2011. május 6.

Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem, 2011. 2. negyedév

írta: Noel Yuhanna
alkalmazásfejlesztési és -terjesztési szakembereknek

FORRESTER® Nap mint nap hozzájárulunk a vezetők sikeréhez

2011. május 6.

Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem, 2011. 2. negyedév

Az IBM, az Imperva és a Sentrigo vezeti a kínálatot, az Application Security, az Oracle és a Fortinet csak kevéssel lemaradva követi őket

írta: Noel Yuhanna,
Stephanie Balaouras és Adam Knoll

VEZETŐI ÖSSZEFOGLALÓ

Az adatbázis-ellenőrzési és valós idejű védelmi megoldásokat kínáló szállítók Forrester által 147 szempont alapján végzett értékelése szerint a piacon rengeteg kiforrott termék található. A felhasználói tevékenység hatékony ellenőrzése, az irányelvkezelés, a valós idejű védelem és az alkalmazástámogatási képességek, valamint a jövőre irányuló stratégia miatt az IBM, az Imperva és a Sentrigo vezeti a piacot. Az Application Security, az Oracle és a Fortinet erősen teljesít; a termékeik olyan jelentéskészítő, valós idejű észlelési és védelmi, valamint a felhasználói tevékenységeket ellenőrző képességeket biztosítanak, amelyek nem sokkal maradnak le a piacvezetők termékeitől. Elmondható azonban az összes értékelt termékről, hogy átgondolt adatbázis-ellenőrzési és valós idejű védelmi megoldásokkal rendelkeznek. Ennek köszönhetően az alkalmazásfejlesztési és -terjesztési szakemberek az adatbázis-ellenőrző és valós idejű védelmi termékek kiválasztásakor nem csak a hagyományos ellenőrzési funkciókra alapozhatnak, hanem döntéseiket a fejlettebb funkciók szerint hozhatják meg, például a támadási tevékenységek valós idejű blokkolása, a kiemelt felhasználók megfigyelése, a ráközelítéselemzés és a központosított tárolás alapján.

TARTALOMJEGYZÉK

MEGJEGYZÉSEK ÉS FORRÁSOK

A Forrester 2010 októberében végezte el a termékek értékelését: 20 szállító és felhasználó vállalatot keresett meg, hogy értékeljék az Application Security, a Fortinet, az IBM, az Imperva, az Oracle és a Sentrigo adatbázis-ellenőrzési és valós idejű védelmi ajánlatait.

Kapcsolódó kutatási dokumentumok

„Creating An Enterprise Database Security Plan”, 2010. július 29.

„Your Enterprise Database Security Strategy 2010”, 2009. szeptember 28.

„Market overview: Database Security”, 2009. február 27.

© 2011 Forrester Research, Inc. Minden jog fenntartva. A Forrester, a Forrester Wave, a RoleView, a Technographics, a TechRankings és a Total Economic Impact a Forrester Research, Inc. védjegyei. Az összes többi védjegy a megfelelő tulajdonosok tulajdona. Írásbeli engedély nélkül ezen tartalom másolása vagy megosztása semmilyen módon nem engedélyezett. A dokumentum másolatának megvásárlásához küldjön e-mailt a clientsupport@forrester.com címre. A másolással és használattal kapcsolatban további információkért tekintse meg a Forrester idézési irányelveit a www.forrester.com webhelyen. Az információk a legjobb elérhető forrásokból származnak. A vélemények az adott időpontban született megítéléseket tükrözik, és változhatnak.

AZ ADATBÁZIS-ELLENŐRZÉS ÉS A VALÓS IDEJŰ VÉDELEM BEVEZETÉSE EGYRE SZÉLESEBB KÖRŰ

Az adatbázis-ellenőrzés kritikussá vált az összes olyan vállalat számára, amelynek a törvényi megfelelőséggel és azok biztonsági követelményeivel kell foglalkoznia. Az adatbázis-ellenőrzés a következőkhöz hasonló adathozzáférési kérdésekre összpontosít: „Ki fért hozzá a hitelkártyaszámokhoz?"; „Mikor módosították az egyik ügyfél címét?"; „A módosítás előtt mi volt a tartalom?" és „Milyen alkalmazással fértek hozzá a bizalmas adatokhoz?" Bár az adatbázis-ellenőrzés alapvető módszere évtizedek óta változatlan, a központban most a mélyebb, finomabb adatellenőrzési elemzés, a több száz és több ezer adatbázis központi felülvizsgálati elemzése, az átfogó felülvizsgálati jelentések, a szerepkör-szétválasztás és valós idejű védelem áll. Ezenkívül megnőtt az adatbázis-rendszergazdák és egyéb kiemelt felhasználók tevékenységének ellenőrzése iránti igény, különösen mivel a vizsgálatokat végzők és a biztonsági csoportok megkövetelik a bizalmas adatokkal kapcsolatos megfelelőségi követelmények, például a Gramm-Leach-Bliley törvény (Gramm-Leach-Bliley Act – GLBA), az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (Health Insurance Portability and Accountability Act – HIPAA), a hitelkártyaipar adatbiztonsági szabványa (Payment Card Industry Data Security Standard – PCI DSS) és a Sarbanes-Oxley (SOX) teljesítését.
A támadások valós idejű megállítása létfontosságúvá vált az összes szervezet számára, különösen azért, mert ezek a támadások kifinomulttá és nehezen észlelhetővé váltak. Ha egy hacker feltör egy alkalmazást vagy egy adatbázist, kevesebb mint 20 másodpercre van szüksége ahhoz, hogy végrehajtson egy lekérdezést és lekérje a bizalmas információkat.
Mivel az emberek nem képesek észlelni ezeket a támadásokat, kulcsfontosságúvá vált az adatbázisok valós idejű védelme.

Az ezen Forrester Wave™ dokumentumban értékelt adatbázis-ellenőrzési és valós idejű védelmi termékek a következőkben segítik a szervezeteket:

- **A törvényi megfelelőség követelményeinek betartása:** Az adatbázis-ellenőrzés olyan bevált gyakorlat, amelyet a bizalmas adatokat (például hitelkártyaszámokat, társadalombiztosítási azonosítókat, személyazonosításra használható információkat (PII), személyes egészségügyi információkat (PHI) vagy bármilyen más bizalmas vállalati adatokat) kezelő összes vállalatnak alkalmaznia kell. Ha a PCI, HIPAA, GLBA vagy SOX törvényekkel kapcsolatos megfelelőségi követelmények teljesítését is megkövetelik, szükség van a bizalmas adatokat kezelő adatbázisok adatbázis-ellenőrzésének lehetővé tételére. Ma a legtöbb felülvizsgáló az adatbázis-ellenőrzésre helyezi a hangsúlyt a bizalmas adatokkal kapcsolatos összes tevékenység nyomon követése érdekében.
- **Az adatbázisok biztonsága a támadások és adatlopás ellen:** Ma a legtöbb vállalat környezetében több száz, vagy akár több ezer adatbázis is működhet, és ezek közül sok tartalmaz bizalmas vállalati adatokat. Nagyon nehéz kézi módszerrel érzékelni az adatbázis gyanús tevékenységeit és valós időben blokkolni az adathozzáférést. Az adatbázis-ellenőrzési és a valós idejű védelmi megoldások proaktív módon figyelik az adatbázis-hozzáféréseket, riasztják az adatbázis-rendszergazdákat (DBA) és biztonsági szakembereket, valamint valós időben blokkolják a kapcsolatokat és a munkameneteket.
- **Átfogóbb adatvédelmi stratégia kialakítása:** A sikeres adatvédelmi stratégia kritikus eleme az adatbázis-ellenőrzés és a valós idejű védelem, valamint a nem használt adatok titkosítása, az adatmaszkolás, a felhatalmazások kezelése és a sebezhetőség értékelése.[1]

© 2011, Forrester Research, Inc. A másolás tilos

Az adatbázis-ellenőrzési piac kiforrott és konszolidálódott

Amikor a biztonságról van szó, az adatbázisok nem eléggé intelligensek a felhasználók és a hackerek megkülönböztetéséhez és az adatok bizalmasságának megállapításához. Amellett, hogy az adatbázis-ellenőrzés és a valós idejű védelem segít a szervezeteknek a törvényi megfelelőség betartásában, e megoldások a biztonságot is növelik.
Három évvel ezelőtt a vállalatok olyan ellenőrzési és védelmi eszközt kerestek, amelyek néhány, bizalmas adatokat tartalmazó kulcsfontosságú adatbázist kezeltek. Ma a hangsúly a vállalatokon belüli több száz és több ezer adatbázis védelmére tolódott el, és sok szervezet olyan vállalati adatbázis-ellenőrző és valós idejű védelmi megoldást keres, amely központi felügyeletet, szerepkör-szétválasztást, irányelvkezelést, kiváló teljesítményt, adatfelderítést, valamint osztályozást és egyszerűsített felügyeletet nyújt.

A Forrester becslései szerint az adatbázis-biztonság ma körülbelül 650 millió dolláros piaca – amelybe az új licencek, a támogatás és a szolgáltatás is bele tartozik – 2015-re várhatóan megduplázódik, ahogy egyre több vállalat keres teljes vállalatra kiterjedő ellenőrzési stratégiát. Ma a legnagyobb adatbázis-ellenőrzési és valós idejű védelmi szállítók közé tartozik az Application Security, a Fortinet, az IBM, a Imperva, az Oracle és a Sentrigo.2 Az adatbázis-biztonság piaca kiforrott, de az évek során konszolidálódott, többek között az alábbi felvásárlásoknak köszönhetően: Sentrigo (McAfee), IPLocks (Fortinet), Tizor Systems (Netezza), Netezza (IBM), Guardium (IBM) és Secerno (Oracle). Néhány nagy szállító önállóan is megpróbált betörni az adatbázis-biztonság piacára, de ez nem sikerült, és végül meg kellett szüntetniük a termékcsaládot. Az ilyen megoldások közé tartozik a Symantec Database Security és a Quest Software adatbázisokhoz készült InTrust terméke.

A vállalati adatbázis-ellenőrzési és valós idejű védelmi piac két fő szegmensből áll:

- **Az adatbázis-kezelő rendszerek (DBMS-ek) beépített alapvető ellenőrzési képességei:** Minden jelentős DBMS termék – beleértve az IBM, az Ingres, a MarkLogic, a Microsoft, az Oracle és a Sybase termékeit is – beépített ellenőrzési lehetőségeket biztosít a hozzáférésekről és módosításokról készített alapvető eseménynaplók létrehozásának támogatása érdekében. Bár ezek a szolgáltatások elég jók a kis és kevésbé összetett rendszerek esetében, túl lassúak, amikor a nagy adatbázisfarmok jelentéskészítéséről, szerepkör-szétválasztásáról, valós idejű védelméről és támogatásáról van szó. A Forrester szerint a DBMS-szállítók az elkövetkezendő években folytatják az egyre fejlettebb beépített ellenőrzési szolgáltatások alkalmazását, így az ők és a vezető külső szállítók ajánlatai közötti különbségek egye kisebbé válnak.
- **A külső szállítók által kínált átfogó ellenőrzési megoldások:** Ma tucatnyi szállító kínál adatbázis-ellenőrzési és valós idejű védelmi megoldásokat. Ezen szállítók közül néhány nagyon nagy – például a Fortinet, az IBM és az Oracle –, mások pedig induló vállalatok, például ilyen az Application Security, az Imperva és a Sentrigo. A szállítók elsősorban kétféle típusú architektúrát kínálnak, ezek a 1) hálózatalapú készülék és a 2) szoftveralapú megoldás. Manapság a legtöbbször a szoftveralapú architektúratípust alkalmazzák; ezek a megoldások ügynök nélküliek vagy ügynökalapúak lehetnek, és az adatbázis megosztott memóriájából, az adatbázisnaplókból és a folyamatkapcsolatokból olvassák ki az ellenőrzési információkat. A külső szállítók megoldásai az architektúrájuktól függetlenül erőteljesen összpontosítanak az egyszerűsítésre, a szerepkör-szétválasztásra, az irányelvkezelésre, a központosított felügyeletre és a megfelelőségi jelentésekre.

© 2011, Forrester Research, Inc. A másolás tilos

AZ ADATBÁZIS-ELLENŐRZÉS ÉS A VALÓS IDEJŰ VÉDELEM ÉRTÉKELÉSÉNEK ÁTTEKINTÉSE

Az adatbázis-ellenőrzési és valós idejű védelmi piac állapotának értékeléséhez és annak áttekintéséhez, hogy a szállítók hogyan viszonyulnak egymáshoz, a Forrester kiértékelte az adatbázis-ellenőrzési és valós idejű védelmi megoldások hat legnagyobb szállítójának erősségeit és gyengeségeit.

Értékelési feltételek: jelenlegi ajánlat, stratégia és piaci jelenlét

A múltbéli kutatások, a felhasználók igényeinek felmérései, valamint a szállítókkal és szakértőkkel folytatott interjúk vizsgálata után átfogó értékelési feltételeket fejlesztettünk ki. 147 szempontból értékeltük a szállítókat, a szempontokat három magas szintű csoportra osztottunk:

- **Jelenlegi ajánlat:** A termékek erősségének megállapításához a jelenlegi ajánlatot nyolc magas szintű kategória szerint értékeltük: az adatbázis-ellenőrzés, a felhasználók és alkalmazások felülvizsgálata, a felülvizsgálati irányelvek, a felülvizsgálati tár, a jelentéskészítés és elemzés, a valós idejű védelem, az architektúra és a felügyelet szempontjából.
- **Stratégia:** Áttekintettük az összes szállító stratégiáját, és figyelembe vettük az ügyfelek jövőbeli igényeinek megfelelő termékpozicionálás érdekében tervezett fejlesztéseket. A vállalat termékének támogatásához elérhető pénzügyi erőforrásokat, a piaci ármeghatározást és a vállalat stratégiáját is megtekintettük.
- **Piaci jelenlét:** A termékek piaci jelenlétének megalapozásához kombináltuk az egyes szállítók telepített példányainak, pénzügyi teljesítményének, szolgáltatásainak, alkalmazottainak, technológiai partnereinek és nemzetközi jelenlétének információit.

Az értékelt külső szállítók hiteles telepítésekkel és vállalati szintű megoldásokkal rendelkeznek

A Forrester hat külső szállítót vizsgált ebben a felmérésben: ezek az Application Security, a Fortinet, az IBM, az Imperva, az Oracle és a Sentrigo voltak. Ezen szállítók mindegyike rendelkezik a következőkkel (lásd az 1. ábrát):

- **Vállalati szintű adatbázis-ellenőrzési megoldás:** Csak azokat a külső szállítókat értékeltük, akik felismerték az adatbázis-ellenőrzési követelmények növekvő igényét és a DBMS rendszerek beépített ellenőrzési szolgáltatásain kívül különös hangsúlyt fektetnek a nagy teljesítményt és méretezhetőséget biztosító termékekre, a jelentéskészítésre, az irányelvkezelésre és a könnyű használatra. A terméknek 2010. augusztus 15-én már elérhetőnek kellett lennie.
- **Láthatóság az ellenőrzés területén:** Csak azokat a külső adatbázis-ellenőrzési és valós idejű védelmi szállítókat értékeltük, amelyeket az ügyfelek legalább 10 alkalommal említettek a Forrester felméréseiben az elmúlt évben.
- **Hitelesített telepített példányok:** Csak azokat a külső szállítókat értékeltük, amelyek legalább 100 vállalati ügyféllel rendelkeznek. Az összes értékelt szállító megfelelt ennek a feltételnek.

© 2011, Forrester Research, Inc. A másolás tilos

1. ábra Az értékelt szállítók: termékismertető és kiválasztási feltételek

Szállító	Értékelt termék	Értékelt termék változata	Változat kiadási dátuma
Application Security	DbProtect	6.1 változat	2010. június
Fortinet	FortiDB	4.1 változat	2010. július
IBM	InfoSphere Guardium	7.0 változat	2008. július
Imperva	SecureSphere Data Security Suite	8.0 változat	2010. július
Oracle	Audit Vault	10.2.3 változat	2008. június
Sentrigo	Hedgehog Enterprise	4.0 változat	2010. augusztus

Szállítók kiválasztási feltételei
A termék átfogó vállalati szintű adatbázis-ellenőrzési megoldást nyújt, amely segít a törvényi megfelelőség biztosításában és az adatlopás elleni védelemben, beleértve a megfelelőségi jelentések elkészítését, a szerepkör-szétválasztást, a valós idejű adatvédelmet, az eseménynaplók tárolását, valamint az ellenőrzési folyamatok és eljárások automatizálását.
A terméket a Forrester ügyfelei legalább 10 felmérésben megemlítették az elmúlt 12 hónapban.
A terméknek legalább 100 vállalati ügyfélből álló ügyfélbázisa van.
A termék 2010. augusztus 15-én elérhető volt.

Forrás: Forrester Research, Inc.

AZ ADATBÁZIS-ELLENŐRZÉSI PROGRAMOK LEGTÖBB SZÁLLÍTÓJA MOST ÁTFOGÓ MEGOLDÁSOKAT NYÚJT

Az értékelés olyan piacot mutat be, amelyen (lásd a 2. ábrát):

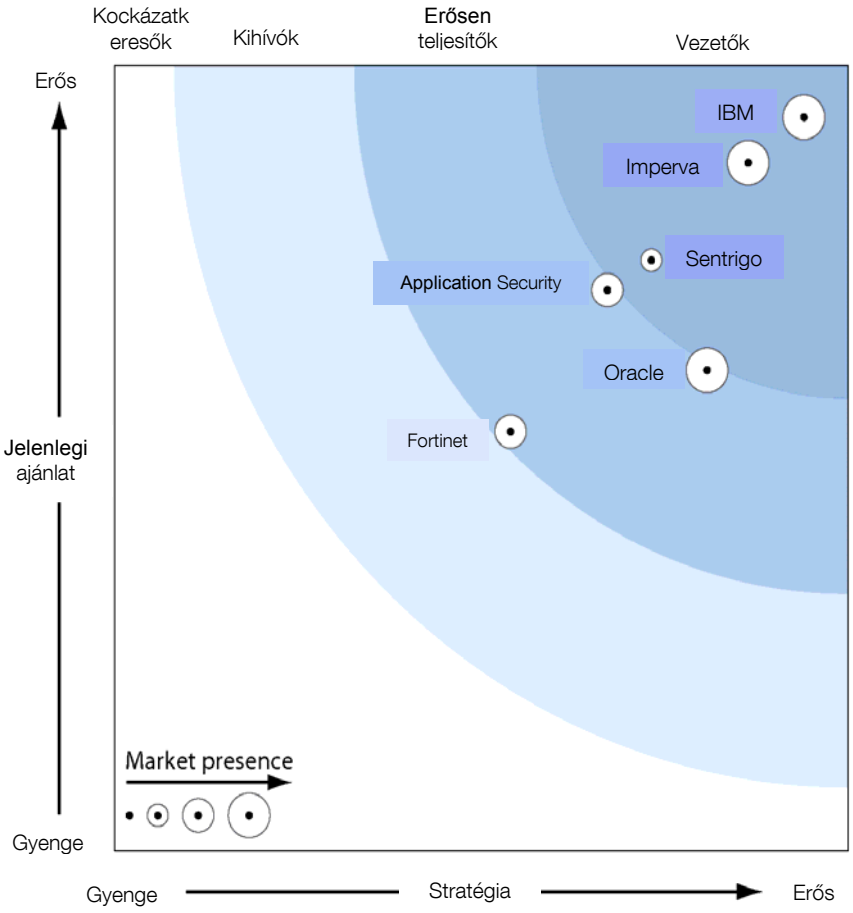
- **Az IBM, az Imperva és a Sentrigo a vezető:** Ezek a szállítók a vállalati ellenőrzési követelmények kielégítése érdekében erőteljes támogatást nyújtanak a legtöbb adatbázis-ellenőrzési szolgáltatáshoz és funkcióhoz. Az IBM InfoSphere Guardium támogatást biztosít szinte az összes ellenőrzési és valós idejű védelmi megoldásban található szolgáltatáshoz. Az InfoSphere Guardium erőteljes támogatást biztosít az adatbázis-hozzáférési ellenőrzésekhez, az alkalmazásellenőrzésekhez, az irányelvkezeléshez, az ellenőrzési tárakhoz és a valós idejű védelemhez. Az Imperva SecureSphere Data Security Suite erős valós idejű védelmet, jelentéskészítést és elemzést, felhasználói tevékenységellenőrzést és irányelvkezelést biztosít. A Sentrigo Hedgehog Enterprise erős az ellenőrzési irányelvek, a teljesítmény, a könnyű használat, a megfelelőségi jelentések és az irányelvkezelés területén.
- **Az Application Security, az Oracle és a Fortinet versenyképes megoldásokat kínál:** Az Application Security DbProtect annak ellenére jól teljesített, hogy a szállító évek óta elsősorban a sebezhetőség értékelésére összpontosít. A DbProtect jó szolgáltatásokkal rendelkezik a felülvizsgálati irányelvek, a megfelelőségi jelentések,

© 2011, Forrester Research, Inc. A másolás tilos

a könnyű használat, a teljesítmény, a központi tárak, valamint a felhasználók és kiemelt felhasználók ellenőrzése terén. Az Oracle minden évben egyre bővíti a biztonsági megoldásokat; jól teljesített az Audit Vault és a Database Vault termékeivel, és most a Secerno felvásárlásával kezd felzárkózni az adatbázistűzfalak területén. Az Oracle erős az adatok ellenőrzésében, a tárak és hozzáférés ellenőrzésében, az értesítésekben és riasztásokban, valamint a felhasználói tevékenységek és kiemelt felhasználók ellenőrzésében. A Fortinet FortiDB az IPLocks 2008-as felvásárlásával lépett be az adatbázis-biztonsági piacra, és az évek során jól teljesített: a kis és közepes méretű ellenőrzési követelményeknek eleget tevő alacsonyabb költségű megoldást biztosított a vállalatoknak.

Az adatbázis-ellenőrzési és valós idejű biztonsági piac ezen értékelése csak kiindulópontot biztosít. Arra ösztönözzük az olvasókat, hogy tekintsék meg a részletes termékértékeléseket és a Forrester Wave Excel-alapú szállító-összehasonlítási eszközzel úgy súlyozzák a feltételeket, hogy azok megfeleljenek az egyéni
igényeiknek.

2. ábra Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem, 2011. 2. negyedév



I Forrester Wave™
I Smart data for smart decisions

Online letöltheti a Forrester Wave eszközt a részletesebb termékértékelésekhez, a szolgáltatások összehasonlításához és a testreszabható osztályozásokhoz.

Forrás: Forrester Research, Inc.

© 2011, Forrester Research, Inc. A másolás tilos

2. ábra Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem, 2011. 2. negyedév (folyt.)

	A Forrester súlyozása	Application Security	Fortinet	IBM	Imperva	Oracle	Sentrigo
JELENLEGI AJÁNLAT	50%	3,57	2,67	4,67	4,38	3,06	3,76
Adatbázis-ellenőrzés	10%	3,81	3,51	4,88	4,40	3,92	4,12
A felhasználók és az alkalmazás ellenőrzése	15%	3,08	2,56	4,68	4,44	2,68	3,56
Ellenőrzési házirendek	10%	3,90	3,30	5,00	4,60	3,20	4,60
Ellenőrzési tár	10%	3,80	3,24	5,00	4,04	4,52	4,28
Jelentéskészítés és elemzés	10%	4,46	3,44	4,76	4,64	3,40	3,56
Valós idejű védelem	15%	2,70	1,10	4,80	4,80	2,20	4,20
Architektúra	15%	3,57	3,00	4,19	4,15	3,17	2,94
Felügyelet	15%	3,80	2,15	4,40	4,04	2,29	3,35
STRATÉGIA	50%	3,36	2,70	4,70	4,32	4,04	3,66
Termékstratégia	60%	2,80	2,50	4,50	4,40	3,40	3,30
Vállalati stratégia	40%	4,20	3,00	5,00	4,20	5,00	4,20
Költség	0%	0,00	0,00	0,00	0,00	0,00	0,00
PIACI JELENLÉT	0%	3,69	3,49	4,92	4,18	4,88	2,64
Telepített példányok	20%	3,00	2,00	5,00	5,00	5,00	2,00
Árbevétel	10%	2,60	4,00	4,20	2,40	3,80	2,60
Szolgáltatások	20%	3,60	5,00	5,00	2,90	5,00	2,20
Alkalmazottak	20%	4,05	4,25	5,00	4,30	5,00	2,40
Technológiai partnerek	20%	5,00	1,70	5,00	5,00	5,00	3,68
Nemzetközi jelenlét	10%	3,00	5,00	5,00	5,00	5,00	3,20

Minden pontszám 0 (gyenge) és 5 (erős) közé esik.

Forrás: Forrester Research, Inc.

SZÁLLÍTÓK LEÍRÁSA

Vezetők: IBM, Imperva és Sentrigo

- **A Guardium felvásárlásával az IBM könnyebben került vezető pozícióba:** Az IBM erősen teljesített az adatbázis-ellenőrzési és valós idejű védelmi piac 2007 4. negyedévi Forrester Wave értékelésében, amelyben az IBM Consul InSight és az IBM DB2 Audit Management Expert (AME) megoldásokat értékeltük. A Guardium 2009-es felvásárlásával azonban minden megváltozott, így az IBM e piac egyik vezetőjévé vált. Az IBM InfoSphere Guardium továbbra is vezetőnek bizonyul a rendkívül nagy, heterogén környezetekben, kiváló teljesítményt és méretezhetőséget biztosít, leegyszerűsíti a felügyeletet, és az adatbázisok valós idejű védelmét nyújtja. Az IBM továbbra is az újításokra összpontosít és bővíti a Guardium terméket, hogy más IBM termékekkel (például az InfoSphere Discovery és az InfoSphere Optim eszközökkel) integrálja azt. Ma az IBM InfoSphere Guardium sok vállalatban

© 2011, Forrester Research, Inc. A másolás tilos

és több száz kulcsszerepet játszó adatbázison működik. Ezenkívül az IBM átfogó professzionális szolgáltatásokat biztosít, amelyek segítenek az összetett környezetekben dolgozó ügyfeleknek és azoknak, akiknek erre szükségük van a vállalaton belüli adatbázis-biztonság megvalósításához.

- **Az Imperva az IBM nyomában van:** Az Imperva rendkívül jól teljesített az évek során, annak ellenére, hogy most nagyobb óriásokkal versenyez, mint például a Fortinet, az IBM és az Oracle. Az Imperva vezető az erősen teljesítő és méretezhető adatbázis-ellenőrzési megoldások terén, mivel magas pontszámot kapott az értékelt legtöbb területen. Az Imperva erős támogatást nyújt az ellenőrzéshez és az előírások teljesítéséről szóló jelentésekhez, a tranzakciók és lekérdezések ellenőrzéséhez, a valós idejű felderítéshez, a felhasználószintű és a kiemelt felhasználók ellenőrzéséhez, az irányelv-definiáláshoz és a megfelelőségi irányelvekhez, az értesítésekhez és a riasztásokhoz, valamint a valós idejű védelemhez. Az Imperva erőteljes termék- és vállalati stratégiával is rendelkezik, és a piaci jelenléte minden bizonnyal segíteni fog tovább növelni a céget az elkövetkezendő években. Az Imperva továbbra is az egyik legagresszívabb szállító az adatbázis-ellenőrzési piacon. Az adatbázis-biztonság mellett az Imperva a webes alkalmazásokhoz és fájlbiztonsághoz is nyújt megoldásokat. A Forrester szerint az Imperva vállalatot az elkövetkezendő években megpróbálja majd felvásárolni egy nagy biztonsági megoldásszállító.
- **A Sentrigo rendkívül jól teljesített, így a vezetők között foglalhat helyet:** A Sentrigo vállalatot a jelen Forrester Wave dokumentum kiadása előtt nem sokkal vásárolta fel a McAfee. A Sentrigo Hedgehog Enterprise termék jelenlegi neve McAfee Database Activity Monitoring, és a Sentrigo Hedgehog DBscanner terméket pedig McAfee Vulnerability Manager for Databases néven forgalmazzák. A 2006-ban alapított Sentrigo számos adatbázis-biztonsági megoldást biztosít, többek között adatbázis-ellenőrzést, sebezhetőségi értékelést, adatfelderítést, virtuális javításokat és valós idejű védelmet. A Sentrigo erős pontszámokat kapott az ellenőrzési irányelvekért, a könnyű használatért, a valós idejű támadásészlelésért, a teljes körű elemzésekért és a megfelelőségi jelentésekért. Ezenkívül erőteljes a termékekkel kapcsolatos jövőképe, az elkötelezettsége és a partnerhálózata. Bár a Sentrigo nem rendelkezik annyi ügyféllel, mint az IBM vagy az Imperva, a Fortune 1000 listán szereplő vállalatok közül jó néhány a Sentrigo termékével támogat több száz kritikus fontosságú adatbázist.

Erősen teljesítők: Application Security, Oracle és Fortinet

- **Az Application Security életképes adatbázis-ellenőrzési megoldást biztosít vonzó áron:** A 10 éve alapított Application Security vezető az adatbázisok sebezhetőségi értékelésében, és folyamatosan bővíti DbProtect termékét, amely támogatja az adatbázis-ellenőrzést és a valós idejű védelmet. Az Application Security azonban az évek során kemény versenytársakra akadt az IBM, az Imperva és az Oracle személyében. Az Application Security erős teljesítő az értékelésünkben. Erős pontszámokat kapott a felhasználói tevékenységek megfigyeléséért, a megfelelőségi jelentésekért, a ráközelítéselemzésekért, a valós idejű támadásészlelésekért és a teljesítményért.
- **Az Oracle az ellenőrzésen túlmutató átfogó adatbázis-biztonsági megoldást kínál:** Az Oracle nyújtja a legátfogóbb adatbázis-biztonsági megoldást; az Oracle megoldásában az adatbázis-ellenőrzés, az adatmaszkolás, a sebezhetőségi értékelés, az adatfelderítés, a címkebiztonság, a nem használt adatok titkosítása, a jogosultságkezelés és a szoftverjavítások felügyelete is helyet kapott. Az Oracle erős teljesítő az értékelésünkben, és továbbra is elkötelezett a biztonsági

© 2011, Forrester Research, Inc. A másolás tilos

megoldások iránt. Ezenkívül az Oracle az egyetlen DBMS-szállító, amelynek megoldása az adatbázis szintjén (Oracle Database Vault termék) biztosítja a bizalmas adatok adatbázis-rendszergazdák elleni védelmét. Az Oracle nemrég adta ki a Database Firewall terméket, amely valós idejű védelmet és a felhasználók és hozzáférések erős ellenőrzését végzi; ez a termék jól kiegészíti az Oracle Audit Vault és Database Vault termékcsoportját. Mivel a termékértékelés lezárásának dátuma 2010. augusztus 15. volt, nem értékeltük az Oracle Database Firewall terméket.

- **A Fortinet életképes adatbázis-biztonsági megoldást kínál alacsony áron:** A Fortinet 2008-ban vásárolta fel az IPLocks vállalatot, így belépett az adatbázis-biztonsági piacra. A Fortinet összességében jól teljesített a felvásárlás óta, és ma több mint 100 ügyfele van, amelyek fele Fortune 500 listán szereplő vállalat. Bár a Fortinet főleg a hálózati biztonsági készülékekre és az egyesített fenyegetéskezelésre (UTM) összpontosít, az adatbázis-biztonság továbbra is fontos számukra. A Fortinet erőssége a beépített adatbázis-biztonsággal kialakított integrációban, a jelentéskészítésben, a proaktív riasztásokban, az egyéni irányelvekben és a felhasználószintű és tranzakciószintű ellenőrzésben rejlik. A Fortinet valószínűleg egyre erősebb versenytársakkal fog szembenézni, ahogy a szállítók konszolidációja folytatódik. A Fortinet vállalatnak továbbra is a megfelelő megoldásokra kell összpontosítania és innovatívnak kell maradnia, hogy versenyképes maradjon.

KIEGÉSZÍTŐ ANYAG

Online források

A 2. ábra online verziója egy Excel-alapú szállító-összehasonlító eszköz, amely részletes termékértékeléseket és testre szabható osztályozásokat biztosít.

Az ezen Forrester Wave dokumentumban használt adatforrások

A Forrester két adatforrás kombinációjával értékelte a megoldások erősségeit és gyengeségeit:

- **Termékbemutatók:** Megkértük a szállítókat, hogy mutassák be a termék funkcióit. Ezen termékbemutatók alapján ellenőriztük, hogy az egyes szállítók termékeinek részletes képességeit.
- **Referenciabeszélgetések ügyfelekkel:** A termék és a szállító alkalmasságának ellenőrzéséhez a Forrester referenciabeszélgetéseket is végzett a szállítók két-két jelenlegi ügyfelével.

A Forrester Wave módszerei

Elsődleges kutatást végzünk a piacon a feltételeinknek megfelelő, értékelni kívánt szállítók listájának megállapításához. A szállítók ezen kezdeti csoportja alapján szűkítjük a végső listát. A következők alapján választjuk ki a szállítókat: 1) megfelelő termék; 2) ügyfelek körében aratott siker; és 3) a Forrester ügyfelei részéről jelentkező igény. Kizárjuk azokat a szállítókat, akik korlátozott mennyiségű ügyfél-referenciával rendelkeznek, és akik nem illenek az értékelésünk hatókörébe.

A múltbéli kutatások, a felhasználók igényeinek felmérései, valamint a szállítókkal és szakértőkkel folytatott interjúk vizsgálata után megállapítjuk a kezdeti értékelési feltételeket. A szállítók és azok termékei feltételeink alapján végzett értékeléséhez

© 2011, Forrester Research, Inc. A másolás tilos

a laborértékelések, kérdőívek, bemutatók és/vagy az ügyfelekkel végzett megbeszélések kombinációja alapján részleteket gyűjtünk a termékek minősítéséről. Az értékeléseket elküldjük a szállítóknak áttekintésre, majd úgy módosítjuk az értékeléseket, hogy a szállító ajánlatainak és stratégiáinak legpontosabb képét tükrözze.

Megállapítjuk az alapértelmezett súlyozásokat, hogy azok a nagy felhasználói vállalatok igényeinek elemzését – és/vagy a Forrester Wave dokumentumban részletezett más eseteket – tükrözzék, majd egy egyértelmű skálán pontozzuk a szállítókat. Ezek az alapértelmezett súlyozások csak kiindulópontként szolgálnak, és arra ösztönözzük az olvasókat, hogy az Excel-alapú eszközzel úgy súlyozzák a feltételeket, hogy azok megfeleljenek az egyéni igényeiknek.
A végső pontszámok alkotják a piac grafikus ábrázolását a jelenlegi ajánlat, stratégia és piaci jelenlét alapján. A Forrester szándékai szerint rendszeresen frissíti majd a szállítók értékelését a termékek képességeinek és a szállítók stratégiájának fejlődésével.

ZÁRÓ MEGJEGYZÉSEK

[1] Az átfogó adatbázis-biztonsági stratégia kialakításáról további kutatásokat a 2009. szeptember 28-i „Your Enterprise Database Security Strategy 2010” című jelentésben olvashat.

[2] A Sentrigo vállalatot a jelen Wave dokumentum kiadása előtt nem sokkal vásárolta fel a McAfee.

 © 2011, Forrester Research, Inc. A másolás tilos

FORRESTER®

Nap mint nap hozzájárulunk a vezetők sikeréhez

Központ

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
E-mail: forrester@forrester.com
Nasdaq megjelölés: FORR
www.forrester.com

Kutatási és értékesítési irodák

A Forrester nemzetközileg több mint 27 városban rendelkezik kutatóközpontokkal és értékesítési irodákkal, többek között Amszterdamban, Cambridge-ben (Egyesült Államok, Massachusetts), Dallasban, Dubaiban, Foster Cityben (Egyesült Államok, Kalifornia), Frankfurtban, Londonban, Madridban, Sydney-ben, Tel Avivban és Torontóban.

A világszerte működő irodák teljes listáját a www.forrester.com/about címen találja.

A fizikai vagy elektronikus másolatok készítésével kapcsolatos információkért lépjen kapcsolatba az ügyféltámogatással a +1 866.367.7378 számon, a +1 617.613.5730 számon vagy a clientsupport@forrester.com címen.
Mennyiségi kedvezményeket és speciális árengedményeket biztosítunk a tudományos és nonprofit intézményeknek.

A Forrester Research, Inc. (Nasdaq: FORR) független kutatóvállalat, amely pragmatikus és előrelátó üzleti és technológiai tanácsokat nyújt a globális piacvezetőknek. A Forrester a vezető vállalatok 19 fontos területen dolgozó szakembereivel működik együtt, és saját kutatásokat, ügyféligény-felméréseket, tanácsadást, eseményeket és vezetői találkozókat bonyolít le. A Forrester több mint 27 éve teszi sikeressé nap mint nap az információtechnológiai, marketing és technológiai ipari vezetőket.
További információért látogasson el a www.forrester.com címre.

FORRESTER®

57500