IBM Security

Agent X, You Work for Me!

Lee Wei

March, 2017

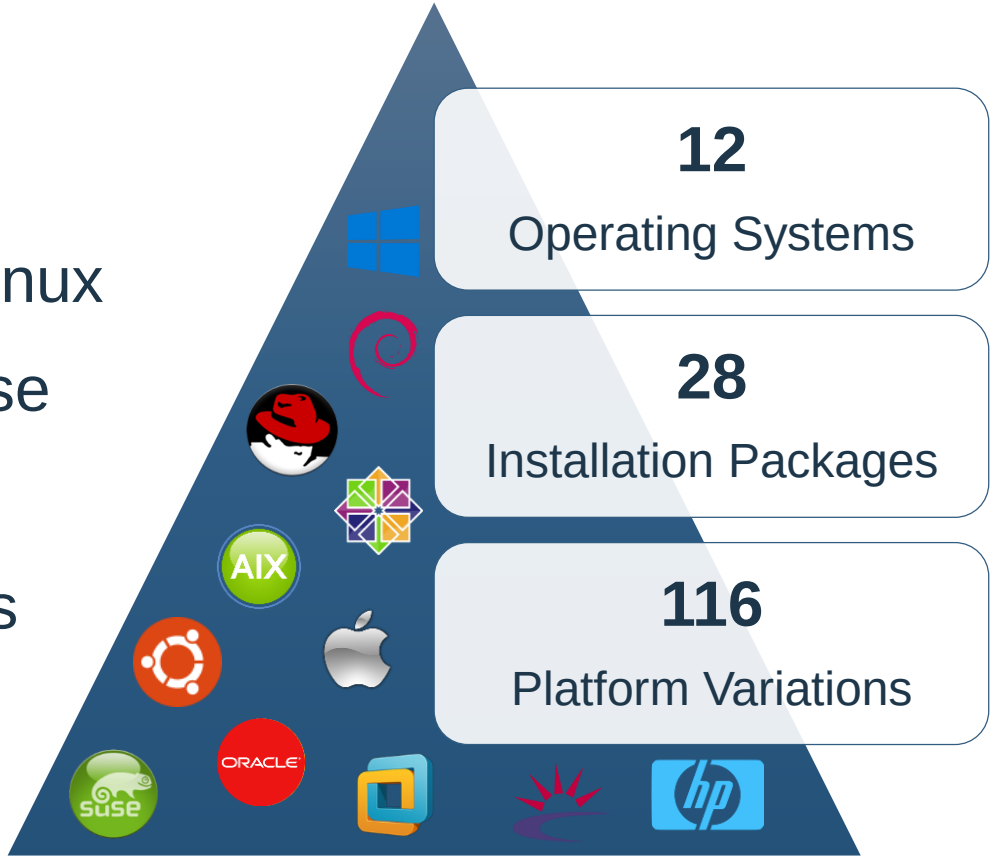
IBM

Topics

- Technical session
- What does the BigFix Agent do
- Agent CPU utilization
- Agent profiling

BigFix Agent supported platforms

- AIX
- CentOS
- Debian
- HP-UX
- Mac OS X
- Oracle Linux
- Red Hat
- Solaris
- SUSE Linux
- Enterprise
- Ubuntu
- Windows
- VMware ESX



12
Operating Systems

28
Installation Packages

116
Platform Variations

BigFix Agent

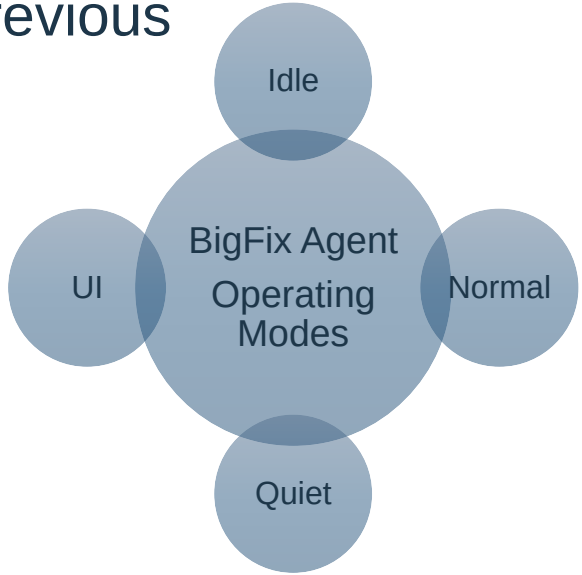
- The BigFix Agent basically has a big `while {...}` loop that processes Relevance, report properties and states, and waits to obey other commands send its way
- One key characteristic is the highly optimized tuning of the client to use the least resources to behavior properly
  - Caches appropriately
  - Backs off as needed
  - Very stable from the years of tuning in the real-world at customer sites
- The BigFix Agent has no other external dependencies

BigFix Agent main functions

- Registration, Relay selection, authentication
- Gathering site content
- Relevance evaluation (Fixlets, properties, actions, etc.)
- Action processing
- Reporting (Properties, Fixlet and action states)
- Client user interface
- Archiving and uploading data
- Client compliance API processing
- Fast Query processing, communication and control
- BigFix Detect agent communication and control

BigFix Agent CPU utilization

- CPU usage and utilization is throttled
- Given throttling, the percentages quotes are "average" usage not maximum
- CPU usage using actual CPU time over previous elapse time (new in 9.0)
- What 2%?
- The many modes of CPU usage
  - Idle
  - UI
  - Normal
  - Quiet



BigFix Agent modes

Idle
The default mode when not in the other modes (including Quiet)

UI
Elevates CPU usage when the end-user opens the Client UI

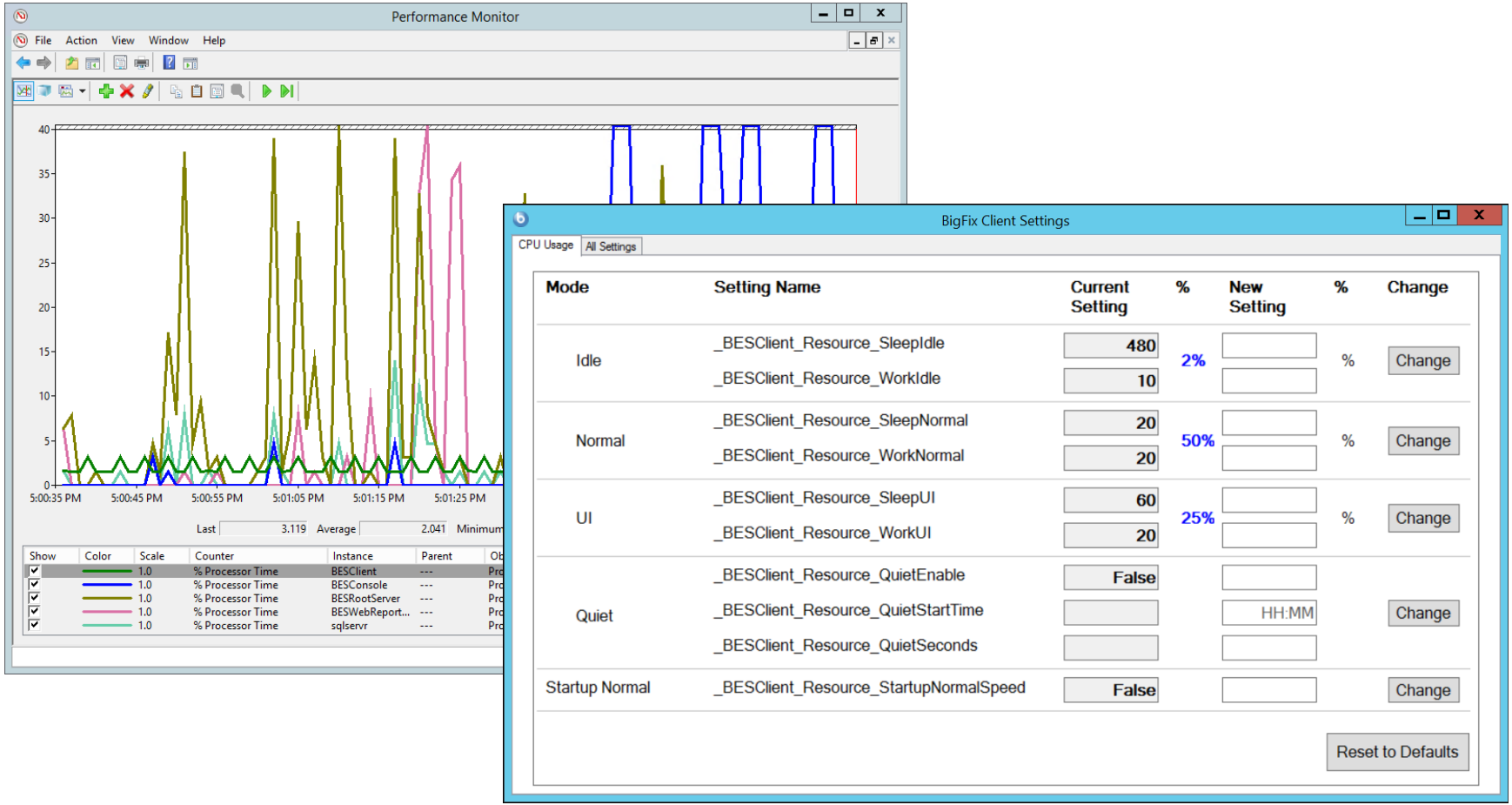
Normal
Elevates CPU usage while performing actions

Quiet
Allows the Agent to be completely quiet (0%) for a set period within a day

BigFix Agent CPU resource configuration settings

- All settings are configured and stored in the common settings locations
  - Windows Windows Registry
  - Unix/Linux /var/opt/BESClient/besclient.config
  - Mac OS X /Library/Preferences/com.bigfix.BESAgent.plist
- Configure as per other computer settings
- All are configured as Work/Sleep balance

Using Perfmon and Client Setting utility

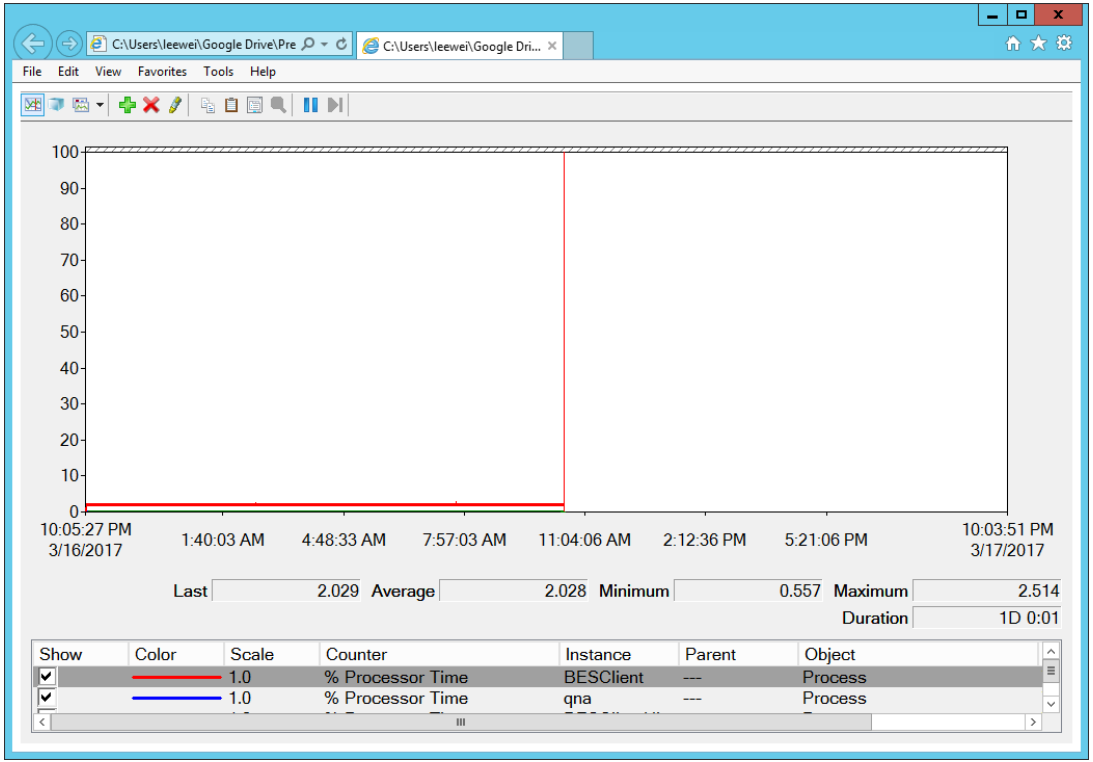


Idle mode (2%)

- Idle is the default mode when the Agent is not in other modes
- The "2% CPU utilization" famously references this mode in its default
- Idle is a misnomer in that the agent is performing a lot of work
- When should I and why would I want to change this?
- 10ms work cycle is a good rule of thumb
- Demo
  - Switch to 190/10 (5%)

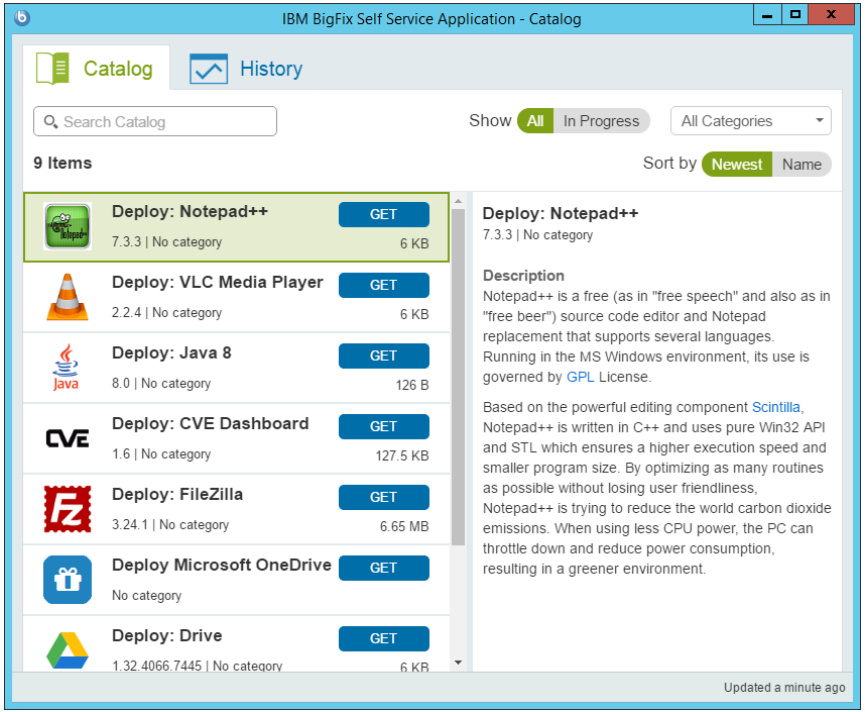
Idle mode

- If not in other modes, the Agent is expected to maintain the average CPU utilization configured
- Example of an Agent in Idle mode for a period of 12 hours



UI mode (25%)

- When the user opens the Client UI (aka Self Service Application), the Agent enters into the UI mode
- This helps speed up agent execution for a better user experience
- The Agent UI will exit this mode based on completion of work to be done
- The default is an average of 25% of the CPU



Normal mode (50%)

- Increases CPU utilization when agent is performing important tasks
- By default, the agent will use on average 50% of the CPU
- Before version 8.5, it was <5%
- The Agent goes into Normal Mode when:
  - Processing actions
  - Performing a force refresh
  - Servicing the Client Compliance API
- Note that the agent does not have control of processes spawned – for example, Microsoft patch executables
  - Windows Updates will likely take 100% of the CPU
- Demo
  - Use Self-Service Application to take action
  - Force Refresh

Quiet mode

- Quiet mode addresses the use case and need to be absolutely quiet for a block of time per day
  - For example during banking or retail hours
- The Agent is expected to use 0% CPU
- The Agent will not evaluate any content, report status, or take actions
- There are 3 setting required to configure this mode
  - Enable the setting
    - `_BESClient_Resource_QuietEnable`
  - Specify the time of day
    - `_BESClient_Resource_QuietStartTime`
  - Specify the duration
    - `_BESClient_Resource_QuietSeconds`

BigFix Agent CPU usage modes summary

Mode	Default CPU %	Trigger for Entry	Trigger for Exit	Control Settings
Idle	2%	• When not in other modes	• Entering other working modes	`_BESClient_Resource_SleepIdle` `_BESClient_Resource_WorkIdle`
UI	25%	• User opens the Client UI	• User exits the Client UI	`_BESClient_Resource_SleepUI` `_BESClient_Resource_WorkUI`
Normal	50% (5% <9.0)	• Running actions • Forced refresh	• Completed action • Posted refresh report	`_BESClient_Resource_SleepNormal` `_BESClient_Resource_WorkNormal`

Quiet	0%	• Based on setting	• Based on setting	`_BESClient_Resource_QuietEnable`
				`_BESClient_Resource_QuietStartTime`
				`_BESClient_Resource_QuietSeconds`

Agent evaluation profiling (aka resource tracking)

- Logs time spent evaluating content
- Tracks the top 100 (default) content (Fixlets, properties, etc.) that take the longest time
- 2 Tasks in the BES Support site provided to enable/disable profiling
  - Enable BES Client Usage Profiler
  - Disable BES Client Usage Profiler
- Results in seconds
- Remember this is the Agent performing at low CPU utilization
- Enterprise Security is synonymous to Patches for Windows

usageprofiler.0001.log (1.6 KB) - BareTail

File Edit View Preferences Help

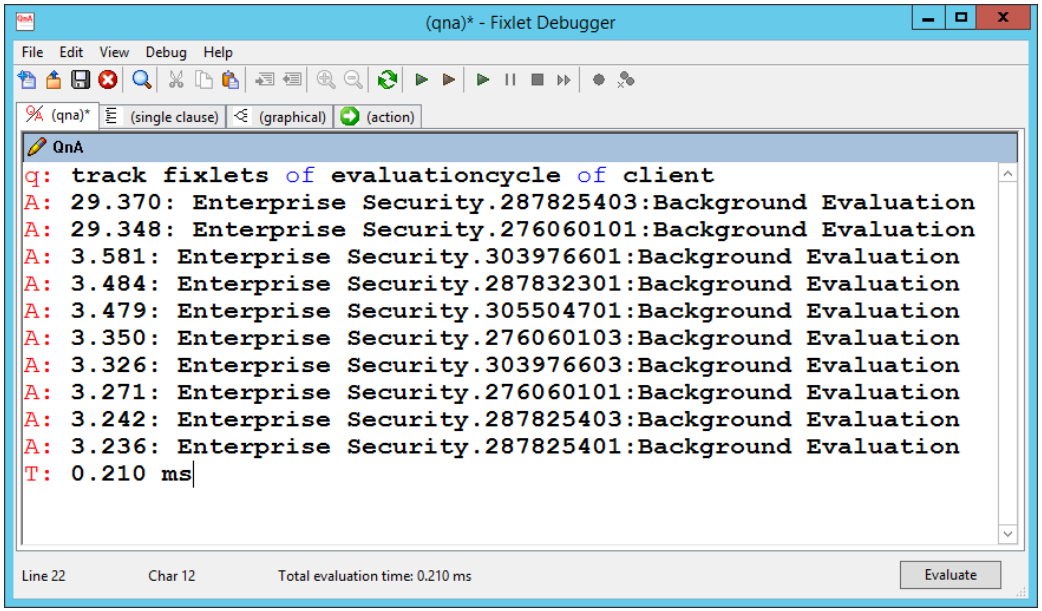
Open Highlighting Follow Tail ANSI C:\Program Files (x86)\BigFix Enterprise\BES Client\usageprofiler.0001.log (1.6 KB)

```
Start:Tue, 14 Mar 2017 21:18:19 -0700
Elapsed Time:00:08:13
Tracking: Top 25
Samples:2173
Elapsed Evaluation Time:00:06:20

0000) 56.971: Enterprise Security.311547503:Background Evaluation
0001) 56.895: Enterprise Security.287825401:Background Evaluation
0002) 55.571: Enterprise Security.276060101:Background Evaluation
0003) 55.483: Enterprise Security.287825403:Background Evaluation
0004) 53.231: Enterprise Security.287832301:Background Evaluation
0005) 51.677: Enterprise Security.287832303:Background Evaluation
0006) 3.863: Enterprise Security.316575601:Background Evaluation
0007) 3.122: BES Support.709:Background Evaluation
0008) 2.299: Enterprise Security.1613617:Background Evaluation
0009) 1.572: Client Manager for Anti-Virus.207:Background Evaluation
0010) 1.536: Enterprise Security.315827103:Background Evaluation
0011) 1.502: BES Support.354:Background Evaluation
0012) 0.891: actionsite.13:Evaluate Property 1
0013) 0.819: BES Support.173:Background Evaluation
0014) 0.778: BES Support.1647:Background Evaluation
0015) 0.771: Enterprise Security.254986401:Background Evaluation
0016) 0.764: BES Inventory and License.54:Background Evaluation
0017) 0.763: BES Inventory and License.46:Background Evaluation
0018) 0.762: CustomSite_Bricks.179:Background Evaluation
0019) 0.760: Client Manager for Anti-Virus.125:Background Evaluation
0020) 0.758: BES Support.840:Evaluate Property 5
0021) 0.758: Enterprise Security.69103:Background Evaluation
0022) 0.758: BES Support.1578:Evaluate Property 2
0023) 0.757: Enterprise Security.29211:Background Evaluation
0024) 0.757: BES Support.1165:Background Evaluation
```

Agent evaluation profiling (aka resource tracking)

- A new Agent inspector has been added in 9.0 to automatically track the top 10 longest running expressions
- However, the settings described in the previous slide will take precedence
- Try:
  - `track fixlets of evaluationcycle of client`
- Make sure to run QnA in “Local Client Evaluator” mode



Query settings

- Query uses a different processing channel to service requests
- QnA program is invoked do the Relevance evaluation
- There is a separate set of work/sleep settings for Query
  - `_BESClient_Query_WorkTime` (defaults to 10)
  - `_BESClient_Query_SleepTime` (defaults to 480)

`_BESClient_Resource_StartupSleepSecond` setting

- Make the Agent sleep until the desired time has elapsed during startup
- Similar to Windows service Automatic (Delayed Start)
- Use cases include:
  - Prevent race conditions (e.g. Relay selection)
  - Avoid boot storms

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular**, **purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM