GSE GUIDE SHARE EUROPE UK REGION

GSE UK Conference 2018
Better, stronger, faster; The Mainframe….. the Machine!

Still using FTP? Secure Mainframe File Transfers using FICON as the Network

Colleen Gordon
Luminex Software, Inc.

Mark Wilson
RSM Partners

November 2018
Session FI

Mainframe File Transfer: An RSM Perspective

Mark Wilson, *Technical Director*

Introduction

GSE GUIDE SHARE EUROPE
UK REGION

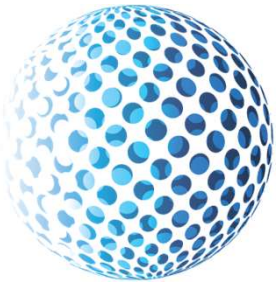
"Look at you - folding laundry. And last night it was doing the dishes. Just exactly what part of 'No you're not buying another bike' don't you understand?"

Providing a Wide Range of Services ….

- **Skilled Resources** – onsite, remote or hybrid
- **Consultancy**
- **Full Project Delivery** *(fixed price driven)*
- **Managed Services/RIM** *(SLA driven)*
- **24*7 Incident Support & Help Desk** – via phone, VPN, onsite

Mainframe Security Challenges

- Mainframe Security is our thing
- Services Offered:
  - Pen Test
  - Security Assessment
  - Vulnerability Scanning
  - Training



RSM Security Server
Interfacing your mainframe with your enterprise solutions

racfGUI
Intuitive RACF admin

zDetect
Powerful real time security monitoring

Breakglass
Secure access control made easy

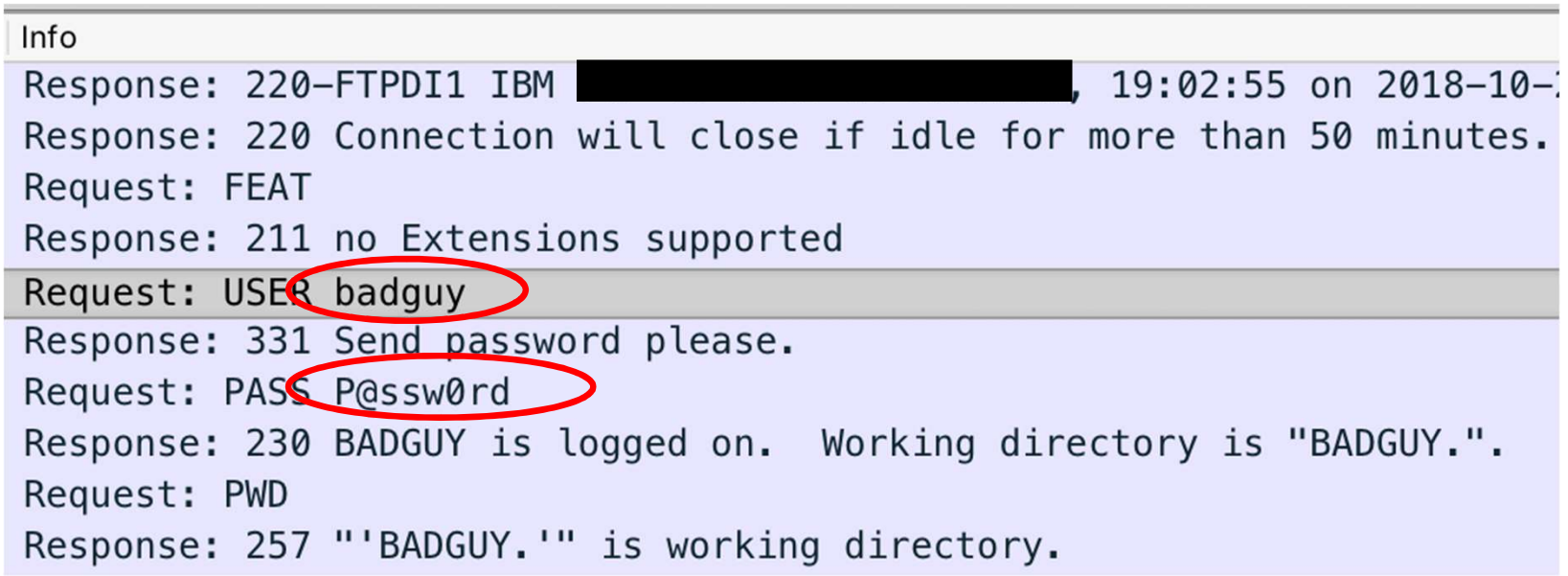
Self Service Password Reset
Simple & secure password reset

exceptionReporter
Security monitoring made easy, highlighting exceptions

The perception of M/F Security!

Horror story

- While testing z/OS found packet capture file
- Offloaded and saw FTP protocol was in the capture
- Looking at the capture – found credentials!

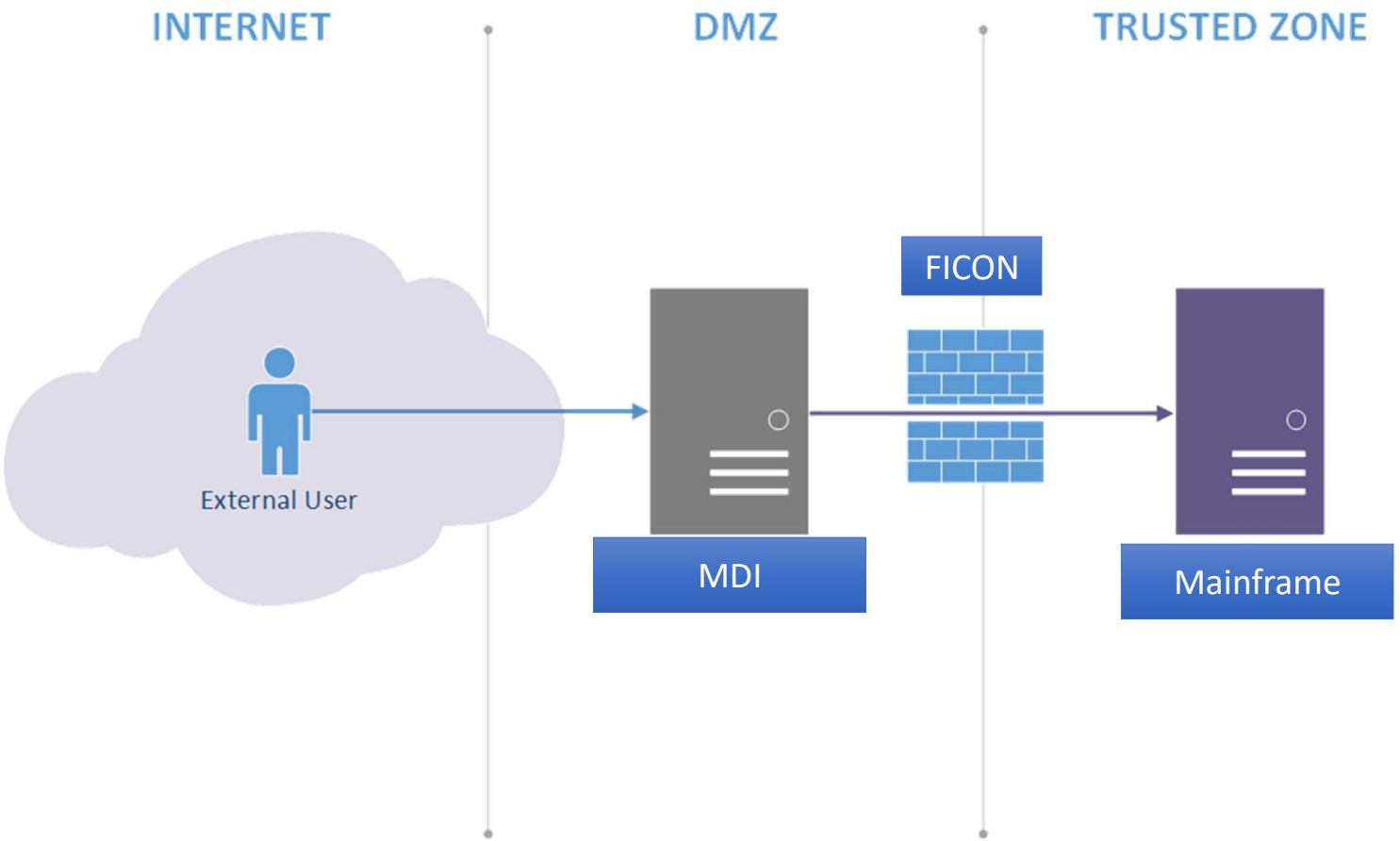


… continued

- Those credentials had no access to TSO
- However, they did have access to update 1 APF-authorized library!
- But the Userid had access to FTP!
- The rest is history
- Disabling or encrypting FTP would have prevented this
- Disabling may be better as locking down FTP is very difficult – shrink the MF attack surface

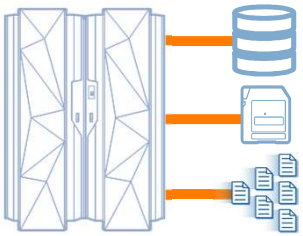
A DMZ for File Transfer

A DMZ for File Transfer



A DMZ for File Transfer

- If we can remove the use of FTP on the mainframe, even closing the ports and disabling the service, this wards off some of the bad folks as that maybe their attack vector
- Move all of that data transfer workload to MDI its faster (Ficon) and its secure
- FICON was designed specifically for the mainframe its attributes are Fast, Efficient and Secure
- Uses are:



- DASD
- Tape
- … and now possibly File Transfer

The Good News

- File transfer from mainframe is a huge attack surface
- Moving it to a separate, hardened “dmz” type host improves security posture
- Flexibility of having a host with multiple secure forms of transport is a huge plus
- Doing so with little or no change to existing code on the mainframe is also a plus

Summary

Summary

- Shrinking the attack surface on the mainframe by moving file transfer to a secure, smaller-footprint, easily-hardened box is the right answer
- Not doing security right from the get-go might actually make things worse: high concentration of customer data in one place, with weak controls
- Patching & patch visibility are paramount!
- Turning off legacy protocols (like FTP) is a huge win

GSE GUIDE SHARE EUROPE UK REGION

GSE UK Conference 2018
Better, stronger, faster; The Mainframe….. the Machine!

Still Using FTP? Secure MF File Transfers Using FICON as the Network

Colleen Gordon

MDI Solution Specialist

Still Using FTP?

- Luminex has completed dozens of File Transfer SMF analyses for our Clients
  - Type 119 subtype 3,70 for FTP Client and Server records
  - Type 119 subtype 96,97 for IBM SSH (SFTP & Co:z)
  - Type 30 records
  - Type 70,72 RMF

General Observations

- Most have no idea how much FTP activity goes on
  - Insufficient reporting or auditing of FTP usage
- FTP ports are wide open
  - Insufficient controls or restrictions on what type of data can/cannot be sent via FTP Credentials in the clear
- Very little use of SFTP, FTPS or other secure file transfer protocol
- Clients that have a secure product don't use it for all file transfers
- Generally a "nobody has said I need to secure it" attitude

It’s like the Wild Wild West Out There!

Client Data on FTP

Company	FTP Client	FTP Server	SFTP	C:D	Other	Other #	Days	Average
A	52,947	237,188					53	5,474.25
B	180,876	1,248,780					7	204,236.57
C	9,118	52,788					30	2,063.53
D	631,836	1,912	49				7	90,535.43
E	3,709			80,000			30	123.63
F	12,268						58	211.52
G	68						7	9.74
H	31,979						14	2,284.21
I		1,343					7	191.86
J	82	3,632	902		CoZ	1,460	14	265.29
K	17,231	17,920					31	1,133.90
L	5,844			92			6	974.00
M	3,712				XCOM		7	530.29
N	17,505				CoZ	37	7	2,500.71
O	6,015	1,535					44	171.59
P	3,650	1,118					9	529.78
Q	80						7	11.43
R	1,306	26					7	190.29
S	63,086	48,025					7	15,873.00
Totals	**1,041,312**	**1,614,267**	**951**	**80,092**		**1,497**		

FTP: Why are you still using it?

- FTP turned 47 years old in 2018
- Still functional as a technology to move files but…
  - Not secure (no encryption)
  - Not designed to provide delivery results
    - Not designed to retry/restart
  - Passwords in clear text susceptible to attack
    - Any network sniffer can hijack it
  - Data is at risk of being retrieved and shared
  - No audit trail or logging

FTP Related Data Breaches

GUIDE SHARE EUROPE UK REGION

Major American Retailer with locations all over the world

Data was moved to drop locations on **hacked servers** all over the world **via FTP** where hackers retrieved the data (Krebs, 2014h)

$200M

to replace credit cards

140

lawsuits

46%

drop in 4th quarter sales

Major American Service Provider

Largest ever invasion and theft of personal data via **hacked FTP servers** outside the company's firewall.

1.6 Billion

customer records containing:

- Names
- Addresses
- Emails

Major American Home Goods Retailer

"**FTP** was never designed with security in mind and because of that, it's become one of **the favorite venues for hackers** looking to get into a corporate network."

$25M

paid in damages

$134.5M

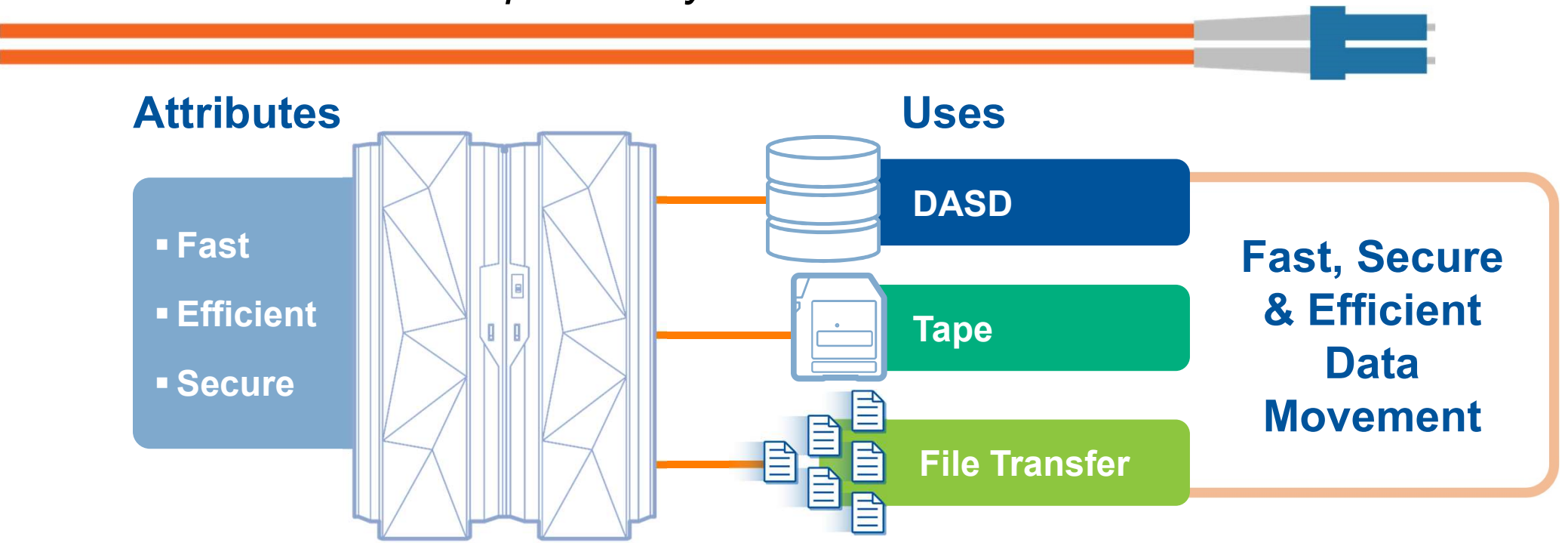
in compensation to consortiums (Visa, Mastercard, various banks)

$19.5M

settlement to affected customers

FICON is a Better Alternative!

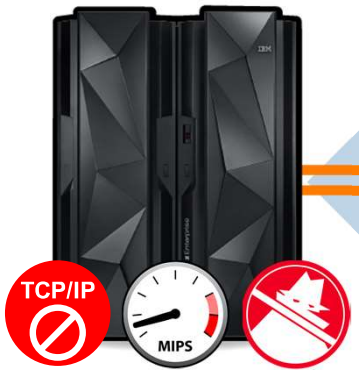
FICON is an I/O channel technology designed
specifically for the mainframe



MDI is a Data Transfer & Co-Processing Platform

GUIDE SHARE EUROPE UK REGION

Mainframe FICON

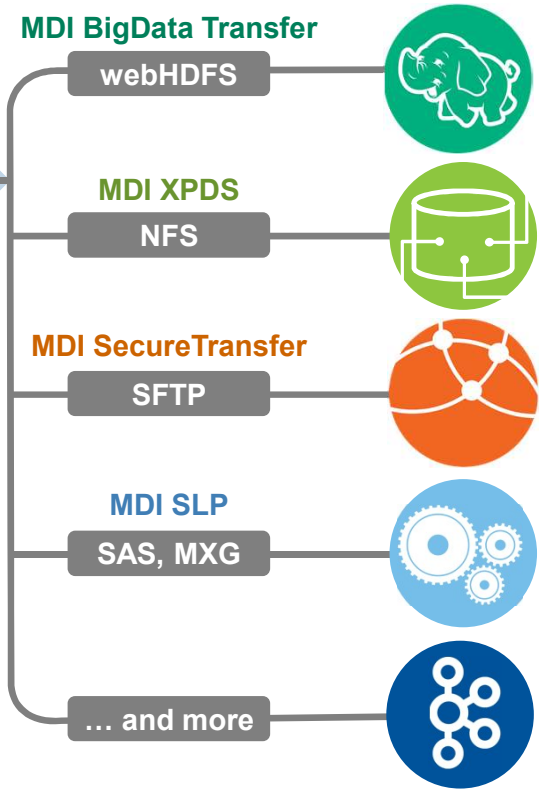


- Secure
- High speed
- Efficient, redundant I/O channels

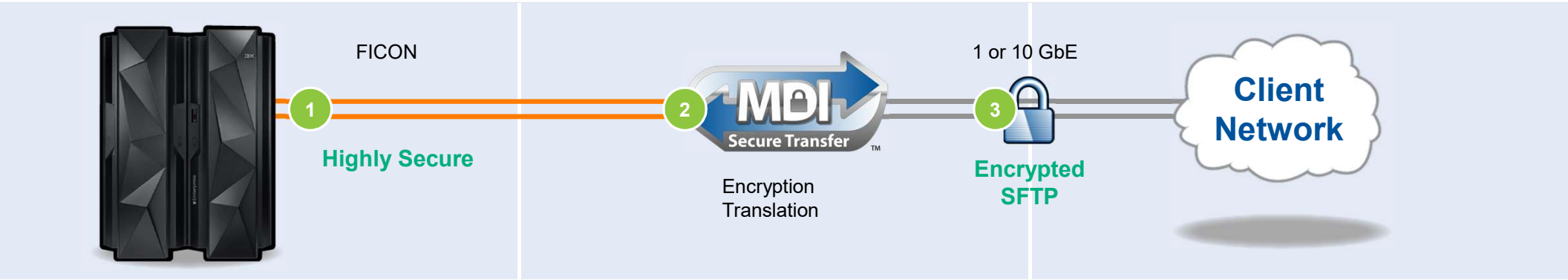
MDI Platform

- Profile-based architecture for extending processing & interface capabilities
- High speed, scalable transfer rates
- SAF integration & protocol-based encryption
- Bi-directional movement and communication for multi-platform workflows and co-processing
  - Including data translation from EBCDIC to ASCII and between character sets

Data Sharing Targets/Sources



MDI SecureTransfer: Sending Files to/from the Mainframe



1. Data is transferred off-host via tape FICON channels
   - Up to 800 MB/s per MDI Platform
   - Concurrent file transfers supported
2. Data is encrypted and translated off-host, saving CPU cycles
3. Encrypted data is transferred over the client's network via SFTP over redundant 1 or 10 GbE
4. PUTS and GETS managed via mainframe batch job

Simple JCL Deployment

```
JOBCARD…
//GENER    EXEC PGM=ICEGENER
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   DUMMY
//SYSUT1   DD   DSN=PROD.FTP.TXDATA,
//              DISP=SHR
//SYSUT2   DD   DSN=PROD.FTP.TXDATA.MDI,
//              DISP=(NEW,CATLG),
//              UNIT=MDITAPE,RETPD=0,
//              DCB=*.SYSUT1
```

Step 1: Write the file you want to transfer to an MDI SecureTransfer owned tape. This is a simple ICEGENER to tape.

MDI JCL – Step 2

```
//STEP2    EXEC LUMXPROC,PROFILE=MDIST
//XPROCLOG DD   SYSOUT=*
//COPYFILE  DD   DISP=OLD,
//               DSN=PROD.FTP.TXDATA.MDI,
//               UNIT=MDITAPE
//SYSIN     DD *
-PARM destination=206.154.7.19
  cipher=aes192-ctr
  login=<loginid>
  password=<password>
  conversion=ascii_CRLF
-DD_COPYFILE=prod.ftp.txdata
```

Step 2: Execute LUMXPROC. Communicates to MDI what you want to do with the data.

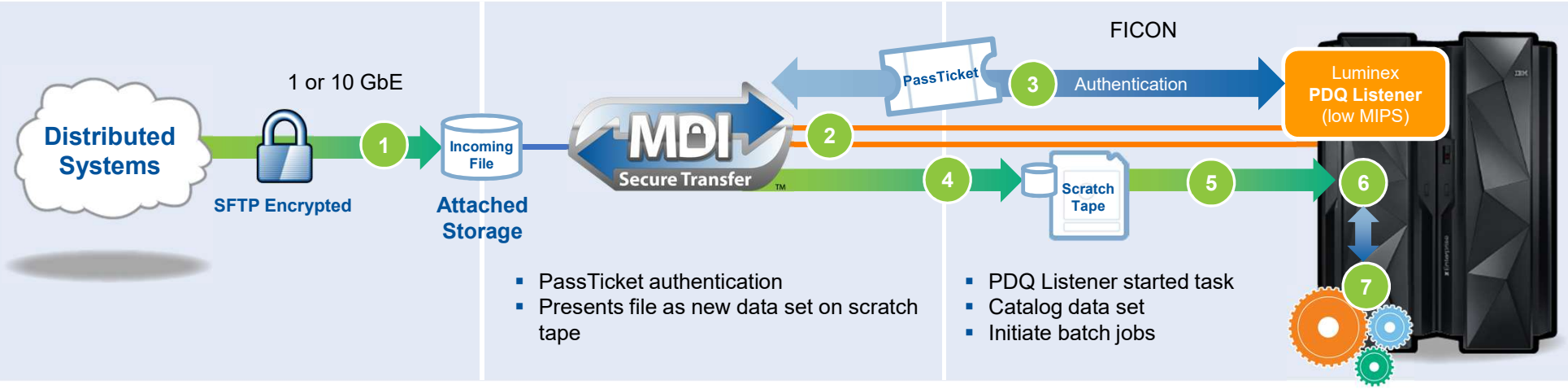
Destination IP, DNS/server name

Multiple ciphers supported

Credentials externalized in JCL

Convert EBCDIC to ASCII

Distributed to the Mainframe MDI:ST and MDI:XPDS



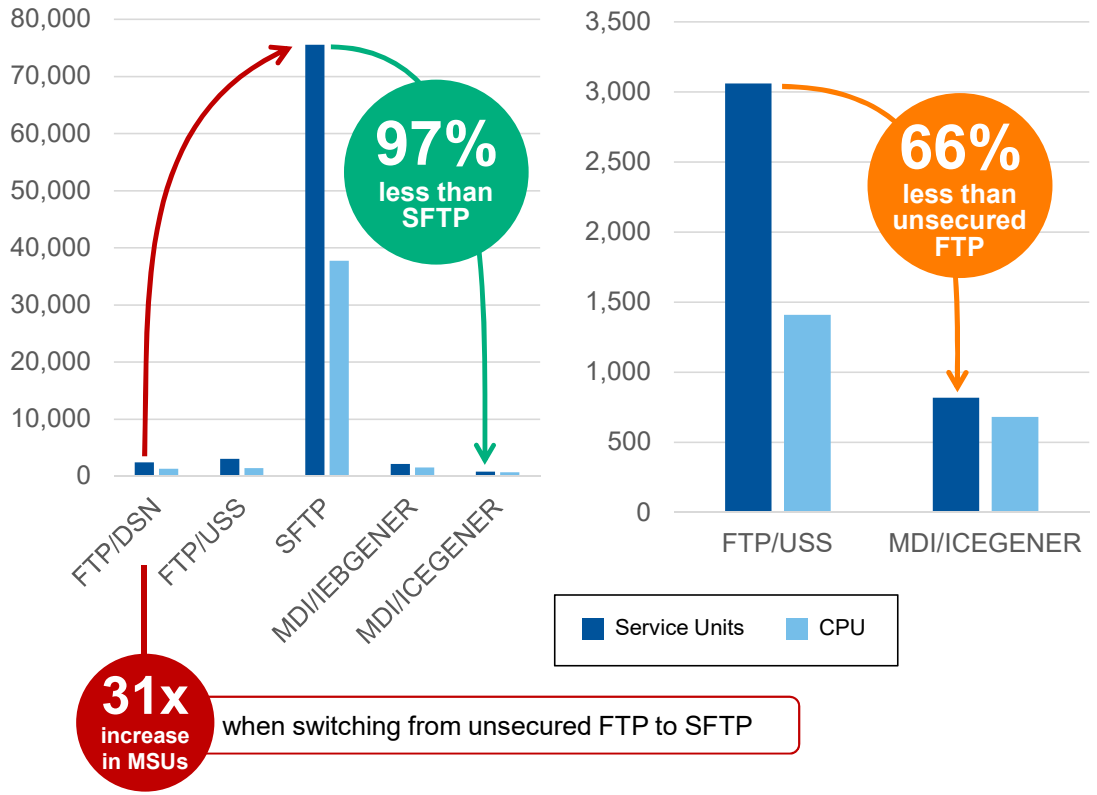
1. File is transferred via SFTP to folder on MDI:ST attached storage
2. File Watcher detects the file and communicates to PDQ on the mainframe
3. File Watcher constructs a Pass Ticket and passes to PDQ for security validation
4. PDQ validates security; mounts a scratch tape and opens a new data set
5. MDI:ST copies incoming file to new data set on the given scratch tape
6. PDQ closes the data set and catalogs it on mainframe
7. Catalog event “triggers” downstream batch processing to be initiated

Benchmark Testing: 30 MB File

Method	Job	Program	Elapsed	Service Units	CPU
FTP from DSN	BNCHMRK1	FTP	0:00:15.32	2403	1280
(Clear Text)			**0:00:15.32**	**2403**	**1280**
FTP from USS	BNCHMRK2	FTP	0:00:13.96	3060	1409
(Clear Text)			**0:00:13.96**	**3060**	**1409**
SFTP	BNCHMRK3	login	0:00:00.10	150	135
(Encrypted)	BNCHMRK3	tty	0:00:00.02	140	119
	BNCHMRK3	sftp	0:00:00.14	340	317
	BNCHMRK3	ssh	0:00:06.27	68463	34493
	BNCHMRK3	sftp	0:00:08.41	6106	2363
	BNCHMRK3	SH	0:00:08.47	213	163
	BNCHMRK3	BPXBATCH	0:00:08.77	129	107
			0:00:32.18	**75541**	**37697**
MDI/IEBGENER	BNCHMRK4	IEBGENER	0:00:03.24	2010	1407
	BNCHMRK4	LUMXPROC	0:00:09.34	156	134
			0:00:12.58	**2166**	**1541**
MDI/ICEGENER	BNCHMRK5	ICEGENER	0:00:00.79	667	550
	BNCHMRK5	LUMXPROC	0:00:09.19	151	131
			0:00:09.98	**818**	**681**

Benchmarks performed on z13 Model 2965-N10 using SMF Type 30 records

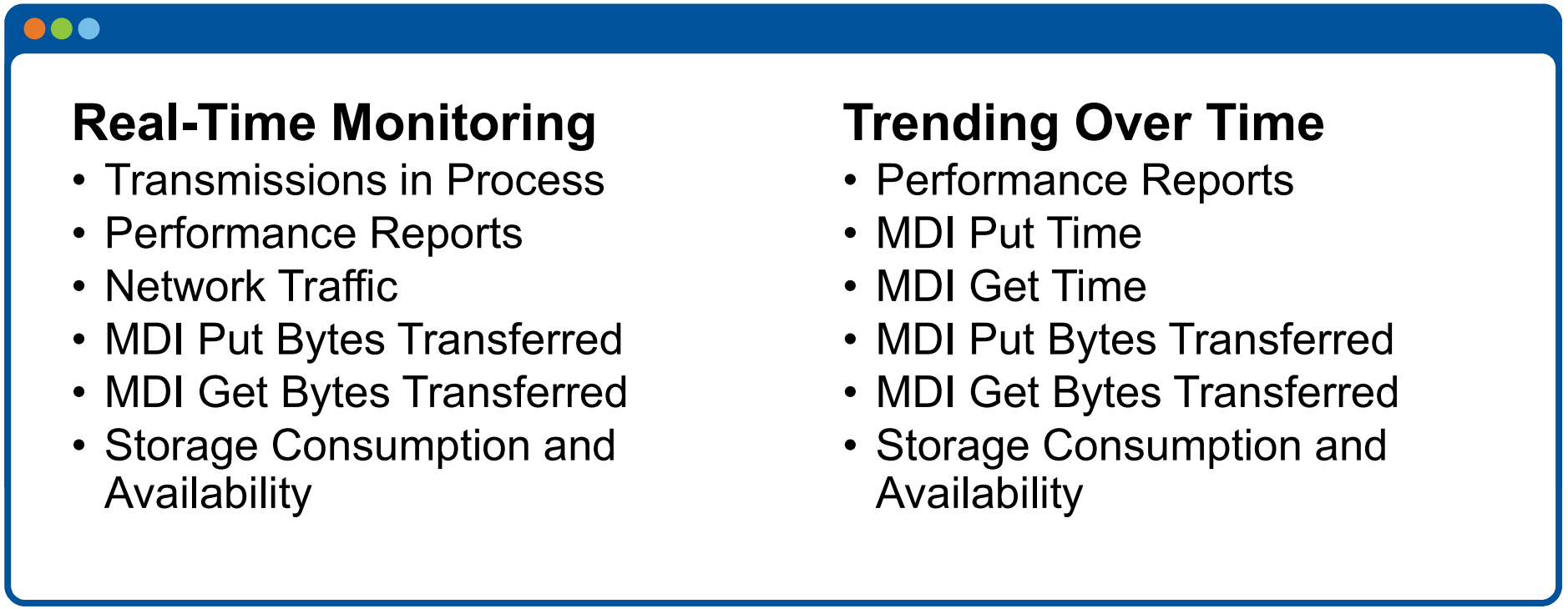
MDI/ICEGENER System Resources Savings



No x.509 Digital Certificates Required

- SecureTransfer *does not* require the use of x.509 Digital Certificates
  - Data is transferred from the MDI Platform (not the mainframe) to the destination server using Secure Shell (SSH) File Transfer Protocol or SFTP
- SFTP is the preferred file transfer protocol for Open Systems
  - Uses UID and password sign-on to the destination server
  - Additionally secured by use of SSH keys
    - Keys are typically generated once, and never expire
  - Supports multiple encryption ciphers including AES-256
  - Approved for FIPS 140-2, SOX, HIPAA, NSA, NIST, GDPR, etc., compliance
- FTPS is also supported

MDI Monitor Reports



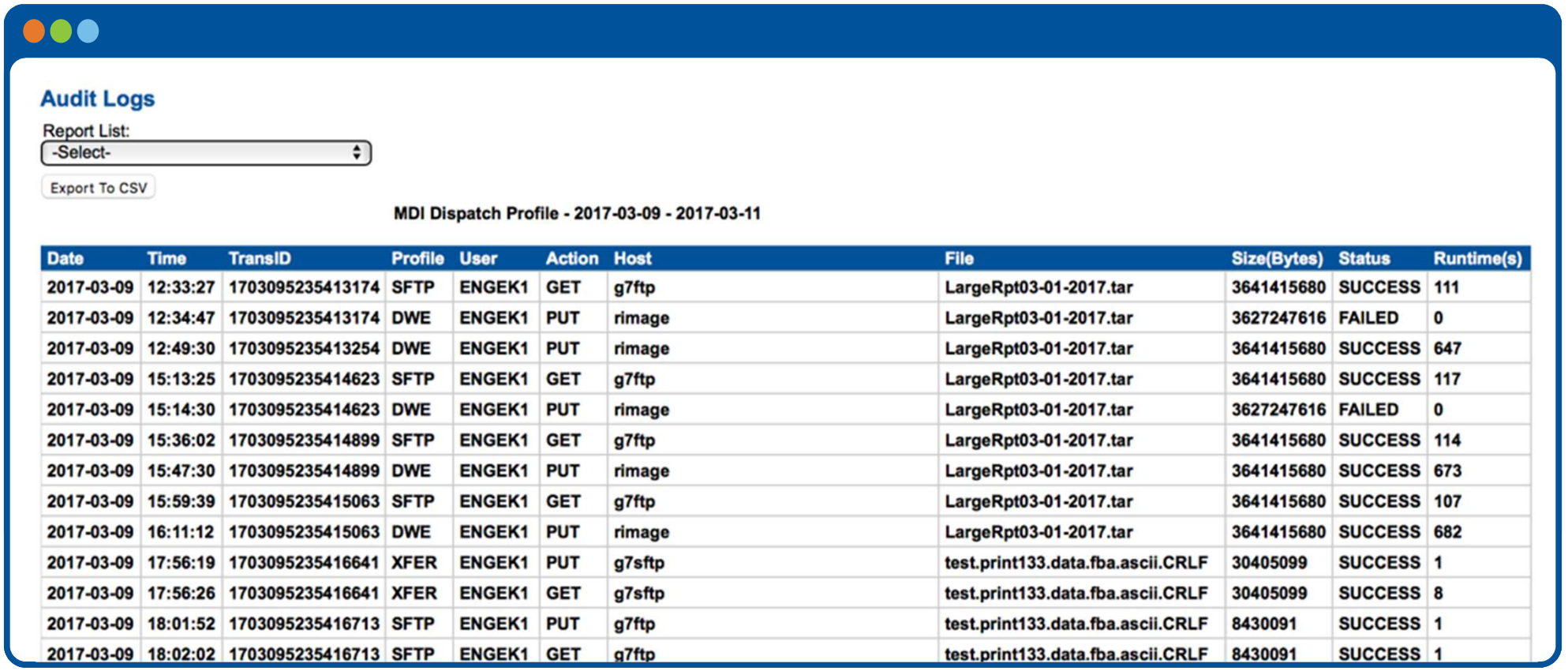
Real-Time Monitoring

- Transmissions in Process
- Performance Reports
- Network Traffic
- MDI Put Bytes Transferred
- MDI Get Bytes Transferred
- Storage Consumption and Availability

Trending Over Time

- Performance Reports
- MDI Put Time
- MDI Get Time
- MDI Put Bytes Transferred
- MDI Get Bytes Transferred
- Storage Consumption and Availability

MDI SecureTransfer Audit Log



Audit Logs

Report List:

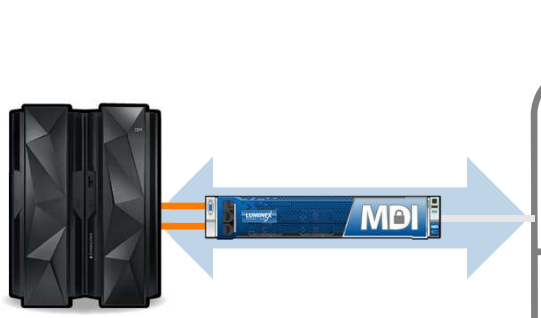
-Select-

Export To CSV

MDI Dispatch Profile - 2017-03-09 - 2017-03-11

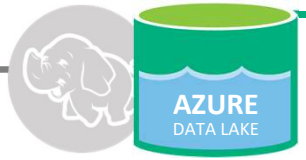
Date	Time	TransID	Profile	User	Action	Host	File	Size(Bytes)	Status	Runtime(s)
2017-03-09	12:33:27	1703095235413174	SFTP	ENGEK1	GET	g7ftp	LargeRpt03-01-2017.tar	3641415680	SUCCESS	111
2017-03-09	12:34:47	1703095235413174	DWE	ENGEK1	PUT	rimage	LargeRpt03-01-2017.tar	3627247616	FAILED	0
2017-03-09	12:49:30	1703095235413254	DWE	ENGEK1	PUT	rimage	LargeRpt03-01-2017.tar	3641415680	SUCCESS	647
2017-03-09	15:13:25	1703095235414623	SFTP	ENGEK1	GET	g7ftp	LargeRpt03-01-2017.tar	3641415680	SUCCESS	117
2017-03-09	15:14:30	1703095235414623	DWE	ENGEK1	PUT	rimage	LargeRpt03-01-2017.tar	3627247616	FAILED	0
2017-03-09	15:36:02	1703095235414899	SFTP	ENGEK1	GET	g7ftp	LargeRpt03-01-2017.tar	3641415680	SUCCESS	114
2017-03-09	15:47:30	1703095235414899	DWE	ENGEK1	PUT	rimage	LargeRpt03-01-2017.tar	3641415680	SUCCESS	673
2017-03-09	15:59:39	1703095235415063	SFTP	ENGEK1	GET	g7ftp	LargeRpt03-01-2017.tar	3641415680	SUCCESS	107
2017-03-09	16:11:12	1703095235415063	DWE	ENGEK1	PUT	rimage	LargeRpt03-01-2017.tar	3641415680	SUCCESS	682
2017-03-09	17:56:19	1703095235416641	XFER	ENGEK1	PUT	g7sftp	test.print133.data.fba.ascii.CRLF	30405099	SUCCESS	1
2017-03-09	17:56:26	1703095235416641	XFER	ENGEK1	GET	g7sftp	test.print133.data.fba.ascii.CRLF	30405099	SUCCESS	8
2017-03-09	18:01:52	1703095235416713	SFTP	ENGEK1	PUT	g7ftp	test.print133.data.fba.ascii.CRLF	8430091	SUCCESS	1
2017-03-09	18:02:02	1703095235416713	SFTP	ENGEK1	GET	g7ftp	test.print133.data.fba.ascii.CRLF	8430091	SUCCESS	1

FICON and MDI Transform Mainframe Data Sharing



MDI BigData Transfer

webHDFS



MDI XPDS

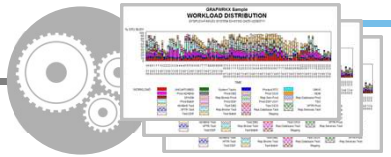
NFS

MDI SecureTransfer

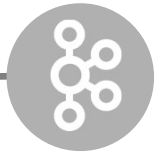
SFTP

MDI SLP

SAS, MXG



… and more



SAMPLE USE CASES

Insurance Provider

Data aggregated into an Azure Data Lake with data from distributed systems, then used for risk analysis by actuaries

Financial Services

DB2 dumped into Apache Ignite, transformed/ sorted off-host, then imported back into DB2 on the mainframe

Bank

Files securely, efficiently and simply shared with business partners via off-host encryption, compression and data movement over SFTP

Logistics Company

SMF data sent to MDI co-processor, reports generated with MXG off-host, then copies are sent back to mainframe ISPF and to Capacity Planning team via email

MDI SecureTransfer: A Better Alternative for Mainframe File Transfers

GUIDE SHARE EUROPE UK REGION

Secure

- More secure than TCP/IP on the mainframe
- Reduce/eliminate open ports on the mainframe
- SFTP is approved for HIPAA, FIPS 140-2, SOX, NSA, NIST

Fast

- Unmatched transfer rates, scales to the largest data centers
- Concurrent transfers means no bottlenecks or need to “time shift” workloads

Efficient

- Reduce CPU overhead for mainframe TCP/IP
- Reduce CPU overhead for encryption/translation

Cost-Effective

- Reduce software licensing costs
- No licensing limits for concurrent transfers
- Licensing not based on MIPS/MSUs

Ease of Implementation

- As simple as executing an ICEGENER
- JCL Conversion Utility and Services

Q&A

GUIDE SHARE EUROPE UK REGION

Thank You

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/nn
- Paper feedback forms are also available from the Chair person
- This session is FI