程序支付租金，而不是购买持有。

平台即服务是 Web 服务进化的下一步。PaaS 提供了托管平台——主要是瘦客户机（thin client）的现代版本——在这里的电脑从服务器上接收操作系统和应用程序。PaaS 是企业和它的开发人员可以关注他们的应用程序在做什么，而不是运行他们的时候需要什么软件和架构。幸亏有了 PaaS，商务过程可以逐渐的虚拟化、可共享，而且企业可以从经济规模、运行时间和灵活性上获益。但是和它前面的 SaaS 一样，它也存在很多相同的数据保护问题，主要是那些数据都正被或在第三方系统上处理货存储。

有了这些种类的服务，企业用户的数据安全就可以依赖于 SaaS 或 PaaS 开发人员的技术和能力。对于只有一两个开发人员的小企业来说，PaaS 大概是安全的可选方法。没有可以的过度劳累的开发人员，小团队、繁重的工作负担和紧张的最后期限会趋向于降低安全的重要性。当考虑 SaaS 和 PaaS 的时候，确保提供商的开发团队有专门的技术——并且已经给予了时间——来建立拥有强大的信息安全基础的应用程序。

尽管如此，大型企业可以负担得起假设在第三方提供商的手里他们的数据很安全吗？放弃对数据存储方式和访问的控制需要很大的信心和对数据处理的位置和方式的理解。对我来说。“位置”是关键的问题。

以一家使用美国提供的 PaaS 的英国公司为例。在欧盟数据指令下（European union Data Directive），公司有在责任保证任何管理他们的数据的第三方要有适当的安全措施。在美国和欧盟的安全海港数据保护协议（Safe Harbor data protection agreement）下，英国的公司只有在第三方在处理满足欧洲隐私保护标准的数据是才能在美国存储数据。因此，在 PaaS 环境中操作的数据保护措施需要清楚地理解；否则英国的公司可能会违反一部或更多的法律。

最后，只能通过其他人的服务器访问的数据请求正常运行时间的保证。在线服务的可能正常运行时间有 99.9%的可用性。即使如此，每年仍然有几乎半天的停工期。还会有服务正常但是负担了性能问题的时候。PaaS 提供商可能会提供比其它机构更多的正常运行时间，但是需要比在 PaaS 环境中更加理解和实施服务等级的协议（SLAs）。

（作者：Michael Cobb　译者：Tina Guo 来源：TechTarget 中国）

数据安全的查漏与补缺

企业数据泄漏是一个令人恐慌的问题。安全从业人员不得不一直在解决由电子邮件、即时消息和其它互联网渠道产生的数据泄漏问题。但是，随着移动技术的普及，数据泄漏事件比以前更容易发生了，无论是意外的还是恶意的数据泄漏都是如此。

为数据保护做好准备

虽然市场上有许多防止移动和固定数据秘密地从公司泄漏的工具，但是，最好的方法是使用把预防和检测方式结合起来的方法，如把检测引擎与数据封锁器结合起来。

然而，在做任何事情之前，重要的是要理解将要保护的是什么数据以及危险的等级。你应该根据机构的 IT 安全标准创建和编写你的公司的全部数据的保密等级。数据类型可以根据数据丢失或者泄露可能造成的风险按照规模从低到高地排列。

一些高风险的数据的例子如下：

- ✓ 包含名字、地址、社会保险号码和其它有关身份的资料的客户或者雇员的信息。
- ✓ 可能被竞争对手用来挖走客户的客户名单。
- ✓ 贸易机密和知识产权。
- ✓ 机密的产品设计和生产计划。
- ✓ 金融信息和即将推出的产品的很快要发布的市场营销计划。

一旦你理解了应该保护什么数据并且对风险级别进行分类和存档，你就能够开始调查什么工具最适合你的企业需求。

数据泄漏预防工具

数据泄漏预防工具大致与应用程序级的防火墙相似。同防火墙一样，这种工具检查出网的数据，而不仅仅是端口和数据包类型，并且最终决定什么数据可以离开公司网络。在调查数据泄漏预防工具的时候，你将发现这个市场的三大厂商是 Vontu、Reconnex 和 Vericept。

Vontu 6.0 套装软件包含一套工具，能够监视各种类型的 Web 通讯，包括 SSL、IM 和 Web 邮件。这个工具能够使用三种算法检测恶意的出网通讯:确切数据匹配、索引的文件匹配和解释的内容匹配。Vontu 6.0 能够通过精细的调整把监视目标对准具体的雇员组、位置或者内容类型。

Reconnex 的 iGuard 平台包含两个有用的设备。iGuard 是一种网络设备，能够监视出网的通讯内容和发现恶意的行为。另一个产品 Reconnex InSight Console 是一个数据库，通过存储敏感数据信息来使检测工作更方便。同 Vontu 公司一样，Reconnex 的平台能够根据企业的需求进行调整。

Vericept 公司的工具“360-degree Visibility and Control”(360 度可见和控制)是一种可以客户化的工具，主要用于内容监视。这个工具使用 Vericept 公司专有的智能内容控制引擎。Vericept 不仅能够监视广泛的网络通讯，如 FTP、SSL、IM 和 P2P，而且还能监视博客信息、聊天室和网站以及敏感的公司数据和机密可能泄漏的一切地方。

另外两家有用的厂商是 PortAuthority 技术公司和 GTB 技术公司。与上面提到的其它产品不同，这些公司提供硬件设备监视出网的 IP 通讯，检查具体类型的企业数据。由于这些设备是安装在防火墙后面的网络设备，保证这些设备与你现有的安全基础设施集成在一起是非常重要的。例如，Vontu 的产品能够与思科、IronPort Systems 和 Blue Coat Systems 等公司的产品结合在一起。Reconnex 和 Vericept 公司的产品能够与 Blue Coat 和其它网络代理公司的产品结合在一起。

移动设备和数据泄漏

移动设备是迄今为止数据泄漏方面的又一个难题。例如，U 盘、蓝牙设备或者可移动 CD 光驱等移动设备都能够在系统管理员不知道的情况下绕过网络控制。作为硬件存储设备，它们胜过了高级的互联网工具和上面介绍的网络监视工具。

Safend Protector V3.0 就是这类工具。它能够作为一台客户机安装在你的企业的全部台式电脑和笔记本电脑中。同网络监视工具一样，它能够通过一个基于网络的界面实施集中的管理。通过设置，这个工具能够检查正在通过 USB 接口、防火墙或者无线端口移动的某种类型的数据。这种工具具有“数据篡改验证(tamper-proof)”能力，对用户是可见的，并且在某些东西连接到外部端口之前一直保持沉默。此外，Safend Protector V3.0 能够经过调整之后完全封锁访问任何可移动设备，根据容量限制某些设备或者允许只读访问。这些政策可以集成到活动目录的组策略对象中，以便为有选择的用户提供这些设备的访问。

乍一看，数据泄漏预防问题似乎是压倒一切的。但是，随着一些新的商业性工具的推出，无论是在线的、通过 Web 的还是通过存储设备的数据泄漏问题都能够解决。

(作者：Joel Dubin 来源：TechTarget 中国)

员工私人设备：安全和网络政策的思考

如今，BlackBerry、iPhone、Treo、 iPod 等能提供上网服务的便携式电子产品已成为我们生活中不可或缺的一部分。人们都会在口袋里携带一种或者一种以上的电子产品，这些产品能够迅速、方便地连接到无线网络。

企业对个人网络设备采取不同的措施。一些企业为员工和来客提供无线网络，方便他们办公，而另外一些企业则严格限制网络，只允许公司的系统使用。许多公司努力避免数据泄漏带来的威胁，这类威胁可能来自员工在私人设备上存储、处理、传递公司数据等过程。

在本文中，我们将讨论在企业内部管理智能手机、手写板和其它终端用户设备具有哪些安全意义。首先，应明确是否允许公司以外的设备连接到你的网络，这一点很重要。简单地回答“不”似乎是解决安全问题的简便方法，但这个问题还需全面考虑。允许私人设备连接互联网，可能需要员工加强道德观念。同样，强硬政策能快速改变现状，尤其是在老板也拥有新型无线设备的情况下。

隔离私人设备

今后，大量的私人设备将会连接到公司的无线（而不是有线）网络。公司可以在接入点添加 SSID，为私人系统提供隔离网络。完成这项工作以后，就应该决定是完全开放网络，还是采用“网页认证”的方式进行身份验证。旅馆和咖啡店通常采用网页认证的方式，将来自未知客户的 HTTP 请求完全转发到专门的 Web 网页，直至用户获得合法证书通过验证；然后，他们就能连接到互联网了。

隔离网路中的设备不应该直接与公司资源相连，尤其是在不需要身份验证的情况下更不能如此。如果政策不允许在私人设备上使用公司数据，客户网络的用户就应该在访问公司资源之前连接到 VPN。这么做的目的旨在维持客户网络的“不可信”状态。

NAC 部署状态

许多企业在尽力找出网络准入控制技术在企业安全架构中合理的布置位置。然而，客户网络是个很清晰的例子，此时查清系统状态能使你获益良多。实际上，如果企业要在全公司范围内部署 NAC，并且希望在有限的范围内测试这种复杂技术，运行 NAC 策略就需要耗费大量空间。企业需要采用 NAC 确保终端符合最低安全标准，比如——至少——拥有配置合理的杀毒软件和主机防火墙软件，然后才能允许其它设备连接到客户网络。

利用公司数据

当员工允许私人设备处理公司数据时，安全问题就越过公司办公楼，抵达员工家里，甚至可能影响员工的工作效率。当今社会，员工经常会在家里工作，晚上或者周末的时候，他们通常会远距离工作或者简单地用电子邮件进行联系。如果你有远程工作的员工，他们采用自己的移动设备，那你就要花点时间明确公司对行为要求的策略：用户在公司以外的系统中处理哪类数据？以什么方式处理数据？如果你没有明确陈述该领域的要求，你的公司很有可能出现非正式利用的“灰色市场”。

决定是否在企业中采用个人设备时，你需要平衡安全需求和实际问题。这种平衡在各个公司之间大相径庭，不仅需要仔细思考，还需要制定合理的安全控制措施。

（作者：Mike Chapple 译者：周姝嫣 来源：TechTarget 中国）

如何锁定移动设备 确保企业数据安全

尽管企业和厂商都对通过 Email 或网络造成的数据泄露相当重视，但事实是，敏感的公司数据更有可能通过丢失的手提电脑、CD 盘或 USB 盘落入他人手中。以下就是几个真实发生的实例：

1. 2006 年五月份，美国退伍军人事务部门透露，一台包括两千六百万名退伍军人个人信息的手提电脑失踪。信息实际上是保存在一个移动硬盘上。
2. 2007 年十月份，英国税务海关总署丢失两张 CD 盘，包括两千五百万名英国公民的财务记录。
3. 2006 年二月份，一名德勤会计公司（Deloitte & Touche）的员工将一张包括 9290 名 McAfee 公司员工信息的 CD 盘遗忘在一家航空公司的座位后面。
4. 2007 年，报告显示，包括敏感军方信息的 USB 盘在阿富汗的街头售卖。

对手提电脑可以采用全磁盘加密（full-disk encryption），但是，可移动设备却带来更多的挑战。移动办公的员工在出差时，有合法的需求需要使用这样的设备来传输数据，甚至敏感数据。以前曾有专用的硬件用于此用途，但价格下跌幅度太大，现在甚至在一个会展上，容量上兆的 U 盘都免费赠送，而且，如今也很难发现一台手提电脑不跟配 CD 或者 DVD 光驱。

虽然仍然有些公司会让技术人员在客户端机器上锁定 USB 端口，限定 CD 为只读，但是，大部分的企业还是依靠软件的解决方式，来管理这些潜在的数据泄露问题。让我们来看一下几个软件解决方案:

1. 在 Windows XP 和 Vista，可以利用组策略对象(GPO)限制设备的安装。Vista 提供的策略比 XP 更加细化，但是，已经由用户安装好的设备可能仍然还是可用，

这要看组策略对象是怎么配置的。这个是免费提供的，但其灵活性可能不如其他解决方案，还有提供的安全性也有限。

2. 许多第三方的软件工具能够限制移动存储的使用，包括 CD-ROM 和 USB 设备。策略可以非常细粒度，只有公司批准的设备才能访问，连接数码相机和音乐播放器只允许只读，而同时仍然可以阻止来自外部的数据传输。多数工具支持基于角色和系统的策略，允许对不同的用户和电脑组规定不同的限制（例如，所有的台式电脑完全禁用写入访问，但高层的手提可以启用）。
3. 阻止或审计对移动存储访问的第三方软件。策略允许访问，但同时保留一份这些文件的安全备份，然后，在下一次手提电脑连接到公司网络时，发送到管理服务器。这样，管理员就可以审阅活动，包括文件的内容，以判断是否符合公司政策。
4. 对移动存储进行可选或必选数据加密的加密软件。用户可以在公司和组密钥或者选择带密码的自身解密归档进行选择（视策略而定），来传送给不使用同一加密软件的合作伙伴。有的工具可以基于用户、组、系统或者存储设备实行策略。
5. 符合集中策略的专用 USB 设备。这恐怕是最贵的选择，不提供任何优于软件解决方案的实际安全好处。
6. 具有终端保护的数据丢失防护（DLP）产品。这些工具能够基于被检测的内容应用动态的策略。例如，可以对一个包括信用卡号码的文件加以限制，但是不包括敏感内容的 PPT 就可以进行传送。最好的工具使用深层内容分析，不仅仅保护易于识别的内容，例如信用卡号码、银行帐号，而且还保护半结构化数据，如被保护文件的一部分。有些工具包括加密，或者使用合作方的加密。DLP 是具灵活性的选择方案，所有工具都将最终包括基于内容的能力。不过，他们定义策略更为复杂，成熟程度的差异不均。

企业有多种方案可以选择，从简单的阻止设备的使用到实时的、与动态加密相连、基于内容的策略。最适合贵公司的解决方案要视公司的具体需求、用户的接受程度、预算和现有的基础设施而定。

（作者：Rich Mogull 译者：Shirley 来源：TechTarget 中国）