Protecting the Data That Drives Business®

אבטחת מסדי נתונים

בקרה והגנה על מסדי נתונים חיוניים

מוצרי Imperva SecureSphere Database Security הם הטובים ביותר מסוגם בשוק:

- מבצעים בקרה על כל אפיקי הגישה לנתונים רגישים.
- מתריעים ו\או חוסמים התקפות או פעילות בלתי-מורשית, בזמן אמת.
- מאתרים ומתקנים וירטואלית פרצות אבטחה.
- מזהים משתמשים עם הרשאות שימוש עודפות, ומאפשרים תהליך מלא של בדיקת הרשאות.
- מזרזים תגובה להתקפות ומספקים יכולות חקירת אירועים בעזרת כלי ניתוח מתקדמים.

מוצרים

SecureSphere Database Activity Monitoring

SecureSphere Database Firewall

SecureSphere Discovery and Assessment Server

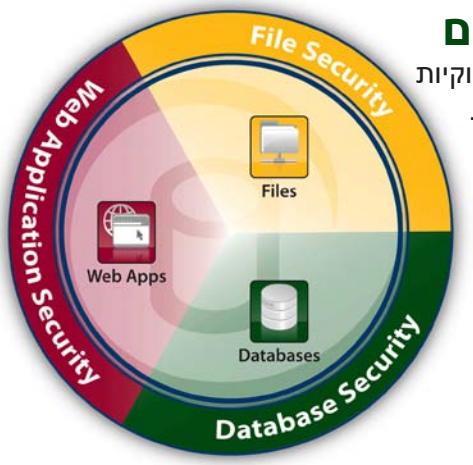
User Rights Management for Databases

ADC Insights

מוצר הבקרה וההגנה הטוב מסוגו עבור מסדי נתונים

מסדי נתונים אוגרים בתוכם נתונים חסויים בעלי ערך רב. מספר הולך וגדל של תקנות חוקיות מחייבות ארגונים לבקר את הגישה למידע רגיש ולהגן עליו מפני התקפות ושימוש לרעה.

מוצרי אבטחת מסדי הנתונים, עטורי הפרסים, מסדרת Database Security Imperva SecureSphere מבצעים בקרה אוטומטית על הגישה למסדים, מזהים התקפות, פעילות זדונית ומרמה. בשילוב עם המוצרים Web Application Security ו-File Security של חברת Imperva, סדרת SecureSphere הופכת לבחירה הטובה ביותר לאבטחת נתונים עסקיים רגישים.



בקרה רציפה על השימוש בנתונים רגישים

מערכת SecureSphere מבקרת באופן רציף את כל הפעולות המבוצעות בכל מסדי הנתונים ובזמן אמת. בכך המערכת מספקת לארגונים ביקורת מפורטת המראה מי ביצע איזו פעולה במסדי נתונים, מתי בוצעה הפעולה, היכן וכיצד. המערכת מנטרת את המשתמשים המורשים הניגשים ישירות לשרת המסדים וכן משתמשים שאינם מורשים הניגשים לנתונים דרך יישומים שונים. המערכת עוקבת גם אחר תגובות המסד כדי להתריע או לחסום דליפות של מידע רגיש.

ניתוח נתונים לצורך חקירת אירועי אבטחה

מערכת SecureSphere מנתחת את הנתונים הגולמיים על פעילות המבוקרות ומציגה ניתוחים אלו באמצעות ממשק אינטראקטיבי המספק תובנות על מצב המסדים ואירועים הקשורים בהם. המערכת מאפשרת לצוותי אבטחת מידע ולאנשי ביקורת הבודקים את מסדי נתונים לצפות, לנתח ולהשוות במהירות פעילויות במסדי הנתונים ולבחון את הנתונים כמעט מכל זווית אפשרית, וכל זאת באמצעות ממשק פשוט וידידותי, וללא צורך בכתיבת תסריטים (סקריפטים) ב-SQL. היכולת לנתח נתונים באמצעות הממשק האינטראקטיבי מפשטת את חקירתם של אירועי אבטחה ומאפשרת זיהוי מגמות ודפוסים שיכולים להעיד על סיכוני אבטחה.

זיהוי גישה בלתי-מורשית ופעילות מרמה

מערכת SecureSphere מזהה את דפוסי הגישה של משתמשים רגילים לנתונים תוך שימוש בטכנולוגיית Dynamic Profiling (פטנט רשום) היוצרת פרופיל דינאמי לכל משתמש. המערכת קובעת רמת בסיס לכל פעילות המשתמש, לרבות DML, DDL, DCL, פעילות קריאה בלבד (SELECTs), ושימוש בפרוצדורות מאוחסנות. המערכת מזהה סטיות מהותיות, המתבטאות בכך שהמשתמש מבצע חיפוש לא צפוי ואז מתריעה על כך או חוסמת את המשתמש המפר את מדיניות הגישה. ניתן גם לבודד (quarantined) משתמשים המבצעים בקשות SQL לא מורשות עד לבדיקה ולאישור זכויות הגישה שלהם.

חסימה בזמן אמת של הזרקות SQL, התקפות DoS ועוד

פעילות הביקורת מבוצעת בצורה סלקטיבית לנתונים רגישים, אבל SecureSphere מנטר את כל הפעילות במסדי הנתונים בזמן אמת במטרה לזהות דליפות מידע בלתי-ידועות, פעולות SQL שאינן מורשות והתקפות תוך ניצול פרוטוקול התקשורת או מערכת ההפעלה. המערכת מתריעה או אף חוסמת התקפות זדוניות כאשר הן מגיעות מיישומים או ממשתמשים מורשים, ברשת או בשרת המסד עצמו.

אכיפת מדיניות, דיווח יעיל של ציות למדיניות

מערכת SecureSphere כוללת מערך הגדרות מובנה של מדיניות ביקורת ואבטחה, שניתן להתאים לצורכי כל ארגון. המערכת "מודעת" אוטומטית ליישומים ארגוניים כגון SAP, Oracle EBS ו-PeopleSoft, וכן מתוכננת לציית לחוקים ולתקנות כגון חוק סרביינס אוקסלי האמריקאי (SOX), תקני האבטחה של ענף כרטיסי האשראי (PCI DSS) וחוק הבריאות האמריקאי (HIPAA). מאפיין זה של המערכת מפשט את תהליך ההתקנה ומקצר את משך הזמן הנדרש כדי לעמוד בדרישות החוקים והתקנות הללו. התרעות אבטחה יכולות להישלח למנהל האבטחה, מערכת תמיכה (ticketing system) ופתרונות צד שלישי אחרים, ובכך מאפשרת לייעל תהליכים עסקיים.

עמידה בדרישות הרגולציה

מערכת SecureSphere מסייעת לארגונים להתמודד עם תקנות רגולציה כגון PCI DSS, SOX ו-HIPAA.

- המערכת מטפלת ב-8 מתוך 12 רמות אבטחה הנדרשות על-ידי PCI, לרבות בסעיפים 10, 7, 8.5.
- עונה על צורכי ביקורת על נתונים פיננסיים בסעיפים 302 ו-404 בחוק סרביינס אוקסלי (SOX).
- אוכפת הפרדת סמכויות.
- מבטיחה את שלמות הנתונים לביקורת.
- מזהה גישה בלתי-מורשית למידע רגיש כגון מידע פיננסי ופרטי כרטיס אשראי.
- מספקת דוחות מובנים המייעלים את תהליך הציות לתקנות.

זיהוי אוטומטי של כל מסדי הנתונים הרגישים

SecureSphere מזהה אוטומטית את כל מערכות מסדי הנתונים עליהן חלות תקנות חוקיות או שדורשים אבטחה מיוחדת (מידע אישי, נתוני כרטיסי אשראי וכדומה). איתור המסדים מתבצע באמצעות Discovery and Assessment Server בגילוי וסיווג של מידע רגיש. בנוסף לכך המערכת כוללת פונקציות להערכת פגיעות המערכת. הודות לשילוב זה בין איתור המסדים הרגישים להערכת פגיעותם, ארגונים יכולים לתעדף את הפעולות לטיפול בנקודות תורפה.

הערכת נקודות תורפה ותיקון וירטואלי

SecureSphere מציע יותר מאלף סוגי הערכות פגיעות ברמת התצורה, מסד הנתונים או המערכת, ובכך מסייע לארגונים לזהות נקודות תורפה ולתקנן. לצורך מתן הגנה מיידית, SecureSphere Virtual Patching מספק טלאי(Patch) אבטחה וירטואליים המסוגלים לחסום ניסיונות ניצול לרעה של נקודות התורפה שהתגלו. מאפיין Virtual Patching מפחית למינימום את החשיפה לסיכוני אבטחה, ובכך מצמצם דרמטית את הסיכון לפריצה לנתונים תוך כדי בדיקה אירגונית ופריסת טלאים על מסדי הנתונים.

ניהול אפקטיבי כולל של זכויות הגישה למסדי הנתונים

SecureSphere אוסף אוטומטית את הרשאות הגישה של משתמשים למגוון מסדי הנתונים בארגון. בזכות המידע הנאסף יכולים ארגונים לתפעל תהליך לניהול זכויות משתמשים (User Rights Management), הסוקר אוטומטית את גישות המשתמשים למסדים, מזהה הרשאות עודפות, ומהווה מענה לדרישות תקנות דוגמת PCI 7,SOX ו-PCI 8.5 ובכלל את הדרישה שהרשאות למידע ינתנו לפי הצורך לדעת.

ביקורת והגנה על מסדי נתונים מקומיים באמצעות שימוש בסוכנים

כדי לאפשר יכולות ניטור, ביקורת (audit) ואכיפה מלאות על כל המשתמשים, כולל בעלי הרשאות לביצוע פעולות מקומיות בבסיס הנתונים עצמו, SecureSphere משתמש ברכיבי תוכנה קומפקטיים, הנקראים סוכנים (agents). סוכנים אלו מותקנים במסדים המארחים (host serves) עצמם. הסוכנים בודקים את הפעילות המקומית (ובכלל) במסדי הנתונים ומגנים על נתונים רגישים תוך הפרעה מזערית לביצועי השרתים. ניהול הסוכנים נעשה מנקודה מרכזית אחת בשרת הניהול תוך גילויי אוטומטי של הממשקים הדורשים הגנה, ובניהול שוטף מינימלי.

פריסה עם השפעה אפסית על הפעילות וביצועים מעולים

» **התקני חומרה**: מספקים תעבורה של גיגה בייט רבים עם השהייה של פחות ממילישנייה.

» **התקנים וירטואליים**: מספקים אבטחה ניתנת להתאמה, אמינה וקלה לניהול שגדלה על פי הצורך.

אבטחת מסדי נתונים וציות לתקנות ברמה חסרת תקדים

מערכת SecureSphere מטפלת בכל היבטי אבטחת מסדי הנתונים, מסייעת לציות לתקני תעשייה בתחום הביקורת ומספקת הגנה בזמן אמת שאינה פוגמת בביצועים או בזמינות המסדים. הודות לארכיטקטורת המערכת של SecureSphere המבוססת על מספר שכבות אבטחה, ניתן להגדיל את הפריסה כדי להגן על מערכי מסדי נתונים בכל גודל. לאור השילוב בין אבטחה וציות לתקנות, אין זה מפתיע שאלפי ארגונים בחרו ב-Imperva SecureSphere כדי להגן על נכסי המידע החשובים ביותר שלהם.

פריסה

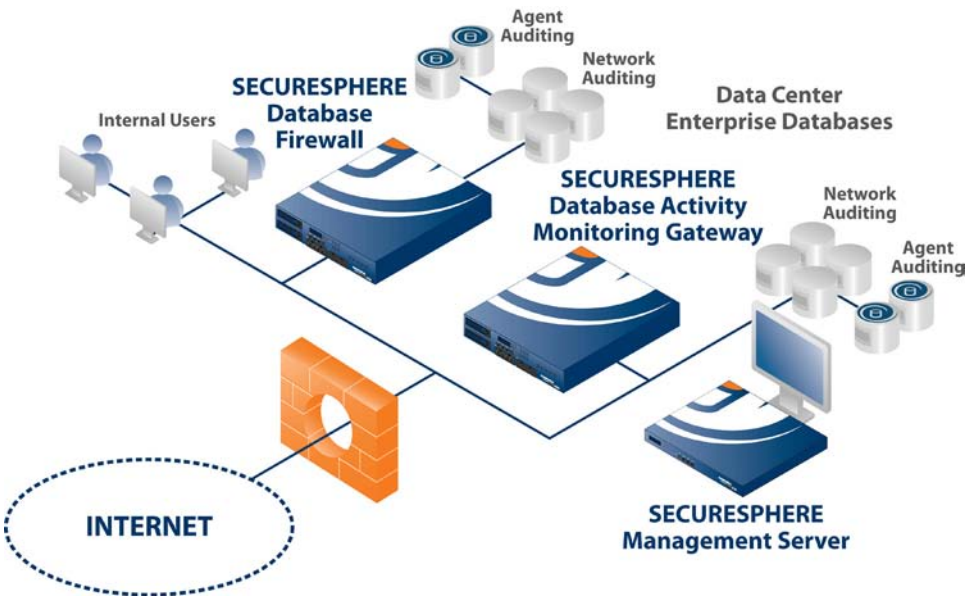
» **פריסה לא-טורית לבקרת הרשת(Snfifing)**: בפריסה זו SecureSphere מותקן בצמוד לעורק הנתונים לצורך בקרה על התעבורה, מבלי להשפיע כלל על ביצועי מסדי הנתונים או זמינותם.

» **הגנה טורית שקופה (Transparent bridge)**: פריסה מהירה וקלה, עם הביצועים הטובים ביותר בתעשייה. ללא צורך בשינוי טופולוגי כל שהוא.

» **ניטור מבוסס סוכנים**: סוכנים הם רכיבי תוכנה המפקחים על גישות ישירות של משתמשים למסדים ובודקים את התעבורה ברשת. התאמה מירבית ללקוחות בתצורה מבוזרת. על ידי ניטור של תעבורת רשת בנוסף לתעבורה מקומית.

» **איסוף נתוני פעילות (log) לצורכי ביקורת**: שימוש בתיעודי פעילות המופקים מיישומים מגוונים של צדדים שלישיים לביצוע ניתוחי פעילות, מתן התרעות ודיווח.

» **פלטפורמות מסדי הנתונים הנתמכות**: ORACLE, Microsoft SQL, IBM DB2 (לרבות DB2 for z/OS וכן DB2/400), Informix, Sybase, MySQL, Teradata ו-Netzza.



מסדי נתונים

חבילת אבטחת הנתונים של Imperva SecureSphere

חבילת SecureSphere Data Security Suite היא הפתרון המוביל בשוק לאבטחת נתונים ולציות לתקנות. מערכת SecureSphere מגנה על יישומי Web, קבצים רגישים ומסדי נתונים בפני האקרים וגורמים זדוניים בתוך הארגון, מהווה אמצעי מהיר ומשתלם לציות לתקנות וממסדת תהליך מסודר ושוטף לניהול סיכונים בהיבט הנתונים.

משפחה	מוצר מסדרת SecureSphere
מסדי נתונים Database	**Database Activity Monitoring** ביקורת ותצוגה מלאה של השימוש במסדי הנתונים ובמידע. **Database Firewall** חומת אש למסדי נתונים. ניטור פעילות והגנה בזמן אמת למסדי נתונים חיוניים. **Discovery and Assessment Server** הערכת פגיעות, ניהול תצורה וסיווג נתונים עבור מסדי נתונים. **User Rights Management for Databases** סקירה וניהול זכויות גישה של משתמשים למסדי נתונים רגישים **ADC Insights** מספק דוחות וכללים עבור SAP, Oracle EBS ו-PeopleSoft לצורך ציות לתקנות ואבטחה.
קבצים File	**File Activity Monitoring** ניטור פעילות בקבצים ביקורת מלאה של השימוש בקובצי נתונים ויכולת לצפות בכל הפעילויות. **File Firewall** חומת אש להגנה על קבצים. ניתור פעילות והגנה על קובצי נתונים חיוניים. **User Rights Management for Files** סקירה וניהול גישת משתמשים לקבצים רגישים.
אפליקציות Web	**Web Application Firewall** הגנה אוטומטית ומדויקת כנגד איומים לאפליקציות חיצוניות באינטרנט וכן אפליקציות פנים ארגוניות. **ThreatRadar** מערכת אבטחה ראשונה מסוגה המבוססת על מוניטין אתרים.

Imperva היא המובילה העולמית באבטחת נתונים

אלפי חברות, ממשלות, ארגונים וספקי שירותים מובילים מסתמכים על פתרונות Imperva למניעת פרצות אבטחה, עמידה בדרישות הרגולציה וניהול סיכוני אבטחה.

SAP Certified Integration

ICSA labs CERTIFIED Web Application Firewall

IMPERVA

אימפרבה בע"מ
דרך מנחם בגין 125
67010 תל אביב
טלפון: 03-684-0100
פקס: 03-684-0204
www.imperva.com

© Copyright 2011, Imperva
All rights reserved. Imperva and SecureSphere are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders.
#DS-DBS-A4-HE-0710rev1