Notices and disclaimers

• © 2019 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

• 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 per 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 follows 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 about 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 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 and [names of other referenced IBM products and services used in the presentation] 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.

- .
Today’s Topics

- Upgrade
- Active Threat Analytics
- Risk Spotter
- Policy Analyzer
- Smart Assistant
- CyberArk Integration
- Data Protection for files (SharePoint and NAS)
- VA Enhancements
- External STAP with Kubernetes
- Monitoring DBaaS w/o STAP
- New web site for platform support
- Miscellaneous
- Sneak peek into 11.1
Upgrade

- Yes, we are going to RHEL7! Yes, no migration needed, it’s as simple installing a GPU
- You can upgrade from v10.1.3 through v10.6, any machine type to v11.0
- Upgrading to v11 uses the standard Top Down procedure for a CM/MU environment, utilizing the same workflow as other Guardium Patches, GPUs, or Bundles.
- How long will the upgrade take? It depends…
- Please make sure to read the backup slides and release notes to learn more about v11.0 upgrade
- V11 is a major release with a new OS and many new features, we’ve spent many months testing it but make sure you give it a good run in your test environment
Active Threat Analytics

Active threat analytics is a new approach of looking at malicious events in the system.

It takes all of Guardium’s monitored data and summarizes it to meaningful events you should look at.

- SQL injection
- Malicious stored procedure
- Data leak
- Denial of service
- Account take-over
- Schema tampering
- Data tampering
- Anomaly
### Active Analytics UI

**Active Threat Analytics**
Cases are derived from Guardium data collection and analysis. All high severity cases indicate a potential threat, and should be thoroughly analyzed. 
**H**: High severity, **M**: Medium severity, **L**: Low severity

#### Top Cases

**Databases with open cases**
- **Severity**
  - **H**: 6
  - **M**: 1
  - **L**: 0

#### DB Users with open cases
- **Severity**
  - **H**: 1
  - **M**: 92
  - **L**: 0

#### File Systems with open cases
- **Severity**
  - **H**: 0
  - **M**: 0
  - **L**: 0

#### File Users with open cases
- **Severity**
  - **H**: 0
  - **M**: 0
  - **L**: 0

---

### Case Log

<table>
<thead>
<tr>
<th>Case #</th>
<th>Threat Category</th>
<th>Severity</th>
<th>Observations</th>
<th>Source</th>
<th>Date</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>612</td>
<td>Insider Threat: Possible data leak</td>
<td>Low</td>
<td>High volume of data extraction by privileged DB user</td>
<td>Server: 9.32.164.142</td>
<td>2019-06-06, 09:00:00 AM</td>
<td>No</td>
</tr>
<tr>
<td>603</td>
<td>SQL Injection</td>
<td>Low</td>
<td>Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query.</td>
<td>Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_2V7H</td>
<td>2019-06-06, 07:15:00 AM</td>
<td>No</td>
</tr>
<tr>
<td>588</td>
<td>SQL Injection</td>
<td>Low</td>
<td>Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query.</td>
<td>Server: 9.32.164.142 Database: DB2INST1 DB User: DB2_428G</td>
<td>2019-06-06, 02:15:00 AM</td>
<td>No</td>
</tr>
</tbody>
</table>
Active Analytics UI

Active Threat Analytics
Cases are derived from Guardium data collection and analysis. All high severity cases indicate a potential threat, and should be thoroughly analyzed.
H: High severity, M: Medium severity, L: Low severity

<table>
<thead>
<tr>
<th>Top Cases</th>
<th>Databases with open cases</th>
<th>DB Users with open cases</th>
<th>File Systems with open cases</th>
<th>File Users with open cases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case #</th>
<th>Threat Category</th>
<th>Severity</th>
<th>Observations</th>
<th>Source</th>
<th>Date</th>
<th>Assigned</th>
</tr>
</thead>
</table>
| 612    | Insider Threat: Possible data leak | Low      | High volume of data extraction by privileged DB user | Server: 9.32.164.142
 Database: DB2INST1
 DB User: DB2INST1 | 2019-06-06, 09:00:00 AM | No       |
| 603    | SQL Injection   | Low      | Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query. Go to Actions: Full report to check if there are more observations for this case. | Server: 9.32.164.142
 Database: DB2INST1
 DB User: DB2_2V7H | 2019-06-06, 07:15:00 AM | No       |
| 588    | SQL Injection   | Low      | Evidence of attempts to access unauthorised tables or stored procedures. Tables that contain information about the database structure were accessed. Evidence of attempts to identify the structure of a dynamic SQL query. Go to Actions: Full report to check if there are more observations for this case. | Server: 9.32.164.142
 Database: DB2INST1
 DB User: DB2_425G | 2019-06-06, 02:15:00 AM | No       |
## Threat Analytics – What can I do with it?

<table>
<thead>
<tr>
<th>Case #</th>
<th>Description</th>
<th>Severity</th>
<th>Observations</th>
<th>Source</th>
<th>Date</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>612</td>
<td>Data leak</td>
<td>Low</td>
<td>High volume of data extraction by privileged DB user</td>
<td>Server: 32.164.142</td>
<td>2019-06-06, 09:00:00 AM</td>
<td>No</td>
</tr>
<tr>
<td>603</td>
<td>Access</td>
<td>Low</td>
<td>Evidence of attempts to access unauthorised tables or stored procedures.</td>
<td>Server: 32.164.142</td>
<td>2019-06-06, 07:15:00 AM</td>
<td>No</td>
</tr>
<tr>
<td>588</td>
<td>Access</td>
<td>Low</td>
<td>Evidence of attempts to access unauthorised tables or stored procedures.</td>
<td>Server: 32.164.142</td>
<td>2019-06-06, 02:15:00 AM</td>
<td>No</td>
</tr>
</tbody>
</table>

[Image of a screenshot showing a Threat Analytics dashboard with case details and action options.]
**DB User Behavioral Analytics**

**DB User:** DB_USER_20  
**Database:** ON2P1LRH  
**Server IP:** 9.32.164.216

**Tracked since:** 2019-06-06 07:00  
**Avg. activities per hour:** 20.18  
**Max. activities in any one hour:** 3357  
**Avg. exceptions per hour:** 1.12

**User Risk Indicators**

### Case Management

<table>
<thead>
<tr>
<th>Case #</th>
<th>Assign Case</th>
<th>Severity</th>
<th>Observations</th>
<th>Date</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>Add to Group</td>
<td>Low</td>
<td>Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity</td>
<td>2019-06-05, 14:00:00 PM</td>
<td>No</td>
</tr>
<tr>
<td>501</td>
<td>Close Case</td>
<td>Low</td>
<td>Exceptionally high volume of activities of some type: verb, verb/object, application, connection, etc. Exceptionally high level of activity</td>
<td>2019-06-05, 13:00:00 PM</td>
<td>No</td>
</tr>
<tr>
<td>495</td>
<td>Full Report</td>
<td>Low</td>
<td>Exceptionally high volume of different types of activities, for ex-</td>
<td>2019-06-05,</td>
<td>No</td>
</tr>
</tbody>
</table>

*Total: 3 Selected: 1*
Digging deeper

Risk details

DB user: DB_USER_20
Server: 9.32.164.216

Risk indicators

- Outliers
- Violations
- Vulnerability
- Sensitive objects
- Administrative queries
- DDL queries
- DML queries
- Select queries
- High volume activity
- Off-work activity

Outliers: 0.46
And even deeper
Risk Spotter – When policy alone is not enough

- **Dynamic Risk Assessment**
  - Based on all risks factors (outliers, vulnerability, volume of activities, access to sensitive data, etc.)

- **Sampling strategies**
  - Scanning un-monitored users’ activities
  - Expand our focus area
Risk Spotter - Configure, view and take action

- IBM Guardium

Active Risk Spotter

- Risk Spotter is running
- Policy and related modules

Average risk score: 4.07/15
Risky users: 12
Scanned users: 100
Scanned Server IPs: 2
Date: May 30, 2019

Users by risk level: 5/30/19

Users average risk during: Last month

Risky users

- View the top 50 risky users, see the evidence, and take action.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Auditing</th>
<th>DB User</th>
<th>Server</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>🟢</td>
<td>DB_USER_11</td>
<td>9.42.29.160</td>
<td>Actions</td>
</tr>
<tr>
<td>🟢</td>
<td>🟢</td>
<td>ENCORESPFARM</td>
<td>9.70.164.163</td>
<td>Actions</td>
</tr>
<tr>
<td>🟢</td>
<td>🟢</td>
<td>DB_USER_16</td>
<td>9.42.135.96</td>
<td>Actions</td>
</tr>
<tr>
<td>🟢</td>
<td>🟢</td>
<td>DB_USER_15</td>
<td>9.42.135.95</td>
<td>Actions</td>
</tr>
</tbody>
</table>
Prioritized and actionable

View the top 50 risky users, see the evidence, and take action.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Auditing</th>
<th>DB User</th>
<th>Server</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>●</td>
<td></td>
<td>DB_USER_11</td>
<td>9.42.20.110</td>
<td></td>
</tr>
<tr>
<td>●</td>
<td></td>
<td>ENCORESPFARM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>●</td>
<td></td>
<td>DB_USER_16</td>
<td>9.42.135</td>
<td></td>
</tr>
<tr>
<td>●</td>
<td></td>
<td>DB_USER_15</td>
<td>9.42.135.95</td>
<td></td>
</tr>
</tbody>
</table>
Investigate risks

<table>
<thead>
<tr>
<th>Source Program</th>
<th>DB User</th>
<th>OS User</th>
<th>Client Host name</th>
<th>Client IP</th>
<th>Object Verb</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2JCC_APPLICATION</td>
<td>DB2_9GRG</td>
<td>ROOT</td>
<td>9.32.164.228</td>
<td>9.32.164.228</td>
<td>...</td>
</tr>
</tbody>
</table>
Policy Analyzer – Understanding how you policy works

Policy analyzer provides rule counts for installed DAM policy rules.

Collection profiles, FAM and session-level policies are not supported.

What’s in it:

• 2 modes: continuous and ad hoc

• Continuous mode runs in the background and provides historical graphs for comparison

• Ad hoc mode run for a specified time period. It can be scheduled.

Benefits:

• Can identify which rules fire the most

• Can identify which rules are NOT firing at all

• Can view impact of things like rule ordering on fire counts.
View continuous analysis results

Time frame: Last 10 Minutes

% hit among transactions for each rule

Top 5 rules (fire count)

Details for all policy rules

<table>
<thead>
<tr>
<th>Number</th>
<th>Rule</th>
<th>Action</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed Login - GDPR Personal Data - Log Violation by Admin Users</td>
<td>LOG ONLY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>Failed Login - GDPR Personal Data - Alert if repeated</td>
<td>ALERT PER MATCH</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>SQL Error - GDPR Personal Data - Alert on Risk Indicative errors</td>
<td>ALERT PER MATCH</td>
<td>104</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details</td>
<td>ALERT PER MATCH,LOG FULL DETAILS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>
### View continuous analysis results

#### Time frame: Last 10 Minutes

#### % hit among transactions for each rule

<table>
<thead>
<tr>
<th>Rule number</th>
<th>% hit among transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Top 5 rules (fire count)

<table>
<thead>
<tr>
<th>Rule number</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>104</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>

### Details for all policy rules

<table>
<thead>
<tr>
<th>Number</th>
<th>Rule</th>
<th>Action</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed Login - GDPR Personal Data - Log Violation by Admin Users</td>
<td>LOG ONLY</td>
<td>0</td>
<td></td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>Failed Login - GDPR Personal Data - Alert if repeated</td>
<td>ALERT PER MATCH</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>SQL Error - GDPR Personal Data - Alert on Risk Indicative errors</td>
<td>ALERT PER MATCH</td>
<td>104</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details</td>
<td>ALERT PER MATCH, LOG FULL DETAILS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>
### View continuous analysis results

**Time frame:** Last 10 Minutes

#### % hit among transactions for each rule

<table>
<thead>
<tr>
<th>Rule number</th>
<th>% hit among transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td>100</td>
</tr>
</tbody>
</table>

#### Top 5 rules (fire count)

<table>
<thead>
<tr>
<th>Rule number</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>

#### Details for all policy rules

<table>
<thead>
<tr>
<th>Number</th>
<th>Rule</th>
<th>Action</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed Login - GDPR Personal Data - Log Violation by Admin Users</td>
<td>LOG ONLY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>Failed Login - GDPR Personal Data - Alert if repeated</td>
<td>ALERT PER MATCH</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>SQL Error - GDPR Personal Data - Alert on Risk Indicative errors</td>
<td>ALERT PER MATCH</td>
<td>104</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details</td>
<td>ALERT PER MATCH, LOG FULL DETAILS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>
View continuous analysis results

Time frame: Last 10 Minutes

% hit among transactions for each rule

Top 5 rules (fire count)

Details for all policy rules

<table>
<thead>
<tr>
<th>Number</th>
<th>Rule</th>
<th>Action</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed Login - GDPR Personal Data - Log Violation by Admin Users</td>
<td>LOG ONLY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>Failed Login - GDPR Personal Data - Alert if repeated</td>
<td>ALERT PER MATCH</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>SQL Error - GDPR Personal Data - Alert on Risk Indicative errors</td>
<td>ALERT PER MATCH</td>
<td>104</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details</td>
<td>ALERT PER MATCH, LOG FULL DETAILS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>
View ad hoc analysis results

Start time: 2019-06-10 14:15:00

transactions for each rule

Top 5 rules (fire count)

Details for all policy rules

<table>
<thead>
<tr>
<th>Number</th>
<th>Rule</th>
<th>Action</th>
<th>Fire count</th>
<th>% hit among transactions</th>
<th>% hit among rules</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failed Login - GDPR Personal Data - Log Violation by Admin Users</td>
<td>LOG ONLY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>2</td>
<td>Failed Login - GDPR Personal Data - Alert if repeated</td>
<td>ALERT PER MATCH</td>
<td>39</td>
<td>3</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>3</td>
<td>SQL Error - GDPR Personal Data - Alert on Risk Indicative errors</td>
<td>ALERT PER MATCH</td>
<td>233</td>
<td>7</td>
<td>1</td>
<td>Smart Assistant GDPR</td>
</tr>
<tr>
<td>4</td>
<td>REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details</td>
<td>ALERT PER MATCH, LOG FULL DETAILS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Smart Assistant GDPR</td>
</tr>
</tbody>
</table>
Viewing legend and changing rules shown on graph
Changing rules

- DDL, DML and Select Commands, GDPR Personal Data Sensitive Objects - Log Violation
- Failed Login - GDPR Personal Data - Log Violation by Admin Users (Smart Assistant GDPR)
- Failed Login - GDPR Personal Data - Alert if repeated (Smart Assistant GDPR)
- GDPR Personal Data Admin User - Alert per match (violation) on DML and Select
- GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects
- GDPR Personal Data Unauthorized User, Alert per match (violation) (Smart Assistant GDPR)
Smart Assistance

Enables new users (or existing users needing to meet a new compliance standard) an end-end flow for quickly setting up compliance policies, groups and reports.

Follows best practices flow

What’s New

• No longer need to have S-TAPs installed before using the Smart Assistant/Quick Start
• More options for sensitive data identification
• More contextual information: prerequisites, individual step help, how to videos.

Benefits

• Better fit to diversity of customer environments
• Easier to understand full scope of functionality
• Addresses key customer pain points
Get Started on Data Protection with Guardium

- **Inventory your databases**
  - Learn more
  - See it in action

- **Discover sensitive data**
  - Learn more
  - See it in action

- **Set up compliance monitoring**
  - Learn more
  - See it in action

- **Active threat analytics**
  - See it in action

- **Risk spotter**
  - See it in action

- **Investigation dashboard**
  - See it in action

- **Learn more**
Get Started on Data Protection with Guardium

Inventory your databases
Learn more
See it in action

Discover sensitive data
Learn more
See it in action

Set up compliance monitoring
Learn more
See it in action

Active threat analytics
See it in action
Risk spotter
See it in action
Investigation dashboard
See it in action
Learn more
Get Started on Data Protection with Guardium

- **Inventory your databases**
  - Learn more
  - See it in action

- **Discover sensitive data**
  - Learn more
  - See it in action

- **Set up compliance monitoring**
  - Learn more
  - See it in action

- **Active threat analytics**
  - See it in action
  - Risk spotter
  - See it in action
  - Investigation dashboard
  - See it in action
  - Learn more
Get Started on Data Protection with Guardium

- **Inventory your databases**
  - Learn more
  - See it in action

- **Discover sensitive data**
  - Learn more
  - See it in action

- **Set up compliance monitoring**
  - Learn more
  - See it in action

- **Active threat analytics**
  - See it in action

- **Risk spotter**
  - See it in action

- **Investigation dashboard**
  - See it in action

- **Learn more**
Guardium v11 welcome videos

Discover sensitive data
Set up compliance monitoring

Step 1  Before you begin

The smart assistant for compliance monitoring automates the following activities through a simple workflow:

- Identify databases to monitor
- Install compliance monitoring policies
- Schedule policy updates
- Populate groups with objects to monitor
- Run activity-monitoring reports
- Scan for database tables containing sensitive data

Configuring scans for database tables containing sensitive data requires database credentials with the correct permissions. Gather the credentials and verify permissions before you begin or optionally configure the scans later. Get scripts illustrating the required permissions.

After completing the smart assistant workflow, compliance monitoring policies are distributed to all collectors attached to the central manager and you are ready to begin protecting data.

Important: monitoring agents (S-TAPs) can be installed on your database servers after completing the smart assistant workflow, but database traffic is not examined until after the agents are installed. Open Deploy Monitoring Agents to get started.

Next
Set up compliance monitoring

Step 1

Before you begin

Step 2

Select compliance type

Which compliance type do you want to configure?

- Basel Committee on Banking Supervision (BASEL II)
- General Data Protection Regulation (GDPR)
- General Data Protection Regulation for Db2 for z/OS (GDPR for Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI)
- Personally Identifiable Information (PII)
- Sarbanes-Oxley Compliance (SOX)

Run setup  Cancel
Set up compliance monitoring

Step 4

Search for sensitive data

Compliance monitoring policies contain rules for monitoring access to database tables. Effective compliance monitoring depends on identifying tables that contain sensitive data like credit card numbers or personally-identifiable information.

How do you want to identify database tables containing sensitive data?

- [ ] Scan for tables
- [ ] Manually define table names
- [x] Skip for now

When establishing a Guardium deployment, you may initially want to focus on monitoring and traffic volume. Selecting Skip for now allows you to identify tables containing sensitive data at a later time.

**Important:** your compliance monitoring strategy is not complete without identifying and monitoring the sensitive data in your databases.
Set up compliance monitoring

Step 4: Search for sensitive data

Compliance monitoring policies contain rules for monitoring access to database tables. Effective compliance monitoring depends on identifying tables that contain sensitive data like credit card numbers or personally-identifiable information.

How do you want to identify database tables containing sensitive data?
- [ ] Scan for tables
- [ ] Manually define table names
- [x] Skip for now

Select databases to scan for sensitive data. Tables containing sensitive data are added to a sensitive-objects group for monitoring, and the scan is scheduled to run once weekly.

<table>
<thead>
<tr>
<th>Test datasource credentials</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance name</td>
<td>Database name</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>DS2102006</td>
<td>DN0KALP</td>
</tr>
<tr>
<td>in2kalp</td>
<td>INFORMIX</td>
</tr>
</tbody>
</table>

Total: 2 Selected: 2
Set up compliance monitoring

Step 5
Summary

Clicking Run Setup takes the following actions:

- Install compliance monitoring policy
- Schedule policy reinstallation
- Populate server IP group
- Install classification policy
- Schedule classification
- Create audit process
- Send results to contacts

Smart Assistant GDPR
Run once every day
GDPR Personal Data Authorized Server IPs
Smart Assistant GDPR scenario
Run once on specific days
Audit process for Smart Assistant GDPR scenario
admin

You must complete the following actions:

- Populate groups
- Install monitoring agents (S-TAPs) for databases
- Review classification results and remove false positives

Add to my to-do list
Set up compliance monitoring

Step 5

Summary

Clicking Run Setup takes the following actions:

- Install compliance monitoring policy
- Schedule policy reinstallation
- Populate server IP group
- Install classification policy
- Schedule classification
- Create audit process
- Send results to contacts

Smart Assistant GDPR
Run once every day
GDPR Personal Data Authorized Server IPs
Smart Assistant GDPR scenario
Run once on specific days
Audit process for Smart Assistant GDPR scenario

View details
Edit
View details
Edit
Add

You must complete the following actions:

- Populate groups
- Install monitoring agents (S-TAPs) for databases
- Review classification results and remove false positives

5
2

View details
Install monitoring agents
Learn more

Add to my to-do list
Smart Assistant GDPR policy rules
The following rules are installed with the policy.

1. SQL Error - GDPR Personal Data - Alert on Risk Indicative errors
2. DDL, DML and Select Commands, GDPR Personal Data Sensitive Objects - Log Full Details
3. GDPR Personal Data Unauthorized User - Alert per match (violation)
4. Authorized Clients access to Personal Data Sensitive Objects - Alert Per Match
5. GDPR Personal Data Authorized User, GDPR Personal Data Sensitive Objects - Log Full Details
6. REVOKE Commands, GDPR Personal Data Sensitive Objects - Log full details and alert
7. Failed Login - GDPR Personal Data - Log Violation by Admin Users
8. Failed Login - GDPR Personal Data - Alert if repeated

Close
Compliance Monitoring

Known databases: 2
Configured databases: 2
GDPR: 2
Unconfigured databases: 0

General Data Protection Regulation (GDPR)
- Scanning for sensitive data
  - Last scan: None
  - Matches found: None
- Databases without monitoring agents installed: 2
- Monitoring enabled

Set up compliance monitoring

Help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.
Get Started on Data Protection with Guardium

- Deploy Monitoring Agents
- Compliance Health Monitor Dashboard

- Tools and Views
- Central Management
- Custom Classes
- Reports

- Discover sensitive data
  - Learn more
  - See it in action

- Set up compliance monitoring
  - Learn more
  - See it in action

- Active threat analytics
  - See it in action
  - Risk spotter
    - See it in action
  - Investigation dashboard
    - See it in action
    - Learn more
CyberArk Integration

- Remove credentials from application or scripts and put them into a secured centralized place (called the Vault)
- Periodical password changes are much easier and can be handled by your company’s policy automatically, including saving the Guardium admin and DBA’s time
- Allow access to only trusted applications to enhance application security
Guardium integration with CyberArk

Setup → Tools and Views—CyberArk configurations
Guardium integration with CyberArk

Add a datasource as an account in CyberArk

CyberArk password vault web access (PVWA)

HTTPS://x.x.x.x/PasswordVault/
Create a Data Source in the Guardium GUI
File Classification and Monitoring – new capabilities

- **Frequency of the scan**
- **Scan directories only and ignore the documents themselves. This will not trigger criteria and will not be classified**
- **Scans everything including files and directory tree and will match to criteria**
- **Only return records that trigger criteria**

Guardium Appliance hostname or IP address

Hostname of IP address of the device to be scanned. Localhost in case of SharePoint

Name of Share

How deep into directory structure should the scan go

Scan Status
File Classification and Monitoring – new capabilities
File Classification and Monitoring – new capabilities

The New Way

Scan Every: 1 Days At 9:01:59 PM Run Now

The Old Way

Scan Every: 1 Hours

IBM Security Guardium FDEC for NAS Configuration

Scan Options:
- Containers Only
- All Objects
- Matches Only

Scan: Scan 1
- Guardian Appliance: 5.76.147.235
- Scan Host: femc-001
- Scan Path: C:
- Scan Every: 1 Days At 9:01:59 PM

Scan Status: Idle
- Started Last Scan: 2019-06-14 21:00:00
- Finished Last Scan: 2019-06-14 21:00:00
- Next Scan: 2019-06-15 12:00:00

Purge Scan DB

Purge Scan DB Every: 1 Days At 12:00:00 PM
- Last Purge Time: ------
- Next Purge Time: 2019-06-15 12:00:00

Purge Scan DB Now

OK Cancel
File Activity Monitoring: Policy Configuration in Guardium

New Policy

* Type: Network Attached Storage

* Policy Name: NASpolicy

Use the 'New' tool bar icon to create a new rule
File Activity Monitoring: Policy Configuration in Guardium

Create New Rule

- Rule name: rule1
- Data source: victor2k8:emo-asis01:FAM-NAS

Define rule criteria

- Include file path: abc
- Exclude file path: xyz
- Exclude account: me@ibm.com
- Exclude extension: exe,dll

- Suppress subsequent Read operation in the same folder
- Suppress Microsoft Office operations on temporary files

Define rule action

- Read | Alert and Audit | SYSLOG
File Activity Monitoring: Policy Configuration in Guardium

Create New Rule

- Rule name: rule1
- Choose datasources: datasource victor2k8:emc-cifs01:FILEMAS
- Define rule criteria: me@ibm.com, abc
- Define rule action: Specify the action to take

Specify action for specific operation or group

- Operation
  - Select operation
  - Operation options:
    - Add directory
    - Add file
    - Change directory permission
    - Change file permission
    - Delete directory
    - Delete file
    - Read
    - Rename directory
    - Rename file

Add another action | Remove

Save | Cancel
New to VA - Datasource Group

- You can now create datasource groups based on criteria or selected datasources.
- You can use datasource groups to change usernames and passwords in bulk.
- You can run security assessments using groups of datasources.
- You can create exceptions using datasource groups.
- All of this functionality can be done using grdapi.
Datasource Group Credential update

- When changing the password for a group of datasources, you can update both username (optional) and password.

- This is useful when you have a group of datasources using the same credentials like Windows Active Directory for SQL Server logins.
Test Exceptions Enhancement for VA

- Use test exceptions to overwrite findings for a specific test within a duration.
- Test exceptions can be created for a single assessment or all assessments.
- Test exceptions can be created for a single, group or all data sources.
Test Detail Exceptions Enhancement for VA

- Use test detail exceptions to whitelist a finding for a specific grantee on a given test.
- Test detail exceptions can be created for a single assessment or all assessments.
- Test detail exceptions can be created for a single, group or all data sources.
- Test detail exceptions can be created using regular expressions or exact text match.
Update datasource

- Application type: Security Assessment
- Name: DPS: DSE 6.0.2 FAIL on dba-datastax-sa01 SSL
- Database type: DATASTAX CASSANDRA (DataDirect)
- Description:
  - Share datasource
  - Use SSL
  - Import server ssl certificate
  - Use LDAP

Authentication
- Credential type
  - Assign credentials
  - External password
  - None
- User name: sqlguard
- Password: 
- Location
- Host name/IP: 9.98.176.188
- Port number: 9042
- Database: system
- Connection property: Ex: prop1=value,prop2=value
- Custom URL

Show advanced options
- Connection successful

Test connection  Save  Close
Making the External STAP more scalable

- Support for Kubernetes
  - AWS
  - Azure
Monitoring DBaaS in the cloud – No STAP!!
Connecting to the streams (AWS Aurora PostgreSQL)

Cloud DB Service Accounts

Gils-aws

Cloud DB Service Account
Name: Gils-aws
Provider: Amazon

Hide Discover Streams

<table>
<thead>
<tr>
<th>Amazon Region</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-gov-west-1</td>
<td>kinesis.us-gov-west-1.amazonaws.com</td>
</tr>
<tr>
<td>us-east-1</td>
<td>kinesis.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>us-east-2</td>
<td>kinesis.us-east-2.amazonaws.com</td>
</tr>
<tr>
<td>us-west-1</td>
<td>kinesis.us-west-1.amazonaws.com</td>
</tr>
<tr>
<td>us-west-2</td>
<td>kinesis.us-west-2.amazonaws.com</td>
</tr>
</tbody>
</table>

Discover
A new way to check for supported databases and platforms

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>Red Hat 7.5</td>
<td>Oracle</td>
<td>Oracle 18c</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>A-TAP (ASO, SSL)</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.0</td>
<td>Red Hat 7.4</td>
<td>Oracle</td>
<td>Oracle 18c</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>A-TAP (ASO, SSL)</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.0</td>
<td>Red Hat 7.0</td>
<td>Oracle</td>
<td>Oracle 18c</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>A-TAP (ASO, SSL)</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.0</td>
<td>Red Hat 5</td>
<td>Oracle</td>
<td>Oracle 18c</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>A-TAP (ASO, SSL)</td>
<td>K-TAP</td>
<td>K-TAP</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We’ve added more information to deployment health and introduced new states

For z/OS mainframe, V11 added the ability to map several new common event format (CEF) values to the alert message for DB2 and IMS databases

If you have GBDI, you can now stream data in real time, faster than periodic datamarts

A bunch of great S-TAP changes to fix pain points and enable encrypted SSL traffic monitoring

Check out our new QRadar integration app in the Guardium App Exchange
What’s coming in 11.1?

• Continue to help you show the value of Guardium and making it easier to deploy and maintain

• IPV6 Support for your growing data center

• ServiceNow Integration to help with handling cases

• Mapping monitored databases to business functions to help you show what’s protected

• Adding support for more DBaaS direct stream monitoring

• Keep delivering RFEs and fix pain points
Useful Links


• V11 Support page: https://www-01.ibm.com/support/docview.wss?uid=ibm10870596

• Go directly to supported platforms page: https://www.securitylearningacademy.com/mod/data/view.php?d=12&mode=asearch