4ª edição
IBM Security Forum

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

28 / 04 / 2011

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

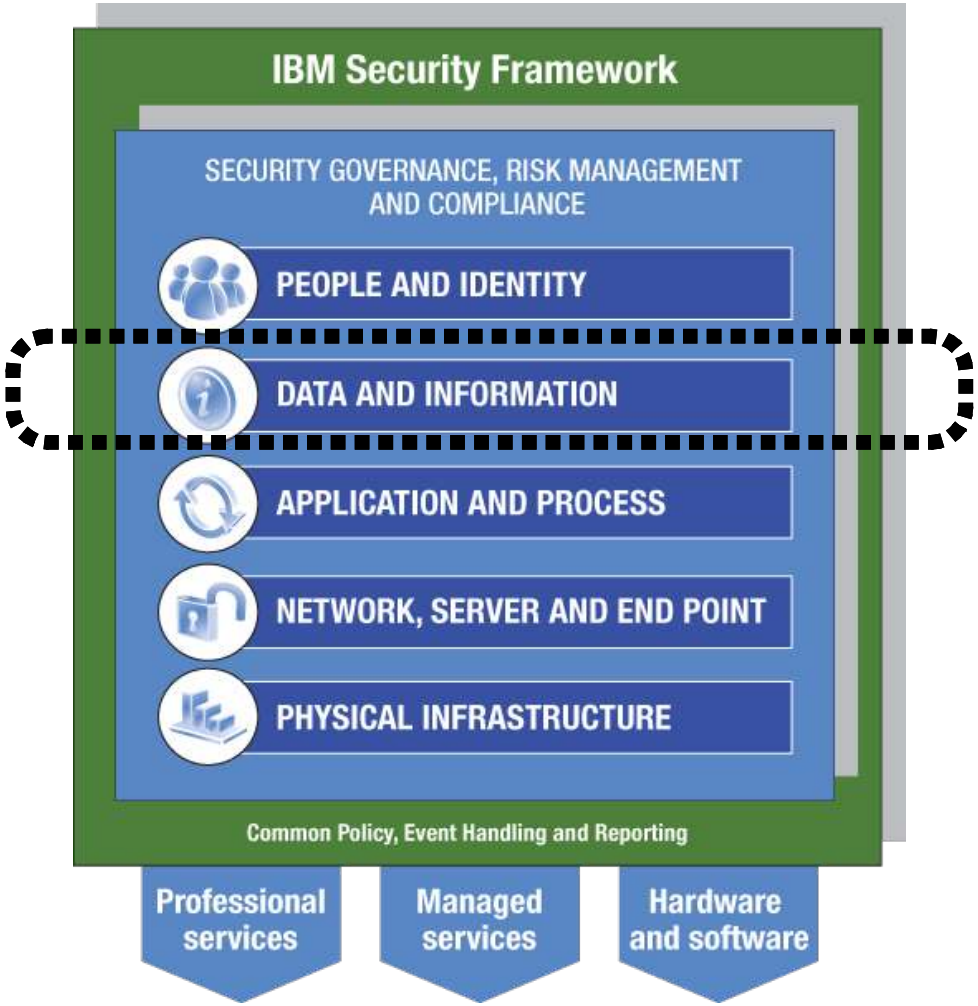
Inteligente

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

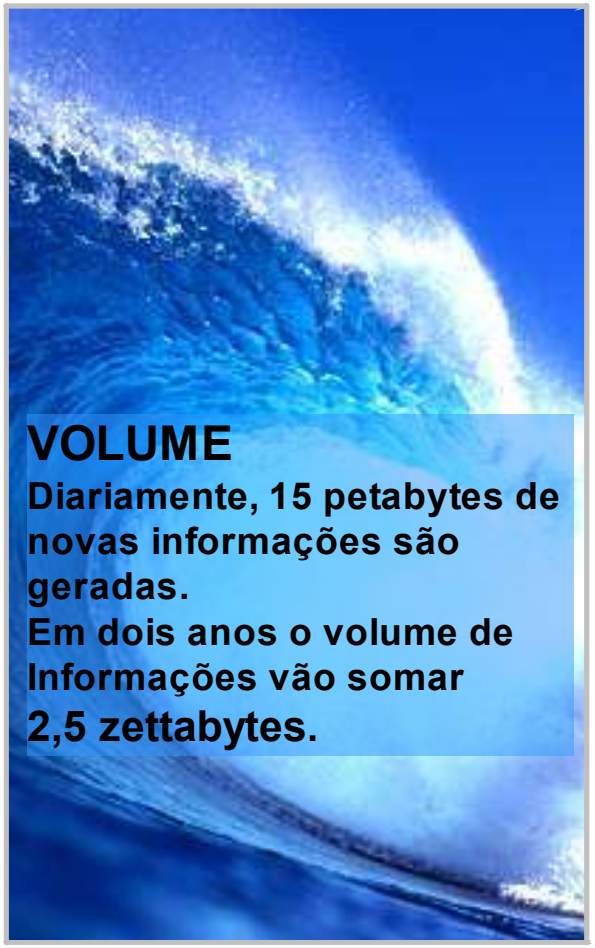
4ª edição IBM Security Forum

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

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

4ª edição IBM Security Forum

Solução lider 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.

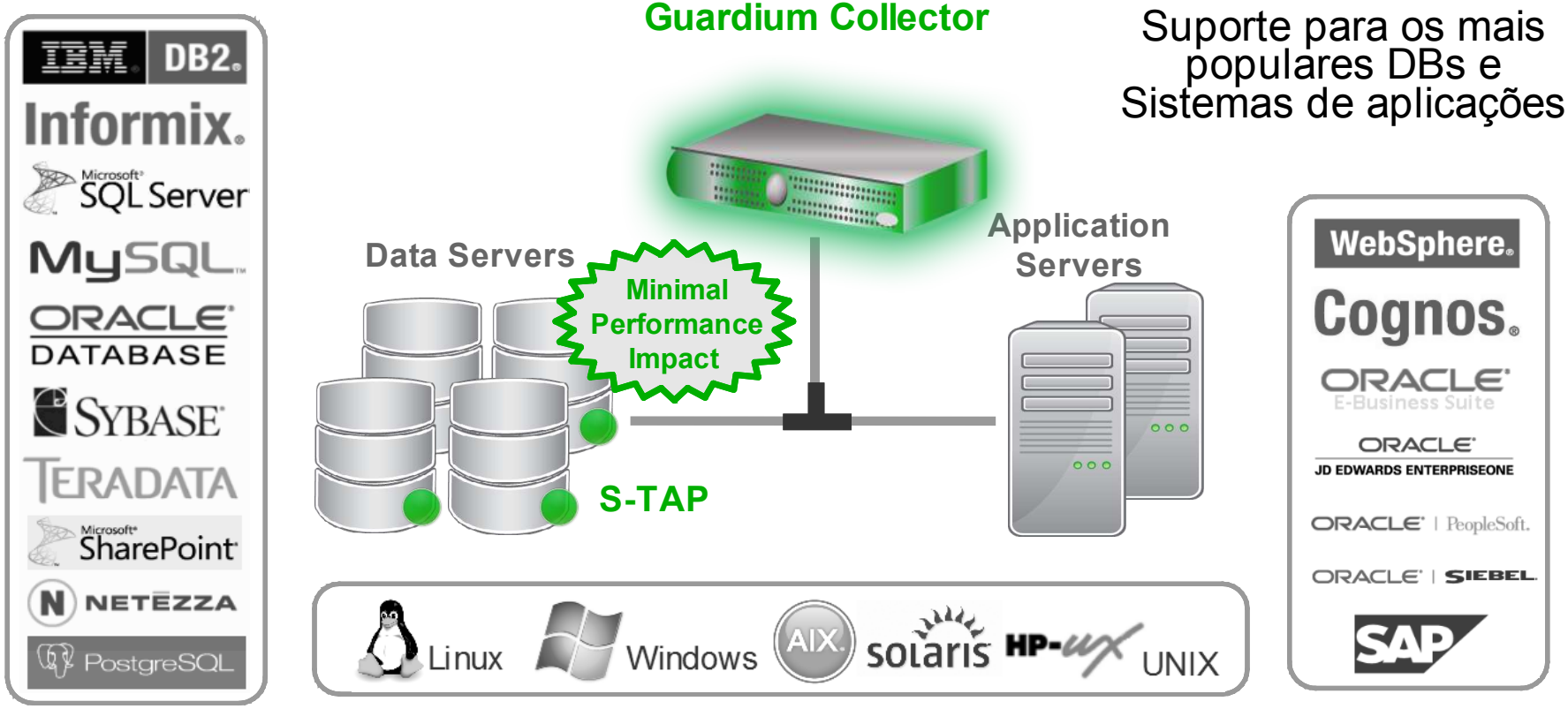
Arquitetura escalável e com suporte à ambientes heterogêneos.

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

Guardium - Solução DAM

Database Activity Monitoring

4ª edição IBM Security Forum

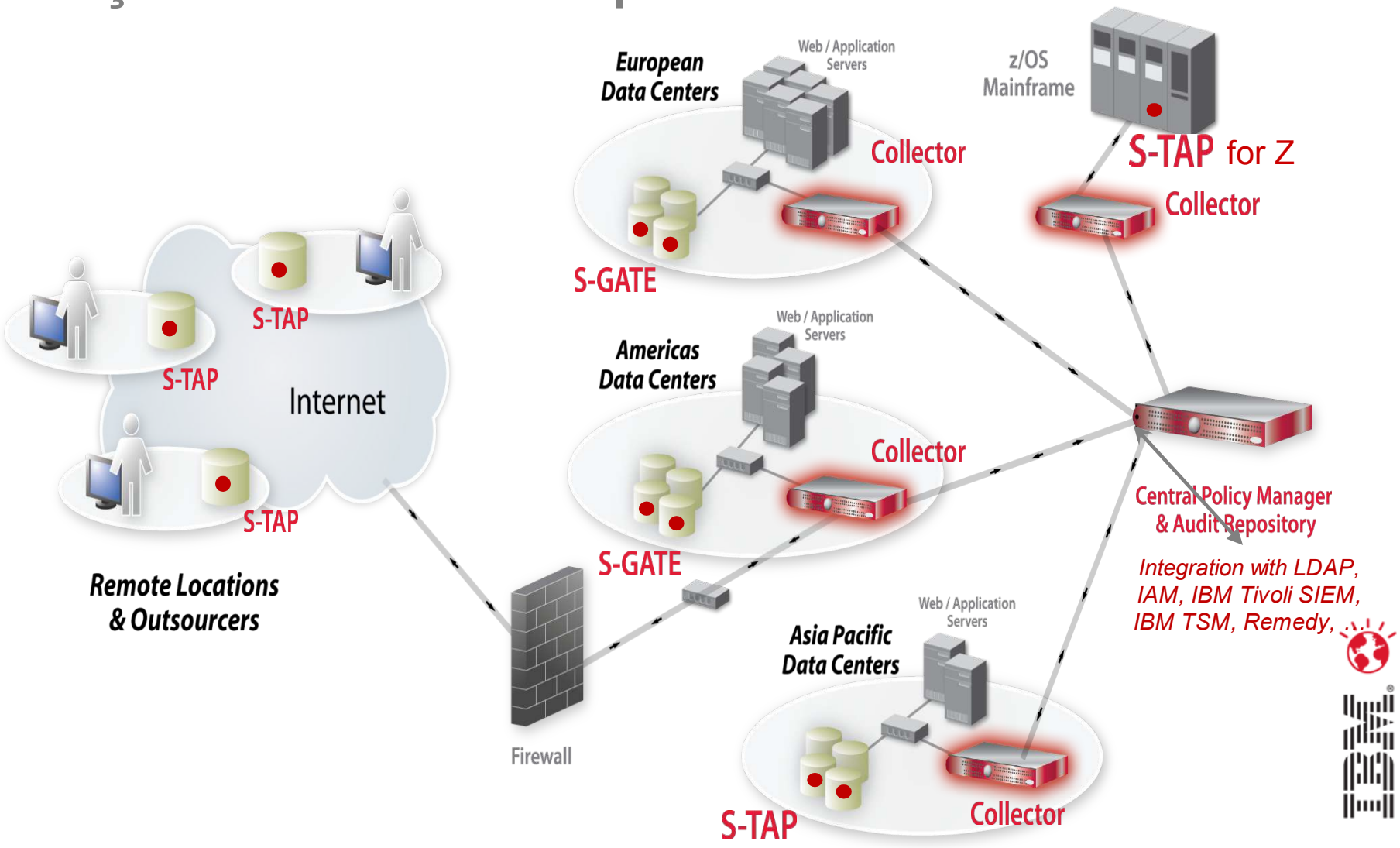


Suporte para os mais populares DBs e Sistemas de aplicações

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

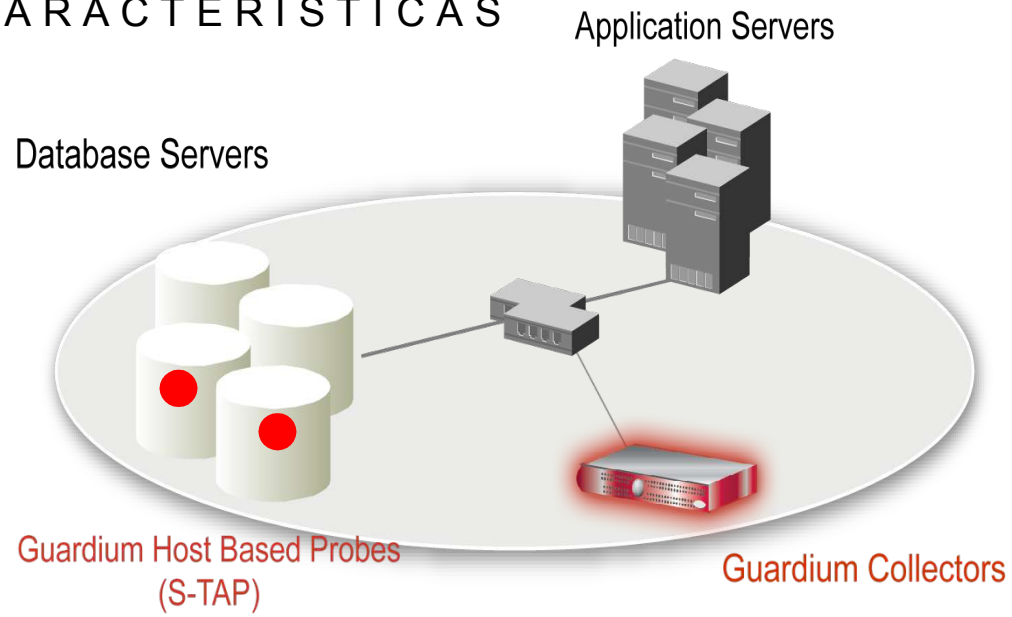
Guardium

Solução Escalável - Multi-plataformas



Monitoramento Real-time

CARACTERÍSTICAS



IBM IMS, ORACLE, IBM DB2, Microsoft Office SharePoint, TERADATA, Microsoft SQL Server, PostgreSQL, NETEZZA, MySQL, IBM Informix, SYBASE

- 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

4ª edição IBM Security Forum

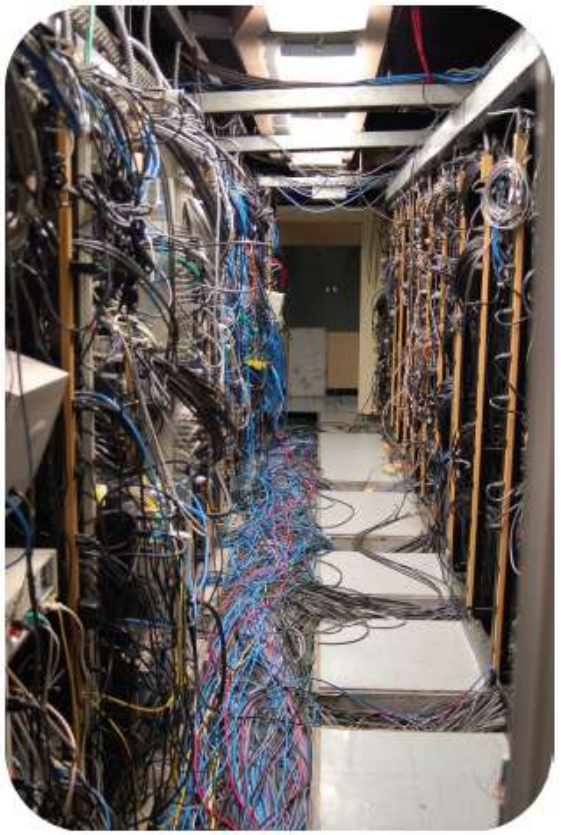
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security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

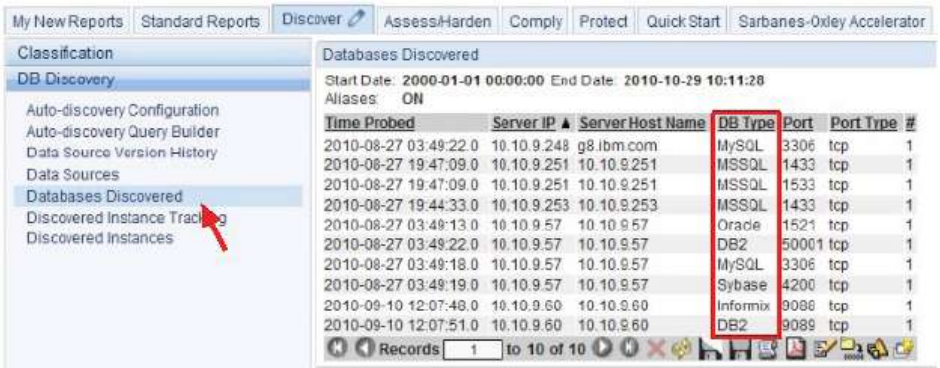
DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

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.



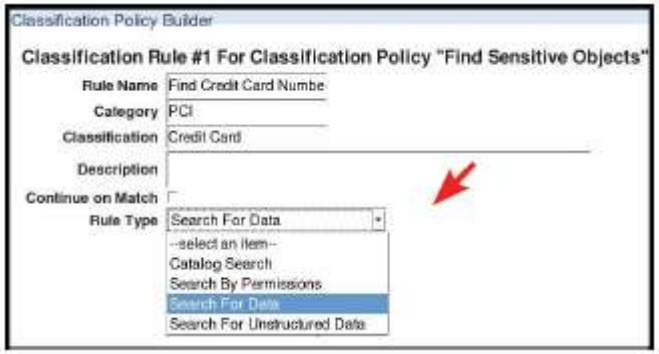


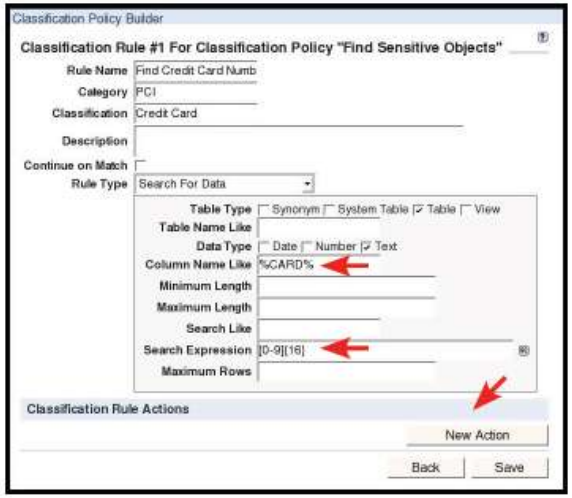
Guardium – Classifier

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

IBM DB2
Informix
Microsoft SQL Server
MySQL
ORACLE DATABASE
SYBASE
TERADATA
NETEZZA
PostgreSQL



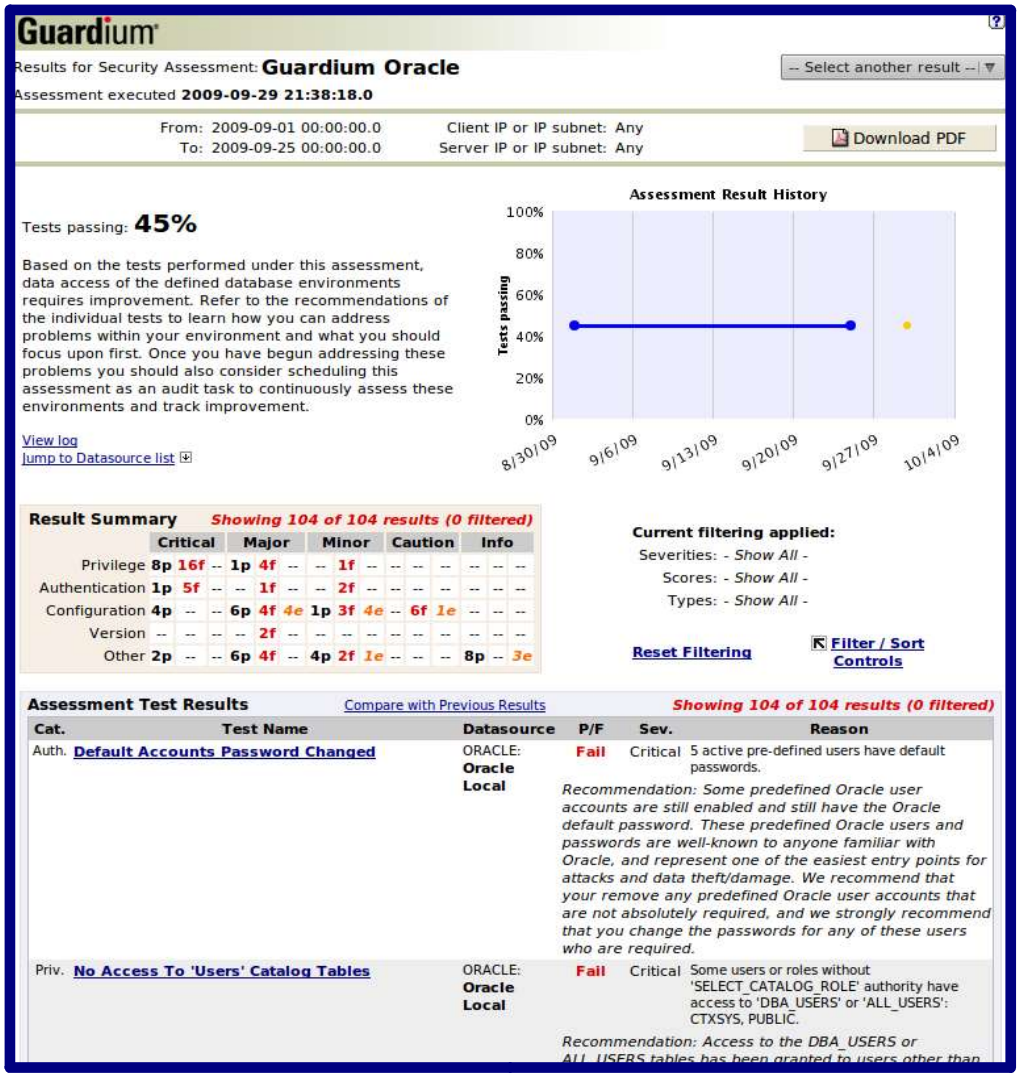


Guardium – Análise de Vulnerabilidade

- 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

4ª edição IBM Security Forum



Histórico dos Resultados

Resumo dos Resultados

Filtros e ordem dos controles

Detalhes Resultados dos testes

Descrição detalhadas das correções

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.

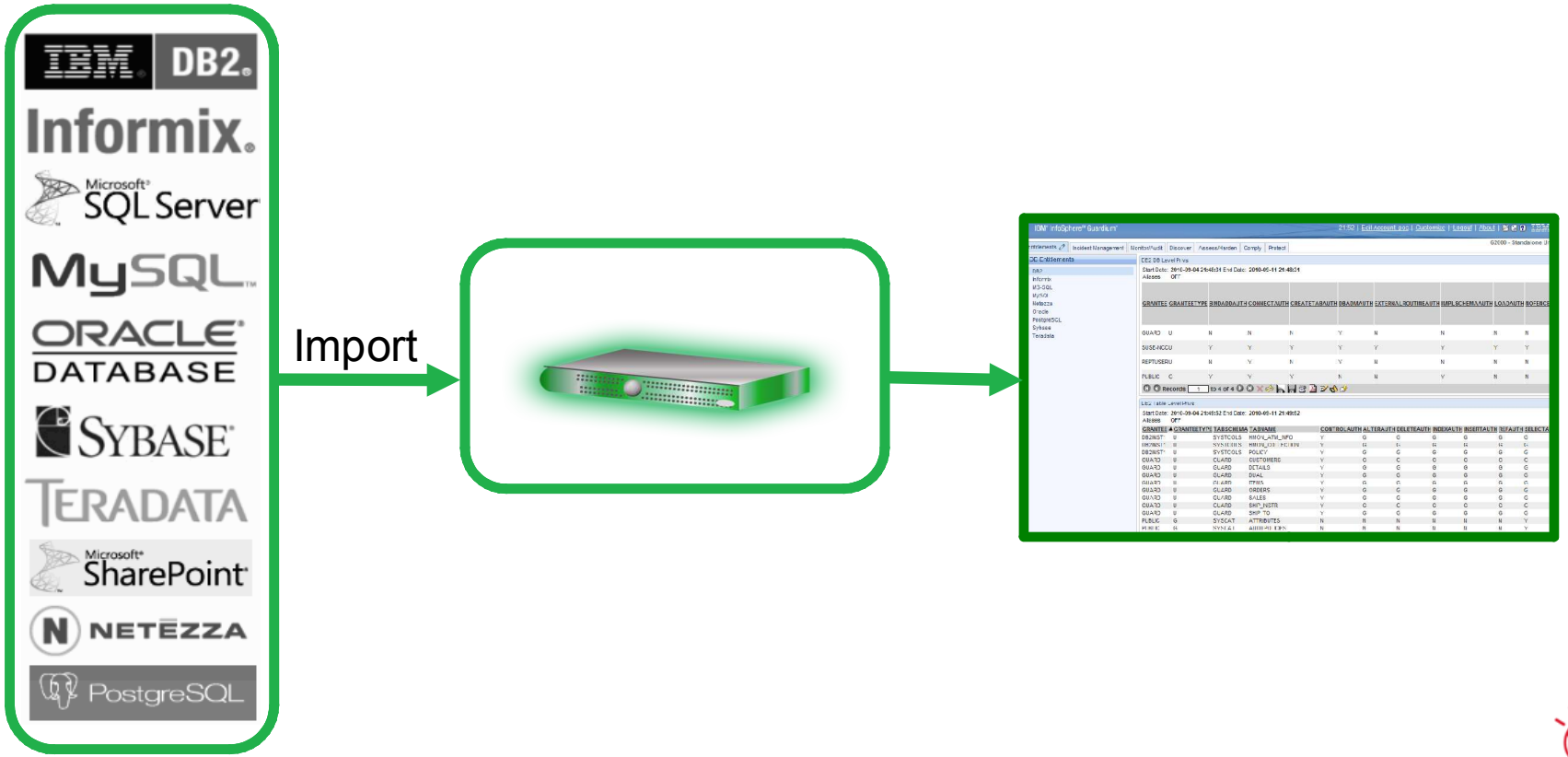
```
SQLCMD
C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID       LastName                  FirstName       SSN_Number
----------- ------------------------- --------------- -----------
          0 Anthony                   joe             *******-6780
          1 Thomas                    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



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

Principais interessados

4ª edição IBM Security Forum

SECURITY OPERATIONS

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

COMPLIANCE AUDIT

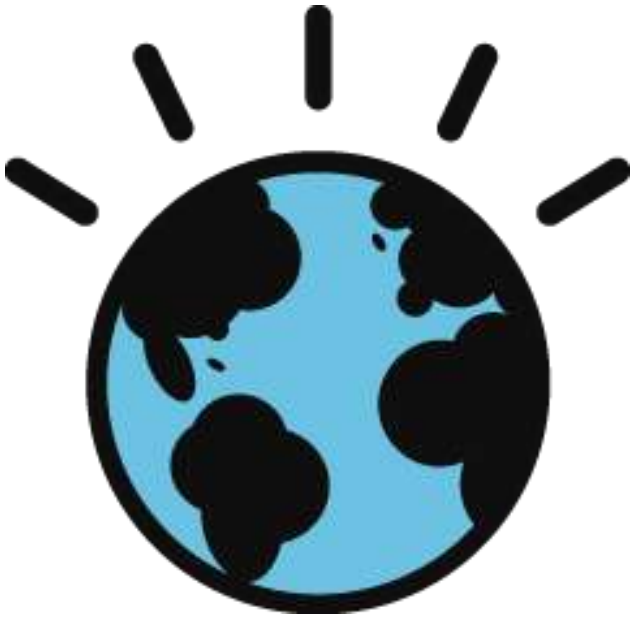
- ✓ Separação de Funções
- ✓ Relatórios com melhores práticas
- ✓ Controle automatizado

APPLICATION & DATABASE

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

Guardium:

100% de Visibilidade & Visão unificada

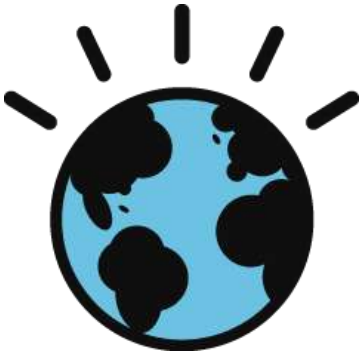


Essas são algumas das soluções de Segurança que têm auxiliado as principais empresas do planeta...

IBM

PERGUNTAS & RESPOSTAS

Contato:
JULIO FIGUEIREDO
juliofig@br.ibm.com



Obrigado pela Presença!

IBM