BLOOMBASE®
博隆兴中

产品小册子

Bloombase Spitfire StoreSafe

网络存储数据加密和安全

不安全的企业存储电子数据

过去十年里，网络基建和技术的发展为网络计算机开创了一个新的舞台。以往只存在于全球或者大规模的企业中的网络环境，如分布处理，网络存储和电子信息交换等，现在对于很小的企业来说，也是很普遍的事项。

商业数据，由主要为分析和归档使用的历史性数据，很快地发展成为实时的企业核心操作数据，机要且敏感，必需妥善保密保护，不可任意改动。同样的，计算架构管理也从企业内部专属的专业技术部，外向变为外包的服务。如此一来，缺乏数据控制，将对企业有着极大潜在的风险和威胁。

此技术走向，为近年来不断出现的企业数据威胁如网络黑客侵入和网络病毒，逐渐深化转向成为未授权的数据更改和数据窃取，无论是通过电子远程进行的还是传统的物理性的攻击。数据窃取和未授权的数据大大改降低了消费者对电子商务的信心，并且在很多情况下，为企业和政府机构带来巨大的经济损失和繁重的后期补救工作。

传统的技术解决方案及其问题

以前的安全控制措施：防火墙和数据过滤，主要是为了防止外部侵入，然而，数据显示，现在内部入侵已经发展成为新的风险。为了杜绝内部数据窃取，企业可以采取数据加密的办法，把明文的敏感数据变换为看似垃圾一样的乱码来，哪怕加密数据真的被窃取，也没有人可以看到加密信息的真实内容。

尽管企业数据外泄主要原因是明文数据窃取，但企业管理者往往忽略数据加密的重要性，滞后于实施数据加密措施也是不容置疑的因素之一。

其根源是，传统的数据加密软件一般性能都很差，需要很复杂的跟应用系统整合才能使用，而最大的难题是这些传统的加密软件都不支持动态实时更新的数据库存储系统，更不用说其可开展性和可靠性。

开创性的技术发展

为此，博隆兴中科技开发 Spitfire StoreSafe 网络存储数据安全服务台，为所有或者绝大多数企业提供一个网络数据存储的整体解决方案，它将数据进行全透明的加密处理，也把密钥管理统一起来。

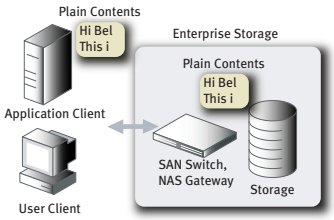
Spitfire StoreSafe 是应用端全透明的企业存储保护产品，保护公司和用户数据，同时，不用改变或影响现有的应用系统结构和用户工作流程，部署方便，大大减低企业因进行数据安全实施所带来的技术阻力及风险。

工作流程

数据化财产包括财政报告，法律文件，企业及机构的人力资源信息，机要合同和敏感的用户数据，这些都是企业无价的财产。企业不可冒险丢失这些信息，什或被人擅自更改。

然而，若用户及应用系统生成的机要数据在企业的存储系统中以明文保存，管理者和操作者便可以直接接触核心存储系统，这也就给企业数据丢失或者非法侵入带来潜在的威胁。

不良的企业资讯科技管理或薄弱的数据安全管理意识，造就数据外泄的条件及风险。

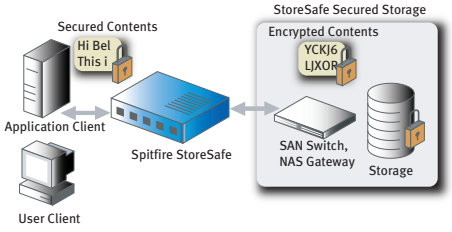


这是一个典型的存储架构，在绝大多数企业和组织机构里都可以看到。对核心和直接的侵入全无抵抗力量，窃取企业最机密及无价的商业和用户数据毫无难度。

Spitfire StoreSafe 是一个高性能的网络加密系统，可以看成是一个加密的数据传递中间人，作为企业应用服务器和存储网络系统的联结点，Spitfire StoreSafe 将企业应用服务器生成的明文信息加密成看似垃圾的乱码信息，然后才发送到存储网络系统。

相反，应用服务器若从存储网络系统读取加密了的资讯，Spitfire StoreSafe 便把数据实时解密，让应用服务系统安全地取得明文的机要数据。

Spitfire StoreSafe 作为存储网络中的代理角色，实现了机要存储数据的虚拟化，安全化和自动化。？



Spitfire StoreSafe 作为存储网络的加密解密器，实现了机要存储数据的虚拟化，安全化和自动化。

高度安全性和可管理性

Spitfire StoreSafe 拥有高性能的加密和解密技术，并且已达到很高的加密解密效能。Spitfire StoreSafe 的加密算法非常丰富，例如，AES, Camellia, DES, 3DES, RC4 等。Spitfire StoreSafe 可以与所有企业级的硬件和操作系统相兼容，并且支持众多国际及业界的存储协议。

除数据保密性以外，Spitfire StoreSafe 更配备网络存取控制功能，满足各客户的部署需求。

存储数据的完整性也是当今企业时时刻刻担心的问题，请放心，Spitfire StoreSafe 已为您提供解决方案，其专利数据水印 Watermark 技术也已配备妥当，严防数据给偷偷篡改。

其配有高性能的审核工具，管理和控制可以通过网络管理直接完成，不需要任何特殊培训。Spitfire StoreSafe 与 Spitfire KeyCastle 及 PKCS#11 密钥管理系统无缝结合，以达到企业数据的最大安全化。

功能一览

硬件和操作系统独立
■ 支持所有现有的平台及一般的存储通信协议存储系统

档案系统独立性
■ Spitfire StoreSafe 能在网络存储平台上与不同的档案系统运行

用户独立 透明处理
■ 无需培训，数据加密予以存储和自动解密程序，对用户的工作流程丝毫没有任何影响

透明的加密和解密运作
■ 智能的加密系统可以感知存储数据需要的网络通讯情况，并且在用户预先规定的规则下执行加密或者解密程序

实施简单并毫无风险
■ 无需对应用程序进行更改，没有复杂的系统集成，工作流，管理和操作流程都无需任何改变

灵活和安全的访问控制
■ 出色的用户访问控制和权限控制可以满足企业所有存储安全需求

多用户支持和资源共享
■ 用户通过自己的加密钥匙保护自己的数字财产，安全地进行资源共享

与 Spitfire KeyCastle 无缝集成。
■ 为加密钥匙更容易管理，可使用 Spitfire KeyCastle 与之无缝集成

高实用性和可集群性
■ 提高可靠性，可用性及适用性，满足大型企业的高流量存储加密需求

企业好处和应用

存储数据透明加密
■ 通过网络存储加密保护 ERP，财务和用户数据。在不影响性能的情况下享受真实的数据安全呈现

安全的复制和错误恢复
■ 当出现错误，进行数据恢复时，数据依然处于加密状态。企业可以完全确信机密数据毫无安全隐患

Spitfire StoreSafe 管理和控制可以通过网络管理直接完成，不需任何特殊培训

邮件库加密
■ 企业高级管理者邮件中经常包含有机密的商业信息，当机密信息保存在企业数据库时，数据会被 Spitfire StoreSafe 自动加密解密供用户使用，用户无需改变任何工作流程

知识产权保护
■ 设计文件，原始代码，产品原型和市场开发资料在存储系统里被严密的保护，用户不需适应新的工作流程

安全的数据备份和档案
■ 通过强大的加密系统保护备份数据，以避免企业的机要信息被泄露

技术规格

加密安全
■ NIST FIPS 140-2 安全模块资质认证
■ IEEE 1619 存储安全标准资质认证
■ RSA, AES, Camellia, 3DES, CAST5, RC2 等加密算法
■ 512/1024/2048-bit 长度的 X.509 非对称性密钥
■ 支持 PKCS#11 硬体密钥
■ 支持 OSCCA 国密硬体算法模块

访问控制安全
■ 优秀的读写访问控制
■ 专利数据水印技术，严防数据给偷偷篡改

存储通信协议支持
■ FC-SAN, IP-SAN, i-SCSI, SCSI
■ NFS, CIFS, FTP, HTTP 和 REST 支持
■ 用户证明和授权
■ 应用服务台证明和授权

网络管理
■ SNMP (v1, v2c, v3), syslog
■ 日志自转
■ 自动备份

系统管理
■ 网页化的中央管理控制台
■ RS-232 连接口管理控制台

博隆兴中科技 **Bloombase** - 信息安全专家　　电子邮件 info@bloombase.cn　　网站 www.bloombase.cn

BLOOMBASE® 博隆兴中