imperva

DATENBLATT

# Imperva Data Security

## Reduzieren Sie das Risiko einer Datenschutzverletzung bei gleichzeitiger Ermöglichung der digitalen Transformation

Die Landschaft der Datensicherheit verändert sich rasant, und die heutige Digital- und Wissensökonomie befeuert das exponentielle Datenwachstum mit beispiellosem Nutzerzugriff. Da mehr legitime Benutzer auf mehr Daten zugreifen, um den Wert für das Unternehmen zu steigern, sollte Ihre Sicherheitsstrategie einen datenzentrierten Ansatz verfolgen. Dies ermöglicht den kompletten Zugriff auf Daten, anstatt den Zugriff standardmäßig zu sperren und zu beschränken. Imperva Data Security hilft Unternehmen dabei, die Potenz ihrer Daten freizusetzen und gleichzeitig das Risiko einer Datenschutzverletzung zu verringern.

## Versteckte Risiken durch Entdeckung und Bewertung aufdecken

Ein wesentlicher Schritt beim Schutz der Daten ist die Aufdeckung von Schwachstellen, wie bösartige oder gefährdete Datenbanken. Durch diese Schwachpunkte entstehen Sicherheitsrisiken, da Angreifer versteckte oder falsch konfigurierte Datenbanken ausnutzen können, die sensible Daten enthalten. Imperva Data Security hilft Unternehmen, das Risiko einer Datenschutzverletzung zu verringern, indem sie sensible Daten lokalisiert und Datenbank-Schwachstellen identifiziert.

Imperva Data Security entdeckt Datenbanken im Netzwerk, klassifiziert sensible Daten und erkennt Datenbank-Schwachstellen. Entdecken Sie Datenbanken, indem Sie bestimmte Netzwerksegmente nach Bedarf oder in planmäßigen Abständen scannen. Sobald Datenbanken entdeckt werden, klassifiziert Imperva Data Security die in der Datenbank gespeicherten Daten mithilfe eines Wörterbuchs und Muster-Matching-Klassifizierungsmethoden. Führen Sie Bewertungen von Sicherheitslücken mit mehr als 1.500 vordefinierten Schwachstellenprüfungen durch, die auf CIS und DISA STIG-Benchmarks basieren.

## Erkennen und stoppen Sie Datenschutzverletzungen mithilfe kontinuierlicher Datenüberwachung und -analyse

Um das Risiko einer Datenschutzverletzung zu mindern, müssen Unternehmen sehen können, wer auf welche Daten zugreift und ob diese Datenzugriffsaktivitäten gut oder schlecht sind. Doch die heute eskalierende Bedrohungslandschaft, das exponentielle Datenwachstum und die zunehmende Anzahl der Nutzer mit berechtigtem Zugriff auf Daten machen es unmöglich, festzustellen, ob ein Datenzugriff in Ordnung ist, indem man sich nur auf rollenbasierte Zugangskontrollen verlässt.

### WICHTIGE MERKMALE UND VORTEILE

- Daten-Bedrohungen mithilfe von Datenwissenschaft, Maschinenlernen und Verhaltensanalytik erkennen und priorisieren
- Riskante Datenzugriffsaktivitäten direkt lokalisieren – für alle Nutzer, einschließlich privilegierter Nutzer
- Mehr Einsicht durch Überwachung und Prüfung aller Datenbankaktivitäten
- Schutz von Daten durch Echtzeit-Benachrichtigung oder Sperrung des Benutzerzugriffs bei Verstößen gegen die Richtlinien
- Verdeckte Risiken mit Datenentdeckung, Klassifizierung und Schwachstellenbewertung aufdecken
- Angriffsfläche mit statischer Datenmaskierung reduzieren

Imperva Data Security bietet eine kontinuierliche Überwachung mit der Trennung von Aufgaben. Es erfasst und analysiert alle Datenbankaktivitäten sowohl seitens der Anwendung als auch seitens privilegierter Benutzerkonten, indem es detaillierte Protokolle bereitstellt, die zeigen, wer wann auf welche Daten zugreift und was mit den Daten gemacht wurde. Unsere robuste Security-Rules-Engine ermöglicht es Unternehmen, Sicherheitsrichtlinien anzupassen, und bietet Echtzeit-Warnungen oder Sperren bei Verstößen gegen die Richtlinien.

Imperva Data Security legt Nachdruck auf eine einheitliche Sicherheits- und Compliance-Politik in heterogenen Datenumgebungen. Es standardisiert Protokollereignisse über verschiedene Plattformen hinweg und bietet einen konsistenten Überblick über relationale Datenbanken, Mainframes, Big-Data-Plattformen und Datenlager. Es unterstützt auch Datenbanken in Microsoft Azure und Amazon Web Services (AWS) – Dazu gehören PaaS-Angebote wie Azure SQL und Amazon Relational Database Services (RDS). Detaillierte Datenaktivität wird automatisch erfasst, was die Erfüllung von Prüfungsanforderungen sehr erleichtert.

Um gefährliche Datenzugriffsaktivitäten aufzudecken, die die Organisation einem höheren Risiko einer Datenschutzverletzung aussetzen, nutzt Imperva Data Security Datenwissenschaft, maschinelles Lernen und Verhaltensanalysen. Die Datenrisikoanalysefähigkeiten erstellen eine kontextbezogene Verhaltensbasis, indem sie das Nutzerverhalten und die Informationen über Datenbank-Aktivitäten analysieren, um normales Verhalten von „normalem, aber nicht richtigem Verhalten“ zu unterscheiden. Es destilliert Millionen von Datenzugriffsereignissen und zeigt hochriskante Vorfälle an, wodurch sich die Zahl der Alarme auf eine Handvoll überschaubarer Berichte reduziert (siehe Abbildung 1). Es priorisiert diese kritischen Vorfälle dann, indem es Gruppierungs- und Scoring-Fähigkeiten einsetzt. Vorfälle werden in einfacher Sprache erklärt, sodass Sicherheitsteams besser reagieren können (siehe Abbildung 2). Dadurch werden nur wenige hochriskante Zwischenfälle und deutlich weniger Vorfälle an einen SIEM geschickt.

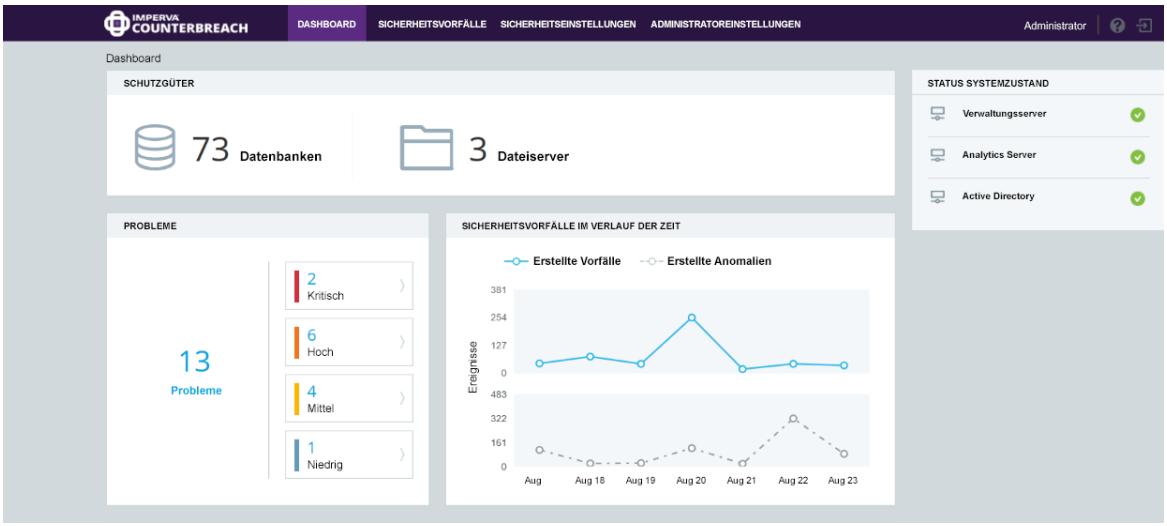


Bild 1: Das Dashboard lässt sich leicht lesen und ermöglicht es Sicherheitsexperten, sich auf wenige risikoreiche Vorfälle zu konzentrieren.


Bild 2: Vorfälle werden mit einer Risiko-Bewertung versehen und mit verwandten Vorfällen gruppiert, die Sicherheitsexperten handlungsfähige Einblicke geben, um schnell reagieren zu können.

## Angriffsfläche mit statischer Datenmaskierung reduzieren

Da Organisationen versuchen, den Wert der Daten, die sie speichern, zu nutzen, werden Kopien von Produktionsdaten für nicht-produktive Umgebungen wie Entwicklung, Test, Forschung und Analytik sowie Outsourcing, erstellt. Branchenanalysten schätzen, dass 82 % der Organisationen mehr als 10 Exemplare jeder Produktionsdatenbank besitzen.[1] Die exponentielle Verbreitung sensibler Produktionsdaten in einem Unternehmen erhöht das Risiko von Datenschutzverletzungen und Verstößen gegen die Compliance. Um Datenschutzverletzungen und Verstöße gegen die Compliance zu verringern, können Unternehmen die Angriffsfläche reduzieren, indem sie die Landschaft der sensiblen Daten verkleinern.

Die statischen Datenmaskierungsfunktionen von Imperva Data Security bieten eine proaktive Steuerung, die sensible Daten vor unnötiger Veröffentlichung schützt und gleichzeitig datengesteuerte Geschäftsprozesse ermöglicht. Es de-identifiziert Daten, sodass die Daten den Gegenstand nicht mehr direkt identifizieren können. Mit einer Vielzahl von Transformationstechniken ersetzt es reale Daten, die sensible Informationen enthalten, durch fiktive, aber qualitativ hochwertige realistische Daten, die funktional und statistisch genau sind. Die Originaldaten enthalten zum Beispiel eine Aufzeichnung von Adam Smith, der 60 Jahre alt ist, und seine SVN ist 123-44-5555. Nachdem die Daten maskiert wurden, könnten sie zu Tom White, 56 Jahre alt, mit der SVN 747-88-9999 werden.

**ORIGINALDATEN**

| NAME | SVN | ALTER | GESCHLECHT |
|---|---|---|---|
| Adam Smith | 123-44-5555 | 60 | Männlich |
| Jenny Park | 987-65-4321 | 28 | Weiblich |

**MASKIERTE DATEN**

| NAME | SVN | ALTER | GESCHLECHT |
|---|---|---|---|
| Tom White | 747-88-9999 | 56 | Männlich |
| Amy Kim | 747-88-9998 | 24 | Weiblich |

Bild 3: Beispiel Datenmaskierung

FlexProtect ist ein flexibler Ansatz zur Datensicherung. Eine Einzellizenz bietet Ihnen die Möglichkeit, Imperva Data Security bereitzustellen, wie und wann immer sie es benötigen. Sie sind geschützt, unabhängig von der Anzahl, dem Ort oder der Art der verwendeten Geräte oder Dienste. FlexProtect hilft Ihnen, Ihre Daten überall dort zu schützen, wo immer sie sich befinden – in der Cloud, vor Ort oder in einer Hybrid-Konfiguration.

### FLEXPROTECT-VORTEILE

- Reduzieren Sie die Kosten der Unsicherheit beim Umzug in die Cloud
- Prognostizieren Sie Kosten, auch wenn sich Ihre Infrastruktur in der Cloud und vor Ort im Laufe der Zeit verändert
- Skalierbar, um sich dem Wachstum Ihres Geschäfts anzupassen

[1]Copy Data Management Report, IDC, April 2016

**Imperva ist ein von Analysten anerkannter führender Anbieter von Cybersicherheit, der sich für den Kampf zur Sicherung von Daten und Anwendungen einsetzt, wo immer sie sich befinden.**

+ 1 (866) 926-4678
imperva.com



imperva