



IBM InfoSphere Guardium

Management von Datenbanksicherheit und Compliance während des gesamten Lebenszyklus Ihrer Daten

Immer mehr führende Unternehmen vertrauen bei der Absicherung ihrer kritischen Unternehmensdaten auf IBM InfoSphere Guardium. Der Grund hierfür: Wir bieten eine denkbar einfache und robuste Lösung für die Absicherung aller in Unternehmenssystemen gespeicherten Daten – von Finanz- und ERP-Informationen über Kunden- und Karteninhaberdaten bis hin zu geistigem Eigentum wie Forschungsergebnisse, Patente oder interne Firmeninformationen.

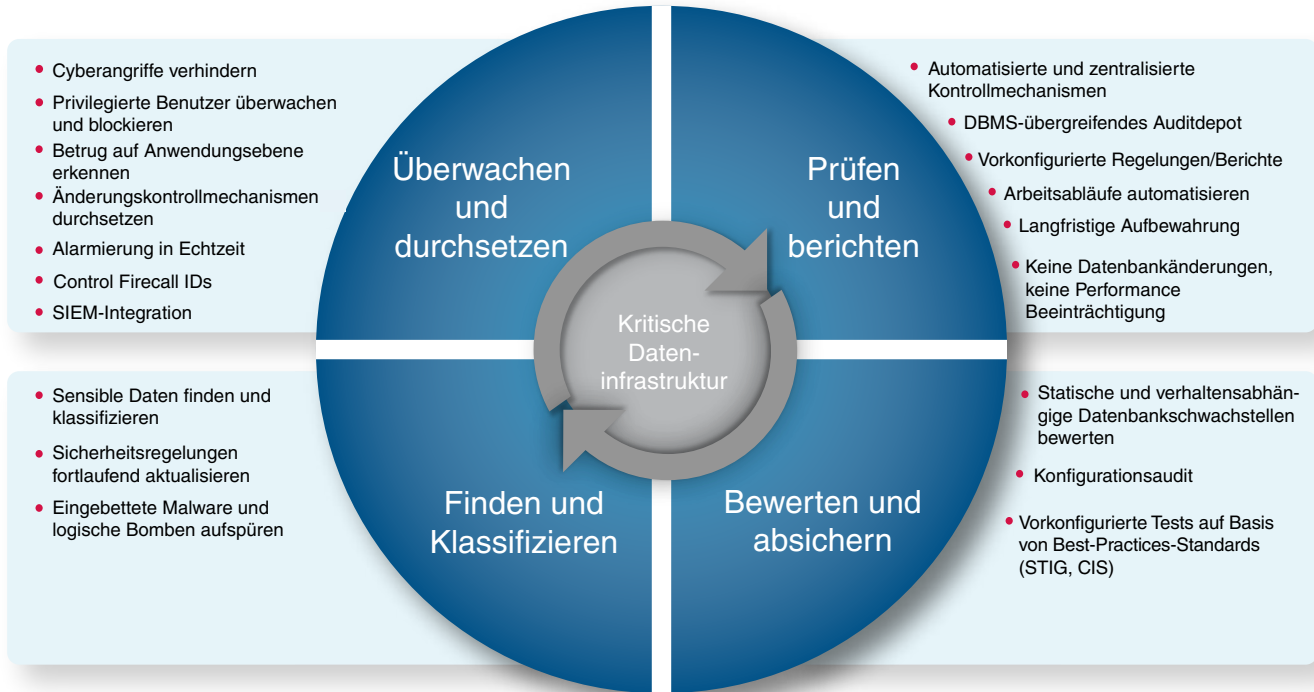
Unsere Enterprise-Security-Plattform verhindert unberechtigte oder verdächtige Aktivitäten durch privilegierte Nutzer oder potenzielle Hacker. Durch fortlaufende Überwachung erkennt die Plattform auch den potenziellen Betrug über Benutzerkonten von Unternehmensanwendungen wie Oracle E-Business Suite, PeopleSoft, SAP und unternehmensinternen Systemen.

IBM InfoSphere Guardium bietet eine skalierbare, mehrschichtige Architektur, die Compliance- und Kontrollmechanismen über die gesamte Anwendungs- und Datenbankinfrastruktur hinweg automatisiert und zentralisiert.

Ebenso überzeugend wie das Leistungsspektrum unserer Lösung ist ihre Effektivität: Sie hat nahezu keine Auswirkung auf die Performance, erfordert keine Änderungen in den überwachten Datenbanken und arbeitet unabhängig von nativen Datenbankprotokollen oder Audit-Dienstprogrammen.



Datenbanksicherheit und Überwachung in Echtzeit



Einheitliche Lösung: Basierend auf einer gemeinsamen Webkonsole und einem gesicherten Back-End-Datenspeicher bietet InfoSphere Guardium eine Lösung aus integrierten Modulen für das Management des gesamten Datenbanksicherheits- und Compliance-Lebenszyklus.

InfoSphere Guardium ist die einzige Lösung, die mit einer einheitlichen Webkonsole, einem Back-End-Datenspeicher und einem System zur Automatisierung von Arbeitsabläufen den gesamten Datenbanksicherheits- und Compliance-Lebenszyklus abdeckt. Damit können Unternehmen:

- sensible Informationen in Unternehmensdatenbanken lokalisieren und klassifizieren.
- Datenbankschwachstellen und Konfigurationsmängel erkennen.
- Konfigurationen nach der Umsetzung empfohlener Änderungen sichern.
- 100 % Transparenz bei allen Datenbanktransaktionen erzielen – plattform- und protokollübergreifend – mit einem sicheren, nicht manipulierbaren Prüfprotokoll, welches eine klare Aufgabentrennung unterstützt.
- Aktivitäten in File Sharing-Plattformen wie Microsoft Share Point verfolgen und überwachen.
- Richtlinien überwachen und durchsetzen – für den Zugriff auf sensible Daten, die Aktionen privilegierter Benutzer, Änderungskontrollen, Aktivitäten der Anwendungsbenutzer und sicherheitsrelevante Vorkommnisse wie z. B. fehlgeschlagene Anmeldungen.
- den gesamten Compliance- und Auditprozess automatisieren – einschließlich der Generierung und Weiterleitung von Berichten an die Datensicherheitsbeauftragten zur Freigabe oder Eskalation – nach Vorgabe gemäß SOX, PCI DSS und weiteren Datenschutzrichtlinien.
- ein zentralisiertes Auditdepot für das Compliance-Reporting, Performance- und Forensikuntersuchungen im gesamten Unternehmen anlegen.
- vom Schutz einer einzelnen Datenbank zur Absicherung tausender Datenbanken in weltweit verteilten Rechenzentren übergehen.

Lokalisieren und klassifizieren

Sensible Informationen automatisch lokalisieren, klassifizieren und schützen

Je größer das in Unternehmen entstandene und gespeicherte Volumen digitaler Informationen wird, desto schwerer fällt es, sensible Informationen aufzufinden und zu klassifizieren.

Dies stellt insbesondere Unternehmen, die Fusionen und Akquisitionen bewältigt haben, oder IT-Umgebungen mit Altsystemen, die bereits ihre Entwickler überdauert haben, vor große Herausforderungen. Selbst im günstigsten Fall können ständige, durch neue geschäftliche oder rechtliche Anforderungen bedingte Änderungen an Anwendungs- und Datenbankstrukturen dazu führen, dass sensible Daten nicht als solche erkannt werden und daher ungeschützt bleiben.

Unternehmen fällt es insbesondere schwer,

- alle Datenbankserver zu erkennen, die sensible Informationen enthalten, und zu verstehen, wie auf diese zugegriffen wird (Anwendungen der Geschäftsbereiche, Batchprozesse, Ad-hoc-Abfragen, Anwendungsentwickler, Administratoren usw.).
- Informationen abzusichern und Risiken zu bewerten, wenn die Sensibilität der gespeicherten Informationen unbekannt ist.
- die Einhaltung gesetzlicher Vorgaben zu gewährleisten, wenn nicht klar ist, welche Informationen welchen Regularien unterliegen.

Mit InfoSphere Guardium lässt sich durch eine automatische Datenbankerkennung feststellen, wo vertrauliche Informationen gespeichert sind. Diese lassen sich automatisch 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 zeitplangesteuert erfolgen, um sicherzustellen, dass nur autorisierte Datenbanken vorhanden und alle kritischen Informationen erfasst sind.

Bewerten und absichern

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), industrienspezifische 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.

Überwachen und durchsetzen

Richtlinien für die Datenbanksicherheit und Änderungen überwachen und durchsetzen

InfoSphere Guardium garantiert die Einhaltung feingranularer Richtlinien zur Verhinderung unberechtigter oder verdächtiger Aktionen durch privilegierte Datenbanknutzer sowie Angriffe durch unbefugte Benutzer oder externe Hacker. Darüber hinaus können Anwendungsbenutzer identifiziert werden, die über einen gemeinsamen Service-Account auf Datenbanken zugreifen, und dabei unerlaubt Änderungen an Datenbanken durchführen. Zu diesen Anwendungen zählen z. B. Oracle EBS, PeopleSoft, Siebel, SAP und auch kundenspezifische Systeme auf Basis von Anwendungsservern, beispielsweise IBM WebSphere, Oracle WebLogic und Oracle AS.

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 – dem „Wer, Was, Wo, Wann und Wie“ jeder SQL Transaktion – 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.

Proaktive Sicherheit in Echtzeit

InfoSphere Guardium bietet zahlreiche Mechanismen, mit denen proaktiv 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 die Abstimmung mit IDS/IPS-Perimetersystemen.

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 Workflow-automatisierung 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.

Auditieren und berichten

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. Beispielsweise überwacht das System

Folgendes:

- Sicherheitsausnahmen wie SQL-Fehler und fehlgeschlagene Anmeldungen
- DDL-Befehle wie „Tabelle erzeugen“, „Tabelle löschen“ oder „Tabelle ändern“, die Datenbankstrukturen ändern und für Data-Governance-Bestimmungen wie SOX besonders wichtig sind
- SELECT-Abfragen, die für Datenschutzbestimmungen wie PCI DSS besonders wichtig sind
- DML-Befehle (Einfügen, Aktualisieren, Löschen), einschließlich Bind-Variablen
- DCL-Befehle, die Accounts, Rollen und Berechtigungen kontrollieren (GRANT, REVOKE)
- Die von der jeweiligen DBMS-Plattform unterstützten prozeduralen Programmiersprachen wie PL/SQL (Oracle) und SQL/PL (IBM)
- XML-Ausführung in der Datenbank

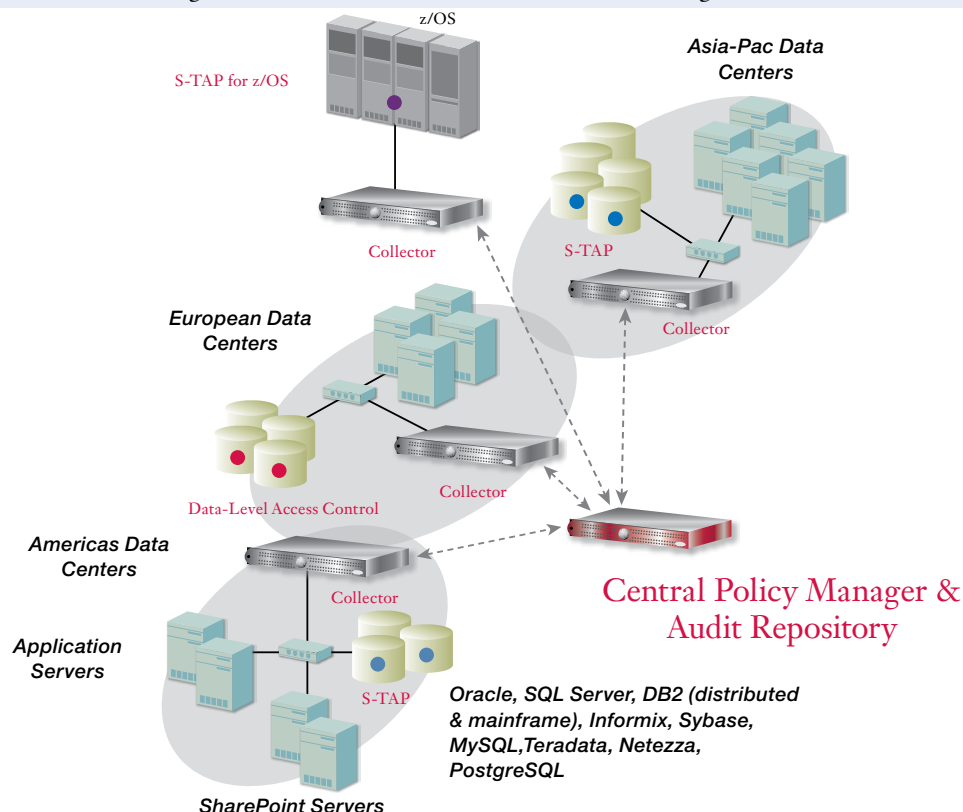
Branchenführendes Reporting

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 an SIEM oder sonstige Systeme exportiert werden.

Skalierbar für Ihr Unternehmen

- **Nicht invasiv:** 100 % Transparenz aller Datenbanktransaktionen – einschließlich des lokalen Zugriffs durch privilegierte Benutzer – ohne Performance-Beeinträchtigung oder Datenbankänderungen.
- **DBMS-unabhängig:** Plattformübergreifende Lösung, die nicht auf datenbankspezifischem Logging oder Audit-Dienstprogrammen beruht.
- **Appliance-basiert:** Modulare Software-Suite, aufgebaut auf einem abgesicherten Linux-Kern, für den schnellen Einsatz mittels „Black Box“-Systemen (autarker Datenspeicher, vorinstallierte Anwendungen, integriertes Management).
- **Flexible Überwachung:** Mittels leichtgewichtiger, hostbasierter Probes, SPAN-Ports, Netzwerk-TAPs oder einer beliebigen Kombination.
- **Infrastrukturbereit:** Unterstützt SNMP, SMTP, Syslog, LDAP, Kerberos, RSA SecurID, Change-Ticketing-Systeme wie BMC Remedy und CEF sowie die Integration mit allen namhaften SIEM-Plattformen.
- **Mehrschichtig:** InfoSphere Guardium verdichtet und normalisiert Auditinformationen aus mehreren Systemen und Speicherorten zu einem einzigen, zentralisierten Auditdepot.
- **Zentralisiertes Management:** Unternehmensweites Management der DBMS-übergreifenden Sicherheitsregeln über eine Webkonsole.
- **Skalierbar:** Wenn die Anzahl der überwachten Server oder das Transaktionsvolumen wächst, können einfach weitere Systeme hinzugefügt werden, um die zunehmende Last zu bewältigen. Patentierte, intelligente Speicher-Algorithmen bieten eine um das Hundertfache bessere Speichereffizienz als traditionelle Verfahren, die bei „flachen“ Dateistrukturen ansetzen.
- **Manipulationssicheres Auditdepot:** Verlässliche Authentifizierung ohne Rootzugriff und verschlüsselte Archive.
- **Rollenbasiert:** Der Zugriff auf Module und Daten richtet sich nach organisatorischen Rollen.



Skalierbare, mehrschichtige Architektur

Die skalierbare Architektur von InfoSphere Guardium unterstützt große wie kleine Umgebungen unternehmensweit – durch die zentralisierte Verdichtung und Normalisierung der Auditdaten und durch zentralisiertes Management der Sicherheitsregeln über eine Webkonsole. S-TAPs sind leichtgewichtige, hostbasierte Probes, die die gesamten Datenbankzugriffe, einschließlich des lokalen Zugriffs durch privilegierte Benutzer, überwachen und an InfoSphere Guardium Collector-Systeme zur Analyse und Berichterstellung leiten. Collector-Systeme erfassen die überwachten Daten aus S-TAPs bzw. per Direktverbindung mit SPAN-Ports in Netzwerkschwitches. Aggregatoren verdichten automatisch die Auditdaten aus mehreren Collector-Systemen. Um maximale Skalierbarkeit und Flexibilität zu erreichen, können Aggregatoren auch mehrschichtig konfiguriert werden. S-GATE ist als Erweiterung der InfoSphere Guardium S-TAPs implementiert, verbessert die Sicherheit und setzt die Aufgabenteilung durch, indem verhindert wird, dass Datenbank-administratoren sicherheitsrelevante Funktionen wie das Anlegen neuer Datenbankaccounts oder die Erhöhung der Zugriffsrechte für vorhandene Accounts ausführen.

Automatisierung des Compliance-Workflows

InfoSphere Guardium vereinfacht den gesamten Compliance-Workflow-Prozess und trägt zur Automatisierung der Audit-berichterstattung, der Verteilung an die Verantwortlichen, der elektronischen Freigabe sowie des Eskalationsprozesses bei. Workflow-Prozesse können zu einem sehr genauen Detaillierungsgrad komplett von den Anwendern angepasst werden, damit spezifische Audits individuell durch Freigaben verteilt und verfolgt werden können.

Einheitliche Lösung für heterogene Umgebungen

Umfassende DBMS-Plattformunterstützung

Die plattformübergreifende InfoSphere Guardium-Lösung unterstützt alle namhaften DBMS-Plattformen und -Protokolle auf allen wesentlichen Betriebssystemen (Windows, UNIX, Linux, z/OS) sowie Microsoft SharePoint und FTP-Umgebungen.

Unterstützte Plattform	Unterstützte Versionen
Oracle Database	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle Database (ASO, SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10, 11,11.50
Sun MySQL und MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.X, 12, 13
FTP	

Hostbasierte Überwachung

Unsere hoch entwickelten S-TAPs sind leichtgewichtige Softwareprobes, die sowohl Netzwerk- als auch lokale Datenbankprotokolle (Shared Memory, Named Pipes usw.) auf Betriebssystemebene des Datenbankservers überwachen. S-TAPs minimieren jede etwaige Beeinträchtigung der Serverperformance, indem sie den gesamten Verkehr für die Echtzeitanalyse und das Reporting auf separate InfoSphere Guardium Appliances umleiten, anstatt eine Verarbeitung und Speicherung von Logdateien auf dem Datenbankserver auszuführen.

S-TAPs werden oft bevorzugt, weil sie ohne dedizierte Hardware-Appliances an externen Standorten oder freie SPAN-Ports im Rechenzentrum auskommen.

Betriebssystem	Version	32-Bit und 64-Bit
AIX	5.2, 5.3,	Beides
	6.1	64-Bit
HP-UX	11.11, 11.23, 11.31	Beides
Red Hat Enterprise Linux	3, 4, 5	Beides
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Beides
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris – SPARC	8, 9, 10	Beides
Solaris – Intel/AMD	10	Beides
Tru64	5.1A, 5.1B	64-Bit
Windows	2000, 2003, 2008	Beides
iSeries	i5/OS*	

Anwendungsüberwachung

Um potenzielle Betrugsfälle zu erkennen, zeichnet InfoSphere Guardium auch die Aktivitäten von Benutzern auf, die nicht per Direktzugriff, sondern über Unternehmensanwendungen auf kritische Tabellen zugreifen. Dies ist erforderlich, weil diese Anwendungen typischerweise einen Optimierungsmechanismus namens „Connection Pooling“ nutzen. In einer Pooling-Umgebung verdichtet sich der gesamte Benutzerverkehr auf wenige Datenbankverbindungen, die nur einen einzelnen generischen Anwendungaccount nutzen und daher keinen Rückschluss auf den eigentlichen Benutzer erlauben. InfoSphere Guardium unterstützt die Anwendungsüberwachung aller namhaften und gängigen Unternehmensanwendungen. Zur Unterstützung weiterer Anwendungen, einschließlich Eigenentwicklungen, kann die Transaktionsüberwachung auf dem Anwendungsserver erfolgen.

Unterstützte Unternehmensanwendungen	<ul style="list-style-type: none"> • Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
Unterstützte Anwendungs-serverplattformen	<ul style="list-style-type: none"> • IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform



IBM InfoSphere Guardium

InfoSphere Guardium ist Bestandteil des IBM InfoSphere Produktportfolios, IBM InfoSphere stellt eine einheitliche Informationsplattform bereit, die Daten und Inhalte aus verschiedenen Silos oder den Systemen verschiedener Anbieter unabhängig von ihrem Typ, ihrem Umfang oder ihrer Komplexität integriert, abgleicht, verwaltet und analysiert und sie den Benutzern, Anwendungen und Geschäftsprozessen im jeweiligen Kontext zur Verfügung stellt. So entsteht eine „Single Version of the Truth“, eine einzige, zuverlässige Version der Daten, die für alle Aspekte von Kunden, Produkten, Konten oder beliebiger anderer Gebiete eine verlässliche Grundlage darstellt. Die Produkte von IBM InfoSphere sind in der Lage, den gesamten Lebenszyklus aller Arten von Informationen (langfristig oder transaktionsorientiert, Daten oder Inhalte) zu verwalten und neue Geschäftsentitäten, Informationsquellen, Definitionen und Nutzungen einfach zu integrieren, wenn sie hinzugefügt oder geändert werden.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo, ibm.com, Guardium und InfoSphere sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark Information“ unter:

ibm.com/legal/copytrade.shtml

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Unternehmen sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2010
Alle Rechte vorbehalten.



Recyclingfähig, bitte der Wiederverwertung zuführen.