
# 安全加密秘籍

# 安全加密秘籍

无论是企业的自身需要还是安全标准的强制规定，为了更好的保护数据，加密已经成为企业的不二选择。那么，在数据的存储、访问、传送等过程中，企业应该分别使用什么加密方法？针对不同的数据级别，加密算法是否应该有所不同？移动设备的数据加密该如何实现？

针对以上问题，本技术手册将给出答案。我们将分别介绍存储加密技术，网络加密技术，应用程序级加密技术，并分三大部分，详细介绍支付卡加密方法，移动设备加密方法，数据库加密方法。

## 加密技术分类

制定加密策略计划的第一步是理解主要的加密技术类型，包括存储加密技术、网络加密技术、应用程序级加密技术。虽然各种方法都有各自的优点，但它们也有不足的地方，我们也需要把这些因素考虑进去。

- ❖存储加密技术
- ❖网络加密技术
- ❖应用程序级加密技术
- ❖如何选择合适的加密技术保障数据安全

## 支付卡加密方法

由于规则遵从（比如支付卡行业数据安全标准 PCI DSS）和 FFIEC 信息安全检查要求方面的压力，企业正试图找到最好的方法来保护持卡人的数据以及其他敏感数据的安全。“端到端加密技术”和“标记化技术”都是比较理想的解决方案，但每种方案都有各自的优缺点，所以在技术投资之前需要仔细考虑。

- ❖PCI 委员会发布点到点加密验证要求
- ❖权衡“端到端加密技术”和“标记化技术”的优缺点
- ❖标记化 vs. 加密

## 移动设备加密方法

现在越来越多的商务用户使用高端移动设备，当用户不在办公室时，都用这些移动设备来计算电子表格中的数据、读取敏感文件、存储敏感数据。 然而，移动设备在企业环境中的大量使用却带来了新的风险，即敏感数据被盗或丢失的潜在危险。一种保护移动设备数据的方法是进行加密。

- ❖如何为移动智能手机选择加密软件？
- ❖加密短信防范移动木马
- ❖防止笔记本数据丢失用 DLP 技术还是全盘加密？
- ❖便携式 USB 驱动器加密：软件和安全策略

## 数据库加密方法

通常情况下，公司一些最敏感的数据存储在数据库中。这些数据包括医疗记录、员工记录、信用卡号码、社会保障号码等，它们受隐私法规的监管，必须加以保护。最强大的数据隐私保护技术是加密。

- ❖数据库应用安全：如何平衡加密与访问控制
- ❖数据备份安全战略：云安全、加密与数据销毁
- ❖OpenWorld 案例分享：Oracle 透明数据加密技术

## 存储加密技术

存储加密技术是一种简单的加密机制，用于加密存储在硬盘和其它一些媒介如备份磁盘上的数据。这种加密技术主要用以应对突发的物理安全攻击事件，如包含敏感数据的笔记本电脑被盗。在这种情况下，Windows 操作系统至少会提供一些保护。假定硬盘使用的是 NT 文件系统并且也应用了适当的文件系统权限，那么，除非小偷知道用户密码，否则他是不能访问用户数据的。

然而，熟悉电脑的小偷会利用一种方法去重新设置本地管理员的密码，从而访问数据，或者只需移去硬盘并把它装在另一台电脑从而避开 Windows 操作系统的限制。所以，除非这些硬盘上的数据加密了，否则这两种方法可以很快就让小偷访问用户的数据。

在以上情况出现时，存储级加密可以保护数据，但有其他一些加密技术达到的效果可以更好。例如，Windows 加密文件系统（EFS）可以对数据卷进行加密，但它不能加密包含启动 Windows 所需特定硬盘文件的系统卷。这意味着，只有在电脑本身的物理安全得到保障的前提下，EFS 加密的数据才会继续受到保护。

如果计算机被盗，加密的硬盘又被移除并安装到另一台计算机上，此时 EFS 加密将会防止数据的泄密。然而，由于系统卷是不受保护，这样就无法阻止小偷采用一种可行的方法重新设置管理员密码，进而启动 Windows，用新密码登陆，并获取数据。

Windows Vista 和 Windows Server 2008 提供 BitLocker 功能，从而解决了这个问题。它使用的可信平台模块去加密系统卷。因为这是一个 BIOS 级的加密机制，所以它能防止密码重置攻击（假设系统卷已被加密）。

如果您正在考虑使用存储级加密，此时仔细制定密钥管理计划，并拥有一个密钥恢复机制就显得很重要了。密钥的丢失是一个相当普遍的问题。当钥匙丢失时，加密的数据无法读取。除非有备份的密钥可用，否则其结果将是数据永久性的丢失。

第三方的存储级加密产品大多与 EFS 的工作机制类似，但其管理起来更加容易。除了采用不同的加密算法外，EFS 和其他产品一个很重要的区别是密钥存储的方式。

Windows 把 EFS 密钥存储在系统盘上，这将产生一些棘手的问题。第一，当系统盘无法正常工作时，密钥便丢失，这将导致数据永久性的丢失，除非有备份的密钥可用（作为域的一部

分的 Windows 工作站通常会指派域管理员作为恢复密钥的代理）。第二，如果一台笔记本电脑被盗，熟练的黑客可以从系统盘上提取到密钥，并利用它们来解开加密的数据。许多第三方的加密产品通过把密钥存储在 U 盘或网络服务器上来应对这种盗取密钥的方法。

*（作者：Brien Posey　译者：Sean　来源：TechTarget 中国）*

## 网络加密技术

虽然存储级加密在保护存储媒介文件方面做得很好，但它无助于保护传输中的数据。数据流在通过网络或互联网时是不受保护，除非该会话被加密。当数据包通过网络时，黑客使用数据包嗅探器可以轻松地捕获个人的信息包，并做一个拷贝，最近那些频繁曝光的的信用卡信息盗窃事件利用的就是这种技术。这些数据包可以被重新组合，其中的数据就能被提取出来。有一段时间，这被认为是相当先进的攻击类型。然而，目前只需使用一些工具就可以完成所有的网络嗅探攻击工作，即使是不熟练的黑客都可以使用这种工具来窃取数据。

目前有无数可供使用的机制用于保护流经网络的数据。Windows Server 提供了 IPSec 加密技术。对于通过 Windows 的虚拟专用网进入 Windows 网络的移动用户，可以通过点对点通道协议、第 2 层通道协议或安全套接字层（SSL）加密得到保护。当然，这些都只是基于软件的加密方案。同时，也有工作在硬件和软件层的第三方加密方案。

对网络数据包进行加密主要存在两个缺点。第一个缺点，传统上网络加密一直难以实施。例如，使用 IPSec 加密技术通常需要具备企业证书颁发机构。管理员还必须了解密钥的管理流程，知道如何去制定一些政策去要求网络上的计算机使用 IPSec 加密。此外，IPSec 加密还可能会失败，除非网络客户端所使用的操作系统支持 IPSec 加密。

对网络数据包进行加密的另外一个主要缺点是它会使性能降低。每当客户端进行网络通讯时，都需要发起一个对话，并对将要发送的数据进行加密，接收端还需要对该数据进行解密。这个过程造成了网络流量的增加，迫使网络客户端主机不得不耗费更多的时间和系统资源来加密、解密数据。

有了网络适配器以后，可以减轻 CPU 加密解密的负担。虽然这种方式不会减少网络上的流量，但它可以缓解网络客户端主机性能下降的情况。

*（作者：Brien Posey　译者：Sean　来源：TechTarget 中国）*

## 应用程序级加密技术

应用程序级加密从本质上来说是一个复合方法，其基本思想是开发人员假设他们的程序会在不安全的环境下运行，因此需要给他们的工具加上专有的加密功能。

现在市场上很多软件产品都加上了应用程序级加密功能。像一些大家熟知的压缩软件，如WinZip，用户可以使用它来创建一个加密的压缩文档。不管所存的硬盘是否开启了加密功能，这个文档会一直保持加密的状态。同样地，即使是通过非加密的会话进行网络传送，这个文档的加密状态依然会保持不变。这是因为文档的加密算法直接应用与文档的数据上，与存储文档的介质和传送文档的网络连接无关。

应用程序级加密在增强你当前的安全性方面能起到很好的作用，但往往很难控制。每个内置加密功能的应用程序运作起来都不太一样，但总的来说，大多都是要求文件创建者输入密码才能访问该文件。该密码被当做一个加密密钥，但通常没有办法去集中管理这些密码。如果一个用户忘记了分配给主机所创文件的密码，那也就意味着他失去了文件中的数据。

此外，很多带加密功能的应用程序并没有考虑到多用户的情况。这就意味着如果某用户想跟其他用户使用同一个加密过的文档则必须共享同一个密码。

不管你选择怎样的方式，都需要成为“终端用户验证”的模式。大多情况下，提供了内置加密功能的应用程序会让用户选择是否进行数据加密。如果可以选择的话，用户会以最省事的方式来回避麻烦，而不会选择加密。

*(作者：Brien Posey　译者：Sean　来源：TechTarget 中国)*

# 如何选择合适的加密技术保障数据安全

多年来，如果公司想使得数据具备一个额外的安全度，他们可以选择性的使用加密技术。然而非强制性进行加密的日子已经一去不返了。现在，各行业的公司都受制于那些强制加密和其他安全标准的规章制度的限制，如果公司未能充分保护好他们的数据，将受到严厉的处罚。即使一个公司不受到这样规章制度的限制，许多法律还要求公司对那些未加密客户数据遭到破坏的安全攻击事件进行披露。

因此，这已经不再是公司是否应该使用加密技术的问题，而是一个公司应该如何对数据进行加密的问题。制定加密策略计划的第一步是理解主要的加密技术类型，包括存储加密技术、网络加密技术、应用程序级加密技术。虽然各种方法都有各自的优点，但它们也有不足的地方，我们也需要把这些因素考虑进去。

**权限管理**

权限管理是一个更高级的应用程序级加密技术，越来越多的人正在使用它。权限管理是一项可以给加密文档分配权限的技术。举例来说，这种加密政策会阻止用户从文件中拷贝数据，或者打印一个受保护的文档。

权限管理的一个优点是权限可以在后台服务端进行分配。这意味着如果一个用户打算把授权限控制的文件拷贝到移动介质上带出公司，管理员只需把相应的权限移除，就可以阻止这个用户获得该文档的数据。

Windows 系统本身就支持权限管理，一些第三方的产品也提供了类似的功能。大多数情况下，权限管理在安全方面起着很好的作用，但是由于产品的不同，初始化安装有时会很复杂。并且，根据权限管理的设定方式，移动用户如果不连接到公司的权限管理服务器上，则将无法打开受权限控制的文档。另外一个潜在的不足是，并非所有的数据类型都支持权限控制。理想情况下，权限控制的确可以把应用程序级加密功能结合起来，从而解决这些管理难题。

**如何选择**

由于存在多种类型的加密技术，选择一种最适合自身需要的技术对公司而言将成为一件很困难的事情。第一步，确定你的公司是否需要遵守联邦或行业的法规，这些法规强制规定了数

据该如何进行安全保护。如果需要遵守的话，可以把这些法规当成指导，进而决定应该选择何种加密方案。

大多数企业想要采取分层的方法。当涉及到加密时，一般的规则要求数据在静态和动态下都可以对其进行保护。如果数据只是在存储级、或者只在传输中进行加密，那么面对那些潜在的风险，数据并没有得到完整的保护。尽管应用程序级加密均满足这两个准则，但它也只能用来加强你的网络安全，并不能作为一种唯一的加密手段，因为不是所有的应用程序都提供了内置加密的功能，而那些具有加密功能的软件，其加密的强度也有所不同。

如果一个公司不受要求加密的行业规则影响，那么关键的问题就是技术部署和维护上的总成本以及对员工的要求。加密可能会在硬件、软件和技术支持上花费大量的费用，所以确保合理的收支效益很重要。

无论一个公司选择什么样的加密方案，对于终端用户来说都应该是透明的，并且要与自身的网络基础设施相兼容。一些加密方案会使得备份数据，或是对存储区网络上数据的访问、加密变得困难起来。一旦完成最初的安装，要确保你所考虑的方案不会造成重大的行政负担。

虽然加密技术在企业安全策略拥有一席之地已是不争的事实，但企业不能只依靠加密技术来解决其安全方面的问题。大多数安全专家都认为，并没有一个完美的安全解决方案。只要黑客肯付出足够的时间和努力，任何安全机制都能被绕开，即便你使用的强加密技术。一个优秀安全机制的关键是让攻击变得更麻烦，可以通过对安全机制采取分层方法达到这一点，这包括采用广泛的安全政策和使用多种安全技术。

*（作者：Brien Posey　译者：Sean　来源：TechTarget 中国）*

# PCI 委员会发布点到点加密验证要求

PCI 安全标准委员会发布了作为新计划一部分的点到点加密验证要求，该计划旨在为商家提供认证产品列表。

上周发布的 PCI 加密要求文件和 PCI 点到点加密解决方案要求，为厂商，评审员和商家提供了基于硬件的点到点加密部署指导，满足 PCI DSS 规则遵从。委员会表示，发布要求的重点在如何保护和监测硬件，开发和维护安全的应用程序，以及使用安全的密钥管理方法。

从信用卡是一个可以在销售点刷卡的设备，到后来它变成一个卡处理器，点到点或端到端加密提供商一直在宣传加密持卡人信用卡数据的好处。但是，在信用卡数据在传输到处理器和银行系统过程中被捕获到时，商家没有简单的方法来评估各供应商，以确定该设备，应用和功能是否满足 PCI DSS 要求。这个问题已经导致了一些知名的数据安全漏洞，这些漏洞突出了 PCI 评估和所谓的端到端加密部署中的缺陷。

去年，委员会所谓的点到点加密实施太不成熟了以至于不能进行正确的评价。一旦认证目录到位，这个事实可能就会改变（That could change once the certification listing is in place）。委员会将在 2011 年年底前推出测试程序，并计划 2012 年春天在其网站上，提供经验证的点到点加密实施清单。委员会表示，其点到点加密计划的第一阶段，把重点放在结合了基于硬件的加密与密钥管理软件实施的要求上。在第二阶段，经验证的要求将解决纯软件加密部署的问题。

验证文件勾画出了点到点加密实施中需要进行评估的六个部分。委员会将检查评估应用于硬件的安全控制，硬件中应用程序，目前加密硬件的环境，加密和解密间的传输环境，解密环境和密钥管理操作。

文件还规定了设备制造商，应用供应商和点到点加密供应商的责任。根据新的验证文件，供应商和制造商必须遵循的详细步骤使他们的产品在新计划的条件下通过认证。所有点交互设备都要在 PCI PIN 交易安全实验室（PCI PIN Transaction Security laboratory）进行评估，将考验硬件对 PIN 交易的要求。根据文件，一个合格的安全性评估将评估完整的部署，以确保硬件，应用程序和密钥管理进程完全满足 PCI DSS 要求。

“如果按照 PCI 要求实施，P2PE 解决方案可以显着降低商家信用卡数据环境风险，减少潜在的违规，并简化 PCI DSS 的验证工作。”PCI SSC 的总经理 Bob Russo 在一份声明中这样说道。

一个完全经验证的点到点加密实施将减少商家系统上的 PCI DSS 范围，但 PCI 委员会提醒道，商家仍需要根据 PCI DSS 进行评估，以确保系统是被保护和维护的。

*(作者：Robert Westervelt 译者：Ping 来源：TechTarget 中国)*

## 权衡“端到端加密技术”和“标记化技术”的优缺点

在金融服务行业，安全和规则遵从领域中一个有争议的热门话题是“加密技术（存储数据以及传输数据的加密）和标记化技术的对立”。由于规则遵从（比如支付卡行业数据安全标准PCI DSS）和FFIEC信息安全检查要求（其中也包括对加密和数据保护的要求）方面的压力，企业正试图找到最好的方法来保护持卡人的数据以及其他敏感数据的安全。“端到端加密技术”和“标记化技术”都是比较理想的解决方案，但每种方案都有各自的优缺点，所以在技术投资之前需要仔细考虑。

让我们从加密技术开始谈起。端到端的加密意味着需要对静止数据进行加密，然后在运送过程中保持数据的加密状态，直到它们最终到达目的地才进行解密。如果使用的是众所周知的、可信赖的算法对数据进行加密，那么端对端加密技术能够提供最高级别的数据保密性。

举个例子，支付卡业务公司使用的支付卡PIN密码就经常采用一个特殊的硬件安全模型（HSM）（采用3DES或者其他强有力的算法）来进行加密和解密。这些模型通常使用物理的锁和钥匙，只有那些具有管理权限的人才能接触到。在这种情况下，数据泄漏的可能性就比较低。还有一种情况，信用卡数据在各个网点（PoS）终端使用3DES、AES、或者其他的算法进行加密，直到数据最终到达银行处理的时候才进行解密。加密技术的另一个好处是它更容易跟现有的PoS终端、网络和数据库方案，以及金融应用程序集成在一起，因为它面世的时间比较长了。

不幸的是，端到端加密不是那么简单就能够实现的。首先，人们往往有些迷惑，到底端到端技术是怎么构成的。如果金融数据在不同的传输阶段使用不同的操作系统和应用软件进行处理，那么数据可能会经过多次加密、解密以及再加密的过程，这样就违背了端对端加密技术的初衷，因为数据在这些操作过程中是最脆弱的。许多情况下，由于商业原因，人们还会需要数据或数据的一部分；一个常见的例子就是保留经常性充值和返款（退款）的支付卡数据。另外，集中管理加密密钥存储非常复杂，而且也比较昂贵。在这些情况下，标记化（tokenization）技术显得更加实用。

标记化技术工作原理：在初始认证或者初始处理之后，它用一个特殊的值或者标识来代替支付卡数据或者金融账户记录。有人认为这种技术是解决加密与生俱来的在实现和管理方面所存在的复杂性的一个办法，标记化解决方案设置起来更加灵活、更加简单。如果使用这一技术，那么在很多情况下实际传输的就不是真正的金融数据，这也就排除了交易或者使用原始数

据。这个标识可以无限期的存储，这样就能够把这个值保留下来并在交易中继续使用，或者允许人们在这之后的任何地方都能访问实际数据。大多数情况下，企业都会把标记化技术外包给能够进行处理和数据控制的公司，这样在某种程度上也减少企业的安全管理负担。

然而，这种外包可能成为双刃剑。许多大型金融机构无疑会犹豫是否需要将诸如此类的安全管理技术外包出去。由于某些具体的政策、技术要求可能跟标记化不兼容，而且在环境中定位和“标记”所有的金融数据存在困难，他们可能不会采用标记化技术。对于有些大型机构来说，只需要简单的加密整个数据库或者整个存储环境就可以让金融数据得到保护，甚至那些管理员都不知道的数据也一样受到了保护。而标记化技术依靠的是显式的修改数据本身，如果为了使用标记化而移除这些加密控制的话，就会不经意的引起泄漏或数据丢失。由于这些原因，标记化技术现在似乎最适合那些有更多灵活要求或者需要更加精确控制数据的小型企业——比如数据存储在哪里，数据是怎么使用的，以及谁在管理那些标识和标识处理/存储程序等等。

展望未来，金融服务行业可能不会只选择其中的一种技术。尽管加密技术和标记化技术各有优点和缺点，但是它们共存的机会非常多。如果企业内部采用了标记化技术，那么进行标记化的服务器和存储区域基于安全的目的也还需要加密技术。而且由于标记化技术不能 100%的覆盖所有的应用程序和敏感的金融数据的使用情况，所以加密技术依然有用武之地。所以，并不存在简单的解决办法。不管是企业自己进行，还是把这些业务外包给供应商，两种技术都需要我们对其进行管理和维护。

*（作者：Dave Shackleford 译者：Sean 来源：TechTarget 中国）*

## 标记化 vs. 加密

目前，支付行业的管理人员和安全专家正在讨论保存和保护信用卡数据的正确方法。商家可以选择多种格式，其中包括保存加密格式（这种格式用加密算法代替 16 位数字的信用卡号码）、基于卡的标记格式（这种格式使用随机标记代替卡号，以减少 PCI DSS 评估的范围）等。EMC 公司安全部门 RSA 的技术总监 Robert Griffin 一直是许多加密和标记化项目的首席架构师。Griffin 是一位公认的加密专家，他还是 OASIS 密钥管理协作协议技术委员会的联合主席。在此次参访中，他谈论了为什么 RSA 保护信用卡数据的方法(该技术使用基于卡的标记)是最有效的防护方法（保护敏感信用卡数据不受网络罪犯的攻击）。该安全供应商最近发表了一份白皮书《Secure Payment Services: Credit Data Security Transformed（安全支付服务：信用数据安全变换）》，阐述了该公司对此技术的立场。

**零售商们有很多比较旧的系统，他们采用新技术的进程似乎比较缓慢。有没有商家已经着眼实施某种形式的保存/加密技术来保护信用卡数据呢？**

Griffin：我认为，市场上其实存在着一个很大的分歧。比如，我们 RSA 第一次实施标记化技术是在 Staples 公司，他们从 2004 年开始就已经完成了最初的架构工作。那时，他们已经做出决定，不使用加密模型而是使用标记化模型来保护 PCI 跟踪以及数字信息。在这种情况下，标记化的定义取决于替代模型而不是变换模型。这里面存在着一个重大的行业分歧——“使用原始值的变换来创建任何相关值的模型”与那些“没有使用这种变换的方法”之间的分歧。标记化是指你把原始值映射为一个新的值，并把这个新的映射值作为标记来使用。我曾经参与 PCI DSS 范围委员会有关标记化的工作，该委员会面临的最基本问题就是这种分歧到底有多明显，以及怎样出现在确定范围的指导意见中。

**你认为我们将会更多地使用混合模型吗？**

Griffin：从一个方面看是肯定的。我们的感觉是，在你做替换的模型中，映射数据库与应用程序的分离非常重要。基本模型是指你把真正的值转移到某种标记化的服务上面。这意味着当你把值从所在地点转移到标记化服务的时候，你必须保护转移过程中的值。你可以简单地进行运输级别保护，但是我们认为，在数据移动的过程中，你应该实施多层次的保护措施。这种情况下，对数据进行加密极为重要。对于我们来说，你送回到交易时的内容与你送到标记化服务器的值没有任何算法、数学和变换上的关系。这就意味着所有的强力变换攻击、所有的密钥攻击（一旦你发现某次变换的密钥，你就可以知道所有其他变换的密钥）——所有这些威胁

都不复存在。我认为这是加密模型（不管是保存格式还是扩展加密）与这种基于映射、没有变换的模型之间的巨大区别。我们对这个问题的看法是，替代模型非常有效。

**这些传统的业务分析系统和数据库似乎是较大的多达。保存加密格式可以在这方面发挥作用，因为你可以用加密格式保存 16 位信用卡号码。你能用基于卡的标记来这样做吗？**

Griffin：当然可以。我们在两个客户项目中建立了我们自己的标记化解决方案。Staples 公司是其中的一方，另一方是一家包裹运输公司。我们与他们进行讨论，首先让他们理解一件事件，那就是一定要尽可能的减小对当前应用程序架构的影响，而最好的办法就是保持信用卡号码的长度不变，并且保留信用卡号码的最后四位数字。只要你把号码的最后四位数字映射到标记上，并保持同样的 16 位数字结构，那么这个标记其实跟保存加密格式同样有效。

**在 First Data-TransArmor 处理过程中，First Data 把 PAN 与先前处理过的信用卡做对比，以检查一个标记是否被使用过。由此，我可以知道在 First Data 中保存着这样一个文件，里面既有标记也有信用卡号码。如果网络罪犯掌握了这个文件，应该会造成重大的数据泄漏事件吧？**

Griffin：这个映射表格是这个架构真正的核心所在。这个文件一定要受到保护，这极为重要。你应该像保护密钥管理相关事宜那样严格地保护它。映射表格式中包含的敏感信息也需要得到很好的保护。如果把所有的信用卡信息都聚集在一个地方，那么你就可以在该处实施保护措施；而如果信用卡信息很分散的话，那保护起来就相当的困难了。你需要像保护密钥管理那样使用高级别的多层防御来保护这个表格。你必须采用适当的身份管理，对个人数据元素进行加密是绝对需要的，而且加密级别越细致越好。同样，你还应该关注物理环境和虚拟环境中的基础设施模型。

**另外一个问题是延迟问题。对于商家来说，让客户的支付过程快速便捷非常重要。现在计算机的处理能力真的可以让延迟问题不再是问题了吗？**

Griffin：这包括网络关系以及标记化操作的延迟。在这种情况下，我认为一个更重要的问题是网络连接的带宽。举个例子，我们第一次在 Staples 公司遇到这种情况，那时他们已经为几个商店提供了拨号连接，早在架构设计时他们就非常担心这是否会造成交易中出现一到两秒的时间延迟。但是后来他们发现，情况并非如此。他们非常高兴自己推出的产品可以适应各种环境。即便是环境中的带宽和传输速度千差万别，但是由于数据包（你的数据传输量）非常小，实际上不会对支付终端上的客户反应时间产生多大的影响。

**还有一个问题是关于大型商家使用多个支付处理商的讨论。这意味着将会有不同种类的标记化解决方案。那么对于标记化来说，为什么没有任何标准呢？**

Griffin：关于标记化我们需要知道两件事。其中之一就是我们在 PCI DSS 特殊利益集团内部所做的有关标记化的工作。如果你在使用这种替代模型的话，那这部分工作主要侧重于确定范围和操作指南。另外就是由美国国家标准学会所做的工作，可惜的是要靠这方面工作来阐明标记化意味着什么却显得更加的困难。可以拿 API 作为例子，我认为在这个领域内还没有任何重大的进展，这一点是我们 RSA 感兴趣的地方。相对于范围确定的问题，它只能屈居次席，我认为这跟密钥管理是一个道理。我们看到许多供应商不仅使用标记化来保护 PCI，而且还用它来保护其他类型的信息，那么供应商就不会被禁锢在单一的支付处理商以及他们的基础设施上面，所以标准 API 的发展将非常重要。不过我们还没有开始那方面的工作。

*(作者：Robert Westervelt 译者：Sean 来源：TechTarget 中国)*

## 如何为移动智能手机选择加密软件？

现在越来越多的商务用户使用高端移动设备，它们具有文字处理、银行帐户认证、网页浏览、收发电子邮件以及其他许多功能。随着远程工作人员的不断增加，当用户不在办公室时，都用这些移动设备来计算电子表格中的数据、读取敏感文件、存储敏感数据。

然而，智能手机在企业环境中的大量使用却带来了新的风险，即敏感数据被盗或丢失的潜在危险。一种保护智能手机数据的方法是对手机进行加密。和笔记本电脑加密一样，手机加密产品可以从内置操作系统功能、企业管理工具、第三方软件中获得。

总体而言，商业智能手机加密软件的产品数量仍然很小，可随着越来越多的企业认识到这些设备可能导致的严重安全隐患，加密产品的数量也会快速地增长。企业评估智能手机加密产品时应考虑哪些方面？下面列出了一些最关键的因素：

- 费用：几乎没有公司提供内置加密服务，而通常那些免费或廉价的服务也只对个人提供，几乎没有集中管理功能或政策功能的服务，不能面向企业用户。鉴于这种情况，企业在将来应该为这些产品增加支出，并做出相应的预算。

- 平台支持：大多数企业规定只能使用一个智能手机操作系统，如黑莓的操作系统，但某些特殊的用户（如行政人员或销售团队）却使用不同的设备，像苹果的 iPhone 或 Windows Mobile 手机。因此，在大多数情况下，你应该尽可能的选择一个可以支持多种平台的加密产品。

- 政策重点：针对使用移动设备和保护敏感数据，所有企业都有自己独特的安全需求和政策。一些企业会重点加强认证和密码防护，而其他企业则可能会更多地关注加密。不过，其他企业可能会需要远程数据清除功能以替代诸如加密或认证这样的安全控制。确定企业关于智能手机的安全需求，并由此制定政策重点，不管是在当前还是今后，都将有助于企业选择适合自己的加密产品。

- 集中管理：对智能手机加密技术进行集中管理的政策，以及实时监控每部手机的加密状态，对于具备众多设备的企业而言往往是必要的。此外，在许多不同的规则中都要求的记录和报告，通常只在企业级的管理控制台和产品中才会提供。密钥管理几乎总会被集成到每个企业级的产品中。

接下来，让我们概括一下现在人们所使用的智能手机加密技术的类型。第一类是内置的智能手机加密，它位于手机的操作系统中。几乎没有智能手机具备这种独特的加密技术，即使有也往往只包含有限的加密特性。

目前发现的最强大的智能手机加密技术应用在 Windows Mobile 智能手机上。为保护电子邮件、任务、日历信息以及用户的“我的文档”文件夹，Windows Mobile 提供了可供企业使用的 AES 128 位加密技术。此加密技术同样可以保护存储在安全数字卡（SD cards）上的所有文件，当这些文件加密后，其他任何智能手机都将无法读取。

黑莓是最流行的商务智能手机，它通过黑莓企业服务器（BES）应用程序（一种拥有所有权的独立产品）来提供加密技术。智能手机上的本地文件可以通过集中管理政策（通过激活内容保护功能）来进行加密，也可以通过设备的验证密码进行加密，这些验证密码是利用 AES 加密技术进行安全存储的。

苹果 iPhone 提供了它所形容的“强大的硬件加密技术”，但这名不符实。该功能实际上旨在加强其远程擦除功能，在设备丢失或被盗时消除一切数据。Palm Pre 手机新的 WebOS 没有内置加密技术，但这些仍然使用较旧 PalmOS 的公司可能会发现一些可用的应用程序（包括所有的附加组件）。

大多数智能手机的加密技术来自第三方的商业产品。PGP 公司和 Aiko 解决方案有限公司都为 Windows Mobile 提供了加密产品，而且 PGP 也支持黑莓设备。虽然苹果 iPhone 在个人消费市场非常流行，但因其缺乏管理和安全功能，它在企业中用得较少，并且现今几乎没有真正的企业加密产品适用于此平台。多种加密应用程序，如用户可用的 Firebox、My Eyes Only 和 SMobile ContactCrypt，都只能在本地对数据进行管理。一个确实可以对 iPhone、Windows Mobile 和 Palm 手机进行加密和集中管理的产品是 GuardianEdge 科技公司的智能手机保护，它集成了 Microsoft Exchange，可以对 SD 卡进行加密，还可以提供诸如智能手机防火墙和应用程序控制等额外安全功能。

无论智能手机是在企业环境中还是作为一个独立的设备使用，智能手机加密技术适用于所有的用户。由于这些设备要存储和获取数量越来越大的敏感数据，保护个人和公司数据的需求也变得更加重要。通过对这些设备进行加密，企业通过确保他们的数据安全（无论是手机丢失还是被盗），进一步加强了移动智能手机的安全性。现在最大的问题是：你要如何开始？

对智能手机加密各个方案进行评估时，企业应该做的第一件事情就是确定他们的真正需求是什么，而且这应该是有政策依据的。确保政策明确列出了用户在智能手机平台上可以发送、接收和储存的数据类型，并确保把智能手机的一致类型（consistent type，也可能是模型）

作为企业的标准。一旦这些政策得以实施，下一步就是评估数据分类政策和可接受的智能手机使用规范，以作为企业用户每天工作的依据，让他们知道数据保护需求最终是什么样子的。确定哪些用户有智能手机，这些用户可以访问什么类型的数据，然后进行风险评估，以确定这些数据有可能被破坏或丢失的途径。

经过这一过程之后，应该会有助于缩小企业最适合产品类型的范围。其他的一些因素，比如成本、实施的便利性和安全性以及弹性需求，可有助于进一步减小选择的范围。一般来说，确定需要智能手机的任何企业都应确保强大的、值得信赖的加密技术是可能的（例如 AES 128 位或更高位），确保集中管理和政策控制是可用的，而且当智能手机丢失或被盗时，数据可以被清除。

*（作者：Dave Shackleford 译者：Sean 来源：TechTarget 中国）*

# 加密短信防范移动木马

**问：什么是防范移动电话上的木马的最佳方法？特别是针对那些试图窃取消息的木马？有没有在企业中加密移动电话间 SMS 消息的方法？**

答：在最近的专家答疑中，我们已经谈到了一些保护智能手机安全的方法。同样的安全步骤可以保护你的智能手机免遭窃取 SMS 消息的木马。安装在 Android 平台智能手机上的许多应用程序要求更多的权限，已超过必要的权限。甚至可能在不需要的时候要求 SMS 消息的权限。在应用程序安装时，用户可能没有仔细审查他们赋予应用程序的访问权限，可能会不必要地允许应用程序访问 SMS 消息。如果应用程序需要访问 SMS 消息，在允许访问和安装应用程序前，用户应该仔细审查。

对短信进行加密，可以帮助防止流氓软件或木马程序窃取 SMS 消息。有许多方法可以加密个人移动电话（使用 Android 智能手机免费获得的应用程序）间的 SMS 消息。例如，WhisperSystems TextSecure 允许你发送和接收加密的短信并加密存储在智能手机上的短信。发信者和收信者都要安装 TextSecure，但是该软件除了密码外，不需要其他的配置。使用这个应用程序可以确保 SMS 消息的安全使用。一些商业应用，如 Protected SMS，可用于企业保护 SMS 消息安全。

*（作者：Nick Lewis　译者：Ping　来源：TechTarget 中国）*

## 防止笔记本数据丢失用 DLP 技术还是全盘加密？

**问：我有一个关于风险优先级的问题。我们让信息管理人员在他们的笔记本电脑上管理敏感数据，但最近我们遇到了这样一件事情，一名雇员因泄漏数据而被抓捕（他随后被解雇）。我想在我们所有管理人员的笔记本电脑上部署一个数据丢失防护（DLP）产品（防止潜在的数据泄漏）、全磁盘加密和远程擦除软件软件，但所获得的资金只允许部署一个产品。你有什么好的建议吗？**

答：很好的问题！关于风险优先级存在着很多不同的观点，但我更倾向于用最容易的方法处理更高一级的风险。我的选择是对企业中所有笔记本电脑进行全磁盘加密。

原因有很多，以我在全盘加密方面的经验来看，全盘加密是一个相当强大和成熟的技术。此外，它对用户是透明的，这意味着在运行机器时，用户需要记住几个按钮或选项。相比之下，我对数据丢失防护（DLP）技术的看法是，它们对保护企业电子邮件和其他对外电子信息中的敏感数据很有用，但未必能解决电脑安全问题。

2009 年 4 月，Ponemon Institute 发布了一篇报告：《丢失笔记本电脑的企业风险》。该报告包括了对来自世界各地（包括美国、英国、德国和巴西）的 3100 个信息技术从业人员的 Web 调查结果。

该报告询问受调查者员工通常在什么地方丢失他们的笔记本电脑。以下是调查结果（从高到低显示）：

1. 宾馆
2. 租用车
3. 开会场所
4. 机场
5. 住所
6. 出租车
7. 火车或地铁

8. 客户办公室

我觉得这个结果很有趣，因为在一周里持笔记本电脑的管理人员可能出现在以上场所中的一个或多个。因此，丢失笔记本电脑的风险很高，这意味着在应对紧急的风险时，全盘加密可能是更容易和更快捷的解决方案。

*（作者：Ernest Hayden 译者：曾芸芸 来源：TechTarget 中国）*

# 便携式 USB 驱动器加密：软件和安全策略

便携式驱动器上的文件同步功能使同步、传输以及备份数据变得越来越方便，因此越来越多的企业和消费者开始使用 USB 设备。

根据圣克拉拉咨询集团的调查，仅在 2009 年，便携式驱动器的出货量就近 1 亿 9000 万，平均容量为 8GB。但是这些小工具很容易从人们的口袋和钱包中丢失，从而使其中存储的数据存在风险。这里，我们将讨论在企业级驱动器加密中便携式驱动器加密如何提供帮助以及需要考虑的问题。

**便携式驱动器加密：袖珍保护**

当一个驱动器因为被盗、遗失或借出，落到错误的人手中时，加密可以防止文件被浏览、复制或者打开。

用于桌面电脑或笔记本电脑驱动器的全磁盘加密，使用一些本地代码来扰乱和解译数据。有了便携式驱动器，就可以将文件从一台机器上移到另一台机器，把工作带回家做，携带用于展示的幻灯片，和同事一块合作。因此，USB 驱动器的优点是，它自带一个便携式的数据加密功能；它是一个加密数据的容器，同时还自带一个便携程序，可以挂载卸载和读写数据。

在 Windows7 的商业版和终极版里，便携式驱动器加密可以通过 BitLockerToGo 来完成。当它在一个便携式驱动器使用时，Windows 创建一系列文件：一个 BitlockerToGo.exe 阅读器，一个当驱动器插入系统时自动运行阅读器的文件，以及组成一个 AES 加密卷的系统文件。这些文件被复制到驱动器上，存储在那个加密卷里，只要输入这个驱动器的密码就可以在任何一台安装有 Windows XP、Windows Vista 和 Windows 7 的个人电脑里打开。

**符合企业需求**

一些免费的程序，如 BitLockerToGo、TrueCrypt（旅行者磁盘模式）和 CryptArchiver Lite，使个人用户可以很方便地保护自己的便携式驱动器。企业用户也可以决定是否以及如何使用这些免费加密软件。举例来说，商业用户可以使用 BitLockerToGo 策略来阻止文件被复制到没有加密的驱动器上，还可以设置打开加密驱动器密码的最小长度。

但是，商业用户应该考虑使用商业程序来满足需要在便携式驱动器上存储敏感数据的大量人群。提供加密便携式驱动器的企业化可移动介质安全产品的公司有：BitArmor Systems、

Check Point 软件技术有限公司、Credant Technologies、 GuardianEdge Technologies、McAfee、PGP、Sophos、Symantec 以及其它公司。商用加密便携式驱动器则通过存储厂商提供，如：Corsair、IronKey、Kanguru Solutions、金士顿科技公司、SanDisk 公司以及 Verbatim Americas LLC。

企业级相关的产品在价格、性能和功能上有很大的区别。下面是在采购便携式驱动器加密时需要咨询的一些问题：

1. **物理安全**：你是否需要坚固耐用、金属包裹、防篡改的驱动器？公司策略或标准需求是否授权一个特定源或装配的组件？

2. **加密**：该产品使用的是硬件加密还是软件加密？提供的密码和密钥长度是什么？你的驱动器或程序是否需要通过 FIPS 140-2 和通用标准 EAL 认证？

3. **密钥**：加密密钥是如何产生、储存、撤销以及收回的？密钥是否可以存储在一个硬件 vault 里？如果密钥是通过 USB 线路发送的，那么是否可以防止被监听和重放攻击？是否支持离线驱动器的工作？

4. **认证**：这个容器是否可以通过密码、智能卡、双因素、预启动或域的 SSO 方法来进行解锁？可以执行的最低安全政策是什么？它是如何阻止强力破解攻击和击键记录器的（比如，远程数据清除、自动数据消除、虚拟键盘）？

5. **范围**：加密硬盘上的所有文件，还是只是安全文件夹？你的用户是否需要选择性地与授权用户或组共享加密文件夹或文件？

6. **用途**：用户需要扩展只读访问到第三方吗？他们是否需要在一个独立的安全环境下进行读写访问？您目前是否允许离线（无人监管）访问，以及允许的时间？

7. **完整性**：这个驱动程序能否提供板载（便携式、主机独立的）保护，阻止恶意软件感染和传播？

8. **可移植性**：哪些操作系统和文件系统支持加密驱动器初始化、文件创建与删除、数据读写和工具执行？

9. **初始化**：是否有可以加速并简化便携式驱动器检测、激活和配置的工具？你是否需要根据类型、牌子、型号、序列号、用户及组或其他政策定义的标准来允许或禁止激活驱动器？

10. **管理**：这个产品是否提供集中化 IT 审计，能否提供驱动器上的加密策略、加密密钥和固件软件的更新？

11. **报告**：此产品是否可以向一台中央服务器发送驱动器、策略、数据状态，以完成一个合规报告或其他用途？加密状态是否足够，公司策略或法规是否要求跟踪和报告文件及文件夹的活动（例如，复制、读写和删除）？

12. **整合**：它将如何与相关的基础设施（如，用户目录）以及你公司的其他安全产品（如端口控制盒桌面电脑硬盘加密）相匹配？

企业需求也各不相同，例如，活动目录认证对一些企业来说很关键，但对其他企业来说无关紧要。不过，这些的问题可以帮助公司选择便携式驱动器的加密产品，理解用于个人、中小型企业和企业的各种产品之间的不同。

*（作者：Lisa Phifer　译者：陈运栋　来源：TechTarget 中国）*

# 数据库应用安全：如何平衡加密与访问控制

通常情况下，公司一些最敏感的数据存储在数据库中。这些数据包括医疗记录、员工记录、信用卡号码、社会保障号码等，它们受隐私法规的监管，必须加以保护。

然而，与此同时，公司必须在敏感数据的安全性与可用性之间进行折中，以满足因合法的商业使用而访问这些数据的需求，包括为保持业务连续性而进行的备份和远程复制。最强大的数据隐私保护技术是加密。但是，为了既切实保证敏感数据的安全性而又不影响业务的连续性，使用加密技术时必须小心。在保护敏感数据以及平衡加密与访问控制方面，数据库应用安全的一些最佳实践值得借鉴：

**数据最小化与模糊处理**

保护敏感数据的最好、最有效的办法是当初就不存储或少存储数据。因此，公司应该经常检查下列数据最小化问题：

- 该数据将来还需要吗？
- 可以只存储用于身份验证的部分数据（例如社会保障号码的后四位）吗？
- 可以使用其他不太敏感的数据（例如宠物的名字）进行身份验证吗？
- 可以使用或存储数据的 hash 值（例如 MD5、SHA）而不是原始数据本身吗？

在许多情况下，这些问题可以减少需要存储的数据量并降低数据的敏感程度。

**数据加密**

公司可以对数据库中的数据进行加密，以防止其被盗或意外泄漏。在加密数据库中的数据时，有三个关键问题需要考虑：在何处加密数据、如何加密数据以及在何处存储密钥。下面将分别讨论这些问题：

**在何处加密数据**——加密可以在应用层、数据库或底层存储器中进行。如果加密在数据库中进行，则还可以对特定字段、列、表或者整个数据库加密。当然，在应用层、数据库和底层存储器中加密各有利弊。

由于应用层加密是在系统的最高层对数据进行加密，所以数据对应用层之下的各层都不可见。如果加密在应用层进行，则数据库、操作系统、网络以及数据经过的所有其他路径都只能看到加密后的形式。

应用层加密的问题在于，通常会有多个高层应用程序需要访问数据，这些应用程序将需要密钥副本对数据进行解密。可以获得密钥副本的应用程序越多，密钥遭到泄漏的可能性就越大。

但是，如果加密在较低的层进行，则你还需要进一步在其他层进行加密。例如，当数据流经数据库和应用程序之间的网络时需要对其进行加密，否则数据对网络层将是可见的。这将会引入需要加以保护的其他加密密钥。在何处进行加密是一种微妙的平衡，取决于应用程序和数据流的体系结构。

**如何加密数据**——加密可以利用软件、硬件或者软件硬件相结合的方式实现。具体采用何种方式加密，取决于你希望达到的吞吐量（Mb/s）。如果希望获得较大的吞吐量，则你可能需要一些硬件加速方式。无论采用何种加密方式，有一个问题别无选择：始终使用先进的、强大的、基于标准的加密和密钥管理系统；不要试图发明自己的加密和密钥管理系统，你自己的加密和密钥管理系统可能奏效也可能不能奏效。目前，一些高端服务器处理器已经内置了支持AES（高级加密标准）的加密基元（Encryption Primitives），可以实现比基于软件的算法快得多（高达 9 倍）的加密。

**在何处存储密钥**——加密最大的挑战不是加密本身，而是密钥的存储和分配。加密数据的安全性和可访问性并不高于密钥本身。密钥必须悉心保护，以防攻击者窃取。同时，密钥必须与加密数据分开存储，但又要可供加密/解密算法访问。另一方面，必须对密钥进行备份和复制，以便当原始数据和原始密钥由于灾难而丢失时可以解密备份数据。你选择的任何密钥管理系统必须支持下列功能：

- 安全存储密钥。
- 认证和跟踪审计对密钥的访问。
- 托管或恢复密钥，以防密钥丢失。
- 备份密钥并将密钥安全地传输到远程位置，以供恢复之用。

**加密标准**

许多加密和密钥管理系统都通过了以下两个实用标准的认证：美国联邦信息处理标准（Federal Information Processing Standard，FIPS）140，其安全级别分为 1 到 4 级；通用标准评估保证等级（Common Criteria Evaluation Assurance Level，CCEAL），其安全级别分为 1 到 7 级。这些标准提供了一个指标，可以比较不同系统的加密算法、密钥存储和密钥管理机制的安全性。级别越高意味着加密算法、密钥存储方法、防篡改硬件和密钥管理机制越好。例如，FIPS 在确定一个认证级别时，考虑了 11 个不同方面的安全性。你应该根据数据的敏感程度和你所在地区的监管要求，选择合适的安全级别。

数据库应用极为复杂，由多层松散耦合的组件构成。数据库应用的安全性难以保证，但又包含了公司最敏感的数据。然而，利用数据最小化和加密技术，公司可以巧妙地在数据的安全性、可访问性和可用性之间取得平衡。

*（作者：Andreas Antonopoulos　译者：王勇　来源：TechTarget 中国）*

# 数据备份安全战略：云安全、加密与数据销毁

2005年美国银行加密的磁带丢失，造成了大量客户资料泄露，从此以后，数据安全性就一直受到人们的关注。

在此之前，一部分银行的系统管理员认为磁带加密设备价格过于昂贵，有些管理员认为数据加密就跟保险一样，并不是首先需要处理的事情，还有些管理员因为不知道应该购买备份软件还是购买安全软件而将此事搁浅。

这次美国银行泄露客户数据违反了地方法律，不过2005 Specter-Leahy 法律规定安全数据和客户个人资料盗窃可以构成联邦级别的犯罪。加利福尼亚州2003年SB-1386法律就开始对泄露数据做出了规定。在1996年制定的Health Insurance Portability and Accountability 法律中，规定了个人的医疗记录不能随意公开。

Michael Versace信息安全机构的研究员兼合伙人Wikibon称：“由此我们可以看到各家公司是如何遵守法律的。法律很多年前就对如何保护客户的隐私信息作出了规定。”

在数据备份中有四个方面跟数据安全密切有关：磁带加密、云备份安全、密匙管理和数据销毁。下面我们就分别来讲一下。

**磁带加密方案**

在2005年时，只有数据加密设备可以为磁带进行加密，而由于这种设备的价格很高，很多银行根本支付不起。基于软件的加密技术稍微便宜一些，而性能却达不到要求。

Versace说:“从那时起，IBM公司和Sun微系统公司就开始研究LTO-4磁带加密产品，希望将它加入到现有的磁带架构中去。”

但是，存储杂志最近组织的购买意向调查显示：大部分公司仍未使用磁带加密设备。大约50%的调查者称他们已经使用加密设备，未使用的人中只有少数部分会在明年购置磁带加密设备，大部分人仍觉得磁带加密并不是非常必须的，可以推迟几年再采购。

同时，数据泄露事件在全球也是频频发生，例如最近英国的农村支付机构。Open Security Foundation的DataLoss DB每天都会对丢失数据的企业进行报道。

Versace 称：“一些用户一直在担心，如果误操作或者加密后的数据无法恢复该怎么办？”

企业策略集团（ESG）公司的分析员 Jon Oltsik 称：“那些没有使用磁盘加密设备的公司已经落后了。”

**编辑推荐：**磁带加密方法优缺点对比——基于主机加密 vs. 基于设备加密，请参阅这篇文章。

**云备份安全性**

数据安全一直是云存储中的关键问题。在今年早期，Gartner 称：很多客户由于害怕数据不安全而放弃云存储。由于风险太大，一些公司并不想把数据外包给第三方的公司。

大部分的云服务提供商，例如 IBM 公司，在传输用户数据时都会进行加密。用户的数据不会以明文的形式显示，只有持有密匙的用户才可以对数据进行恢复。当用户通过 web 界面来监控以及管理后台的云备份系统时，云服务商会使用 SSL 链接对数据进行加密。

Versace 称：“对于一些规模较大的公司来说，由于资金充足，数据加密工作可以由公司独立完成。但如果是中型企业或者小型企业的话，将数据加密外包给专业的公司会更加合算。”

信息安全顾问 Kevin Beaver 在最近的一篇文章中指出，在传输数据时，只采用加密和 SSL 是远远不够的，还有许多潜在的不安全因素需要考虑。

Oltsik 指出，任何持密匙的人员都存在安全风险。收买管理员然后进行数据解密并拷贝，这种事情也时有发生。

**编辑提示：**请参考 Kevin Beaver 的在线和云备份中如何保证数据安全的文章。

**管理密匙**

许多存储厂家效仿一些数据安全厂家，开始提供密匙管理产品。目前各种级别的加密和密匙管理产品已经广泛用于各个数据中心中。

虽然现在市场上的产品很多，但专家认为缺少一个统一的行业标准将他们连接起来，这是现在密匙管理行业遇到的最大的问题。

今年年初，惠普公司，EMC 公司/RSA 安全，IBM 公司和 Thales 集团联合其他的厂家向 OASIS 提交了建立密匙管理系统和加密设备行业标准的申请。这个标准跟 IEEE 在 2008 年 1 月

制定的行业规则重复，但 IEEE 计划将它制定的行业规则整合到更为宽泛的 OASIS 的密匙管理互操作协议中去。

Oltsik 称：“我们会在 2010 年制定正式的 KMIP 标准”

即使制定了标准，有些问题仍然存在。在 11 月初，CA 公司推出了基于 z/OS 大型机的密匙管理器（EKM）软件，并称很多用户都需要这种基于开源系统的密匙加密管理器，如果没有密匙，加密的数据将无法恢复（z/OS 的制造商 IBM 对这件事感到非常惊讶，因为 IBM 的密匙管理系统可以直接部署在开源系统上。）

Versace 说:”密匙管理是分布式还是集中式还没有最终确定。原来所有的密匙管理系统全部都是分布式的，也就是需要部署到每个终端机器上，但有些操作需要集中式管理，例如密匙修改，审计以及登录等。我个人认为最终的产品会将这两种方式结合在一起。“

**编辑提示：**请参考 Kevin Beaver 的采用加密密钥管理让你的数据备份更安全这篇文章

**数据销毁和数据删除更加安全**

每家厂商都提供了很多销毁或者删除数据的方法。 如果磁盘介质上存有敏感数据，常规的手段是无法消除的，因此 EMC 公司通过在原来的数据上再写入数据的方法来达到彻底删除原来数据的目的。消磁是另外一个消除数据的方法，而且不会破坏物理介质。以后通过简单的销毁相关密匙就可以把加密的数据安全删除掉。

分析人士称：“这其实不是数据消除方面的问题，而是数据安全管理中的问题。哪些数据需要删除是这个环节中最重要的问题。”

磁带加密在 2005 年并没有引起太多人的关注。Oltasik 称：“多数人认为数据删除比较简单，这可能是因为公司的数据删除没有军队里面要求的那么严格造成的。”

**编辑提示：**请参考数据销毁技术手册。

*（作者：Beth Pariseau 译者：曹同举 来源：TechTarget 中国）*

# OpenWorld 案例分享：Oracle 透明数据加密技术

*旧金山：*去年六月，一个机器人病毒攻击了宾夕法尼亚州大学的数据库，数据库中存储的15805 条社会保障号码被泄露。更早几年前，一台保存有社会保障号码的笔记本电脑在匹兹堡大学被窃。

Matthew Stewart 是 Robert Morris 大学(RMU)信息安全主管，在他受聘主管学校的安全工作时，他想阻止这类数据库安全事件发生。在本次 Oracle OpenWorld 2010 会议上，Stewart 讨论了保障教育机构信息安全的困难。

Stewart 说：“对大学来说，唯一的事就是他们不得不开放。他们有学术自由;你不能把他们锁死。但是你不得不遵从法律约束，这带来了许多特殊的挑战。”

例如，当人们在一所学校内的这个校区走到另一个校区时，很容易忘记他们有过不同的访问级别。但是内部访问者并不是唯一的威胁，Stewart 说黑客、学生、恶意软件、网络钓鱼软件、物理盗窃，甚至 DBA 的误操作都是所有他关注的重大安全问题。

于是，他向 Oracle 求助。

在 Stewart 加入 RMU 时，安全状况“非常糟糕”。他们运行 Oracle 8.1，打补丁周期非常少，而且有太多的访问权限被授予给太多人员了。但是，通过利用 Oracle Advanced Security(一款可以帮助实现像网络加密，透明数据加密和备份中的数据保护这几类关键领域的产品)，Stewart 可以快速扭转局面。

他说：“我们利用分层的安全方法来覆盖所有方面。”他描述了他创建的六层安全措施：主动软件保障，阻塞基于网络的攻击，阻塞基于主机的攻击，消除安全薄弱环节，安全支持授权用户，管理安全和使效益最大化的工具层。

Stewart 还强调了透明数据加密(TDE)的重要性，它是对静态数据的加密。他说 Robert Morris 选择基于表空间的 TDE，而不是基于数据列的 TDE，是因为大学里要处理大量的事务业务。性能测试表明，增加了安全加密以后对性能的影响是微乎其微的。

Kurt Lysy 是 Oracle 公司一位高级安全部署专家，他说你的 TDE 还应该与你的备份和恢复策略保持一致。

Lysy 说：“当你看到加密静态数据的大视角时，千万不要忘了加密那些备份数据的重要性。”

然而，Stewart 在采取措施保护他组织的数据时，他可能是少数派。来自独立 Oracle 用户组(IOUG)的最新数据安全调查结果显示，在 430 名受访者中，只有 30%以下的人在他们的组织中对所有数据库中的个人身份信息进行加密。

许多受访者还表示他们正在采取反应性的，而不是预防性的方法来保护数据库安全，而且他们中有四分之三组织没有有效方式可以阻止有权限的数据库用户访问 HR 系统，财务系统，或者他们数据库中的其他业务应用数据。

现在，RMU 正迁移向 Oracle 11g 数据库，系统环境是 64 为的企业版 Linux，而且现在有了补丁管理流程。Stewart 说 RMU 正在制定流程，通过 Oracle Advanced Security 的使用来降低数据非法访问。但是，他们仍然有改进的余地。他希望使用的下一代 Oracle 产品之一是 Audit Vault。

他说：“我想看到每个用户都在做什么。这对我们来说是非常大的一块。”

*(作者：Shayna Garlick 译者：冯昀晖 来源：TechTarget 中国)*