



Governança de Dados garantindo a segurança das informações

Monitoramento de Atividade em Banco de Dados

JULIO FIGUEIREDO

juliofig@br.ibm.com

Especialista em Governança de Dados

Agenda



- Introdução Segurança em Banco de Dados
- Solução DAM:
 - IBM InfoSphere Guardium
- Perguntas e Respostas

Introdução



IBM Smarter Planet

Um Planeta mais inteligente
com informações mais inteligentes e seguras



 Instrumentado

 Interconectado

 Inteligente

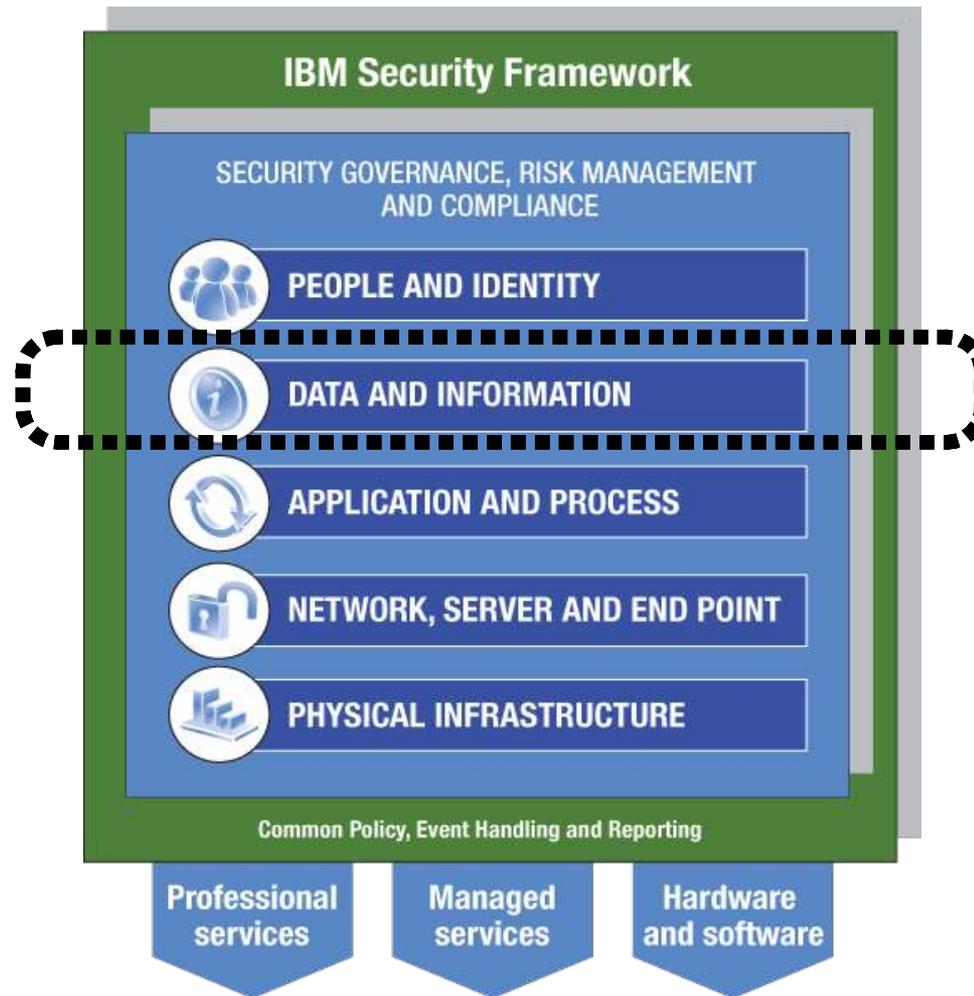
*Criando a necessidade de
Segurança...*

- Envolve o exercício de decisões certas para otimização, segurança e entrega dos dados como informações.
- Envolve orquestrar pessoas, processos, tecnologia e políticas para entregar essas informações.



A estratégia de Segurança da IBM

Framework de Segurança



Explosão de Informações



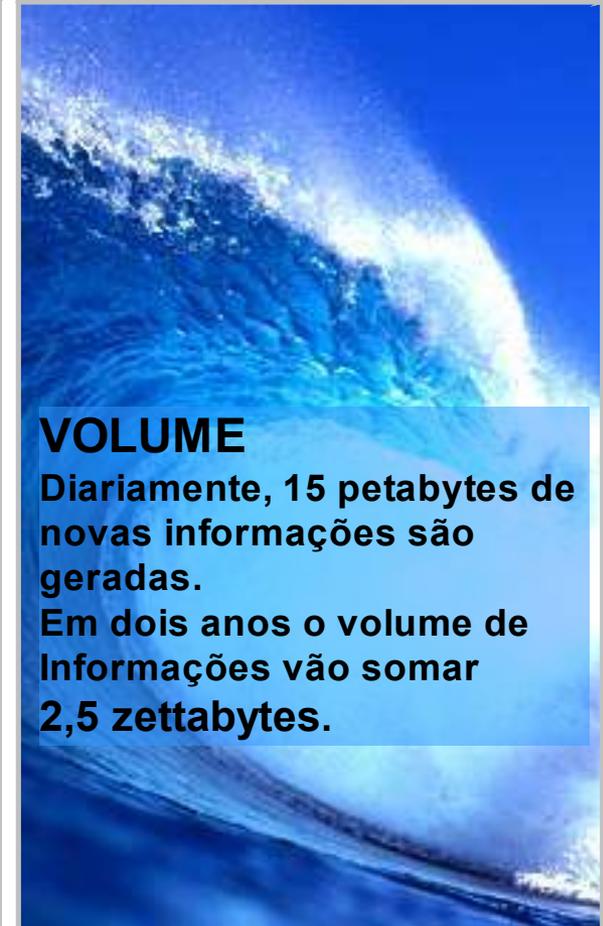
VARIEDADE

Dados estruturados e não estruturados (e-mails, documentos, imagens, etc), informações sensíveis, confidenciais, financeiras...



VELOCIDADE

42% dos gerentes afirmam que utilizam informações erradas pelo menos uma vez por semana.



VOLUME

Diariamente, 15 petabytes de novas informações são geradas. Em dois anos o volume de informações vão somar 2,5 zettabytes.



Explosão de Informações

Variedade + Velocidade + Volume
VALOR



Por que proteger agora?



- ▶ E-commerce, e-business e sistemas integrados.
- ▶ Novas e simplificadas formas de utilizar Bancos de Dados.
- ▶ Aumento das comunidades e ações dos hackers.
- ▶ Regulamentações (normas, leis, etc).



Vulnerabilidades dos Bancos de Dados

- Não separação de obrigações – DBAs e hacker podem facilmente manipular logs, eliminando rastros.
- Impacto em performance quando utilizados Logs nativos dos DBMS.
- Escopo e granularidade limitados dos Logs nativos.
- Não real-time monitoramento.
- Ausência de controle preventivo.
- Logs nativos significam novos DBs que necessitarão de segurança e gerenciamento (\$\$\$).
- Impossibilidade de identificar “end-user” das fraude devido a conexão genérica “connection-pooled” (SAP, PeopleSoft, Siebel, etc.)



Desafios para proteção de Dados



4ª edição
IBM Security Forum



Onde estão meus dados sensíveis?
Quem está acessando os dados?



Como garantir o controle de acesso?
Como policiar as alterações nos DBs?



Como checar vulnerabilidades?



Como reduzir custos com compliance?

IBM InfoSphere Guardium

Solução líder em monitoramento de Acesso à Banco de Dados (DAM-Database Activity Monitoring).

Garante proteção do alto valor das Informações em Base de Dados.

Abrangente sistema de automatização de compliance e procedimentos de auditoria e controles de segurança.

Arquitetura escalável e com suporte à ambientes heterogêneos.

Detém patente líder em software agente para monitoramento de Banco de Dados.

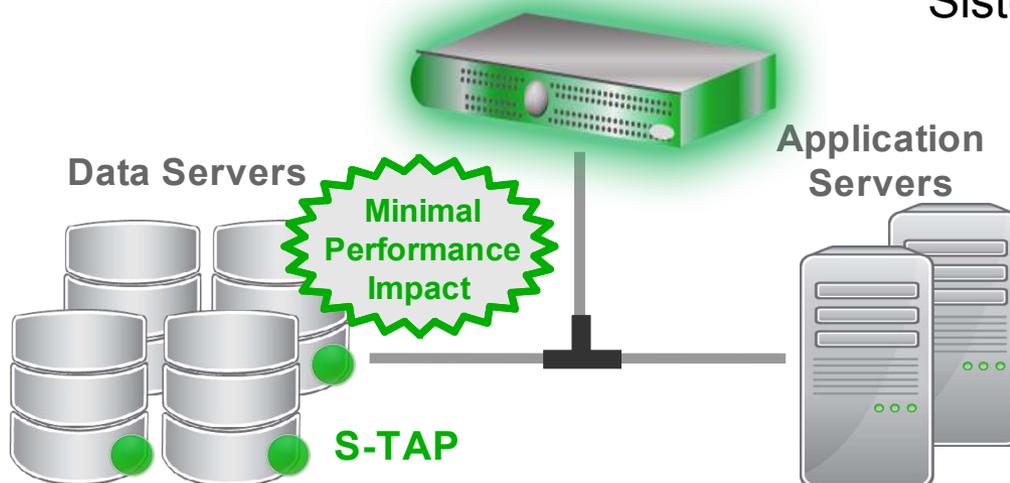


Guardium - Solução DAM

Database Activity Monitoring

Guardium Collector

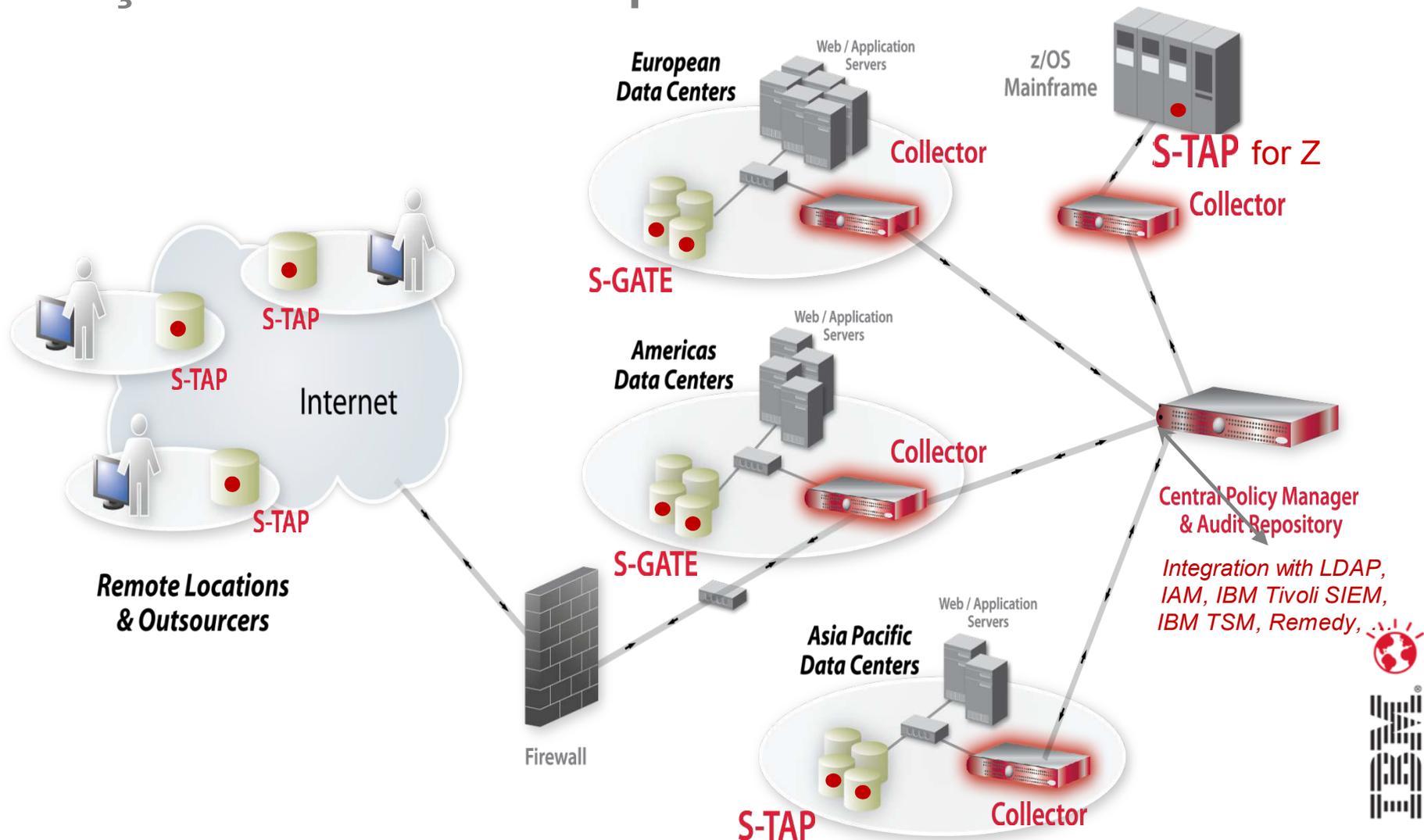
Suporte para os mais populares DBs e Sistemas de aplicações



Collector Ação não-invasiva para controle de políticas e geração de logs.
S-TAP Agente light para monitoramento das atividades em DBs.

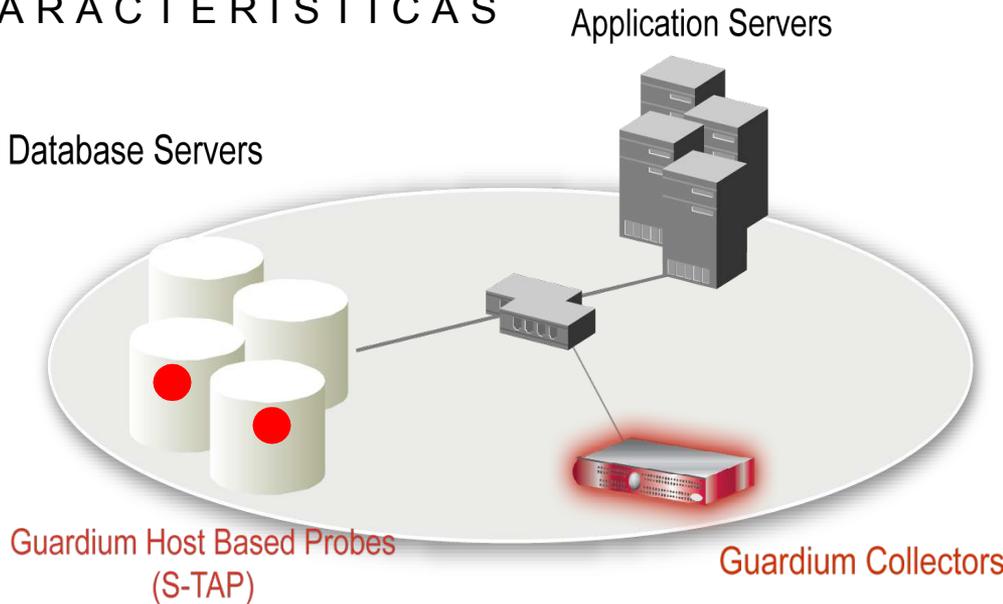
Guardium

Solução Escalável - Multi-plataformas



Monitoramento Real-time

CARACTERÍSTICAS



- Arquitetura não-invasiva
 - Fora do DB
 - Impacto mínimo em performance (2% - 3%)
 - Nenhuma alteração em aplicações
- Diversos tipos de Bancos de Dados
- 100% de visibilidade, incluindo DBAs
- Não é um simples DBMS-residente que possa ser atacado
- Permite auditoria granular (Quem, O_que, Quando, Onde, Como)
- Relatórios automáticos: SOX, PCI, Basiléia II, etc.



Necessidades de Compliance

Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

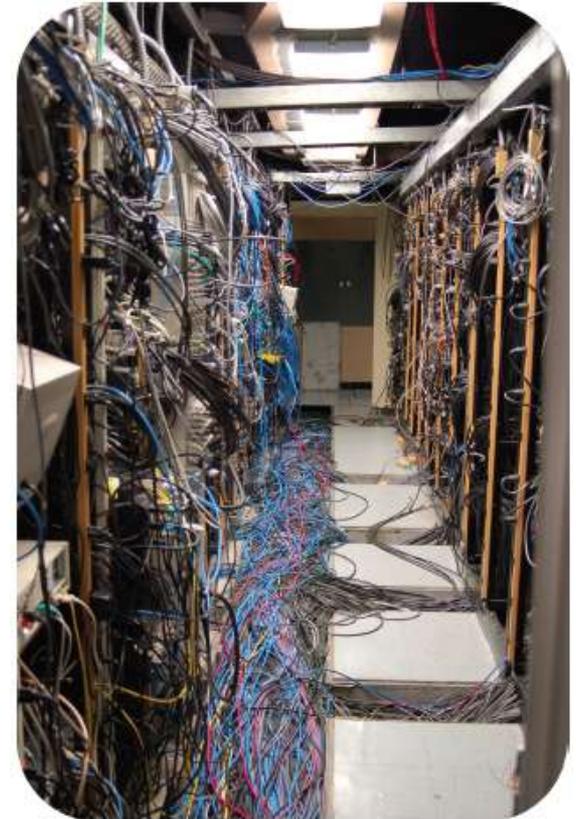
DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language



Guardium - Database Auto-Discovery

Componente que executa o mapeamento de Banco de Dados na Rede.

- Vasculha rede procurando por Portas e Banco de Dados.
- Relatórios com os Banco de Dados encontrados.



My New Reports Standard Reports Discover Assess/Harden Comply Protect Quick Start Sarbanes-Oxley Accelerator

Classification

DB Discovery

Auto-discovery Configuration
 Auto-discovery Query Builder
 Data Source Version History
 Data Sources
Databases Discovered
 Discovered Instance Tracking
 Discovered Instances

Databases Discovered

Start Date: 2000-01-01 00:00:00 End Date: 2010-10-29 10:11:28
 Aliases: ON

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2010-08-27 03:49:22.0	10.10.9.248	g8.ibm.com	MySQL	3306	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1433	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1533	tcp	1
2010-08-27 19:44:33.0	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2010-08-27 03:49:13.0	10.10.9.57	10.10.9.57	Oracle	1521	tcp	1
2010-08-27 03:49:22.0	10.10.9.57	10.10.9.57	DB2	50001	tcp	1
2010-08-27 03:49:18.0	10.10.9.57	10.10.9.57	MySQL	3306	tcp	1
2010-08-27 03:49:19.0	10.10.9.57	10.10.9.57	Sybase	4200	tcp	1
2010-09-10 12:07:48.0	10.10.9.60	10.10.9.60	Informix	9088	tcp	1
2010-09-10 12:07:51.0	10.10.9.60	10.10.9.60	DB2	9089	tcp	1

Records 1 to 10 of 10

Guardium – Classifier

Informações sensíveis podem estar presentes em diferentes Bancos de Dados.

- Procurar por informações sensíveis:
 - Conteudos
 - Nome de colunas
- Informações sensíveis:
 - Número cartão de crédito
 - Transações
 - Informações pessoais
 - Informações financeiras



Classification Policy Builder

Classification Rule #1 For Classification Policy "Find Sensitive Objects"

Rule Name: Find Credit Card Numbe

Category: PCI

Classification: Credit Card

Description:

Continue on Match:

Rule Type: Search For Data

Search For Data

--select an Item--

Catalog Search

Search By Permissions

Search For Data

Search For Unstructured Data

Classification Policy Builder

Classification Rule #1 For Classification Policy "Find Sensitive Objects"

Rule Name: Find Credit Card Numbe

Category: PCI

Classification: Credit Card

Description:

Continue on Match:

Rule Type: Search For Data

Table Type: Synonym System Table Table View

Table Name Like:

Data Type: Date Number Text

Column Name Like: %CARD%

Minimum Length:

Maximum Length:

Search Like:

Search Expression: 0-9[16]

Maximum Rows:

Classification Rule Actions

New Action

Back Save



Guardium – Análise de Vulnerabilidade

- Testes pré-definidos e customizados para identificação de vulnerabilidades
- Medições em real-time e históricas
- Análises baseadas nas melhores práticas de mercado
 - *US DOD Security Technical Implementation Guides – STIG*
 - *Center for Internet Security (CIS) Benchmarks*
- Análises de vulnerabilidade de compliance (SOX, PCI-DSS)
- Atualização **trimestral** com novas práticas
- Sem impacto de performance ou estabilidade



Análise de Vulnerabilidade

Guardium

Results for Security Assessment: **Guardium Oracle** -- Select another result --

Assessment executed **2009-09-29 21:38:18.0**

From: 2009-09-01 00:00:00.0 Client IP or IP subnet: Any
To: 2009-09-25 00:00:00.0 Server IP or IP subnet: Any Download PDF

Tests passing: **45%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus on first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)
[Jump to Datasource list](#)

Assessment Result History

Result Summary

Showing 104 of 104 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	8p 16f	1p 4f	-- 1f	-- --	-- --
Authentication	1p 5f	-- 1f	-- 2f	-- --	-- --
Configuration	4p --	6p 4f 4e	1p 3f 4e	-- 6f 1e	-- --
Version	-- --	-- 2f	-- --	-- --	-- --
Other	2p --	6p 4f	-- 4p 2f 1e	-- --	8p -- 3e

Current filtering applied:

Severities: - Show All -
Scores: - Show All -
Types: - Show All -

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results

Showing 104 of 104 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Auth.	Default Accounts Password Changed	ORACLE: Oracle Local	Fail	Critical	5 active pre-defined users have default passwords. <i>Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that you remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.</i>
Priv.	No Access To 'Users' Catalog Tables	ORACLE: Oracle Local	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <i>Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than</i>

[Compare with Previous Results](#)

Resumo dos Resultados

Detalhes Resultados dos testes

Histórico dos Resultados

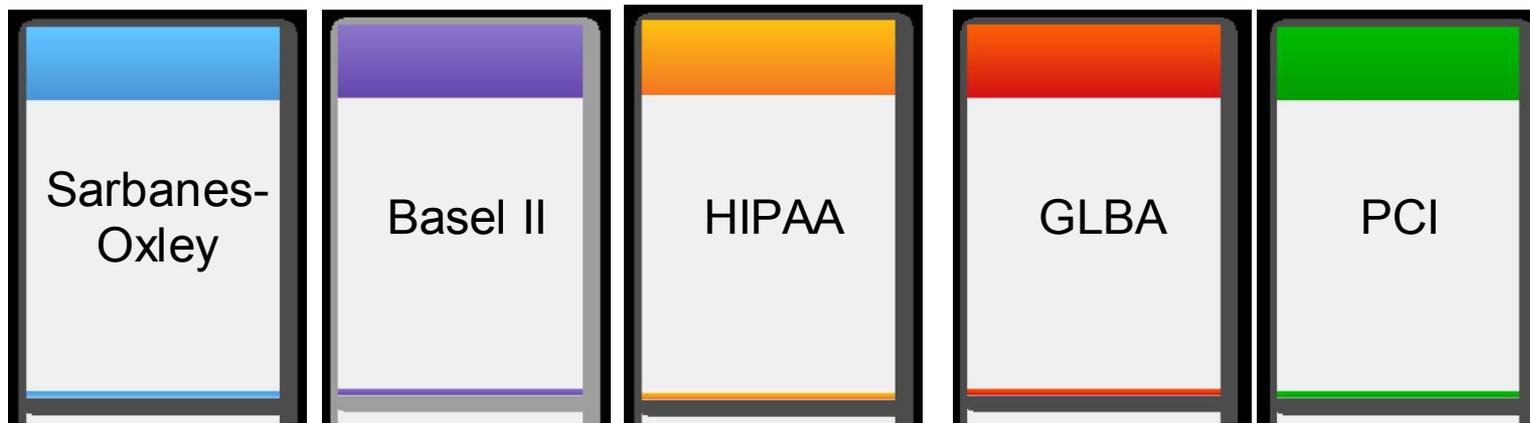
Filtros e ordem dos controles

Descrição detalhadas das correções

18

Guardium – Aceleradores de Compliance

- Módulo opcional para endereçar requerimentos mandatórios de segurança



- Relatórios customizáveis
 - Garante a segurança e requerimentos de auditoria
- Aumento da eficiência operacional através da automação de compliance
- Simplifica a validação de vasta quantidade de requerimentos

Gramm-Leach-Bliley Act (GLBA), a US law (Law 106-102) passed on November 12, 1999, contains privacy provisions relating to consumers' financial information. It imposes restrictions on the disclosure of consumers' personal financial information to non-affiliated third parties.



Guardium – Redaction

Para mascarar informações sensíveis

- Conhecido como “*regra de limpeza*”
- Manipula o dado retornado por uma consulta ao Servidor de dados.
- Permite mascarar uma porção das respostas do Servidor de dados.
- O padrão é parametrizado em expressões regulares.

```
SQLCMD
C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID      LastName      FirstName      SSN_Number
-----
0 Anthony     joe            *****-6780
1 Thomas     joe            *****-6781
2 Smith      Joe            *****-6782
3 Jones      Joe            *****-6783
4 Craven     Joe            *****-6784

(5 rows affected)
1> quit
```



Valores mascarados



Guardium – Relatório de Privilégios



- Reporta usuários privilegiados e detalhes dos grupos de acesso.
- Usuários privilegiados são extremamente difíceis de serem gerenciados.
- Oferecem recomendações de políticas de auditoria e melhores práticas.
- Facilmente integrável com soluções de Gerenciamento de Identidade.



Guardium – Relatório de Privilégios



Import



GRANTEE	GRANTEE_TYPE	DB	OBJECT	OBJECT_TYPE	ACTION	CONTROL	ALTER	TRIGGER	EXECUTE	INSERT	INHERIT	SELECT
GUARD	U	N	N	N	Y	N	N	N	N	N	N	N
DBSECACCU	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
REFUSERU	N	Y	N	N	Y	N	N	N	N	N	N	N
PUBLIC	C	Y	Y	Y	N	N	N	Y	N	N	N	N

- Informações dos privilégio para TODOS os formatos de DBs.
- Relatórios integrados



Principais interessados



SECURITY OPERATIONS

- ✓ Políticas Real-time
- ✓ Trilhas de Auditoria Seguras
- ✓ Análise Forense



COMPLIANCE AUDIT

- ✓ Separação de Funções
- ✓ Relatórios com melhores práticas
- ✓ Controle automatizado



APPLICATION & DATABASE

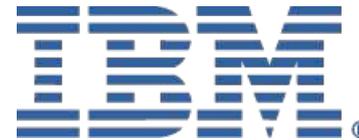
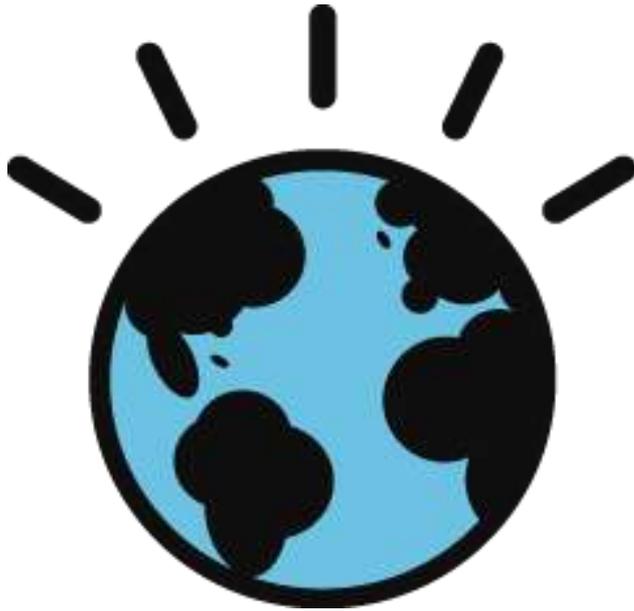
- ✓ Mínimo Impacto
- ✓ Gerenciamento de mudanças
- ✓ Melhora em performance

Guardium:

100% de Visibilidade & Visão unificada



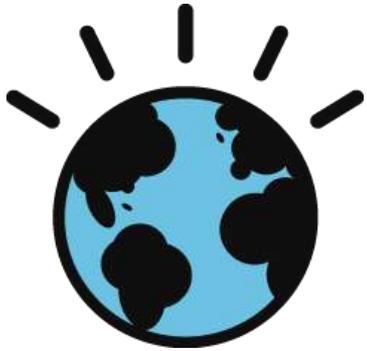
Essas são algumas das soluções de Segurança que têm auxiliado as principais empresas do planeta...



PERGUNTAS & RESPOSTAS



Contato:
JULIO FIGUEIREDO
juliofig@br.ibm.com



Obrigado pela Presença!

