

CURSOR Software AG / IBM Distribution
Vertriebsinfo Nr. 11-11-22 vom 22.11.2011

IBM InfoSphere Guardium

Datensicherheit ist eines der aktuellen Top-Themen für IT-Leiter und Administratoren. Die unlängst bekannt gewordenen massiven Datendiebstähle bei internationalen Unternehmen führen zu Millionenverlusten und schweren Imageschäden. Geschäftsleitungen und Aufsichtsbehörden sind gleichermaßen sensibilisiert für die Frage nach der Sicherheit – **wie sicher sind Ihre Daten?**

Greifen wir die Frage auf: Wie sind Ihre Antworten zur Datensicherheit?

Hacker - der Angriff von Außen

- Woran erkennen Sie, dass jemand versucht sich Zugang zu verschaffen?
- Können Sie den Angreifer finden, nachdem er sich Zutritt verschafft hat? Wo bewegt er sich?
- Erkennen Sie seine Zugriffe und wann erkennen Sie diese?

Mitarbeiter - der Angriff von Innen

- Wie gewährleisten Sie, dass DBAs und andere privilegierte Nutzer ihre Zugriffsrechte nicht missbrauchen?
- Was gibt ihnen die Sicherheit im Bezug auf Ihre Mitarbeiter - Ihr persönliches Verhältnis, Ihre Menschenkenntnis, vertragliche Regelungen, gegenseitige Kontrolle?
- Reichen diese Regelungen auch Ihren Kunden?
- Was ist, wenn es dem äußeren Angreifer gelingt die Identität eines Mitarbeiters anzunehmen?

Wie gut kennen Sie Ihre Systeme

- Haben Sie externe Systeme und Daten integriert?
- Was sind Ihre sensiblen Daten, wo befinden sie sich?
- Wer hat Zugriff und in welcher Tiefe?
- Wie vermeiden Sie, dass Dienstleister sensible Informationen sehen können?

Erfüllung von gesetzlichen Vorgaben

- Können Sie die gesetzlichen Vorgaben und deren Einhaltung gewährleisten?
- Wie ist die Audit- und Compliancefähigkeit Ihrer Datenhaltung?
- Wie hoch sind Ihre Aufwendungen für Audit und Compliance?
- Was kommt auf Sie zu? CobiT (SOX) / PCI DSS / HIPPA / CMS ARS / GLBA / ISO 2700x (Basel II) / BaFin / NIST 800-53 (FISMA) ...

■ Wie sicher fühlen Sie sich?



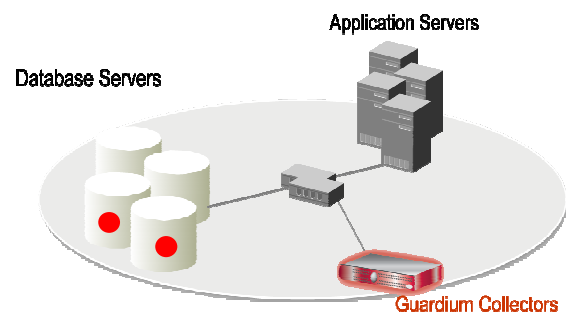
IBM InfoSphere Guardium

- **Nr. 1 der Angriffsziele sind Ihre Datenbanksysteme - über 90% der missbrauchten Daten stammen von Datenbankservern - hier greift Guardium zu Ihrem Schutz ein.**
- **IBM InfoSphere Guardium ist Datenbanküberwachung in Echtzeit**
Klar strukturiert und äußerst robust - für die Absicherung aller sensiblen und unternehmenskritischen Informationen.
- **100%-ige Zugriffstransparenz, auch in heterogenen Systemen**
Guardium arbeitet plattformübergreifend und kontrolliert die verschiedenen, ggf. verteilten, Anwendungen eines Unternehmens. Guardium unterstützt heterogene Systemlandschaften, herstellerübergreifend für alle marktrelevanten Datenbanksysteme.
- **Verhindern von Cyber-Attacken / Überwachung und Blockierung privilegierter Nutzer**
Unabhängig ob ein Angriff von außen oder von innen erfolgt, Guardium erkennt Einbruchs- und Betrugsversuche über die Anwendungsschicht. Real-time Alerts blockieren den Zugriff im Verdachtsfall.
- **Enterprise-Security-Plattform (zentralisiertes Auditing)**
Guardium bietet eine automatisierte Verwaltung der Compliance- und Kontrollmechanismen über die gesamte Anwendungs- und Datenbankinfrastruktur hinweg, von einer zentralen Stelle ausgehend.
- **Trennung der Verantwortlichkeiten**
Guardium ermöglicht ein echtes Vier-Augen Prinzip, durch die vollständige Trennung von Betrieb (Administration/DBA) und Kontrolle (Sicherheitsbeauftragte/CSO).
- **Erkennen sicherheitskritischer Daten und Schwachstellen**
Auffinden und Klassifizierung der sensiblen Daten in den verschiedenen Systemen, Feststellen von DB Schwachstellen.
- **Nachweis der Datensicherheit**
Guardium bietet ein datenbankübergreifendes Audit-Repository.
- **Guardium ist unabhängig**
Es kommen keine nativen Datenbankprotokolle oder Audit-Dienstprogramme der Datenbankhersteller zum Einsatz.
- **Keine Datenbankänderungen / keine Beeinflussung der Laufzeit**
Guardium befindet sich außerhalb der Datenbanksysteme, in der Regel in einer gekapselten Appliance. Es sind keine Änderungen an den Datenbanksystemen notwendig. Die Beeinflussung des Laufzeitverhaltens ist mit 2 – 3% zu vernachlässigen.

Guardium gibt die Antworten auf die Fragen

Wer, Was, Wo, Wann, Wie

und verhindert, dass es soweit kommt.



Guardium - Datensicherheit als Prozess

■ Datensicherheit ist ein fortschreitender Prozess

Der Schutz Ihrer Daten ist keine einmalige Angelegenheit. Eine ständige Beobachtung und Anpassung an die sich ändernden äußeren und inneren Gegebenheiten ist Voraussetzung für den Schutz. Hier unterstützt Guardium durch einen rollierenden Ansatz, in vier Schritten die Sicherheitsbeauftragten eines Unternehmens.

- (1) Lokalisierung und Klassifizierung (wo sind die Daten, welche Information ist sensibel)
- (2) Überwachung und Durchsetzung (wer greift zu, was ist auffällig, Sperrung von Zugriffen)
- (3) Prüfung und Reporting (Protokollierung, Reporting für Audit und Compliance)
- (4) Bewertung und Absicherung (Analyse von Schwachstellen, Maßnahmenkatalog)



(1) Lokalisierung und Klassifizierung – Guardium hilft beim Erkennen

- Guardium zeigt, wo sich in den Systemen die Daten befinden (in heterogenen Systemen, z.B. nach Firmenzusammenschlüssen, eine häufige Frage).
- Guardium hilft bei der Klassifizierung. Welche Interessen haben das Unternehmen, Partner und Kunden sowie der Gesetzgeber am Schutz der Daten. Welche Daten sind öffentlich zugänglich, welche sind als sensibel oder als geheim einzustufen?
- Guardium zeigt, wer auf diese Daten zugreift.

Mit InfoSphere Guardium lässt sich durch eine automatische Datenbankerkennung feststellen, wo vertrauliche Informationen gespeichert sind. Diese lassen sich automatisiert in unterschiedliche, dynamische Informationsklassen kategorisieren, für die entsprechende Sicherheitsrichtlinien gelten, damit sensible Informationen nur von berechtigten Benutzern angezeigt bzw. geändert werden können. Die Erkennung sensibler Daten kann in regelmäßigen Abständen zeitplan-gesteuert erfolgen, um sicherzustellen, dass nur autorisierte Datenbanken vorhanden und alle kritischen Informationen erfasst sind.

(2) Überwachung und Durchsetzung

- Die fein abgestuften Regeldefinitionen bilden die Richtlinien für die Datensicherheit.
- Guardium erweitert die Überwachung durch eine fortlaufende Kontextanalyse aller Datenbank-zugriffe (dem „Wer, Was, Wo, Wann und Wie“ jeder SQL Transaktion).
- Guardium stellt auffälliges Nutzerverhalten fest und schlägt Alarm.
- Guardium bietet pro aktive Überwachung und Durchsetzung der Datensicherheit in Echtzeit.



Guardium - Datensicherheit als Prozess

■ Richtlinien für die Datenbanksicherheit und Änderungen überwachen und durchsetzen

InfoSphere Guardium garantiert die Einhaltung der Richtlinien zur Verhinderung unberechtigter oder verdächtiger Aktionen durch privilegierte Datenbanknutzer sowie Angriffe durch unbefugte Benutzer oder externe Hacker.

Darüber hinaus können Anwender identifiziert werden, die über einen gemeinsamen Service-Account auf Datenbanken zugreifen, und dabei unerlaubt Änderungen an Datenbanken durchführen.

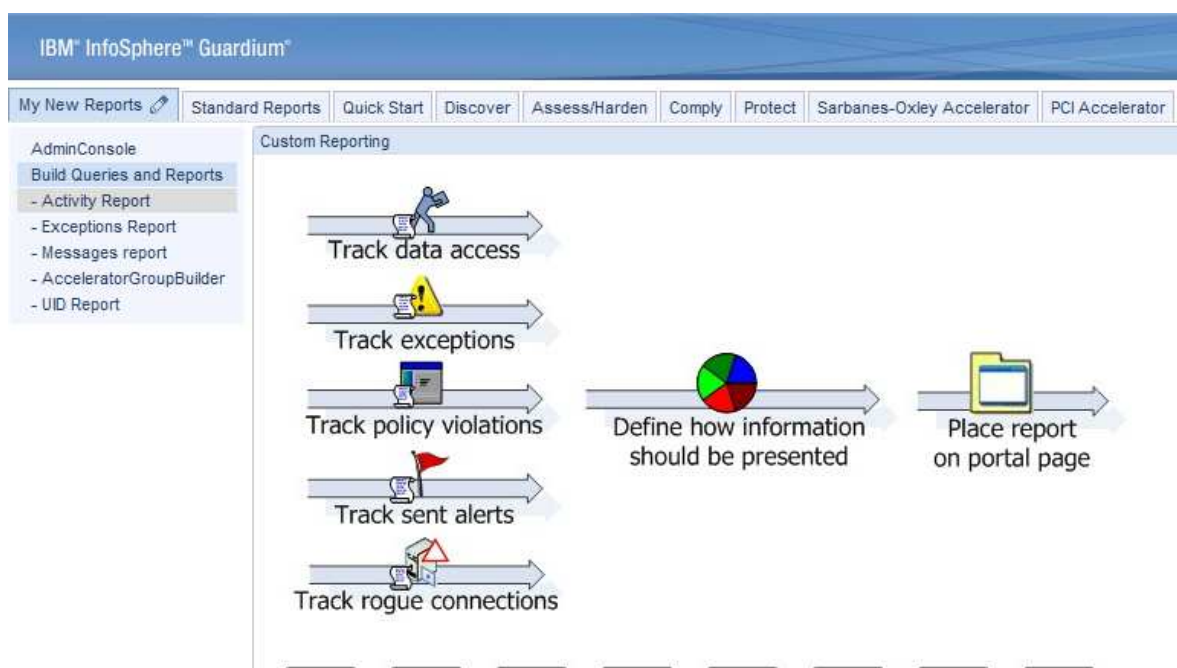
InfoSphere Guardium lässt sich durch Datensicherheitsbeauftragte ohne die Beteiligung von Datenbankadministratoren (DBAs) managen. Darüber hinaus können differenzierte Zugriffsregelungen festgelegt werden, die den Zugriff auf bestimmte Tabellen z. B. nach Benutzer, IP- oder MAC-Adresse, Anwendung, Uhrzeit, Netzwerkprotokoll und SQL-Befehlstyp beschränken.

■ Fortlaufende Kontextanalyse der gesamten Datenbankzugriffe

InfoSphere Guardium überwacht fortlaufend alle Datenbankoperationen in Echtzeit. Es werden zum Patent angemeldete Linguistikanalysen eingesetzt, die unberechtigte Zugriffe und Aktionen basierend auf detaillierten Kontextinformationen erkennen. Diese besondere Methodik minimiert falsche positive oder falsche negative Ergebnisse und bietet im Gegensatz zu herkömmlichen Verfahren, mit denen nur nach vordefinierten Mustern oder Signaturen gesucht wird, eine unerreichte Kontrollqualität.

■ Ermittlung von Vergleichsdaten zur Erkennung von Verhaltensanomalien und zur Automatisierung der Regeldefinition

Durch das Anlegen einer Baseline und der damit verbundenen Identifizierung üblicher Geschäftsprozesse sowie potenziell anormaler Aktivitäten, schlägt das System automatisch Regeln vor, mit denen Angriffe wie beispielsweise SQL-Injections verhindert werden können. Eigene kundenspezifische Regeln können sehr einfach über die intuitive Benutzeroberfläche angelegt werden.



Guardium - Datensicherheit als Prozess

■ Pro aktive Sicherheit in Echtzeit

InfoSphere Guardium bietet zahlreiche Mechanismen, mit denen pro aktiv und in Echtzeit auf unberechtigte oder anormale Zugriffe und Aktionen reagiert wird. Zu den regelbasierten Maßnahmen zählen Sicherheitswarnmeldungen in Echtzeit (SMTP, SNMP, Syslog), Software-Sperrungen, die komplette Protokollierung und kundenspezifische Maßnahmen wie automatische Account-Ausschlüsse, VPN-Port-Abschaltung und das Nachvollziehen und Lösen von Sicherheitsvorfällen. Aufgrund gesetzlicher Vorgaben sind Unternehmen verpflichtet, nachzuweisen, dass alle Vorfälle („Incidents“) aufgezeichnet, analysiert, zeitnah gelöst und dem Management gemeldet werden. InfoSphere Guardium bietet eine Business-Benutzeroberfläche und Workflowautomatisierung für die Lösung von Sicherheitsvorfällen sowie ein grafisches Dashboard für die Verfolgung wesentlicher Messgrößen wie die Anzahl der gefundenen Schwachstellen und deren Risiko für das Unternehmen.

(3) Prüfung und Reporting

- Prüfprotokolle, gesichert und nur für berechtigte Personen einsehbar.
- Reporting, vorkonfigurierte oder individuell erstellte Reports.

■ Erstellen eines lückenlosen Prüfprotokolls

InfoSphere Guardium erstellt ein lückenloses, feingranulares Prüfprotokoll aller Datenbankaktivitäten, die kontextabhängig analysiert und in Echtzeit gefiltert werden, um proaktive Kontrollmechanismen zu implementieren und die von Auditoren geforderten Informationen gezielt bereitzustellen. Dieses Prüfprotokoll wird in einem gesicherten und nicht veränderbaren Repository abgelegt und kann nur von berechtigten Personen gelesen werden. Der erstellte Bericht weist die Einhaltung der gesetzlichen Bestimmungen durch die detaillierte Aufzeichnung aller relevanten Datenbankaktivitäten nach: Fehlgeschlagene Anmeldungen, Eskalation von Berechtigungen, Schemaänderungen, Zugriff außerhalb der Geschäftszeiten oder durch nicht berechtigte Anwendungen sowie den Zugriff auf sensible Tabellen.

■ Branchenführendes Reporting

Die InfoSphere Guardium-Lösung beinhaltet mehr als 100 vorkonfigurierte Regeln und Berichte, die auf Grundlage von bewährten Methoden und Erfahrungen mit Global-1000-Unternehmen, Big-4-Auditoren und Assessoren weltweit erstellt wurden. Die Berichte leisten Hilfestellung bei der Nachweisführung von Regulierungsaufgaben wie SOX und PCI, der Umsetzung von Datenschutzgesetzen sowie der Vereinfachung von Data-Governance- und Datenschutzinitiativen. Neben den mitgelieferten, vorkonfigurierten Berichtsvorlagen bietet InfoSphere Guardium eine grafische Drag-und-Drop-Benutzeroberfläche, mit der sich neue Berichte mühelos erstellen oder vorhandene Berichte modifizieren lassen. Die Berichte können automatisch (als Dateianhang) per E-Mail im PDF-Format an Benutzer gesendet oder als Links in HTML-Seiten eingefügt werden. Sie können auch online über die Webkonsolenoberfläche angezeigt oder in Standardformaten in SIEM oder sonstige Systeme exportiert werden.



IBM InfoSphere™ Guardium 15:13

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

Overview

DB Activities

Activity By Client IP
Database Servers
DML Execution on Sensitive Objects
Sensitive Objects Usage
Sessions By Server Type

Servers Accessed
Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON

Server IP	Server Type	Database Name	Service Name	Count of Source Program	Count of Sessions
10.10.9.251	MS SQL SERVER	Customer		1	1
10.10.9.253	MS SQL SERVER	Customer	MS SQL SERVER2		4
10.10.9.253	MS SQL SERVER	FINANCIAL	MS SQL SERVER2		8
10.10.9.253	MS SQL SERVER	SensitiveDB	MS SQL SERVER2		10
10.10.9.56	DB2	Customer	DB2INST2	1	7
10.10.9.56	DB2	CustomerDB	DB2INST2	2	18
10.10.9.57	DB2	CustomerDB	DB2INST2	1	1
10.10.9.57	ORACLE	Customer	ORACLEXE	2	19
10.10.9.57	ORACLE	Customer	ORCL	1	1
10.10.9.57	SYBASE	Customer	NT40DB	1	1
10.10.9.57	SYBASE	SensitiveDB	SN5U3000	1	6
10.10.9.57	SYBASE	SensitiveDB	SN5U3000	1	3
10.10.9.57	SYBASE	SYBSYSTEMPROCS	SN5U3000	1	2
10.10.9.60	INFORMIX	Customer	DEMO_ON	1	1
10.10.9.60	INFORMIX	IDSGAME@DEMO_ON	DEMO_ON	1	1
10.10.9.60	INFORMIX	SYMASTER	DEMO_ON	1	1

Records 1 to 16 of 16

Databases Discovered
Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON PortNotLike: NOT LIKE

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2010-08-27 03:49:13.0	10.10.9.57	10.10.9.57	Oracle	1521	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
2010-08-27 03:49:22.0	10.10.9.248	g8.ibm.com	MySQL	3306	tcp	1

IBM InfoSphere™ Guardium 15:17 | Edit account: pot | Customize | L

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

Overview

DB Activities

Exceptions

Active Users Last Login
Active Users with no Activity
Exception Count
Exceptions Distribution
Exceptions Monitor
Failed User Login Attempts
Policy Violations
SQL Errors
SQL Records Returned
Terminated Users Failed Login Attempts
Terminated Users Logins

Policy Violations Details
Start Date: 2010-08-25 01:35:38 End Date: 2010-08-30 01:35:38
Aliases: ON ServerPLike: LIKE %

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String
2010-08-27 20:57:17.0	Data Privacy	Find SSN	10.10.9.248	10.10.9.251	sa	[INFO] Created by GuardClassifier Process Run: 'Find SSN Process' Date: Friday, August 27, 2010 8:57:17 PM EDT Datatype: MS SQL SERVER 10.10.9.251: 1433 Object: Sensitivevdb.dbo.SSN SSN_Number Category: 'Data Privacy' Classification: 'Sensitive Information' Rule: Search For Data: Find SSN TABLE_TYPE=TABLE, DATA_TYPE=TEXT, SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4} Action: Log Policy Violation: Policy Violation Severity=0
2010-08-27 20:57:16.0	Data Privacy	Find SSN	10.10.9.248	10.10.9.251	sa	[INFO] Created by GuardClassifier Process Run: 'Find SSN Process' Date: Friday, August 27, 2010 8:57:16 PM EDT Datatype: MS SQL SERVER 10.10.9.251: 1433 Object: Sensitivevdb.dbo.Patient ssn Category: 'Data Privacy' Classification: 'Sensitive Information' Rule: Search For Data: Find SSN TABLE_TYPE=TABLE, DATA_TYPE=TEXT, SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4} Action: Log Policy Violation: Policy Violation Severity=0
2010-08-27 20:56:36.0	Data Privacy	Find SSN	10.10.9.248	10.10.9.251	sa	[INFO] Created by GuardClassifier Process Run: 'Find SSN Process' Date: Friday, August 27, 2010 8:56:36 PM EDT Datatype: MS SQL SERVER 10.10.9.251: 1433 Object: master.dbo.SSN SSN_Number Category: 'Data Privacy' Classification: 'Sensitive Information' Rule: Search For Data: Find SSN TABLE_TYPE=TABLE, DATA_TYPE=TEXT, SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4} Action: Log Policy Violation: Policy Violation Severity=0
2010-08-27 20:56:27.0	Data Privacy	Find SSN	10.10.9.248	10.10.9.251	sa	[INFO] Created by GuardClassifier Process Run: 'Find SSN Process' Date: Friday, August 27, 2010 8:56:26 PM EDT Datatype: MS SQL SERVER 10.10.9.251: 1433 Object: financial.creditcard.SSN SSN_Number Category: 'Data Privacy' Classification: 'Sensitive Information' Rule: Search For Data: Find SSN TABLE_TYPE=TABLE, DATA_TYPE=TEXT, SEARCH_VALUE_PATTERN=[0-9]{3}-[0-9]{2}-[0-9]{4} Action: Log Policy Violation: Policy Violation Severity=0
2010-08-27 00:55:07.0	Mask sensitive data - SSN		10.10.9.56	10.10.9.56	DB2INST2	select * from ssn Extrusion Values: *****-6780,*****-6781,*****-6782,*****-6783,*****-6784,*****-6785,*****-6786,*****-6787,*****-6788
2010-08-27 00:53:46.0	KPI Connection accessing sensitive objects		10.10.9.56	10.10.9.56	DB2INST2	INSERT INTO creditcard(CARDD, FIRSTNAME, LASTNAME, CARDNUMBER, PIN, TXN_ID, SECURITYO

DB Administration

Schema Changes
Detailed Activities
Performance
DB Entitlements
Access Map



Guardium - Datensicherheit als Prozess

(4) Bewertung und Absicherung

■ Schwachstellen-, Konfigurations- und Verhaltensbewertung

Die Datenbanksicherheitsbewertung von InfoSphere Guardium sucht in der gesamten Datenbankinfrastruktur nach Schwachstellen und bietet eine fortlaufende Auswertung der Datenbanksicherheitslage anhand von Echtzeit sowie von historischen Daten. Hierfür steht eine umfassende Bibliothek vorkonfigurierter Tests auf der Grundlage branchenüblicher Methoden (CVE, CIS, STIG) und plattformspezifischer Schwachstellen zur Verfügung. Regelmäßige Updates sind über einen InfoSphere Guardium Knowledge-Base-Service erhältlich. Darüber hinaus können Unternehmen eigene Tests nach Ihren spezifischen Anforderungen definieren. Zur Einhaltung der Vorgaben von z. B. SOX und PCI DSS meldet das Bewertungsmodul auch gesetzlich relevante Schwachstellen wie den unbefugten Zugriff auf reservierte Oracle EBS- und SAP- Tabellen. Die Bewertungen gliedern sich generell in zwei Kategorien:

- Schwachstellen- und Konfigurationstests suchen nach Schwachstellen wie fehlende Patches, falsch konfigurierte Zugriffsrechte und unzureichend gesicherte Standardaccounts.
- Verhaltenstests erkennen Sicherheitslücken anhand von Mustern, mit denen Datenbankzugriffe und -manipulationen üblicherweise erfolgen – beispielsweise eine übermäßige Zahl fehlgeschlagener Anmeldungen, Clients, die Administrationsbefehle ausführen oder Anmeldungen zu später Stunde. Dazu werden die gesamten Datenbankzugriffe in Echtzeit überwacht.

Neben der Erstellung kompletter Berichte mit der Möglichkeit, per „Drilldown“ ins Detail zu gehen, erzeugt das Bewertungsmodul einen Sicherheitsbericht mit gewichteten Messgrößen (auf Grundlage von Best Practices), industriespezifische Referenzkennzahlen und empfiehlt konkrete Maßnahmenpläne zur Verbesserung der Datenbanksicherheit.

■ Konfigurationen sichern und Änderungen verfolgen

Nachdem die durch die Schwachstellenbewertung empfohlenen Maßnahmen umgesetzt worden sind, kann eine Referenz – die sogenannte Baseline – für gesicherte Konfigurationen definiert werden. Mit dem InfoSphere Guardium Configuration Audit System (CAS) lassen sich Abweichungen von der Baseline überwachen, und es kann sichergestellt werden, dass keine Änderungen außerhalb der genehmigten Änderungsrichtlinien und -prozesse erfolgen.

The screenshot displays the IBM InfoSphere Guardium web interface. On the left, a workflow diagram titled 'Database Security Assessment' shows a process flow: 'Define what database you want assessed .. and view result' leading to 'Define an Audit Process'. Below this, three icons represent 'Assessment builder', 'Audit Process builder', and 'Group builder'. On the right, a 'Classifier/Assessment Job Queue' window is open, showing a table of assessment results. The table has columns for Process Run Id, Process Type, Status, Process Result Id, CIs/Asmt Description, Audit Task Description, Queue Description, Start Time, End Time, and Datasources. The current view shows 'No data found' for the selected job.

Process Run Id	Process Type	Status	Process Result Id	CIs/Asmt Description	Audit Task Description	Queue Description	Start Time	End Time	Datasources
No data found									



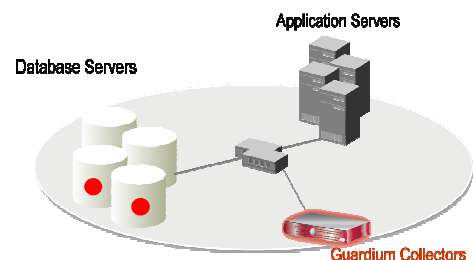
Guardium für ISVs

■ Guardium für Sie als ISV und für Ihre Kunden

- Identifizieren Sie die Kunden, für die Datensicherheit über die physikalische Wiederherstellung hinausgeht.
- Guardium ist plattformunabhängig. Der Einsatz auf gängigen Datenbank- und ERP-Systemen wie SAP, Oracle EBS, PeopleSoft, JDE, Siebel and Business Objects, etc. ist übergreifend möglich. Damit öffnet sich ein weites Feld der Einsatzmöglichkeiten.
- Guardium bietet den Ausgangspunkt für Dienstleistungen, nicht nur bei der Einführung im Kundenumfeld. Dank der Unabhängigkeit von den übrigen Systemen, der Unabhängigkeit von der Administration des Kunden und der hohen Sensibilität des Produktes für Auditanforderungen, kann die Datensicherheit auch von einem Dienstleister (zum Beispiel von Ihnen) gewährleistet und belegt werden.
- Wenn Sie Betreiber eines Rechenzentrums sind, überlegen Sie bitte, ob Sie Guardium Ihren Kunden als Dienst anbieten.



***Sprechen Sie mit uns, wenn Guardium Ihnen und Ihren Kunden helfen kann, Informations- und Com-
pliancesicherheit zu gewährleisten.***



Guardium - Produktvarianten

■ Basisvarianten des Produktes

Um den unterschiedlichen Sicherheitsansprüchen Rechnung zu tragen, wird Guardium in drei verschiedenen Basisvarianten (Audit Stufen) vertrieben.

■ Privileged Users

- Beobachtet nur Aktionen von definierten, real existierenden Personen.
Es werden keine generischen Applikationsuser oder technischen User-Accounts überwacht.
- Bei der Benutzung von S-TAPs (Sensoren zur Überwachung) filtern diese die Ergebnisse und nur eine Untermenge der Auditdaten wird an den Collector gesendet.
- Privileged Users ist die häufigste und günstigste Variante wenn es darum geht zu reporten, wer auf welche Daten zugreift und um zu unterbinden, dass DBAs unautorisierte Datenänderungen vornehmen.
- Diese Funktionalität wird häufig für SOX-Reportig benötigt.

■ Sensitive Objects

Umfasst die Privileged User Funktionalität und zusätzlich:

- Auditiert bestimmte DB Aktivitäten, wie z.B. eine definierte Liste sensibler Objekte oder eine definierte Liste von SQL-Befehlen.
- Es werden alle Informationen von den S-TAPs zur Regelüberprüfung an den Collector gesendet.
- Sensitive Objects auditiert, auf was zugegriffen wird (wer, wie, wann).
- Oft gebraucht für PCI- und Datenschutz Reporting

■ Comprehensive

Sensitive Objects Funktionalität plus:

- Auditieren und Loggen von allen Informationen.
D.h., der Kunde kann „Log Full Detail“ sehen, sollte das aber nur sehr selektiv einsetzen.
- Die Comprehensive Variante ist für DB, FTP, WFS und unstrukturierte Daten nutzbar.
- Es ist die leistungsfähigste Variante, die in der Lage ist, alles aufzeichnen zu können.
Von einigen Anwendern als extrem granular und aufwändig eingeschätzt, wird sie gerade von den Kunden nachgefragt, die einen Datendiebstahl in der Vergangenheit hatten.

■ Zu den Basisvarianten existiert eine Reihe von anforderungsspezifischen Erweiterungen.



Guardium - Produktvarianten

■ Produkt-Suiten gemäß Announcement der IBM vom 01.November 2011

Seit November 2011 wird Guardium auch in vorgefertigten Suiten angeboten, um für bestimmte Unternehmensgrößen und Anwendungsfälle eine Produktpositionierung zu vereinfachen.

- **Core Edition** umfasst die im Database Activity Monitor Modul enthaltenen Funktionen für Privileged Users and Sensitive Objects Auditing.
- **Standard Edition** ist eine Erweiterung der Core Edition um einen vollständigen Satz von Funktionen aus dem Central Manager and Aggregator, dem Database and Sensitive Data Finder, und dem Application End User Identifier Modul. Diese Edition ist für kleine bis mittlere Umgebungen geeignet.
- **Extended Edition** umfasst die Standard Edition und eine der folgenden Funktionen: Data-Level Access Control, Enterprise Integrator, Configuration Audit System for Database Servers, Entitlement Reports, oder Advanced Compliance Workflow Automation. Diese Edition ist für kleine bis mittlere Umgebungen geeignet.
- **Enterprise Edition** umfasst die Extended Edition und zusätzlich einen vollständigen Satz der Funktionalitäten aus dem Enterprise Integrator, Entitlement Reports, Advanced Compliance Workflow Automation, und den Configuration Audit System Modulen. Diese Edition ist für alle Umgebungsgrößen geeignet, bis hin zu internationalen Infrastrukturen von Großkonzernen.

■ Lizenzierung

- Guardium wird als Appliance angeboten, einer Kombination aus Hardware und Software (hier die sogenannten Kollektoren). Der Hardwareanteil der Appliance ist in den Lizenzkosten enthalten. Alternativ dazu ist es möglich eine Lizenzierung auf Basis einer virtuellen Appliance vorzunehmen. Hierbei wird Ihnen eine virtuelle Maschine geliefert, die Sie in Ihrer Hardwareumgebung integrieren können. Je nach Umfang der zu überwachenden Installationen können auch mehrere Appliances zum Einsatz kommen.
- Der Umfang der Lizenzierung richtet sich nach den zu überwachenden Systemen. Die Berechnung erfolgt auf Basis der für die Datenbanken zur Verfügung stehenden Prozessorleistungen. Es ist die Summe der PVU-Werte der Datenbankserver zu ermitteln und zu lizenzieren. Guardium wird ausschließlich auf PVU Basis lizenziert, unabhängig von möglichen Lizenzmetriken der überwachten Systeme.



Guardium

■ Weiterführende Informationen

Bitte sprechen Sie uns an wenn wir Ihr Interesse für Guardium geweckt haben. Guardium verfügt über ein sehr umfassendes Leistungsspektrum, das auf die jeweiligen Gegebenheiten und Anforderungen abgestimmt wird.

Fragen Sie uns, gerne entwickeln wir mit Ihnen eine Lösung für Ihre Anforderungen.

Ihr Ansprechpartner für diese Vertriebsinformation:

Dipl. Inf. (FH) Jürgen Storch
(Geschäftsbereich IBM Distribution)

CURSOR Software AG
Friedrich-List-Straße 31
D-35398 Gießen
juergen.storch@cursor.de
www.cursor-distribution.de



Alle gemachten Informationen sind unverbindlich und können jederzeit Änderungen unterliegen.
Die IBM behält sich das Recht vor, jederzeit Produkte und Angebote zu ändern oder zurückzuziehen.

