IBM Z Fibre Channel Endpoint Security end to end in-flight data protection powered by IBM Z

What is IBM Fibre Channel Endpoint Security?

Fibre Channel is the premier transport for Storage Area Networks. Yet, like with any other component of a datacenter, the need to implement security measures in the SAN exists in order to reduce and eliminate insider threats of unauthorized access of data. Managing a SAN involves not only providing highly-available data access and optimal performance, but it's also essential that all data on the SAN be completely secure at all times.

IBM Fibre Channel Endpoint Security is an end-to- end solution which ensures all data flowing on FICON® and Fibre Channel Protocol (FCP) links from IBM Z® to DS8900F, or between IBM Z platforms over FICON Channel-to-Channel connections is encrypted and protected.

This offering provides in-flight protection for all data, independent of the operating system, file system, or access method in use.

Benefits of end-to-end protection

- Enabled automatically between host and storage endpoints that are 'security-capable'
- Each established link must 'prove' its identity as a trusted component
- Trusted connections are identified; visible to both the Operating System and HMC
- Policy can be established to enforce that only trusted connections can be made
- Each time a link goes down/up re- authentication/ negotiation of device encryption keys will occur
- Integrated key management using IBM Security Key Lifecycle Manager (ISKLM)
- Can be used immediately after Power-on-Reset or enabled later by running IBM Z with minimal or no disruption

Because of these benefits, IBM Fibre Channel Endpoint Security can help you:

- Meet regulatory and compliance mandates
- Minimize the enterprise risk and impact of receiving and storing sensitive data

IBM Fibre Channel Endpoint Security is an additional data security technology that contributes to the IBM Z approach of encryption everywhere. It extends the value of pervasive encryption, further minimizing the risk of security breach, potential noncompliance and financial liability.

Digital business risk is growing due to the challenge of maintaining control over data that is constantly increasing in volume, variety, and value while maintaining compliance with regulations, which continue to grow in complexity. Meanwhile, cyber attackers are finding increasingly innovative ways to compromise IT infrastructure and steal data. Insider threats, like technicians using Fibre Channel analyzers to examine packets during problem determination or unauthorized hosts accessing storage controllers, as well as industry trends towards shared datacenters, make it necessary to protect sensitive data at all times, even within the walls of the datacenter.

What are the components of IBM Fibre Channel Endpoint Security?

There are 3 key components of IBM Fibre Channel Endpoint Security:

IBM z15 T01 with FICON Express16SA

(note: offering not supported on z15 T02)

The IBM z15TM T01 supports new encryption capable 16Gbps FICON cards for securing Channel-to-Channel and Channel-to-Storage Control Unit links.
(Note: Authentication-only is also supported on FICON Express16S+ cards).

IBM DS8900F

The new IBM DS8900F supports new 32GFC encryption-capable and 16GFC authentication-capable host adapter cards to support secured links between IBM Z and the storage control unit.

IBM Security Key Lifecycle Manager

ISKLM version 3.0.1 External Key Manager (EKM) appliance is required to serve a shared key to the server and storage that is used in security association management protocols to authenticate the endpoints and derive key material used to secure messages and data between the endpoints.
Key Management Interoperability Protocol (KMIP) is the standard key management protocol used for key manager communication
The z15 T01 and DS8900F storage system authenticate with the key server and communicate with it for the creation and distribution of shared keys.

Our value proposition

Dataset encryption allows for finer granularity (e.g. only certain people can see certain data), but this adds complexity – requiring additional keys that need to be protected.
IBM Fibre Channel Endpoint Security provides a more “broad brush,” easy implementation. Install the key server, define how the host (IBM Z) and storage controllers (DS8900F) access it, then key management is handled internal to the solution.
This enables clients to quickly encrypt all in-flight storage data, regardless of OS, while they make the incremental changes required to get to dataset encryption.
When used in conjunction with Disk Encryption, IBM Fibre Channel Endpoint Security provides 100% coverage for all in-flight and at-rest data.

System requirements

In order to use IBM Fibre Channel Endpoint Security, the following minimum system requirements are needed:

- IBM z15-T01 or IBM LinuxONE III LT1 with the following features:
  - CPACF feature
  - Endpoint Security feature
  - New FICON Express16SE Channel card on the IBM z15 T01 or IBM LinuxONE III LT1 server (Support for authentication-only on FICON Express16S+ channel cards is being provided as part of the solution)
  - Updated HMC code for key requests
- IBM DS8900F, with the following features:
  - IBM Z Synergy SW bundle
  - New 32GFC HA (encryption-capable) and/or existing 16GFC HA for authentication-only
- IBM Security Key Lifecycle Manager ver.3.0.1

How to move forward

Arrange a workshop to determine how deploying the IBM Fibre Channel Endpoint Security solution on IBM z15 T01 or LinuxONE III LT1 and IBM DS8900F infrastructure can improve your enterprise data security. Contact your IBM sales representative for additional details regarding IBM Fibre Channel Endpoint Security. Evaluate the full IBM security software portfolio to create a layered security defense by visiting these websites:

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 Security Solutions:
https://www.ibm.com/security/solutions

© 2020 IBM Corporation