Umfassender Schutz der geschäftskritischen Daten

IBM Security Guardium bedeutet Datenanalyse, Datenschutz und Anpassungsfähigkeit für eine ganzheitliche Sicherheit auf Datenebene.

Highlights

- Proaktiver ganzheitlicher Ansatz für den Schutz vertraulicher Daten auf allen Plattformen wie den wichtigsten Datenbankplattformen, Hadoop, NoSQL, Cloud- und Dateisystemen.
- Senkung der Gesamtbetriebskosten durch automatische Erkennung vertraulicher Daten, die proaktive Erkennung von Risiken und Einleitung geeigneter Maßnahmen.
- Schutz vertraulicher Daten gegen interne und externe Bedrohungen durch Verschlüsselung, Maskierung, Schwärzung, Aktivitätsüberwachung, dynamische Blockierung, Alarmierung und Quarantäne.
- Automatisierung von Datencompliance-prozessen, um den richtigen Personen zum richtigen Zeitpunkt die richtigen Berichte zukommen zu lassen.
- Einfache Anpassung an Veränderungen im IT-Umfeld und Unterstützung des gesamten Datenschutzprozesses.

Heute sind Datensicherheitsverletzungen fast an der Tagesordnung – und kostspieliger als je zuvor. Weltweite Studien zeigen, dass die durchschnittlichen Gesamtkosten einer Datenschutzverletzung bei mittlerweile 3,8 Mio. US-Dollar liegen.[1] Hinzu kommt, dass der Verlust von Geschäftsgeheimnissen, Produktentwicklungsdaten oder anderem geistigem Eigentum schnell zum finanziellen Ruin eines Unternehmens führen kann. Vertrauliche Daten stehen aufgrund ihrer Bedeutung bei allen geschäftlichen Interaktionen immer im Mittelpunkt – und sind daher auch für Hackerattacken äußerst attraktiv.

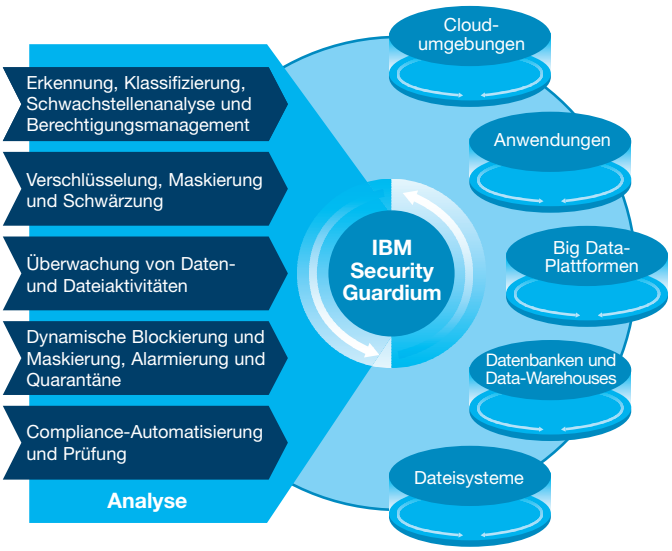
Bisher haben sich die Unternehmen beim Schutz ihrer vertraulichen Informationen immer auf eine konventionelle perimeterbasierte Verteidigungsstrategie verlassen. Konventionelle Tools wie Antivirensoftware und Firewalls sind jedoch für die intelligenten Sicherheitsbedrohungen von heute nicht ausreichend. Hinzu kommt, dass die Datenmenge immer größer wird, sich kontinuierlich verändert und Daten mobil sind. Die richtigen Datenschutzmechanismen müssen also entsprechend anpassungsfähig sein. Immer mehr Benutzer, Anwendungen und Systeme brauchen sofortigen Zugriff auf die unterschiedlichen Typen an vertraulichen Daten. Diese Daten können sich in Datenbanken, Data-Warehouses, gemeinsam genutzten Dateibereichen (File-Shares), Big Data-Plattformen, Cloudumgebungen usw. befinden oder dort repliziert werden. Die Aufgabe, genau zu verfolgen, wer Zugriff auf diese dynamischen, dezentralen und unterschiedlichen Daten hat und wer sie (mit wem) teilt, scheint unlösbar zu sein.

IBM Security Guardium, das bisher unter dem Namen IBM InfoSphere Guardium vertrieben wurde, kann helfen, kritische Daten unabhängig von ihrem Standort zu sichern. Mit dieser umfassenden Datenschutzplattform können Sicherheitsteams automatisch alle Vorgänge in der Datenumgebung analysieren. So lassen sich Risiken minimieren und vertrauliche Daten gegen interne und externe Bedrohungen schützen. Auch die schnelle Anpassung an Veränderungen, die sich auf die Datensicherheit auswirken können, ist gewährleistet.

Zählen Sie auf umfassende Datensicherheit

Guardium bietet einen umfassenden Lösungsansatz für den Schutz der vertraulichen Daten in einem Unternehmen, die für den Erfolg und das Weiterbestehen des Unternehmens besonders wichtig sind. Über die durchgängige grafische Benutzeroberfläche können Sicherheitsverantwortliche Risiken für vertrauliche Daten schnell ermitteln und dagegen angehen. Dabei spielt es keine Rolle, ob die Daten in Bewegung sind oder es sich um statische Daten handelt. Dieser einheitliche Ansatz lässt sich auch auf zahlreiche Repositorys mit strukturierten und unstrukturierten Daten anwenden. Hierzu gehören Datenbanken, Data-Warehouses, Hadoop-, NoSQL-, In-Memory-Systeme, File-Shares usw.

Guardium bietet ein hohes Maß an Flexibilität, um den unterschiedlichsten Anforderungen an Datensicherheit und -schutz gerecht zu werden. Dies reicht von der grundlegenden Einhaltung von Vorschriften bis zum umfassenden Datenschutzkonzept – und zwar auf kosteneffiziente und skalierbare Weise. Diese mehrschichtge Lösung ermöglicht die automatisierte Analyse von Bedrohungen für Datenbestände, den Schutz dynamischer Daten sowie eine unternehmensweite Transparenz, um sich schnell auf Änderungen in Umgebungen mit vertraulichen Daten einzustellen.



Guardium nutzt Analyse- und Automatisierungstechniken für den Schutz vertraulicher Daten in den heutigen heterogenen Umgebungen.

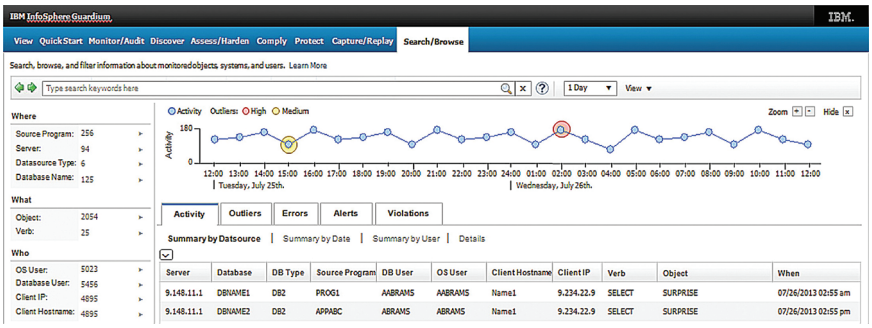
Bedrohungen für vertrauliche Daten analysieren

Für einen wirksamen Datenschutz müssen Unternehmen verstehen, was genau sie schützen müssen, und dann die geeigneten Maßnahmen einleiten. Guardium bietet Sicherheitsteams folgende Möglichkeiten:

- Automatische Erkennung und Klassifizierung vertraulicher Daten – und Aufdeckung von Compliancerisiken.
- Genaue Kenntnis der Benutzer, die auf die Daten zugreifen, Erkennung von Anomalien und Verhindern von Datenverlusten.
- Schnelle Analyse von Datennutzungsmustern zur Aufdeckung und Behebung von Risiken.

Guardium hilft den Sicherheitsteams, über eine benutzerfreundliche grafische Benutzeroberfläche vertrauliche Informationen automatisch zu erkennen und zu klassifizieren. Über eine Reihe von Schritten können Sicherheitsteams alle Datenquellen mit schutzwürdigen Informationen ermitteln (beispielsweise nicht katalogisierte Datenbanken). Mithilfe anpassbarer Klassifizierungsbezeichnungen und Berechtigungsmanagementfunktionen kann dann die Durchsetzung von Sicherheitsrichtlinien ebenfalls automatisiert erfolgen. Die Ermittlung vertraulicher Daten kann so terminiert werden, dass sie regelmäßig erfolgt. So wird verhindert, dass Rogue-Server ins System gelangen, und sichergestellt, dass keine kritischen Informationen übersehen werden.

Als Unterstützung bei der Durchsetzung von Richtlinien und beim Schutz vertraulicher Daten kann Guardium kontinuierlich in Echtzeit überwachen, wer auf vertrauliche Daten zugreift (oder dies versucht). Über die traditionelle Datenüberwachung hinaus verfügt Guardium über Funktionen für die automatische Erkennung von Ausreißern. Dabei hilft Guardiums Intelligenz bei der Analyse und beim Verständnis von Risiken auf Basis von veränderten Verhaltensweisen. Guardium verwendet hierfür einen erweiterten fortschrittlichen Machine Learning-Algorithmus, über den sich unberechtigte Aktionen auf Basis detaillierter Kontextinformationen erkennen lassen – also die Fragen „Wer, was, wo, wann und wie“ bei jedem Datenzugriff. Über einen adaptiven Lernprozess vergleicht Guardium dann die normalen Aktivitätsmuster mit neuen Aktivitäten, sobald diese gehäuft auftreten. Die intuitive Benutzeroberfläche hilft bei der Ermittlung von Anomalien, sodass Administratoren die Ursachen bis ins Detail untersuchen können.



Guardium bietet eine benutzerfreundliche grafische Oberfläche für die Erkennung von und Reaktion auf Ausreißer, die über einen intelligenten Algorithmus entdeckt wurden.

Neben dieser Drilldownfunktionalität können Sicherheitsmitarbeiter mit Guardium nach Auditberichten und anderen Elementen innerhalb der Benutzeroberfläche suchen sowie schnell und unternehmensweit den gesamten Datenbestand durchforsten. Das genaue Verständnis der zugrundeliegenden Topologie, Aggregations- oder Lastverteilungsschemata ist nicht erforderlich. Über entsprechende Suchanforderungen lassen sich aussagekräftige Informationen aus bestimmten Datenzugriffsaktivitäten extrahieren – unabhängig davon, ob sich diese auf bestimmte Datenquellen, Benutzer oder Datumsangaben beziehen. Über das neue Untersuchungsdashboard können ebenfalls Muster, Anomalien und Beziehungen in den Daten sichtbar gemacht werden. Dadurch wird der Suchbereich mithilfe von bewährten Standardansichten eingegrenzt. Dann wäre noch die Funktion des Connection Profiling zu nennen, die alle Versuche einer Verbindungsherstellung zu einer bestimmten Datenquelle in Berichtsform aufzeichnet.

Schutz vertraulicher Daten

Die zunehmenden Sicherheitsrisiken für vertrauliche Daten und die wachsenden Compliancevorgaben zwingen die Unternehmen, ihre Datenschutzstrategien auf den Prüfstand zu stellen. Guardium bietet Sicherheitsteams hier folgende Möglichkeiten:

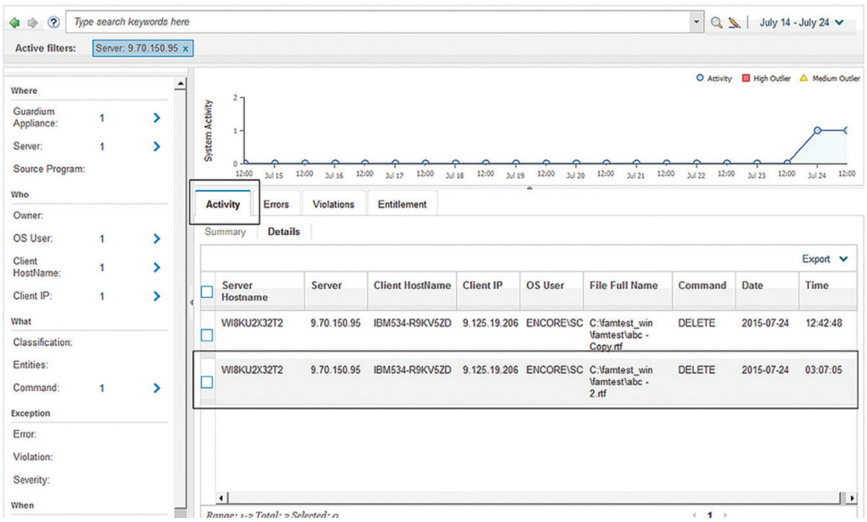
- Abschirmung des Unternehmens gegen finanzielle Risiken durch automatisierte Datencomplianceprozesse und umfangreiche Prüffunktionen.
- Kontrolle kritischer Daten durch Verschlüsselung, Maskierung, Schwärzung, dynamische Blockierung, Alarmierung und Quarantäne.
- Überwachung von Aktivitäten in Echtzeit und Nutzung von Blockierungsmechanismen gegen unerlaubten Daten- und Dateizugriff von innerhalb und außerhalb des Unternehmens.

Guardium hilft bei der Erfassung und Prüfung des gesamten vertraulichen Datenverkehrs. Dies umfasst auch den lokalen Zugriff durch privilegierte Benutzer. Diese Informationen werden in einem sicheren und manipulationssicheren Auditprotokoll gespeichert. Letztendlich steht den Benutzern ein zentrales und normalisiertes Audit-Repository für unternehmensweite Complianceberichte, Maßnahmen zur Leistungsoptimierung, weitere Untersuchungen und forensische Tätigkeiten zur Verfügung. Unternehmen können den gesamten Prüfprozess

für die Datencompliance – u. a. auch die Verteilung des Berichts an die Teamleitung, Freigabe und Eskalation – mithilfe von vorkonfigurierten Berichten für Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS) und Datenschutzzwecke automatisieren.

Hinzu kommt, dass Sicherheitsteams mit Guardium vertrauliche Daten gegen interne und externe Bedrohungen durch dateibasierte Verschlüsselungen, durch Maskieren statischer Daten und mithilfe von Schwärzungsfunktionen schützen können. Außerdem unterstützt Guardium dynamische Datenmaskierungen und -verschlüsselungen in Echtzeit sowie das Blockieren oder unter Quarantäne Stellen verdächtiger Benutzer mit den entsprechenden Alarmierungen. Mit Guardium können auch Zugriffsversuche von nicht berechtigten Personen auf vertrauliche Daten bei den meisten Datenquellen wie Cloudumgebungen, Big Data-Plattformen und Dateisysteme beschränkt werden.

Guardium hilft auch bei der Durchsetzung der Gewaltentrennung. Hierfür werden alle Aktivitäten im Zusammenhang mit vertraulichen Daten fortlaufend überwacht. Dies umfasst auch die Echtzeitüberwachung des Zugriffs auf Dateisysteme. Dadurch können Unternehmen nicht berechtigte und verdächtige Aktivitäten auch von privilegierten Benutzern erkennen, protokollieren und blockieren. So kann Guardium beispielsweise das massenhafte Kopieren von sicherheitskritischen Dateien/Verzeichnissen oder eine plötzliche Lastspitze bei Dateizugriffsaktivitäten eines bestimmten Administrators erkennen, Alarme wegen falscher Zugriffsaktivitäten ausgeben, den Zugriff auf besonders vertrauliche Dokumente blockieren und benutzerspezifische Berichte für alle Aktivitäten generieren.



Mit der in Guardium möglichen Überwachung von Dateiaktivitäten können Unternehmen verdächtige Aktivitäten erkennen und blockieren – auch bei privilegierten Benutzern.

An Veränderungen anpassen

Dateninfrastrukturen verändern sich dauernd und werden immer größer und komplexer. Dadurch wird es immer schwieriger, mit neuen und sich verändernden Sicherheitslücken mitzuhalten. Guardium bietet Unternehmen hier folgende Möglichkeiten:

- Unterstützung traditioneller neuer Datentechnologien wie Hadoop, NoSQL und Cloud.
- Einfache Erweiterung der Datenschutzarchitektur für die Einhaltung neuer gesetzlicher Bestimmungen oder den umfassenden Datenschutz.
- Reduzierung von Kosten und bessere Ergebnisse durch eine zentrale Infrastruktur für den Datenschutz, die in der gesamten Datenumgebung automatisch für eine ausgewogene Lastverteilung sorgt.

Mit Guardium können sich Unternehmen schneller an Veränderungen in der Datenumgebung anpassen und den Datenschutz auf neue Benutzer, Plattformen und Datentypen ausdehnen. Die umfassende Plattformausrichtung beinhaltet auch die Unterstützung konventioneller Datenbanken, Cloud-umgebungen, Hadoop-basierten Systemen sowie NoSQL und In-Memory-Systemen. Guardium überzeugt durch seine flexiblen Kontrollmechanismen, die zunächst für bestimmte Compliance-Anforderungen eingesetzt und dann ohne großen Aufwand so angepasst werden können, dass sie bei weiteren Geschäftsanforderungen zusätzlichen Schutz bieten.

Im Gegensatz zu Einzellösungen unterstützt Guardium die heterogene Integration in andere leistungsfähige Sicherheits-lösungen in der Branche, Standards für Sicherheitslücken, Anwendungen und vieles mehr. Guardium lässt sich auch problemlos in IBM Security-Lösungen wie IBM Security QRadar SIEM einbinden und trägt so zu einem proaktiven Datenschutz bei. Dabei sendet Guardium alle ermittelten Ereignisse und Informationen zur Datenbankerkennung und -klassifizierung an QRadar SIEM, sodass eine wirksamere Korrelation von Bedrohungsaktivitäten gewährleistet ist. Außerdem kann Guardium Status- und Alarmbenachrichtigungen von QRadar SIEM empfangen und so helfen, einen erweiterten Schutz gegen fehlerhafte IP-Quellen, unseriöse Benutzer und neue Schwachstellen zu bieten – sei es in Anwendungen, Betriebssystemen oder anderen Datenquellen. Die Integration von Guardium in QRadar kann Unternehmen beispielsweise in folgenden Fällen helfen: Schutz gegen mögliche anwendungs-basierte Angriffe, Erkennung von Datenbankattacken (wie SQL-Injection) und Blockieren solcher Attacken, bevor Daten extrahiert werden können, Erkennung von Schwachstellen auf der Anwendungsebene, um Korrekturen durch virtuelle Patches vornehmen zu können.

Guardium bietet auch branchenübergreifend ein großes Nutzenpotenzial

- **Ein großes Versicherungsunternehmen kann nun sein Sicherheits-konzept für ca. 1.000 Datenbanken mit nur einem in Vollzeit beschäftigten Mitarbeiter verwalten.**
- **Ein großes Versorgungsunternehmen erzielte einen Return-on-Investment von 55 Prozent in weniger als einem Jahr und stellte die Einhaltung der SOX- und PCI-Vorgaben für 4,5 Millionen Kunden sicher.**
- **Eine internationale Bank kann nun über 5.000 Datenquellen (z. B. Big Data-Transaktionen) in Echtzeit überwachen – ohne dass dies Auswirkungen auf das Leistungsverhalten kritischer Anwendungen hat.**
- **Ein internationales Telekommunikationsunternehmen ist nun in der Lage, Datenzugriffsaktivitäten auf tausenden von Datenbanken, die auf 16 Rechenzentren auf der ganzen Welt verteilt sind, zentral zu überwachen und in Echtzeit entsprechend zu reagieren.**
- **Ein Automobilhersteller kann 500 Produktionsdatenbanken überwachen und auditieren und so die Sicherheit erhöhen. Gleichzeitig konnte der Personalaufwand für Sicherheit um 90 Prozent reduziert werden.**

Warum IBM?

Weltweit vertrauen Unternehmen bei der Datensicherheit auf Lösungen von IBM Security. Bewährte Technologien unterstützen Unternehmen beim Schutz ihrer geschäftskritischen Ressourcen gegen Sicherheitsbedrohungen. Sobald neue Sicherheitsrisiken auftreten, kann IBM Unternehmen mit einem umfassenden Portfolio an Produkten, Services und Business Partner-Lösungen beim Aufbau einer zentralen Sicherheitsinfrastruktur helfen.

IBM verfügt über fundierte Erfahrung bei der weltweiten Servicebereitstellung auch in einigen der am strengsten regulierten Branchen wie Behörden, Gesundheitswesen und Finanzdienstleistungen. Als strategischer Partner hilft IBM Kundenunternehmen, Sicherheitslücken zu schließen und Risiken auch in sehr komplexen IT-Umgebungen zu managen.

Weitere Informationen

Wenn Sie mehr über IBM Security Guardium erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter: **ibm.com**/guardium

Informationen zu IBM Security-Lösungen

IBM Security bietet beim Thema Unternehmenssicherheit eines der innovativsten Produkt- und Serviceportfolios mit dem höchsten Integrationsfaktor. Das Lösungsportfolio, das von der weltweit anerkannten IBM X-Force-Forschungs- und Entwicklungsgruppe unterstützt wird, stellt Sicherheitsdaten bereit, mit denen Unternehmen mit einem ganzheitlichen Ansatz Mitarbeiter, Infrastrukturen, Daten und Anwendungen schützen können. Hierfür steht eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche zur Verfügung: Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social Media- und andere Geschäftsarchitekturen implementieren. IBM betreibt eine der weltweit größten Organisationen im Bereich der Erforschung, Entwicklung und Bereitstellung von Sicherheitslösungen, verwaltet die Überwachung von 15 Mrd. Sicherheitsereignissen pro Tag in mehr als 130 Ländern und besitzt über 3.000 Sicherheitspatente.

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

[1] „2016 Cost of Data Breach Study: Global Analysis“, Ponemon Institute, Juni 2016. **ibm.com**/security/data-breach/

Bitte der Wiederverwertung zuführen

WGS03063-DEDE-00