IMPERVA®

Imperva SecureSphere Data Security

DATENBLATT

Kritische Daten schützen und überprüfen

Konnektivität und der einfache Zugang zum Internet haben völlig neue Formen der Cyber-Kriminalität hervorgebracht. Daher betrachten Verbraucher, Unternehmen und Regierungen die Verantwortung für den Schutz sensibler Daten heute anders. Neben den tatsächlichen Ermittlungskosten, Compliance-Strafen und möglichen Markenschäden muss ein ganz neuer Aspekt beachtet werden. Durch einen aktuellen Gerichtsentscheid[1] hat die Definition des Begriffs „Kundenschaden" eine wesentliche Veränderung erfahren. Das Gericht erkannte Verbrauchern, deren personenbezogene Daten bei einem Datensicherheitsverstoß gestolen wurden, den Sammelklagenstatus zu. Angesichts dieser Entwicklung können die Haftungskosten, die nach einem Datenverlust auf ein Unternehmen zukommen, exponentiell wachsen, wenn man die Rechtskosten und die Kosten für die Schadenregulierung hinzunimmt.

Die Haftungskosten, die nach einem Datenverlust auf ein Unternehmen zukommen, können exponentiell wachsen, wenn man die Rechtskosten und die Kosten für die Schadenregulierung hinzunimmt.

Erstklassiger Datenschutz und überragendes Auditing

Imperva ist die erste Wahl, wenn es um den Schutz sensibler Geschäftsdaten und Anwendungen in der Cloud und vor Ort geht. SecureSphere-Datenschutzlösungen decken alle Bereiche von Datensicherheit und Compliance ab. Dabei beeinträchtigen die branchenführenden Funktionen für Datenbank-Auditing und Echtzeitschutz weder Leistung noch Verfügbarkeit. Mit seiner skalierbaren, mehrstufigen Architektur unterstützt SecureSphere selbst die größten Datenbank- und Big-Data-Installationen. Imperva SecureSphere automatisiert Sicherheit und Compliance. Deshalb ist es nicht überraschend, dass die Lösung von zahlreichen Unternehmen für den Schutz ihrer wertvollsten Ressourcen eingesetzt wird.

[1] 7th Circuit Court of Appeals, Richterin Diane Wood, Erfolgreiche Klage gegen Neiman Marcus wegen eines Datensicherheitsverstoßes

Imperva SecureSphere

- Sensible Datenbanken lokalisieren und klassifizieren
- Exzessive Benutzerrechte und inaktive Benutzer identifizieren und einen durchgängigen Überprüfungszyklus für Berechtigungen ermöglichen
- RDBMS, Data Warehouses, Big-Data-Plattformen und Mainframe-Datenbanken schützen
- Datenbankangriffe und nicht autorisierte Aktivitäten in Echtzeit melden, isolieren und abblocken
- Compliance-Aufgaben und Berichterstellung automatisieren und planen

Daten an der Quelle schützen

SecureSphere für die Überwachung der Datensicherheit und unabhängige Erstellung von Prüfprotokollen für Compliance-Zwecke

- Nur die Aktivitäten protokollieren, für die es erforderlich ist, aber alle Aktivitäten auf Sicherheitsverstöße überwachen
- Datenbanken mit großem Transaktionsvolumen überwachen und schützen
- Verdächtiges Verhalten sofort blockieren – im Kontext untersuchen
- Sicherheits-Alerts, die mehrere Aktionen umfassen, ausführen, um Engpässe und Verzögerungen zu vermeiden
- Umfassender Datenbankschutz durch SecureSphere Web Application Firewall, Schutz vor Account-Takeover und Schadsoftware sorgt für Multifaktor-Datensicherheit

Compliance-Anforderungen einhalten

SecureSphere hilft Unternehmen dabei, Compliance-Vorschriften wie PCI DSS, SOX, My Number und HIPAA einzuhalten.

- Deckt nahezu alle Compliance-Anforderungen für Datenbanken mit vordefinierten Richtlinien und Berichten ab
- Neue und modifizierte Richtlinien schnell konfigurieren und implementieren – keine DBA-Beteiligung erforderlich
- Strikte Trennung von Aufgaben mit manipulationssicheren Prüfdaten
- Automatisierte Aktualisierungen während des Betriebs minimieren die Zahl der Neustarts und die sich daraus ergebenden Prüfdatenlücken.
- Flexible, schnelle Anpassung an sich verändernde IT-Umgebungen und Compliance-Anforderungen
- Überwachung von Datenbanken, die in der Microsoft Azure-Cloud oder der Amazon AWS-Cloud implementiert sind
- Einschränkung des Zugriffs auf sensible Daten durch Datenmaskierung

Datenschutz und -prüfung sind unternehmensweit ein Muss

Hacker und Datendiebe interessiert es nicht, wer in einem Unternehmen für die Datensicherheit oder Compliance verantwortlich ist – sie wollen Daten stehlen, um sich persönlich zu bereichern. Der Einsatz von Multi-Vektor-Angriffen veranschaulicht, wie sie Team- und Systemsilos nutzen können, um Sicherheitsmaßnahmen zu umgehen. Ein DDoS-Angriff dient der Ablenkung. Währenddessen nutzt ein anderer Vektor des Angriffs kompromittierte Anmeldedaten, die der Hacker mithilfe einer Spear Phishing-E-Mail und Schadsoftware erlangt hat, um Tausende von Datensätzen zu stehlen. Manuelle Überwachung und isolierte Sicherheitsmaßnahmen können den Datendiebstahl nicht aufhalten. Korrelierte Sicherheits-Dashboard-Übersichten helfen zwar, aber wenn Alerts das System überfluten, bleibt der „wirkliche" Angriff möglicherweise über Wochen oder länger unerkannt. Die proaktive Sicherheitsüberwachung auf Datenebene ist die letzte Möglichkeit, laufende Datenangriffe zu stoppen. Durch die Integration mit einer Web Application Firewall, Anti-Schadsoftware-Lösungen und anderen Sicherheitsmaßnahmen verbessert sich die Datensicherheitslage zugunsten des Unternehmens. Datendiebe kommen nicht zum Zuge, und IT-, Sicherheits- und Compliance-Teams können ihre sich überschneidenden Datenschutzziele gemeinsam erreichen und dabei die Compliance-Vorgaben und -Vorschriften einhalten.

SecureSphere Database Assessment bestimmt genau, wo sich sensible Daten befinden und ermöglicht eine risikobasierte Priorisierung, die Unternehmen dabei hilft, ihre Risikominimierungsprogramme, -systeme und -richtlinien zu planen.

Datensicherheit mit Imperva Secure Sphere

Datensicherheit beginnt mit Data Discovery

Voraussetzungen für den Schutz und die Überwachung von Daten sind die Erkennung und Klassifizierung der sensiblen Daten. Kleinere Unternehmen können dies möglicherweise durch manuelle Untersuchungen und Prüfungen leisten. Mit zunehmender Unternehmensgröße wächst jedoch auch die Zahl der Datenbanken beinahe exponentiell. Die automatische Erkennung und Klassifizierung ist die einzige zuverlässige Möglichkeit, neue oder veränderte Datenbankinstanzen routinemäßig und konsequent zu erkennen und zu klassifizieren, die zuvor unbekannte sensible Daten enthalten. SecureSphere Database Assessment lokalisiert sensible Daten und ermöglicht eine risikobasierte Priorisierung, um Unternehmen die Planung ihrer Programme, Systeme und Richtlinien zur Risikominimierung zu erleichtern.

Durchgängige Überwachung der Nutzung sensibler Daten

Selbst bei intensivem Datenbankverkehr prüft SecureSphere durchgängig auf Verstöße gegen die Sicherheitsrichtlinien und Einhaltung der Compliance-Anforderungen. Dank der höchst effizienten Dual-Channel-Überwachung für unterschiedliche Zwecke können Unternehmen mit einer einzigen Lösung sowohl Sicherheits- als auch Compliance-Belange abdecken.

SecureSphere analysiert alle Datenbankaktivitäten in Echtzeit. Damit steht Unternehmen ein Tool zur Verfügung, das Sicherheitsrichtlinien proaktiv durchsetzt. Ein detailliertes Prüfprotokoll zeigt „Was, Wann, Wo und Wie"-Informationen für jede Transaktion. SecureSphere prüft die privilegierten Benutzer, die direkt auf den Datenbankserver zugreifen, sowie solche Benutzer, die über einen Browser, eine mobile oder Desktop-basierte Anwendung auf die Datenbank zugreifen.

Überwachung von Big Data-, SharePoint- und Dateispeichern

Datenbanken sind und bleiben zwar eines der Hauptziele von Cyber-Diebstahl, aber sensible Daten sind im gesamten Unternehmen auf vielen verschiedenen Systemen verteilt. SecureSphere automatisiert die schwierigsten Aspekte der einheitlichen Richtlinienimplementierung und -überwachung über verschiedene Datenbanken, Big Data-, SharePoint- und Dateispeicher hinweg.

- Der SecureSphere Agent für Big Data erweitert den SecureSphere Data Activity Monitor auf führende Big Data-Angebote wie MongoDB, Cloudera, IBM BigInsights und Hortonworks-Produkte.
- SecureSphere File Security-Produkte ermöglichen neben der Überwachung und Prüfung auch das Security und User Rights Management für Dateien, die in SharePoint, auf Dateiservern und NAS-Geräten (Network Attached Storage) gespeichert sind, in Echtzeit.

Im Gegensatz zu Lösungen, für die eine DBA-Beteiligung sowie kostenaufwändige Professional Services erforderlich sind, beinhaltet SecureSphere die notwendigen Verwaltungs- und Zentralisierungsfunktionen für das Management zahlreicher Datenbanken, Big Data-Knoten und Datei-Repositorys.

Erkennung von nicht autorisierten Zugriffen und betrügerischen Aktivitäten

Administratoren können mit SecureSphere Richtlinien definieren, die präzise überwachen und kontrollieren, wie die Benutzer auf Datenobjekte zugreifen. Mithilfe der patentierten Technologien Dynamic Learning Method (DLM) und Adaptive Normal Behavior Profile (NBP) von Imperva erstellt SecureSphere für die einzelnen Datenbankkonten eine „White List" der Datenobjekte, auf die die Benutzer regelmäßig zugreifen. Für jedes Konto entsteht ein Aktivitätsprofil, einschließlich DML, DDL, DCL, Read-only-Aktivitäten (SELECTs) und der Nutzung gespeicherter Prozeduren. SecureSphere erkennt, wenn ein Konto mit einem Profil auf ein Datenobjekt zugreift, das nicht in seiner White List enthalten ist.

Mit Alerts für mehrere Aktionen, temporären Quarantänen und bei Bedarf auch durch Blockieren von nicht autorisierten Aktivitäten können Unternehmen ihre Daten schützen, ohne dafür das Konto deaktivieren zu müssen und dadurch möglicherweise kritische Geschäftsprozesse zu beeinträchtigen. Automatische Korrektur-Workflows lösen Sicherheits-Alerts für verschiedene Aktionen aus, die wiederum Informationen an Splunk, SIEM, Ticketing- oder andere Drittanbieterlösungen senden können, um Geschäftsprozesse zu optimieren.

Erkennen und Eindämmen von Insider-Bedrohungen

Integrieren Sie das Aktivitätsprotokoll von SecureSphere nahtlos in Imperva CounterBreach, und schützen Sie so ihre Unternehmensdaten vor Diebstahl und Verlust durch kompromittierte, unachtsame oder böswillige Benutzer. Mithilfe von maschinellem Lernen und Referenzgruppen-Analysen erstellt CounterBreach eine vollständige Kontextbezugslinie des typischen Benutzerzugriffs auf Datenbanktabellen und erkennt auf dieser Grundlage anomale Aktivitäten und kann den Administrator darüber informieren. Wenn gefährliche Aktionen erkannt werden, können Unternehmen risikoreiche Benutzer schnell in einer Quarantäne isolieren, um Datensicherheitsverstöße proaktiv zu verhindern oder einzudämmen.

Einheitliche Richtlinienimplementierung und -durchsetzung

Ein weiterer Vorteil von SecureSphere ist die integrierte Fachkompetenz. Viele Unternehmen tun sich schwer, intern ausreichend Ressourcen vorzuhalten, die über die erforderlichen Kenntnisse verfügen, um ein modernes datenorientiertes Sicherheits- und Prüfsystem zu implementieren und zu betreiben. Eine erfolgreiche Implementierung von Zugriffskontrollen und Prüfprozessen setzt voraus, dass diese wiederholbar sind. Das zentrale Management der Prüfung und Beurteilung heterogener Systeme vereinfacht das Management dieser Prozesse. Die Automatisierung reduziert die Menge der für die Compliance erforderlichen Ressourcen und sorgt für einen positiven Return on Investment (RoI).

Im Gegensatz zu Lösungen, für die eine DBA-Beteiligung sowie kostenaufwändige Professional Services erforderlich sind, beinhaltet SecureSphere die notwendigen Verwaltungs- und Zentralisierungsfunktionen für das Management zahlreicher Datenbanken, Big Data-Knoten und Datei-Repositorys. Vordefinierte Richtlinien, Korrektur-Workflows sowie eine große Anzahl von Berichten verringern den Bedarf an SQL-Skripts und Compliance-Fachkenntnissen deutlich. Dadurch, dass die DBA-Beteiligung nicht durchgängig erforderlich ist, wird die Anforderung der Aufgabentrennung erfüllt. Mithilfe von vorgefertigten Policies, der Verwaltungskonsole, von Workflows, Berichten und Analysetools kann das vorhandene Personal das System implementieren und verwalten.

Optimierte Compliance-Berichte

Imperva SecureSphere umfasst hunderte vordefinierter Berichte, die die häufigsten Anforderungen unserer Kunden abdecken. Darüber hinaus beinhaltet die Lösung einen anpassbaren Report-Generator, unternehmensspezifische Berichtsanforderungen abzudecken. Eingebettete Workflows und Automatisierung sichern die termingerechte Ausführung von Compliance-Aufgaben und -Berichten für den gesamten Datensatz ab.

Angriffe in Echtzeit zu stoppen, ist die einzig wirksame Methode, um Hacker davon abzuhalten, Ihre Daten zu stehlen oder missbräuchlich zu verwenden. SecureSphere DAM überwacht den gesamten Verkehr auf Verletzungen der Sicherheitsrichtlinien und sucht auf Protokoll- und Betriebssystemebene nach Angriffen sowie nach nicht autorisierten SQL-Aktivitäten.

Effektives User Rights Management für alle Datenbanken

Nahezu jede Compliance-Richtlinie beinhaltet Anforderungen an die Verwaltung der Benutzerberechtigungen für sensible Daten. Diese Anforderungen zu erfüllen, zählt zu den schwierigsten Aufgaben für Unternehmen, wenn diese manuell für große Datensätze ausgeführt werden müssen. SecureSphere aggregiert automatisch Benutzerrechte für heterogene Datenspeicher und hilft, einen automatischen Prozess für die Zugriffsrechteüberprüfung einzurichten, um das Vorhandensein von zu umfangreichen Benutzerrechten zu vermeiden. Es ermöglicht den routinemäßigen Nachweis der Einhaltung von Vorschriften wie SOX und PCI DSS. Durch die Automatisierung dieser alltäglichen, jedoch kritischen Aufgaben sparen Unternehmen Personalkosten und verringern das Risiko für Fehler oder Berichtslücken.

Echtzeit-Blockierung von SQL Injection, DoS und anderen Angriffen

Angriffe in Echtzeit zu stoppen, ist die einzig wirksame Methode, um Hacker davon abzuhalten, Ihre Daten zu stehlen oder missbräuchlich zu verwenden. SecureSphere überwacht den gesamten Verkehr auf Verletzungen der Sicherheitsrichtlinien und sucht auf Protokoll- und Betriebssystemebene nach Angriffen sowie nach nicht autorisierten SQL-Aktivitäten. Die höchst effiziente Überwachung kann Aktivitäten, für die die Rechteüberprüfung noch aussteht, unter Quarantäne stellen oder die Aktivität blockieren – ohne dafür durch Deaktivieren des gesamten Kontos die Geschäftsabläufe zu beeinträchtigen.

Das Blockieren ist sowohl auf Ebene der Datenbankagenten als auch auf Netzwerkebene möglich, wodurch das Sicherheitsprofil so abgestimmt werden kann, dass Unternehmen ein ausgeglichenes Verhältnis zwischen dem Bedarf an absoluter Sicherheit und Leistungsfähigkeit für kritische Datenbanken mit hohem Transaktionsvolumen erzielen.

Wenn Sie im Hinblick auf Ihre Sicherheit wirklich proaktiv handeln möchten, implementieren Sie die Imperva SecureSphere Web Application Firewall. Sie nutzt die gleiche Architektur- und Management-Plattform wie die SecureSphere-Datenschutzlösungen. Zusätzliche Integrationen mit Systemen für Schadsoftware-Schutz, einschließlich FireEye, SIEM und anderen spezialisierten Sicherheitssystemen, helfen Unternehmen, Prozesse anzupassen und Sicherheitslücken zu schließen.

Audit-Funktionen für die Untersuchung von Zwischenfällen und forensische Analysen

Imperva SecureSphere stellt eine einheitliche Lösung für unabhängige funktionale Abläufe bereit und unterstützt während einer forensischen Untersuchung die Sicherheits-, Compliance- und Rechtsteams. Benutzer können mit Imperva sowohl auf historische als auch Echtzeitdaten zugreifen. Teams, die an der Reaktion auf Sicherheitsvorfälle arbeiten, erhalten damit eine genaue und kontextbezogene Übersicht über die laufenden Aktivitäten. Mit den Echtzeitfähigkeiten, der Benutzerverfolgung, Korrektur-Workflows, der Korrelation mit SecureSphere WAF sowie den zahlreichen vordefinierten Compliance- und Forensikberichten hebt sich Imperva von anderen Anbietern ab.

Spezielle Splunk-App für die Analyse von Datenbankaktivitäten

SecureSphere stellt standardmäßig Funktionen für die Integration mit verschiedenen SIEM-Produkten wie ArcSight, QRadar und Splunk bereit. Imperva hat in Version 11.0 ein spezielles API-Set für Splunk eingeführt. Dieses ermöglicht es den Benutzern, eigene Aktivitätskanäle zu ihren Splunk-Sicherheits-Dashboards und -Berichten hinzuzufügen. Mit der Freigabe der Imperva Database Activity Analysis Application für Splunk erhalten SecureSphere-Benutzer ein vorkonfiguriertes Dashboard- und Berichts-Set, das für die Analyse von SecureSphere-Datenbank-Alerts und Protokollen optimiert ist. Für die Implementierung ist keine Splunk-Entwicklungserfahrung erforderlich. Die Benutzer können mit vorbereiteten Berichten als Vorlage benutzerspezifische Berichte erstellen.

Automatische Bereitstellung und Konfiguration sind entscheidend für die Amortisierung.

Ein Imperva-Kunde konnte mithilfe der Automatisierungstools selbständig innerhalb von drei Wochen über 1.000 Datenbanken zur Überwachung dem System hinzufügen.

Imperva – bereit für den Unternehmenseinsatz

Zuverlässige Leistung – Skalierung für jede Unternehmensgröße

Dank der höchst effizienten und flexiblen Audit-Technologie erzielt Imperva unerreichte Skalierbarkeit. Im Gegensatz zu Mitbewerbslösungen, die für die Datenüberwachung lediglich auf standardmäßige relationale Datenbanken setzen, nutzt Imperva Techniken, die auch in den technologisch fortschrittlichsten Big Data-Analyselösungen eingesetzt werden. Die Fähigkeit, schnell zu schreiben und noch schneller zu lesen, ermöglicht Imperva eine den Mitbewerbern weit überlegene Skalierung, die am Markt ihresgleichen sucht.

Das System ist so konfigurierbar, dass es alle Aktivitäten auf Verletzungen von Sicherheitsrichtlinien überwacht und andere Aktivitäten für Prüfzwecke protokolliert. Diese Trennung kann im Vergleich zu anderen Lösungen die Datensicherheit, Leistung, Umfang der Audit-Daten und Relevanz erheblich verbessern.

Durch integrierte aktive Redundanzfunktionen eliminiert SecureSphere zentrale Fehlerstellen und unterstützt so Hochverfügbarkeitslösungen. SecureSphere setzt die modernsten und intelligentesten Hochverfügbarkeitsfunktionen ein. Dazu zählen so interessante neue Fähigkeiten wie Agenten, die sich selbst steuern und bedarfsabhängig bewegen können und so zu einem fehlerfreien Datensicherheitsprogramm sowie einem unterbrechungsfreien Prüfprotokoll beitragen.

Schnelle Implementierung

Mit einer zentralen Managementkonsole für die Steuerung und Kontrolle auf globaler Ebene behält Imperva das gesamte Unternehmen im Blick. Durch die übergeordnete Managementkonsole lassen sich globale Richtlinien schneller umsetzen, Aufgaben wie die Datenklassifizierung automatisieren und so die Implementierungsdauer verkürzen.

Imperva kennt die Bedeutung einer reibungslosen IT-Bereitstellung. Daher stehen API-Sets zur Verfügung, die die nahtlose Verteilung von Software, die Aktualisierung von Konfigurationen, die Verteilung von Richtlinien und die Data Discovery unterstützen. Die Automatisierung von Bereitstellung und Konfiguration ist entscheidend für die Amortisierung. Beispielsweise konnte ein Imperva-Kunde mithilfe der Automatisierungstools selbständig innerhalb von drei Wochen über 1.000 Datenbanken zur Überwachung dem System hinzufügen.

Hybride Überwachung

Imperva geht über das typische Bereitstellungsszenario hinaus, bei dem Agenten auf allen Datenbank-Servern erforderlich sind. SecureSphere unterstützt verschiedene Deployment-Methoden wie einen lokalen Agenten, eine netzwerktransparente Bridge-Option und einen „Non-Inline-Sniffer-Modus“. Durch Kombinieren der Deployment-Methoden können Unternehmen sehr flexibel unterschiedlichste Anforderungen erfüllen.

Imperva behält den Überblick über die Umgebung und gleicht sie mit bekannten Schwachstellen ab. So wird eindeutig erkennbar, welche Daten gefährdet sind.

Cloud-fähig

Mit Imperva SecureSphere für AWS stehen die Sicherheits- und Compliance-Funktionen der weltweit bewährten, höchst skalierbaren Datensicherheits- und Prüflösung jetzt auch für die AWS-Umgebung (Amazon Web Services) zur Verfügung. SecureSphere ist die einzige für AWS verfügbare Unternehmenslösung für Datensicherheit und Compliance. Die BYOL-Version von SecureSphere wird nativ auf AWS ausgeführt und nutzt die gleichen marktführenden Funktionen wie die lokale Version. Kunden, die eine der SecureSphere-Lösungen (DBF, DAM oder WAF) in der AWS-Umgebung einsetzen, können optional Imperva SkyFence für den Schutz ihrer Cloud-basierten Web-Anwendungen wie Office 365 und die AWS Management Console aktivieren.

Datensicherheit als Managed Service

Imperva bietet SecureSphere-Lösungen für Datensicherheit als gehosteten Managed Service an. Imperva verfügt über mehr als 14 Jahre einschlägiger Erfahrung im Bereich Datensicherheit und Compliance. Ein weiteres Plus ist der direkte Zugang zu den neuesten Forschungsergebnissen und dem Know-how des Imperva Defense Centers. Ihre Datensicherheit hat für die Experten höchste Priorität – dieser Aufgabenbereich sollte keinem unerfahrenen internen Team mit eingeschränkten Ressourcen übertragen werden müssen.

Risikobewertung für Datenbanken

Unternehmensdaten werden weltweit in zahlreichen Datenbanken gespeichert, die alle potenziell einen anderen Versions- und Patch-Stand aufweisen. Deshalb ist es zwingend erforderlich, über eine einfache Möglichkeit für die Suche nach bekannten Schwachstellen zu verfügen. Imperva ist in der Lage, die bestehende Umgebung zu analysieren und sie mit bekannten Schwachstellen abzugleichen. Damit kann eindeutig aufgezeigt werden, welche Daten gefährdet sind.

Kurze Amortisationszeit

Die flexible SecureSphere-Architektur ermöglicht Wachstum, ohne die vorhandene Umgebung zu beeinträchtigen, und für Unternehmen bedeutet sie, weniger mit mehr erreichen zu können. Imperva bringt effiziente, vorhersagbare Skalierbarkeit für Unternehmen mit. Kürzlich wechselte ein Fortune 500-Unternehmen zu Imperva, da eine zuverlässige Planung oder Budgetierung mit der vorhandenen Lösung nicht länger möglich war. Mit Imperva konnte das Unternehmen nicht nur den Überwachungsumfang und die Betriebskosten erheblich senken, sondern auch präzise für künftiges Wachstum planen und das dafür erforderliche Budget festlegen.

Imperva SecureSphere Cyber Security

Imperva SecureSphere ist eine umfassende, integrierte Sicherheitsplattform. Sie umfasst Module für die Sicherheit von Webanwendungen, Datenbanken und Dateien. Sie lässt sich so dimensionieren, dass sie auch die Sicherheitsanforderungen von Rechenzentren der größten Unternehmen erfüllt. Das Imperva Defense Center ist ein Forschungsteam aus weltweit führenden Experten für Daten- und Anwendungssicherheit. Es sorgt dafür, dass die Plattform immer auf dem neuesten Stand ist und Ihre Anwendungen auch vor neuen Bedrohungen schützt.

	SECURESPHERE DATABASE FIREWALL (DBF)	SECURESPHERE DATABASE ACTIVITY MONITORING (DAM)	SECURESPHERE DATABASE ASSESSMENT (DAS)
Discovery und Klassifizierung	Ja	Ja	Ja
Überwachungs- und Prüfprotokoll	Ja	Ja	-
Blockieren in Echtzeit	Ja	Nein	-
Schwachstellen-analyse[1]	Ja	Ja	Ja
Datenbankagenten[1]	Ja	Ja	-
Gateway-Clustering	Optional	Optional	-
Big Data-Überwachung	Optional	Optional	-
User Rights Management[2]	Optional	Optional	Optional[3]
Erweiterter anwendungs-spezifischer Service (Oracle, EBS, SAP, Peoplesoft)	Optional	Optional	-
Hochverfügbarkeit für Management-Server (MX)	Optional	Optional	-
Verfügbar auf Amazon Web Services (AWS) BYOL[4]	Ja	Ja	-
Verfügbar auf Microsoft Azure	Ja	Ja	-
Datenmaskierung[5]	Optional	Optional	
Erweiterter Schutz vor Insider-Bedrohungen durch maschinelles Lernen[6]	Optional	Optional	-
Threat Correlation für Web-Anwendungen	Optional	Optional	

[1] Enthaltene Anzahl je nach Appliance-Kauf, Details siehe SecureSphere Appliances-Datenblatt

[2] User Rights Monitoring ist auf Big Data-Knoten nicht verfügbar

[3] Funktionen, für die Prüfprotokolldetails erforderlich sind, sind nicht verfügbar, wenn DAS eigenständig implementiert wird

[4] Nicht alle Optionen stehen in der AWS-Umgebung zur Verfügung

[5] Imperva Camouflage Data Masking erforderlich

[6] Imperva CounterBreach erforderlich