IBM Fibre Channel Endpoint Security
基于 IBM Z，为传输中的数据提供端到端的安全

什么是 IBM Fibre Channel Endpoint Security?

光纤通道是存储区域网络 (SAN) 的主要传输方式。但是，与数据中心的任何其他组成部分一样，为了减少和消除未经授权访问数据所带来的内部威胁，也需要在 SAN 中实施安全措施。SAN 管理工作不仅需要提供高度可用的数据访问和最优性能，还必须确保 SAN 上的所有数据始终安全无虞。

IBM Fibre Channel Endpoint Security 是一种端到端解决方案，可确保从 IBMZ® 到 DS8900F 的 FICON® 和光纤通道协议 (FCP) 链路上的所有数据，或通过 FICON 通道到通道连接在 IBM Z 平台之间流动的所有数据都受到加密和保护。

该产品为所有传输中的数据提供保护，与使用的操作系统、文件系统或访问方法无关。

端到端保护的优点

- 在具有“安全能力”的主机和存储终端之间自动实现安全防护
- 建立的每个链路都必须“证明”自己是可信组件
- 能够识别可信的连接；对操作系统和 HMC 均可见
- 可创建并实施策略，以便仅支持建立可信连接
- 每次链路断开/重新连接时，都需要进行重新认证以及重新协商设备的加密密钥
- 使用 IBM Security Key Lifecycle Manager (ISKLM) 实现整合密钥管理
- 可在“加电复位”后立即使用，或者稍后通过运行 IBM Z 启用，基本上不会造成中断。

由于具有这些优点，因此 IBM Fibre Channel Endpoint Security 可以帮助您：

- 遵守法规与合规要求
- 最大程度降低企业在接收和存储敏感数据方面的风险及影响

IBM Fibre Channel Endpoint Security 是一种额外的数据安全技术，是对 IBM Z 随处加密方法的有益补充。它提升了普遍加密的价值，进一步降低了出现安全漏洞、潜在不合规以及经济处罚的风险。

由于既要对数量、种类和价值不断增长的数据始终保持有效控制，又要遵守日益复杂的法规要求，因此数字化企业所面临的风险与日俱增。同时，网络攻击者正不断通过创新方法，攻击 IT 基础架构，窃取数据。由于内部威胁层出不穷（例如技术人员在确定问题期间使用光纤通道分析器检查数据包，或未经授权的主机访问存储控制器），以及行业共享数据中心的趋势越来越明显，因此必须时刻保护敏感数据，即使在数据中心内部也是如此。

IBM Fibre Channel Endpoint Security 包含哪些组件?

IBM Fibre Channel Endpoint Security 包含 3 个组件：

采用 FICON Express16SA 的 IBM z15

IBM z15™ 支持具有加密功能的新型 16Gbps FICON 卡，用于保护通道到通道以及通道到存储控制单元的链路。（注：在 FICON Express16S+ 卡上还支持“仅限认证”功能。）

IBM DS8900F

全新的 IBM DS8900F 产品支持具有 32GFC 加密功能和 16GFC 认证功能的新型主机适配器卡，确保 IBM Z 与存储控制单元之间链路的安全。

IBM Security Key Lifecycle Manager

需要使用遵循 ISKLM 3.0.1 版本的外部密钥管理器 (EKM) 设备，向服务器和存储器提供用于安全协会管理协议的共享密钥，以便对终端进行认证，并生成用于保护终端间传递的消息和数据的密钥内容。

密钥管理互操作性协议（KMIP）是用于密钥管理器通信的标准密钥管理协议

z15 和 DS8900F 存储系统在密钥服务器中进行认证，并与其进行通信，以便创建和分发共享密钥。

我们的价值主张

尽管可以进行颗粒度更细的数据集加密（例如，仅限特定人员看到特定数据），但这会增加复杂性，因为需要保护更多的密钥。

而 IBM Fibre Channel Endpoint Security 较为宽泛，易于实施。只需安装密钥服务器，定义主机 (IBM Z) 与存储控制器（DS8900F）对密钥服务器的访问方式，然后就会在解决方案内部处理密钥管理。

这样，客户端就可以快速加密所有传输中的存储数据，无论采用何种操作系统，同时可以进行所需的增量式更改，实现数据集加密。

与磁盘加密方法一起使用时，IBM Fibre Channel Endpoint Security 可以百分百覆盖所有动态传输和静态存储的数据。

系统需求

要使用 IBM Fibre Channel Endpoint Security，需要满足以下最低系统需求：

- IBM z15 或 IBM LinuxONE™ III，具有以下功能：
  - CPACF 功能
  - 终端安全功能
  - IBM z15 或 IBM LinuxONE III 服务器上的新型 FICON Express16SA 通道卡（解决方案还支持 FICON Express16S+ 通道卡上的“仅限认证”功能）
  - 更新后的 HMC 代码，用于响应一些关键请求
- IBM DS8900F，具有以下功能：
  - IBM Z Synergy 软件包
  - 新型 32GFC HA（具备加密功能）和/或现有的 16GFC HA（支持“仅限加密”功能）
- IBM Security Key Lifecycle Manager V3.0.1

如何推进部署工作

安排一场研讨会，了解如何通过在 IBM z15 或 LinuxONE III 以及 IBM DS8900F 基础架构上部署 IBM Fibre Channel Endpoint Security 解决方案，帮助企业提高数据安全性。

请与贵组织的 IBM 销售代表联系，获取有关 IBM Fibre Channel Endpoint Security 的更多详细信息。

通过访问以下网站，评估完整的 IBM 安全软件产品组合，建立分层的安全防御体系：

IBM z15：
https://www.ibm.com/marketplace/z15

IBM Fibre Channel Endpoint Security：
https://www.ibm.com/marketplace/fibre-channel-endpoint-security

IBM Z Enterprise Security：
https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security

IBM 安全解决方案：
https://www.ibm.com/security/solutions

04027104CNZH