Current Trends in IMS Analytics

David Schipper

BMC Software

November 2018

Session HH

Abstract

This session will provide a brief history of Analytics and how it can be applied to IMS. Areas of interest ranging from predictive analytics to operational analytics to fraud analytics will be discussed. This new way of interpreting data has resulted in new careers like data scientists and big data developers. How does this apply to IMS? What tools are necessary to create an analytics solution? This talk will cover some examples of how BMC is participating in analytic processing and provide you with some points to ponder.

Legal Notice

The information contained in this presentation is the confidential information of BMC Software, Inc. and is being provided to you with the express understanding that without the prior written consent of BMC, you may not discuss or otherwise disclose this information to any third party or otherwise make use of this information for any purpose other than for which BMC intended.

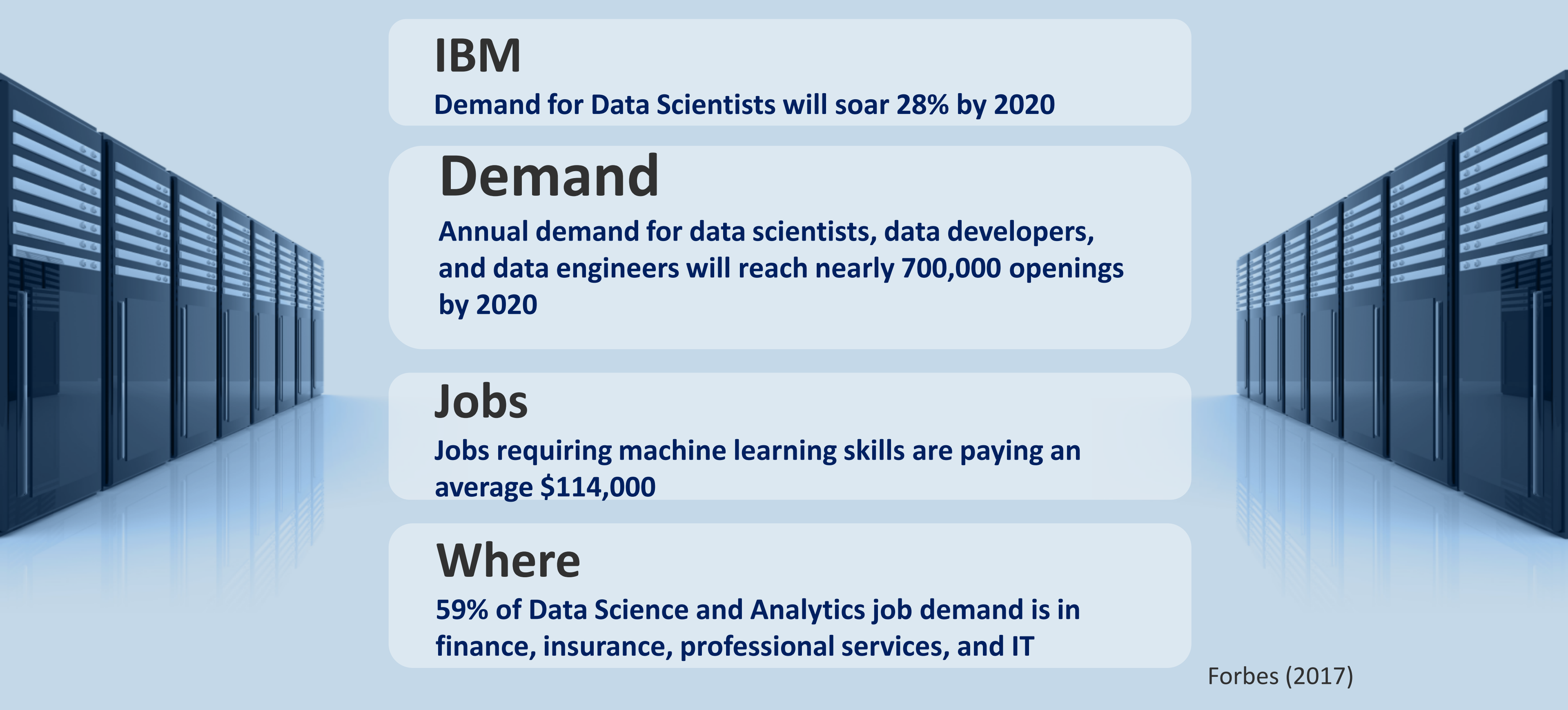
All of the future product plans and releases described herein relate to BMC's current product development considerations, which are at the sole discretion of BMC and are subject to change and/or cancellation at any time. BMC cannot and does not provide any assurance as to whether these plans will result in any future releases of the nature described. These future product plans should not be viewed as commitments on BMC's part and thus should not be relied upon in customer purchase decisions.

AI, ML, Analytics will be Pervasive by 2020

By 2020, **30%** of data centers that fail to apply AI, machine learning, and analytics effectively in support of enterprise business will cease to be operationally and economically viable.[1]

Gartner Report: The IT Implications of the 2018 CIO Survey for I&O Leaders
By Dave Russell, Hank Marquis Published: 8 March 2018

Predictions



IBM

Demand for Data Scientists will soar 28% by 2020

Demand

Annual demand for data scientists, data developers, and data engineers will reach nearly 700,000 openings by 2020

Jobs

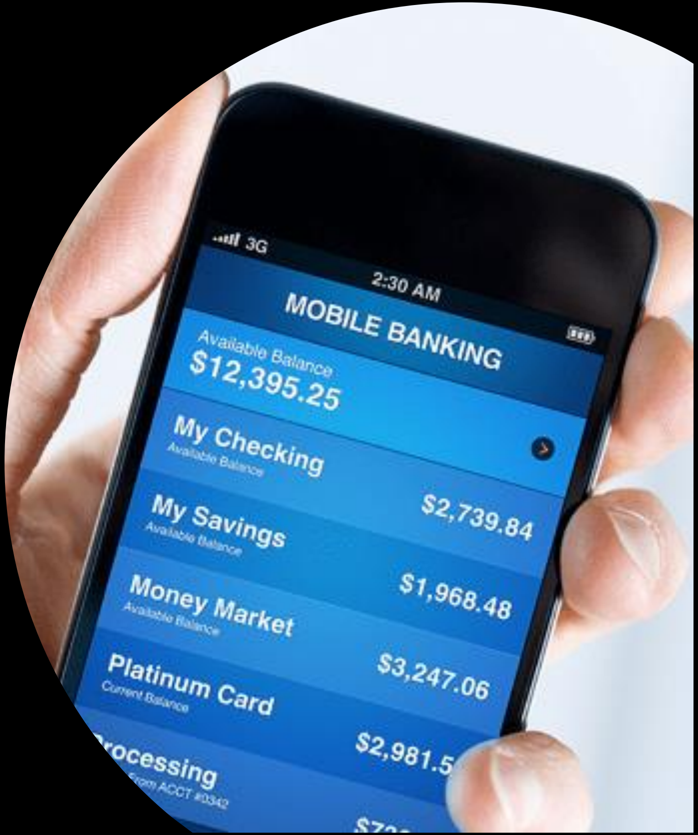
Jobs requiring machine learning skills are paying an average $114,000

Where

59% of Data Science and Analytics job demand is in finance, insurance, professional services, and IT

Forbes (2017)

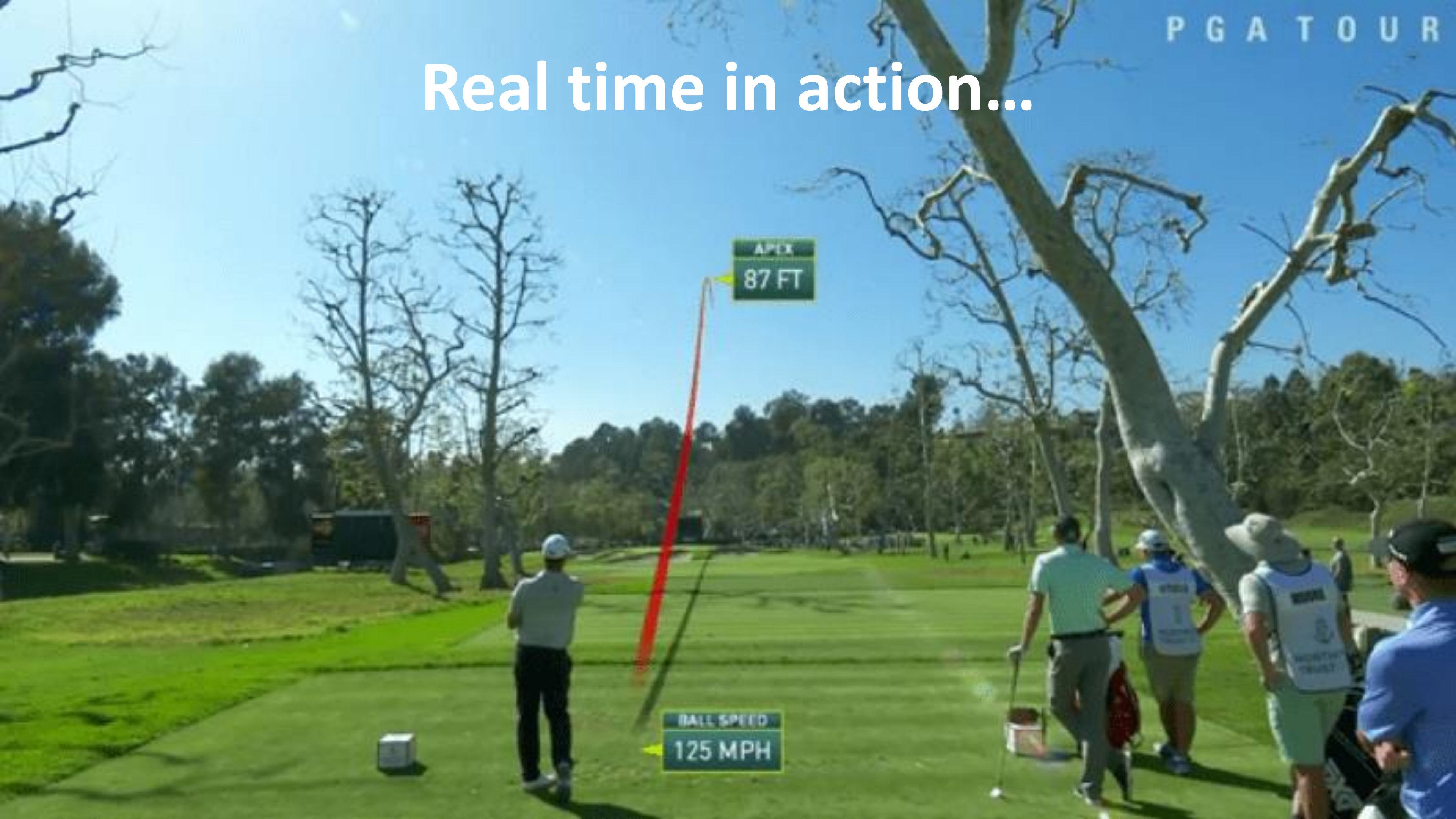
Times are changing

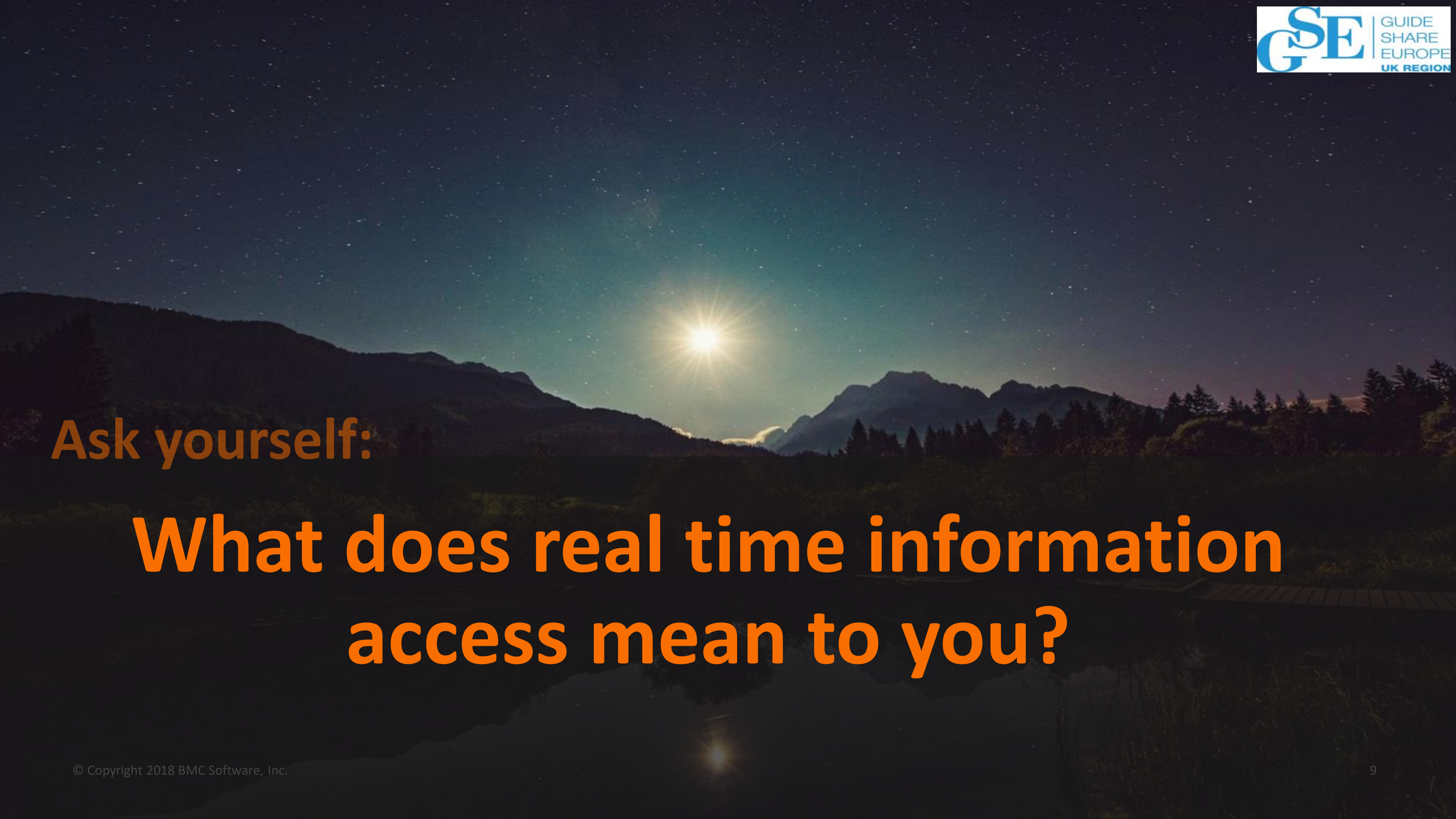


Wi-Fi spatial location analysis

Real-time data

Real time in action…

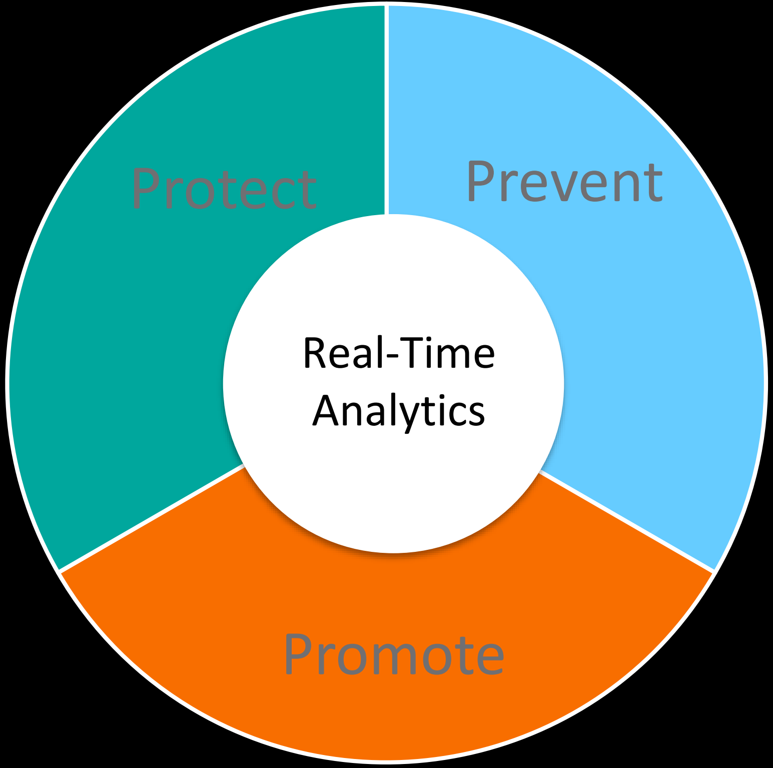




Ask yourself:

What does real time information access mean to you?

Analytics are no longer a “nice to have” luxury



© Copyright 2018 BMC Software, Inc.

Protect

Mainframes can be hacked

– And they have the data hackers want

Mainframe data is essential for enterprise SIEM solutions

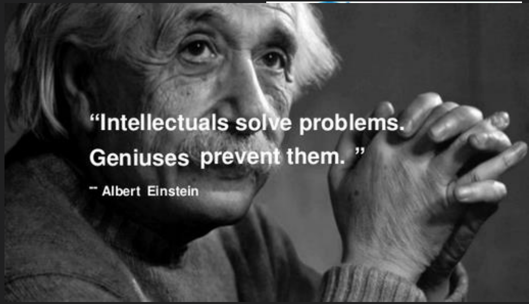
– Without it, you see only part of security picture

Real-time IMS data is essential for protection

– Fixing a security breach is more problematic than preventing it

GDPR demands security

Prevent



You need real-time data to prevent outages/slowdowns

- Outages and slowdowns can mean lost revenue
- You need to be able to find timeouts and abends

Are you meeting SLAs?

- How can you tell?

Promote

Real-time data can help you promote your products

- See what products a customer has
- Offer related products/services

And improve customer service

- During transaction, you can see any open (or past) issues a customer has

How do you plan to use analytics?

SIEM (Security Information and Event Management)/fraud prevention

Operational/ITOA

Root cause analysis/problem analysis

Predictive analytics/prescriptive analytics

Data mining/pattern analysis

SIEM Use Cases

Failed Logons Monitoring

Privileged User Monitoring

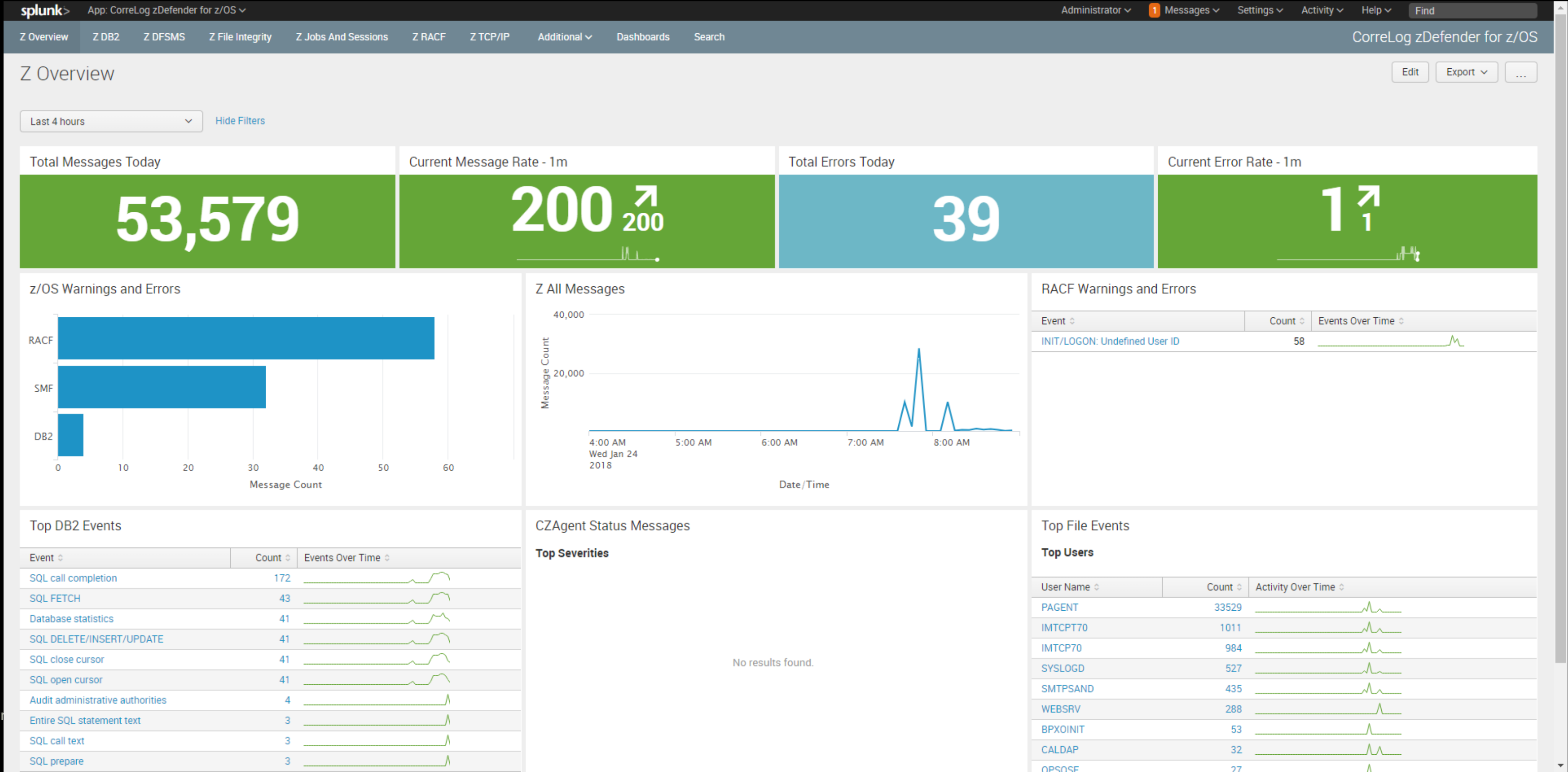
Escalated Privilege Monitoring

File Integrity Monitoring

APF Library Monitoring

Security Compliance Monitoring

z/OS Data in Splunk



Z Overview

Last 4 hours

Total Messages Today	Current Message Rate - 1m	Total Errors Today	Current Error Rate - 1m
53,579	200 ↗ 200	39	1 ↗ 1

z/OS Warnings and Errors

Z All Messages

RACF Warnings and Errors

Event	Count	Events Over Time
INIT/LOGON: Undefined User ID	58	

Top DB2 Events

Event	Count	Events Over Time
SQL call completion	172	
SQL FETCH	43	
Database statistics	41	
SQL DELETE/INSERT/UPDATE	41	
SQL close cursor	41	
SQL open cursor	41	
Audit administrative authorities	4	
Entire SQL statement text	3	
SQL call text	3	
SQL prepare	3	

CZAgent Status Messages

Top Severities

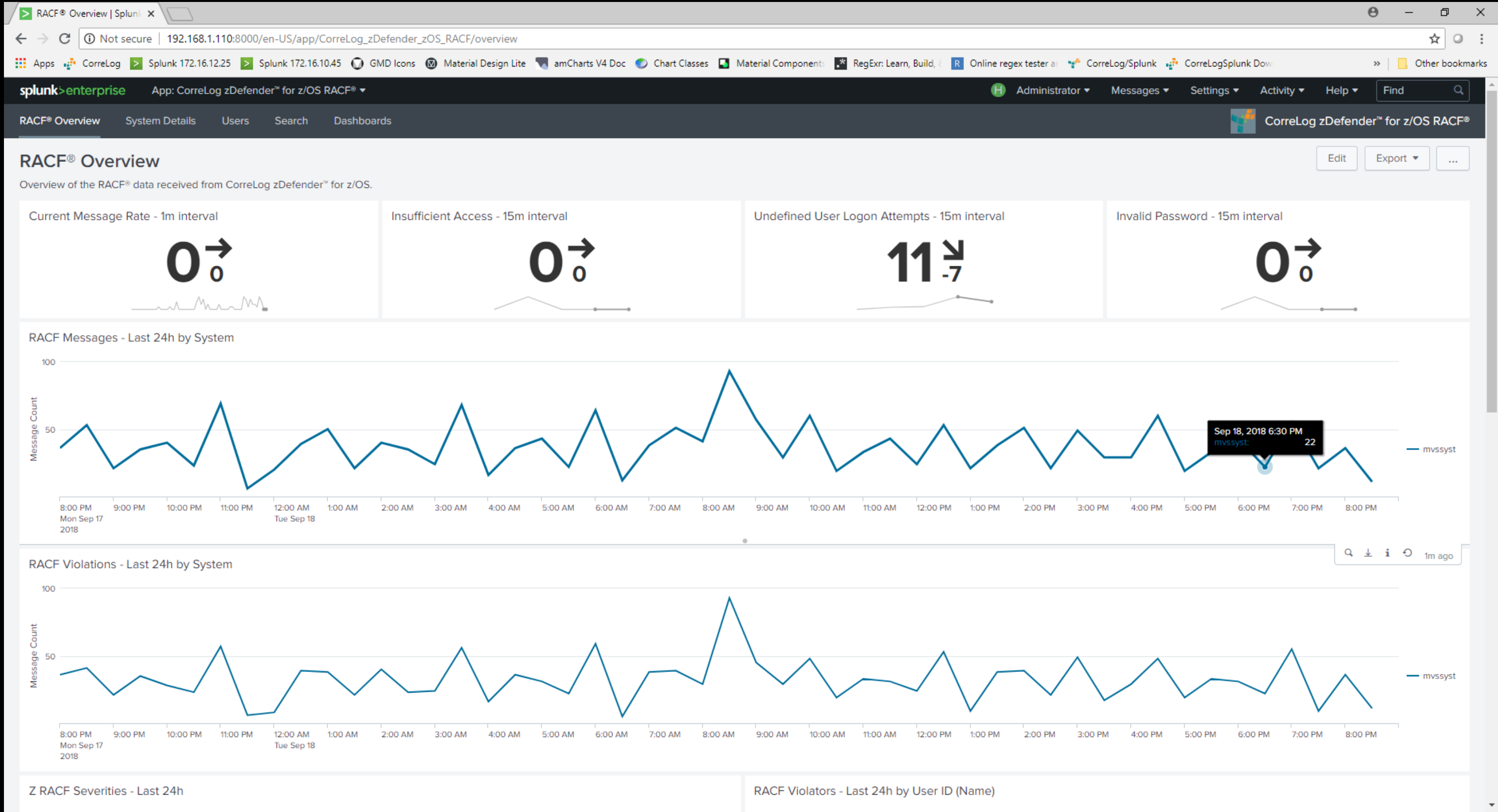
No results found.

Top File Events

Top Users

User Name	Count	Activity Over Time
PAGENT	33529	
IMTCPT70	1011	
IMTCP70	984	
SYSLOGD	527	
SMTPSAND	435	
WEBSRV	288	
BPXOINIT	53	
CALDAP	32	
OPSOSE	27	

RACF® Overview in Splunk



RACF® Overview

Overview of the RACF® data received from CorreLog zDefender™ for z/OS.

Current Message Rate - 1m interval: 0 → 0

Insufficient Access - 15m interval: 0 → 0

Undefined User Logon Attempts - 15m interval: 11 ↘ -7

Invalid Password - 15m interval: 0 → 0

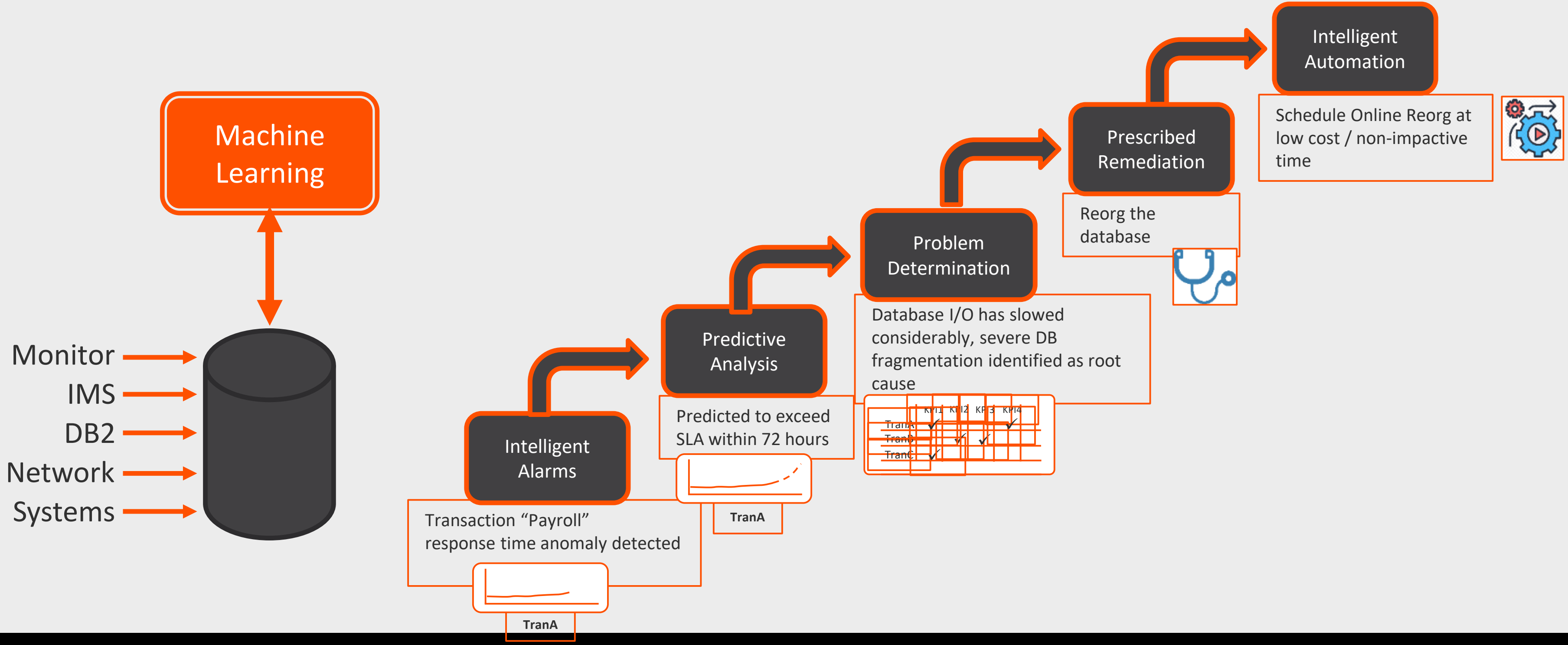
RACF Messages - Last 24h by System

RACF Violations - Last 24h by System

Z RACF Severities - Last 24h

RACF Violators - Last 24h by User ID (Name)

ITOA in Action – Avoiding Application Outages



Machine Learning

Monitor

IMS

DB2

Network

Systems

Intelligent Alarms

Transaction “Payroll” response time anomaly detected

Predictive Analysis

Predicted to exceed SLA within 72 hours

Problem Determination

Database I/O has slowed considerably, severe DB fragmentation identified as root cause

	KPI1	KPI2	KPI 3	KPI4
TranA	✓			✓
TranB		✓	✓	
TranC	✓			

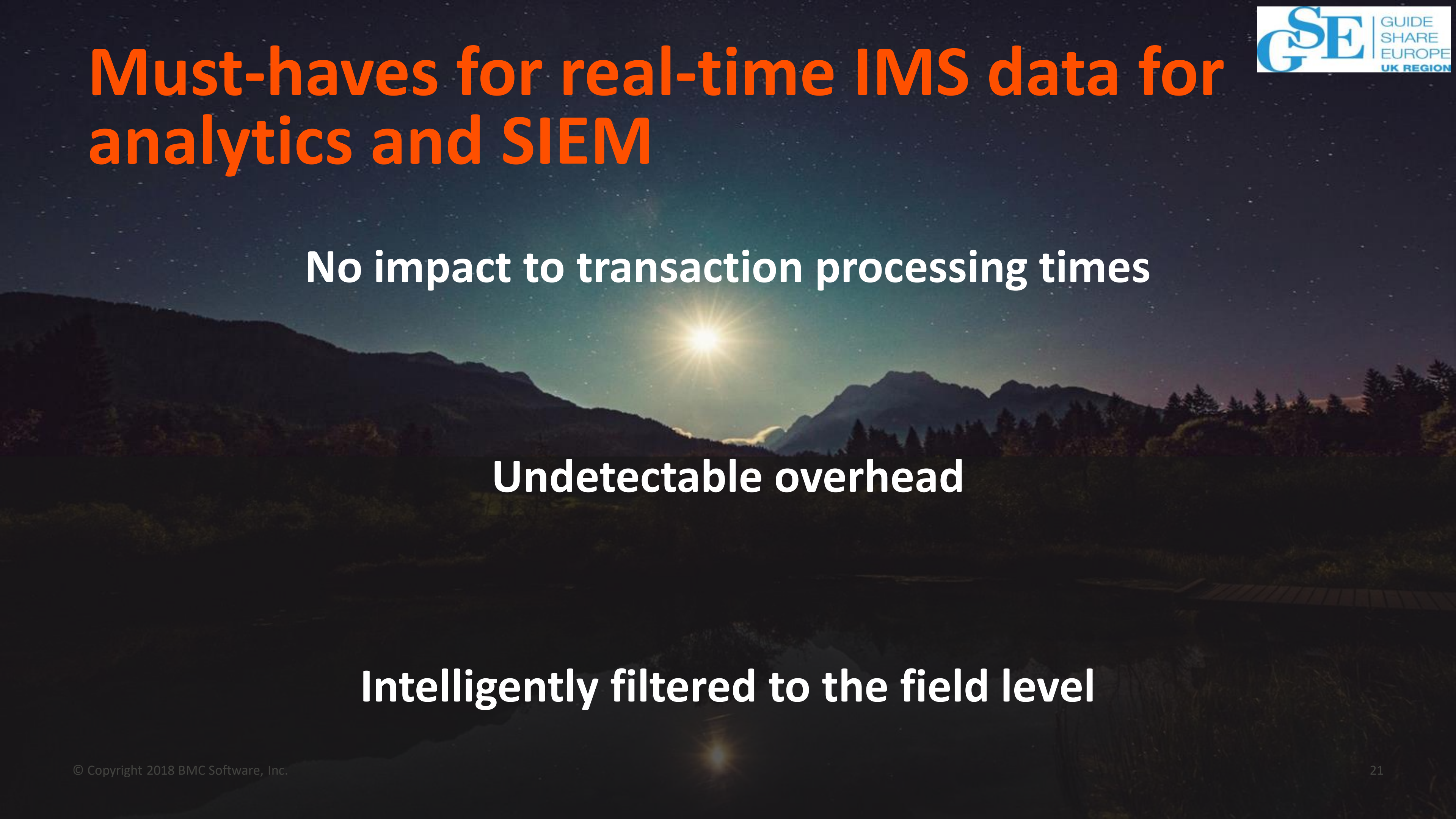
Prescribed Remediation

Reorg the database

Intelligent Automation

Schedule Online Reorg at low cost / non-impactive time

Must-haves for real-time IMS data for analytics and SIEM



No impact to transaction processing times

Undetectable overhead

Intelligently filtered to the field level

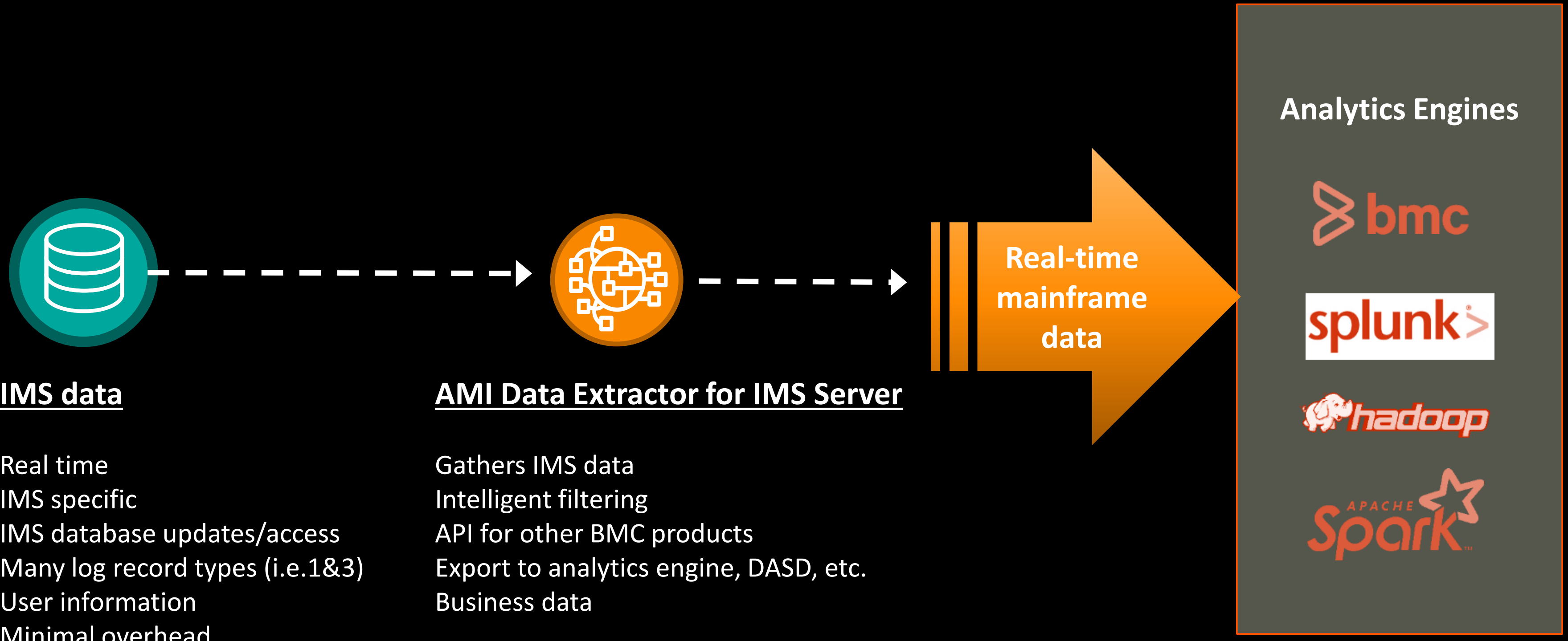
AMI Data Extractor for IMS

Extracts real-time IMS log information for use in SIEM applications or analytics engines

Using proprietary techniques that dramatically reduce overhead associated with data extraction and

Advanced filtering routines to minimize the amount of unnecessary data ingested into the target engines

AMI Data Extractor for IMS



Analytics Engines

Real-time mainframe data

IMS data

Real time
IMS specific
IMS database updates/access
Many log record types (i.e.1&3)
User information
Minimal overhead
No log interruptions

AMI Data Extractor for IMS Server

Gathers IMS data
Intelligent filtering
API for other BMC products
Export to analytics engine, DASD, etc.
Business data

Real time

Real-time access to IMS log record information

Real-time access to BMC product information

- MainView for IMS
- Message Advisor for IMS
- DELTA PLUS

Intelligent filtering

Filtering down to the individual field level

- x’03’ record type
  - Destination name, MFS format, user ID, etc.
- x’07’ and x’08’ record types
  - PSB name, transaction name, etc.

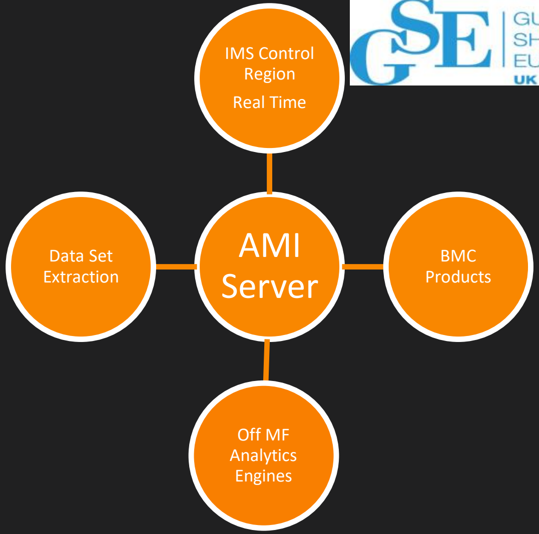
Criteria matching

- Matches whole name, as well as * and % for wildcard matching

Reduces amount of information sent to analytics engines

- Cost saving if analytics engine charges by data size ingested

Components



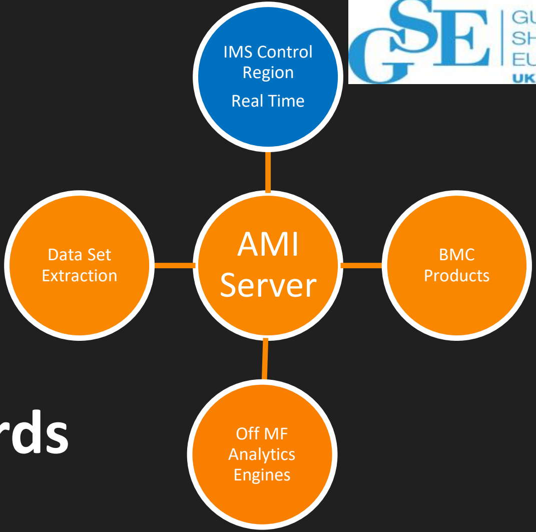
IMS control region

- Small footprint
- No impact rule
- Buffer accessed by AMI Server

AMI Server Address Space

- Most work is done here
- Filtering and extraction rules applied
- Packaging and processing to analytics engines

IMS control region



Low CPU and execution overhead

Preliminary quick filtering to choose log records

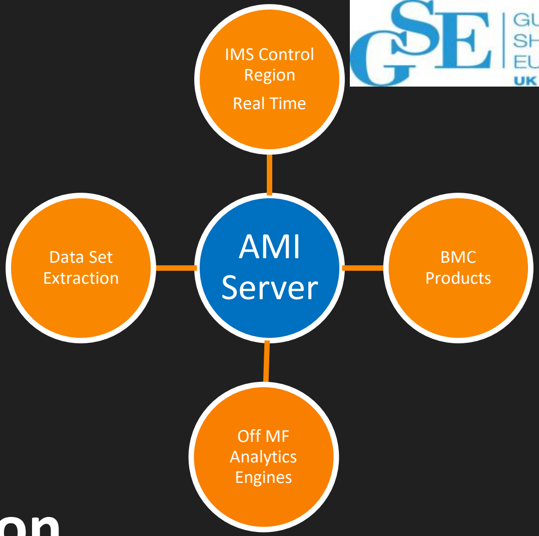
No I/O is done in the IMS control region

Only record types of interest are moved

Cause no outages

Does not use IMS log exit

Server processing



Move records from IMS or API

Apply intelligent filtering

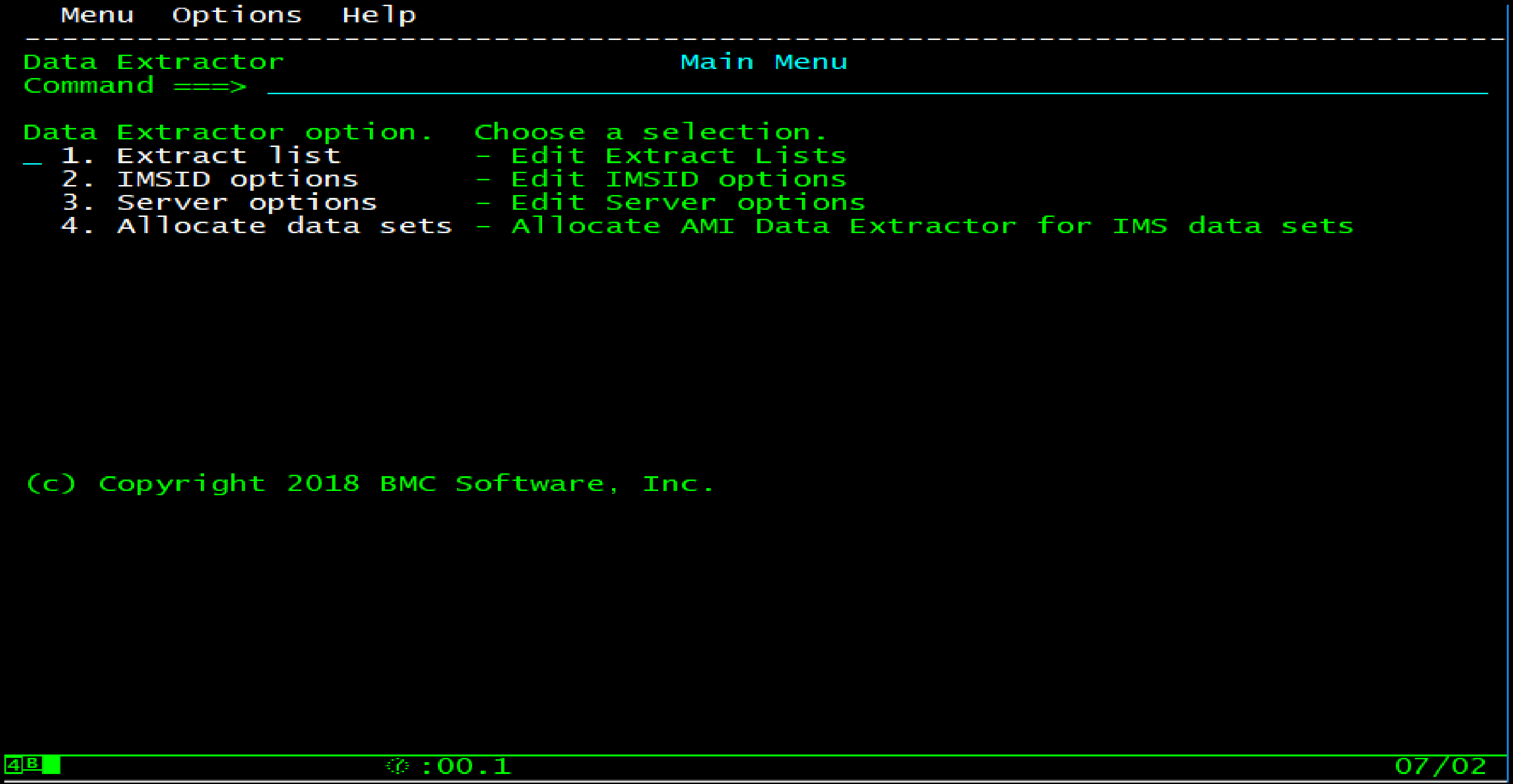
- Test filtering before your run it in production

Extract specified fields

Format into end-user format

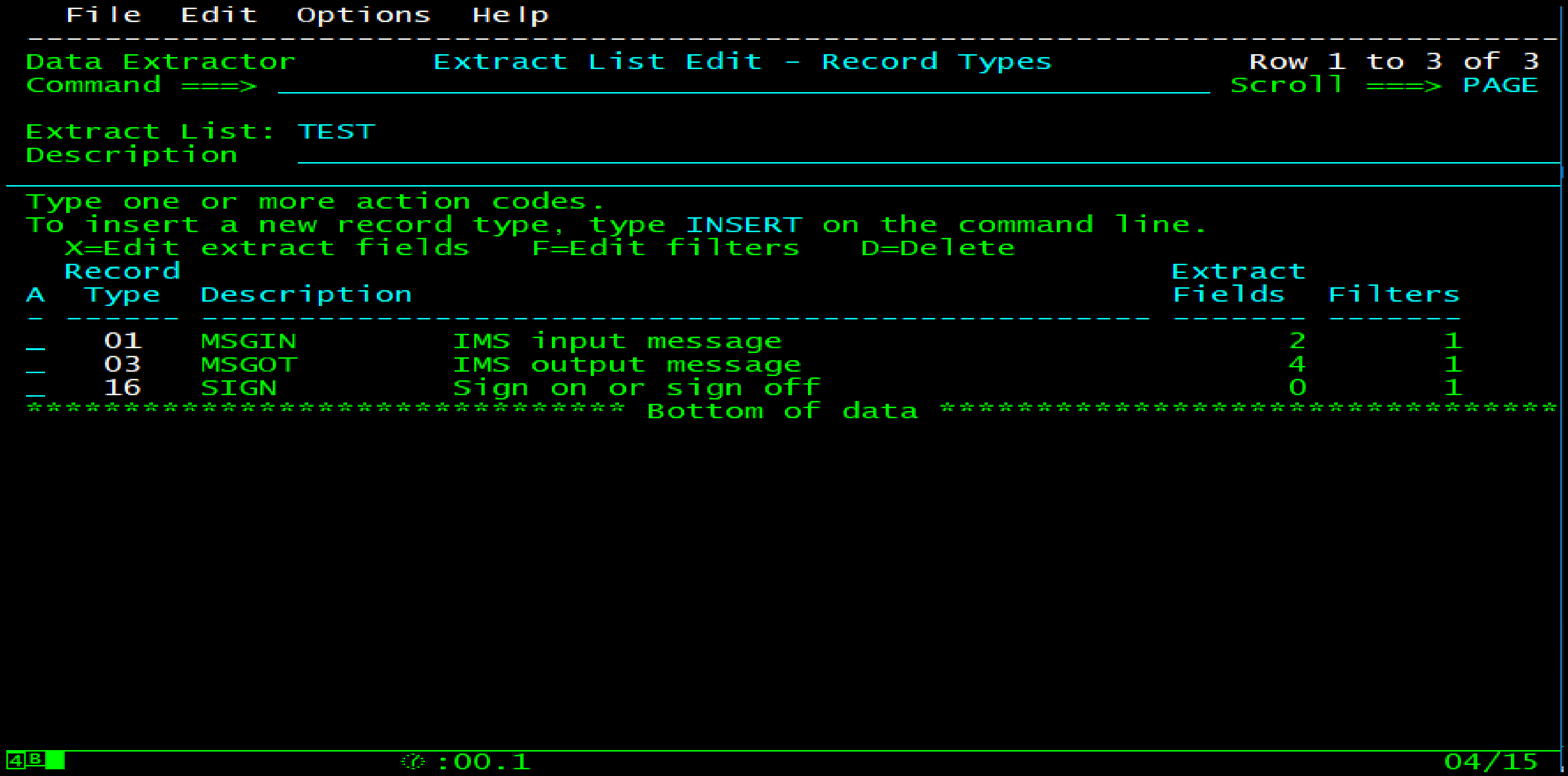
Send data

Intelligent filtering and extraction



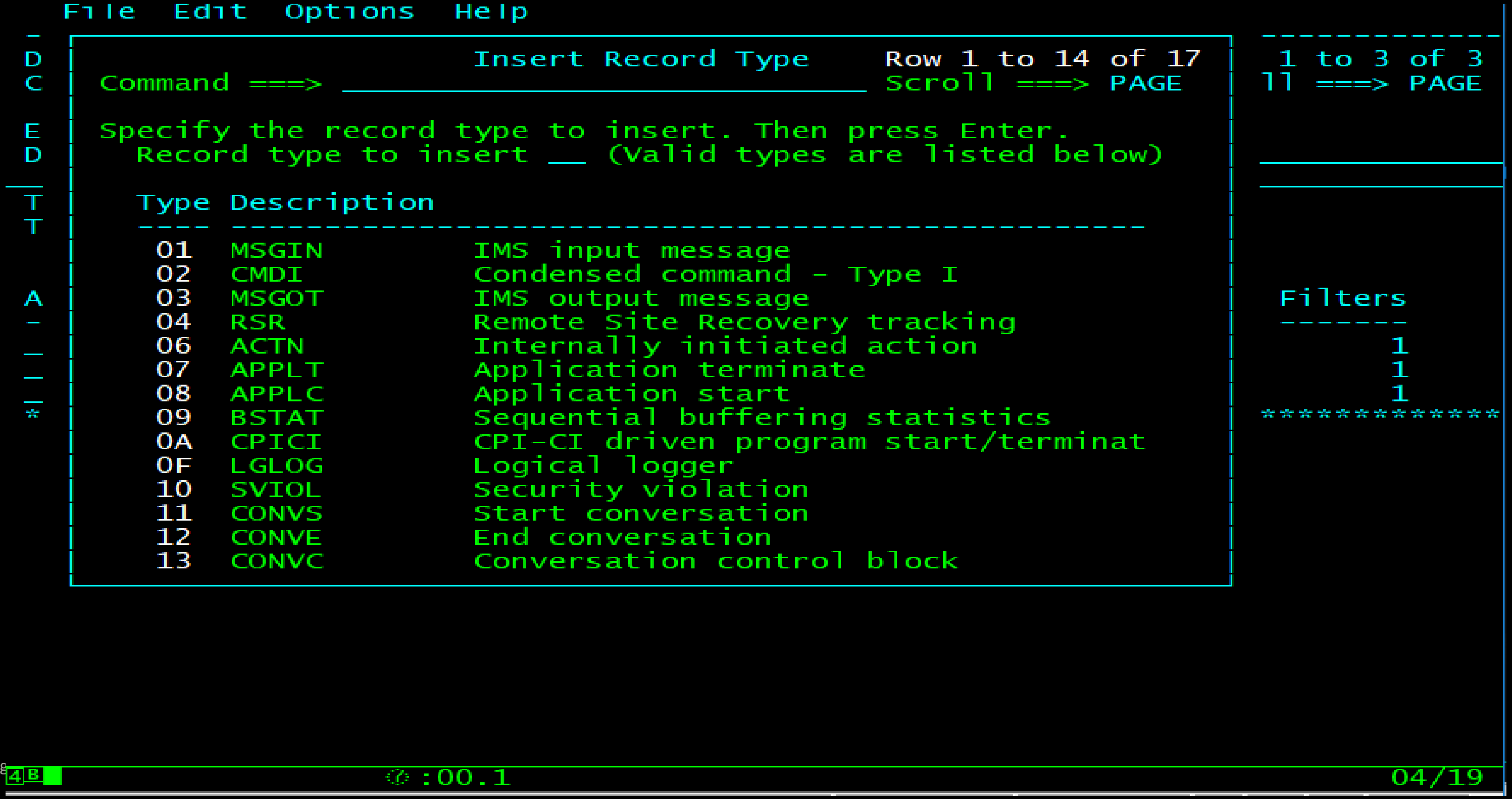
```
   Menu   Options   Help
 ------------------------------------------------------------------------------
 Data Extractor                                   Main Menu
 Command ===> __________________________________________________________________

 Data Extractor option.   Choose a selection.
 _  1. Extract list        - Edit Extract Lists
    2. IMSID options       - Edit IMSID options
    3. Server options      - Edit Server options
    4. Allocate data sets  - Allocate AMI Data Extractor for IMS data sets







 (c) Copyright 2018 BMC Software, Inc.
```

Intelligent filtering and extraction



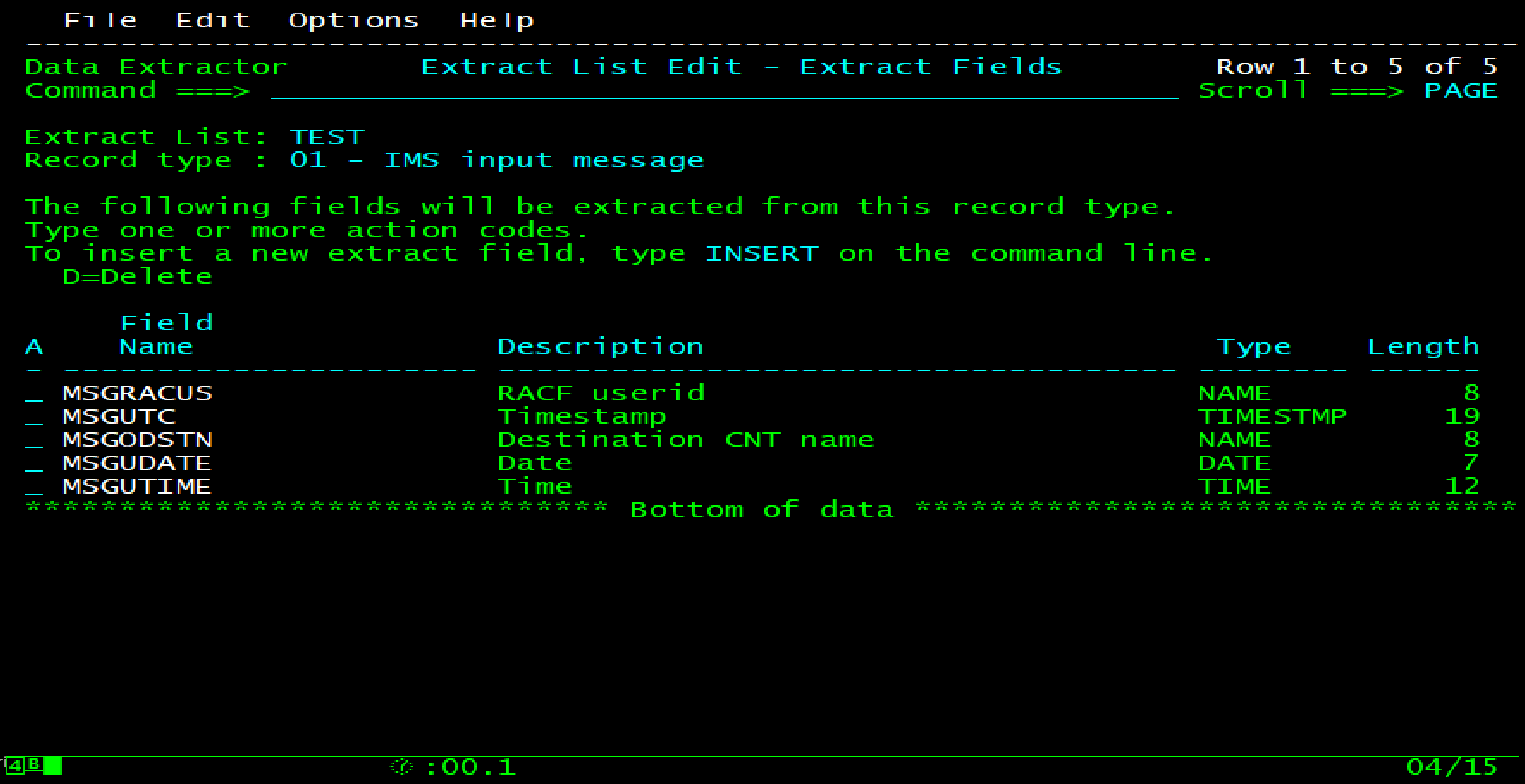
```
   File  Edit  Options  Help
 ------------------------------------------------------------------------------
 Data Extractor          Extract List Edit - Record Types             Row 1 to 3 of 3
 Command ===> ________________________________________________    Scroll ===> PAGE

 Extract List: TEST
 Description   _________________________________________________________________

 Type one or more action codes.
 To insert a new record type, type INSERT on the command line.
   X=Edit extract fields   F=Edit filters   D=Delete
   Record                                                  Extract
 A  Type   Description                                     Fields   Filters
 - ------  ------------------------------------------------ -------  -------
 _    01   MSGIN        IMS input message                        2        1
 _    03   MSGOT        IMS output message                       4        1
 _    16   SIGN         Sign on or sign off                      0        1
 ******************************* Bottom of data ********************************

4B                    :00.1                                               04/15
```

Intelligent filtering and extraction



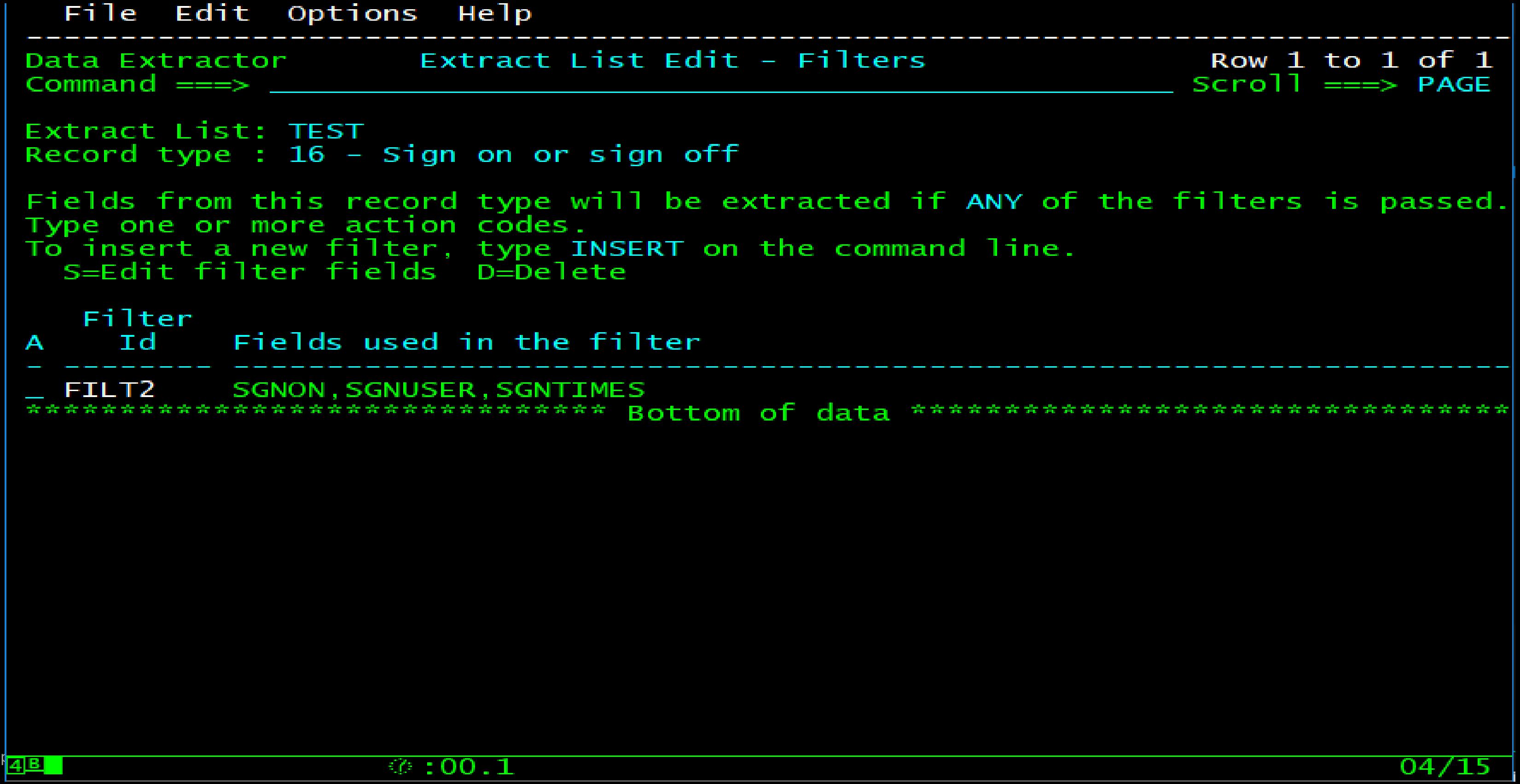
```
   File  Edit  Options  Help
 -                                                                  --------------
 D |                      Insert Record Type    Row 1 to 14 of 17 |  1 to 3 of 3
 C | Command ===> ____________________________  Scroll ===> PAGE  |  ll ===> PAGE
   |                                                              |
 E | Specify the record type to insert. Then press Enter.         |
 D |   Record type to insert __ (Valid types are listed below)    |
___|                                                              |
 T |   Type Description                                           |
 T |   ---- ------------------------------------------------      |
   |    01  MSGIN         IMS input message                       |
   |    02  CMDI          Condensed command - Type I              |
 A |    03  MSGOT         IMS output message                      |   Filters
 - |    04  RSR           Remote Site Recovery tracking           |   -------
 _ |    06  ACTN          Internally initiated action             |         1
 _ |    07  APPLT         Application terminate                   |         1
 _ |    08  APPLC         Application start                       |         1
 * |    09  BSTAT         Sequential buffering statistics         | *************
   |    0A  CPICI         CPI-CI driven program start/terminat    |
   |    0F  LGLOG         Logical logger                          |
   |    10  SVIOL         Security violation                      |
   |    11  CONVS         Start conversation                      |
   |    12  CONVE         End conversation                        |
   |    13  CONVC         Conversation control block              |

4B                  :00.1                                        04/19
```

Intelligent filtering and extraction



```
  File  Edit  Options  Help
------------------------------------------------------------------------------
Data Extractor        Extract List Edit - Extract Fields          Row 1 to 5 of 5
Command ===> ________________________________________________   Scroll ===> PAGE

Extract List: TEST
Record type : 01 - IMS input message

The following fields will be extracted from this record type.
Type one or more action codes.
To insert a new extract field, type INSERT on the command line.
  D=Delete

     Field
A    Name                   Description                         Type     Length
- ----------------------- ------------------------------------ -------- ------
_ MSGRACUS                RACF userid                          NAME          8
_ MSGUTC                  Timestamp                            TIMESTMP     19
_ MSGODSTN                Destination CNT name                 NAME          8
_ MSGUDATE                Date                                 DATE          7
_ MSGUTIME                Time                                 TIME         12
******************************* Bottom of data ********************************

4B                         :00.1                                          04/15
```

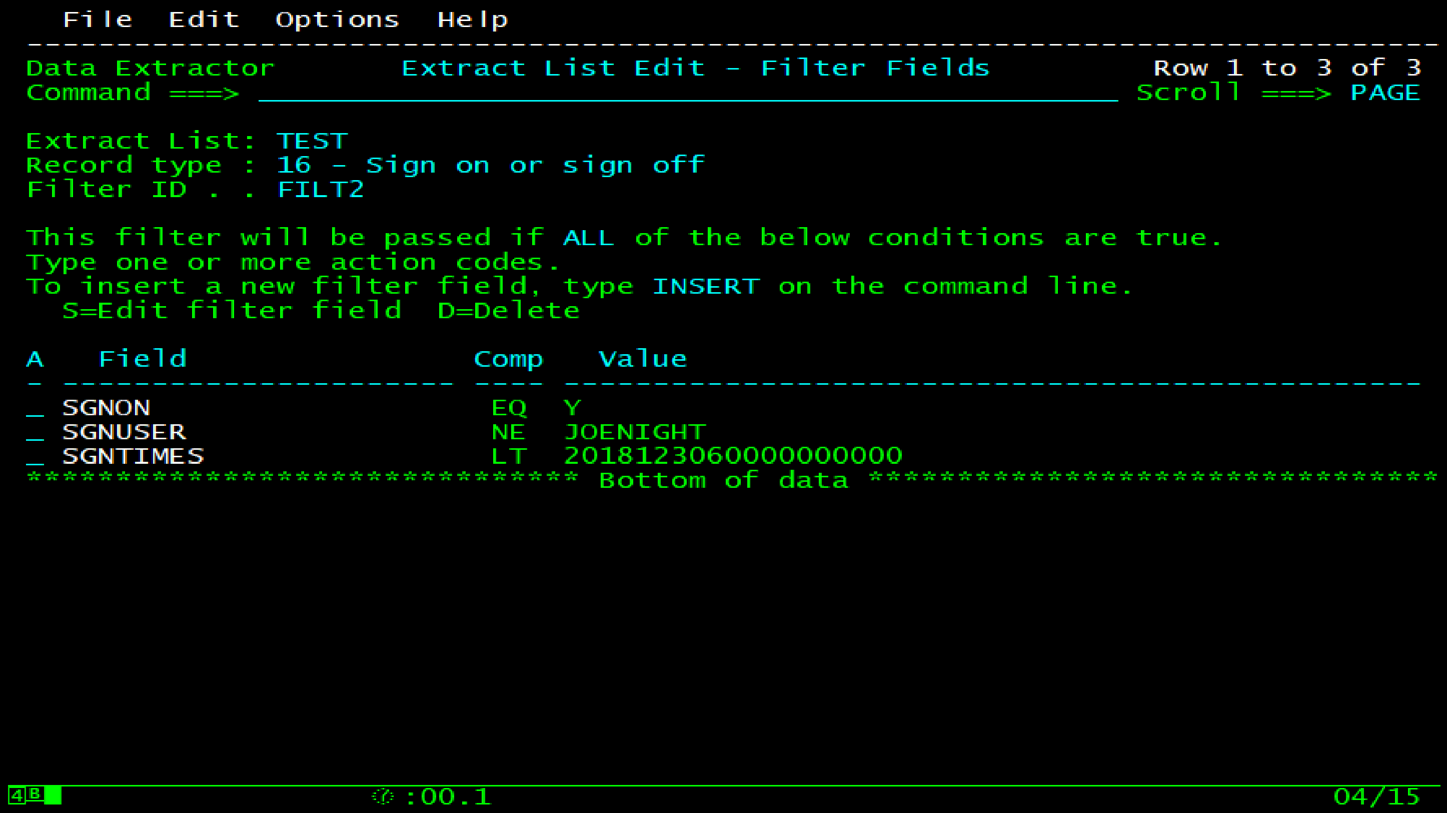
Intelligent filtering and extraction



```
  File  Edit  Options  Help
--------------------------------------------------------------------------------
Data Extractor       Extract List Edit - Filters                Row 1 to 1 of 1
Command ===> ____________________________________________________ Scroll ===> PAGE

Extract List: TEST
Record type : 16 - Sign on or sign off

Fields from this record type will be extracted if ANY of the filters is passed.
Type one or more action codes.
To insert a new filter, type INSERT on the command line.
  S=Edit filter fields  D=Delete

   Filter
A    Id     Fields used in the filter
- --------- --------------------------------------------------------------------
_ FILT2     SGNON,SGNUSER,SGNTIMES
******************************* Bottom of data ********************************
```

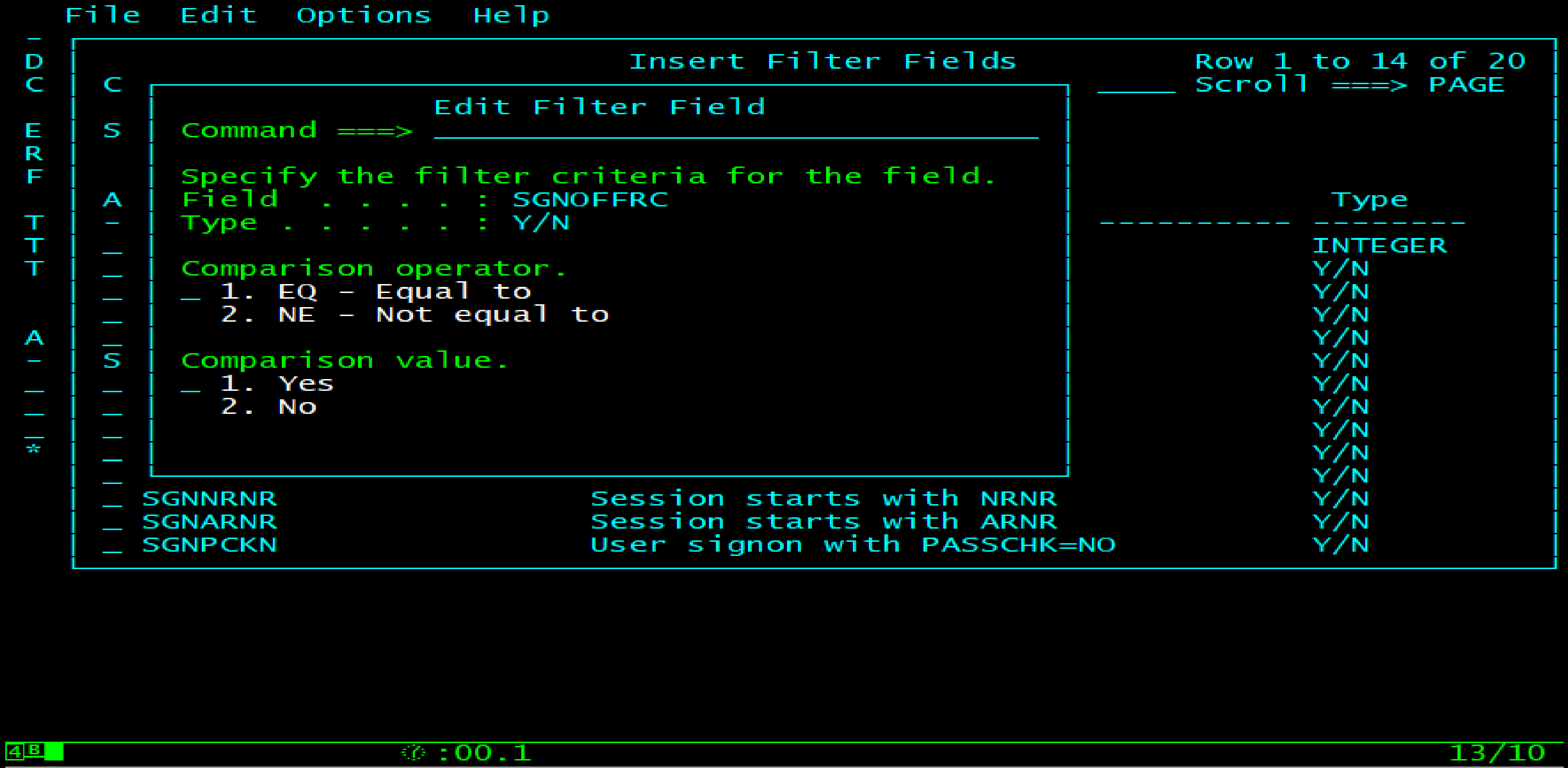
```
4B                         :00.1                                          04/15
```

Intelligent filtering and extraction



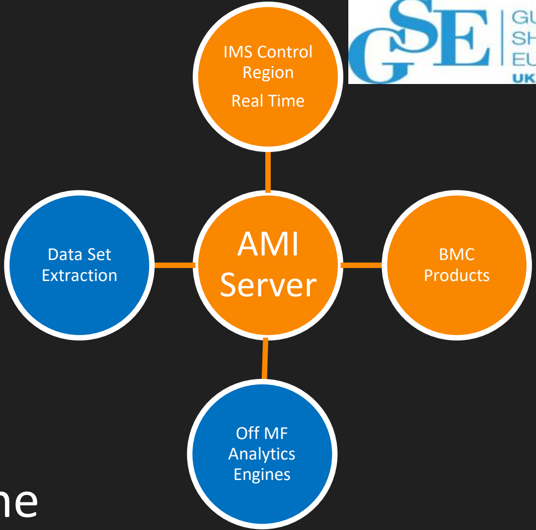
```
   File  Edit  Options  Help
-------------------------------------------------------------------------------
Data Extractor       Extract List Edit - Filter Fields          Row 1 to 3 of 3
Command ===> ________________________________________________ Scroll ===> PAGE

Extract List: TEST
Record type : 16 - Sign on or sign off
Filter ID . . FILT2

This filter will be passed if ALL of the below conditions are true.
Type one or more action codes.
To insert a new filter field, type INSERT on the command line.
  S=Edit filter field  D=Delete

A   Field                     Comp   Value
- ---------------------- ---- ------------------------------------------------
_ SGNON                      EQ   Y
_ SGNUSER                    NE   JOENIGHT
_ SGNTIMES                   LT   2018123060000000000
******************************* Bottom of data ********************************

4B                            :00.1                                      04/15
```

Intelligent filtering and extraction



```
   File  Edit  Options  Help
 -
 D |                             Insert Filter Fields          Row 1 to 14 of 20 |
 C |  C  |                                            | _____  Scroll ===> PAGE  |
   |     |             Edit Filter Field              |                          |
 E |  S  | Command ===> ______________________________ |                          |
 R |     |                                            |                          |
 F |     | Specify the filter criteria for the field. |                          |
   |  A  | Field  . . . . : SGNOFFRC                  |            Type          |
 T |  -  | Type . . . . . : Y/N                       | ---------- ---------     |
 T |  _  |                                            |            INTEGER       |
 T |  _  | Comparison operator.                       |            Y/N           |
   |  _  | _  1. EQ - Equal to                        |            Y/N           |
   |  _  |    2. NE - Not equal to                    |            Y/N           |
 A |  _  |                                            |            Y/N           |
 - |  S  | Comparison value.                          |            Y/N           |
 _ |  _  | _  1. Yes                                  |            Y/N           |
 _ |  _  |    2. No                                   |            Y/N           |
 _ |  _  |                                            |            Y/N           |
 * |  _  |                                            |            Y/N           |
   |  _                                                            Y/N           |
   |  _ SGNNRNR                 Session starts with NRNR           Y/N           |
   |  _ SGNARNR                 Session starts with ARNR           Y/N           |
   |  _ SGNPCKN                 User signon with PASSCHK=NO        Y/N           |

 4B                  :00.1                                             13/10
```

AMI Server Output



TCP/IP - data can be sent to

- Any analytics engine that accepts TCP/IP
- TCP/IP server that can forward to analytics engine
  - Custom TCP/IP server written in Python, C, C++ etc.

Data set extraction

- Data can be written to a data set for mainframe analytics engines
- Supports GDG as well as symbol replacement
  - AFI.%SID.D%AFDATE.T%AFTIME.N%N
  - AFI.JRTP.D2018159.T2140186.N00

Benefits

Real-time data drives real-time decisions

- Real-time IMS data + SIEM tools = immediate threat detection
- Real-time analytics alerts help you prevent slowdowns and outages

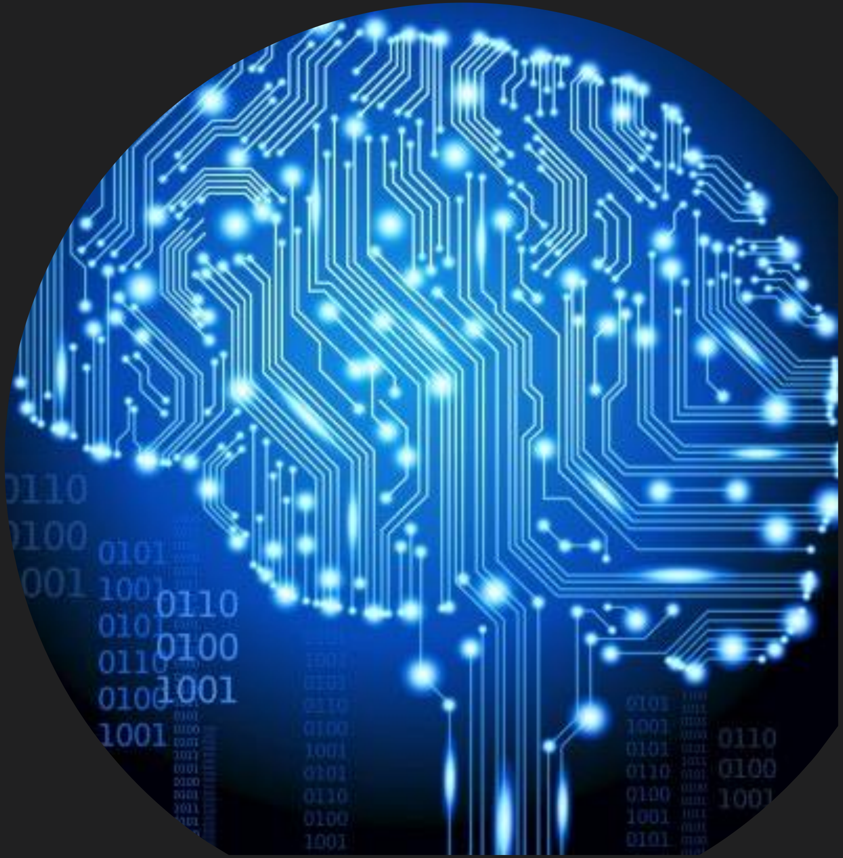
No impact to production IMS systems

Extract only the data you need reducing costs for analytics engines that charge by amount of data ingested

Our direction

Adding intelligence to

- **Provide you more access to YOUR IMS data**
  - In real time
  - No impact to processing times
  - Undetectable overhead
- **Solving YOUR business problems**

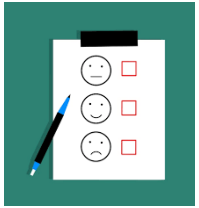


What would you build with real-time access to YOUR IMS log data?

Thank You

We want your feedback!

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



Tuesday 6th November

Start Time	End Time	Stream	Room	Title	Speaker
11:45	12:45	IMS	Wellington B	The No Cost Way to Manage the IMS Catalog	David Schipper
15:00	16:00	IMS	Wellington B	Current Trends in IMS Analytics	David Schipper
16:30	17:30	zCMPA	Woodcote	zIIP stealing GCP MSUs time for Capacity Management	Donald Zeunert

Wednesday 7th November

Start Time	End Time	Stream	Room	Title	Speaker
09:30	10:30	Db2	Nurburgring	Know your onions when it comes to Db2 indexes	Randy Bright
09:30	10:30	IMS	Wellington B	IMS Checkpoint Pacing	David Schipper
10:45	11:45	zCMPA	Nurburgring	How many GCP MSU is my CF stealing?	Donald Zeunert

bmc