IBM InfoSphere Guardium

Tüm Veritabanı Güvenliğinin ve Uyumluluk Yaşam Çevriminin Yönetilmesi

Kritik önem taşıyan kurumsal verilerinin güvenliği konusunda IBM'e güvenen Global 1000 şirketlerinin sayısı, diğer teknoloji sağlayıcılarını tercih edenlerden daha fazladır. IBM, kurumsal sistemlerinizde depolanan finansal bilgilerin ve kurumsal kaynak planlama bilgilerinin, müşteri ve kart sahibi verilerinin ve fikri mülkiyet haklarına tabi malzemenin korunması için en basit ve en güçlü çözümü sağlamaktadır.

Kurumsal güvenlik platformumuz, ayrıcalıklı dahili kullanıcıların ve potansiyel bilgisayar korsanlarının yetkisiz veya şüpheli etkinliklerini önler. Aynı zamanda, Oracle E-Business Suite, PeopleSoft, SAP ve şirket içi sistemler gibi kurumsal uygulamaların son kullanıcıları tarafından gerçekleştirilebilecek dolandırıcılık faaliyetlerini izler.

IBM'in çözümü ayrıca, tüm uygulama ve veritabanı altyapınız çapındaki uyumluluk denetimlerini otomatikleştiren ve merkezileştiren bir ölçeklenebilir, çok katmanlı mimari ile işletim verimliliğini optimize eder.

Bu çözüm yapabildikleri açısından dikkat çekici olduğu kadar, yapmadıkları açısından da dikkat çekicidir. Performans üzerinde kelimenin tam anlamıyla sıfır etkiye sahiptir, veritabanlarınızda değişiklik yapmanızı gerektirmez ve yerel veritabanı günlüklerine veya denetim araçlarına bağımlı değildir.

Gerçek Zamanlı Veritabanı Güvenliği ve İzleme

Birleşik Çözüm: Tek birleşik konsol ve arka uç veri deposu temel alınarak tasarlanan InfoSphere Guardium, tüm veritabanı güvenliğinin ve uyumluluk yaşam çevriminin yönetilmesi için bir grup bütünleştirilmiş modül sunar.

InfoSphere Guardium, birleşik bir Web konsolu, arka uç veri deposu ve iş akışı otomasyonu sistemi ile tüm veritabanı güvenliğini ve uyumluluk yaşam çevrimini ele alan tek çözümdür ve aşağıdakileri yapmanıza olanak sağlar:

- Kurumsal veritabanlarındaki hassas bilgilerin bulunması ve sınıflandırılması.
- Veritabanı güvenlik açıklarının ve yapılandırma kusurlarının değerlendirilmesi.
- Önerilen değişiklikler uygulandıktan sonra yapılandırmaların kilitlenmesinin sağlanması.
- Güvenli, müdahale edilmesi mümkün olmayan ve görev ayrılığını destekleyen bir denetim yolu ile tüm platformlar ve iletişim kuralları çapındaki tüm veritabanı işlemlerine %100 görünürlük ve parçacıklı yapı sağlanması.
- Microsoft SharePoint gibi önde gelen dosya paylaşımı platformları üzerindeki etkinliklerin takip edilmesi.
- Hassas verilere erişim, ayrıcalıklı kullanıcı işlemleri, değişiklik denetimi, uygulama kullanıcısı etkinlikleri ve başarısız oturum açılışları gibi özel güvenlik durumları için ilkelerin izlenmesi ve uygulanması.
- SOX, PCI DSS ve veri gizliliği için önceden yapılandırılmış raporlarla, gözetim ekiplerine rapor dağıtımı, onaylar ve üst seviyeye yükseltmeler dahil olmak üzere tüm uyumluluk denetimi sürecinin otomatikleştirilmesi.
- Kurumsal çaptaki uyumluluk raporlaması, performans optimizasyonu, araştırmalar ve adli incelemeler için tek, merkezileştirilmiş denetim havuzu oluşturulması.
- Tek veritabanının korunmasından dünya çevresinde dağıtılmış binlerce veritabanın korunmasına kolaylıkla ölçeklenebilirlik.

Bulma ve Sınıflandırma

Hassas bilgileri otomatik olarak bulur, sınıflandırır ve güvenliğini sağlar

Kuruluşlar giderek daha fazla dijital bilgi oluşturmakta ve saklamaktadır ve buna bağlı olarak, hassas bilgilerin bulunması ve sınıflandırılması konusunda giderek daha fazla zorlanmaktadır.

Bu durum özellikle birleşmeler ve satın almalar yaşamış olan kuruluşlar veya ilk geliştiricileri şirketten ayrılmış olan eski sistemlerin bulunduğu ortamlar için geçerlidir. En iyi koşullarda bile, yeni iş gereksinimlerinin desteklenmesi için uygulama ve veritabanı yapılarında sürekli olarak değişiklik yapılması kolaylıkla statik güvenlik ilkelerinin ihlal edilmesine neden olabilir ve hassas verilerin tanımlanmamış ve korunmamış bir durumda kalmasına neden olabilir.

Kuruluşlar özellikle aşağıdaki konularda zorlanır:

- Hassas veriler içeren tüm veritabanı sunucularının eşlenmesi ve tüm kaynaklardan (iş kolu uygulamaları, toplu süreçler, anlık sorgulamalar, uygulama geliştiricileri, sistem yöneticileri, vs.) bunlara nasıl erişildiğinin anlaşılması.
- Depolanan bilgilerin hassasiyetinin bilinmediği durumlarda bilgilerin güvenliğinin sağlanması ve riskin yönetilmesi.
- Hangi bilgilerin belirli düzenlemelerin koşullarına tabi olduğunun açık olmadığı durumlarda uyumluluğun sağlanması.

InfoSphere Guardium ile gizli verilerin nerede depolandığını tanımlamak için veritabanı otomatik keşfini ve bilgi sınıflandırmayı kullanabilir ve ardından belirli hassas nesne sınıfları için geçerli olan güvenlik ilkelerinin uygulanmasını otomatikleştirmek için özelleştirilebilir sınıflandırma etiketlerinden yararlanabilirsiniz. Bu ilkeler, hassas bilgilerin sadece yetkili kullanıcılar tarafından görüntülenmesini ve/veya değiştirilmesini sağlar.

Hassas verilerin keşfedilmesi de düzenli bir şekilde gerçekleştirilecek şekilde planlanarak denetim dışı sunucuların sisteme girmesi önlenebilir ve kritik bilgilerin "unutulmaması" sağlanabilir.

Değerlendirme ve Güçlendirme

Güvenlik açığı, yapılandırma ve davranış değerlendirmesi
InfoSphere Guardium'un veritabanı güvenliği değerlendirmeleri, güvenlik açıklarına karşı tüm veritabanı altyapınızı tarar ve hem gerçek zamanlı hem de geçmişe dönük verileri kullanarak veritabanı güvenlik yapınızın sürekli olarak değerlendirilmesini sağlar.

InfoSphere Guardium Bilgi Tabanı hizmeti tarafından düzenli olarak güncellenen endüstri en iyi uygulamalarını (CVE, CIS, STIG) ve platforma özgü güvenlik açıklarını temel alan kapsamlı bir önceden yapılandırılmış test kitaplığı sağlar. Ayrıca, belirli gereksinimlerin karşılanması için özel testler de tanımlayabilirsiniz. Değerlendirme modülü aynı zamanda, SOX ve PCI DSS uyumluluğu için rezerve edilen Oracle EBS ve SAP tablolarına yetkisiz erişim gibi uyumlulukla bağlantılı güvenlik açıklarını işaretler.

Değerlendirmeler iki geniş kapsamlı kategori halinde gruplanmıştır:

- Eksik yamalar, hatalı yapılandırılmış ayrıcalıklar ve varsayılan hesaplar gibi güvenlik açıklarına karşı güvenlik açığı ve yapılandırma testleri.
- Davranış testleri, aşırı sayıda başarısız oturum açma, sistem yönetimi komutları gerçekleştiren istemciler veya mesai saatleri dışında oturum açmalar gibi veritabanlarına erişim ve veritabanlarının işlenme şekillerini temel alarak güvenlik açıklarını tanımlar.

Değerlendirme modülü, ayrıntılı raporlar düzenlenmesine ek olarak alt seviyelerdeki verilere erişme yeteneği ile ağırlıklı ölçüler (en iyi uygulamalar doğrultusunda) ve endüstri standardı referans numaraları ile bir güvenlik durumu raporu kartı oluşturur ve veritabanı güvenliğinin güçlendirilmesi için somut eylem planları önerir.

Yapılandırma kilitleme ve değişiklik izlemeGüvenlik açığı değerlendirmesi sonucunda önerilen eylemleri uyguladıktan sonra, artık bir güvenli yapılandırma standardı belirleyebilirsiniz. InfoSphere Guardium'un Yapılandırma Denetimi Sistemini kullanarak bu standartta oluşan değişiklikleri izleyebilir ve değişikliklerin yetki verdiğiniz değişiklik denetimi ilkelerinin ve süreçlerinin dışında gerçekleştirilmediğinden emin olabilirsiniz.

İzleme ve Uygulama

Veritabanı güvenliği ve değişiklik denetimi için ilkeleri izleyin ve uygulayın
InfoSphere Guardium, ayrıcalıklı veritabanı hesapları tarafından yetkisiz veya şüpheli işlemleri ve ayrıca denetim dışı kullanıcıların veya yabancıların saldırılarını önlemek için parçacıklı, gerçek zamanlı ilkeler sağlar. Aynı zamanda, Oracle EBS, PeopleSoft, Siebel, SAP, Cognos gibi ortak bir hizmet hesabından veritabanlarına erişen veya IBM Web Sphere, Oracle WebLogic ve Oracle AS gibi uygulama sunucuları üzerinde oluşturulan özel sistemler gibi çok katmanlı uygulamalar aracılığıyla veritabanlarında yetkisiz değişiklikler yapan uygulama kullanıcılarını tanımlayabilirsiniz.

Çözüm, bilgi güvenliği personeli tarafından veritabanı yöneticilerinin müdahalesini gerektirmeksizin yönetilebilir. Ayrıca işletim sistemi oturum açma, IP veya MAC adresi, kaynak uygulama, saat, ağ iletişim kuralı ve SQL komutu türü doğrultusunda belirli tablolara erişimi kısıtlayan parçacıklı erişim ilkeleri tanımlayabilirsiniz.

Tüm veritabanı trafiğinin sürekli olarak bağlamsal analizi
InfoSphere Guardium, her SQL işleminin "kim, ne, nerede, ne zaman ve nasıl" olmak üzere ayrıntılı bağlamsal bilgilerini temel alarak yetkisiz işlemleri belirlemek için patent başvurusu yapılmış dilbilimsel analizden yararlanır ve tüm veritabanı işlemlerini gerçek zamanlı olarak sürekli izler.

Bu özgün yaklaşım, yanlış pozitifleri ve negatifleri en aza indirgerken aynı zamanda, sadece önceden tanımlı kalıplar veya imzalar arayan geleneksel yaklaşımların aksine daha önce benzeri görülmemiş bir denetim düzeyi sağlar.

Anormal davranışların belirlenmesi ve ilke tanımlamanın otomatikleştirilmesi için standartları belirleme
Sistem, bir standart belirleyerek ve hem normal iş süreçlerini, hem de anormal etkinlikler gibi görünenleri tanımlayarak, SQL injection gibi saldırıların önlenmesinde kullanabileceğiniz ilkeleri otomatik olarak önerir. Özel ilkeler, kolay anlaşılır açılan menüler aracılığıyla kolaylıkla eklenebilir.

Proaktif, gerçek zamanlı güvenlik
InfoSphere Guardium, yetkisiz veya anormal davranışlara proaktif olarak yanıt verilmesi için çok sayıda gerçek zamanlı denetim sağlar. İlke tabanlı işlemler arasında gerçek zamanlı güvenlik uyarıları (SMTP, SNMP, Syslog); yazılım engelleme; tam günlük kaydını etkinleştirme; kullanıcıların karantinaya alınması ile özel işlemler, örneğin, VPN kapısı kapatma ve çevresel izinsiz giriş algılama ve önleme sistemleriyle koordinasyon yer alabilir.

Güvenlik olaylarının takip edilmesi ve çözülmesi
Uyumluluk düzenlemeleri, kuruluşların tüm olayların kaydedildiğini, analiz edildiğini, zamanında çözüldüğünü ve yönetime bildirildiğini kanıtlamalarını gerektirmektedir. InfoSphere Guardium, açık olayların sayısı, önem düzeyleri ve olayların açık olduğu süre gibi temel ölçülerin takibi için bir gösterge panosuna ek olarak, güvenlik olaylarının çözülmesi için bir iş kullanıcısı arabirimi ve iş akışı otomasyonu sunar.

Denetleme ve Raporlama

Parçacıklı bir denetim yolunun yakalanması
InfoSphere Guardium, proaktif denetimlerin uygulanması ve denetçilerin gerekli gördüğü belirli bilgilerin sağlanması için bağlamsal olarak analiz edilen ve gerçek zamanlı olarak süzülen tüm veritabanı etkinliklerinin çok parçacıklı ve sürekli bir yolunu oluşturur.

Sonuçta oluşturulan raporlar, başarısız oturum açmalar, ayrıcalıkların üst seviyelere yükseltilmesi, şema değişiklikleri, mesai saatleri dışında veya yetkisiz uygulamalardan erişim ve hassas tablolara erişim gibi tüm veritabanı etkinliklerinin ayrıntılı görünümünü sağlayarak uyumluluğu kanıtlar. Örneğin, sistem aşağıdakilerin tamamını izler:

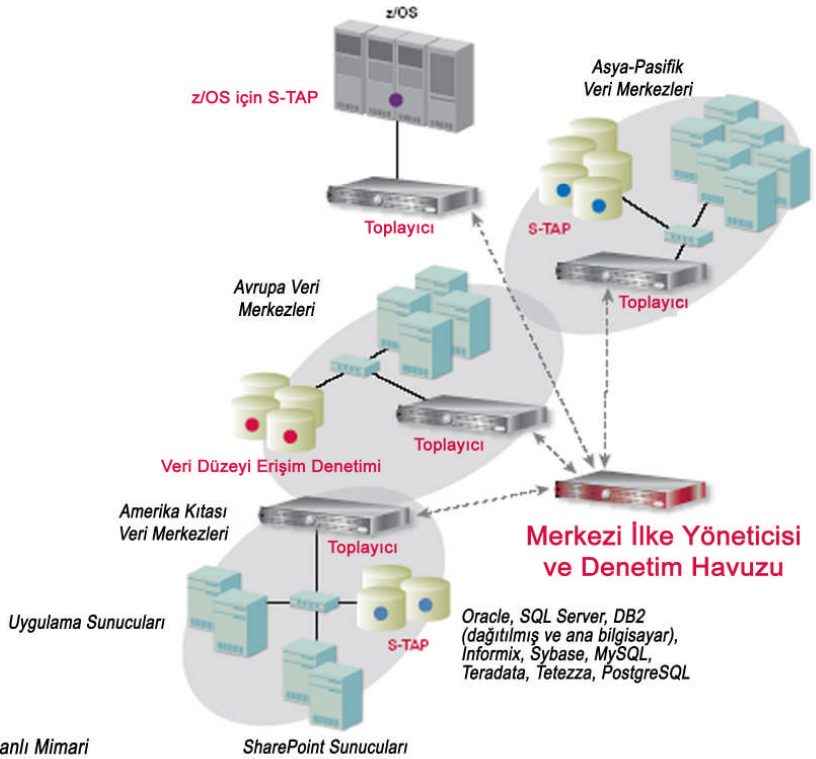
- SQL hataları ve başarısız oturum açmalar gibi özel güvenlik durumları.
- Veritabanı yapılarını değiştiren ve özellikle SOX gibi veritabanı yönetişimi düzenlemeleri açısından önemli olan Tablo Oluştur/Bırak/Değiştir gibi DDL komutları.
- Özellikle PCI DSS gibi veri gizliliği düzenlemeleri için önemli olan SELECT sorgulamaları.
- Bağlama değişkenleri dahil olmak üzere DML komutları (Ekle, Güncelle, Sil).
- Hesapları, görevleri ve izinleri denetleyen DCL komutları (VER, GERİ AL).
- PL/SQL (Oracle) ve SQL/PL (IBM) gibi her DBMS platformu tarafından desteklenen prosedür dilleri.
- Veritabanı tarafından çalıştırılan XML.
- SharePoint nesnelerindeki değişiklikler.

Sınıfının en iyisi raporlama
InfoSphere Guardium çözümü, en iyi uygulamaları ve dünyanın her yanındaki Global 1000 şirketleriyle, Büyük 4 denetçileri ve eksperleriyle çalışma deneyimimizi temel alan 150'den fazla önceden yapılandırılmış ilke ve rapor içermektedir. Bu raporlar, SOX, PCI DSS gibi yasal gereksinimlerin ve veri gizliliği yasalarının karşılanmasına yardımcı olabilir ve veri yönetişimi ile veri gizliliği girişimlerini optimize eder.

InfoSphere Guardium, önceden paketlenmiş rapor şablonlarına ek olarak, yeni raporların kolay oluşturulması veya mevcut raporların değiştirilmesi için grafiksel bir sürükle ve bırak arabirimi sağlar. Raporlar, kullanıcılara PDF biçiminde (ek olarak) veya HTML sayfalarına bağlantılar biçiminde otomatik olarak e-posta ile gönderilebilir. Bunlar aynı zamanda, Web konsolu aracılığıyla çevrimiçi olarak görüntülenebilir veya standart biçimlerde Güvenlik Bilgileri ve Olay Yönetimine ve diğer sistemlere aktarılabilir.

Kuruluşunuz için Ölçeklenebilir

- Müdahalesiz: en düşük seviyede performans etkisi ve herhangi bir veritabanı veya uygulama değişikliği olmaksızın ayrıcalıklı kullanıcıların yerel erişimi de dahil olmak üzere tüm veritabanı işlemlerinde %100 görünürlük.
- DBMS'den bağımsız: yerel günlük kaydına veya denetime bağımlı olmayan platformlar arası çözüm.
- Aygıt tabanlı: "kara kutu" aygıtları (kendi içinde depolama, önceden kurulu uygulamalar, yerleşik yönetim) aracılığıyla hızlı devreye alma için güçlendirilmiş Linux çekirdeği üzerinde oluşturulan modüler yazılım paketi. Donanım birleştirme stratejilerinin desteklenmesi için bir sanal aygıt olarak da mevcuttur.
- Esnek İzleme: hafif, ana bilgisayar tabanlı sensörler, SPAN kapıları, ağ izleyicileri veya bunların herhangi bir kombinasyonu aracılığıyla.
- Altyapı hazır: SNMP, SMTP, Syslog, LDAP, Kerberos, RSA SecurID® desteği, BMC Remedy, CEF gibi değişiklik bildirim sistemleri ve tüm önde gelen Güvenlik Bilgileri ve Olay Yönetimi platformları ile bütünleştirme.
- Çok katmanlı: endüstride benzersiz olan InfoSphere Guardium, çok sayıda veritabanı platformundan ve konumundan denetim bilgilerini otomatik olarak tek merkezi denetim havuzunda birleştirir ve normalleştirir.
- Merkezileştirilmiş yönetim: Web konsolu aracılığıyla DBMS çapındaki güvenlik ilkelerinin kuruluş çapında yönetilmesi.
- Ölçeklendirilebilir: izlenen sunucuların veya trafik hacminin artmasıyla birlikte, artan yükün karşılanması için sadece aygıtlar eklenmesi yeterlidir. Patentli, zeki depolama algoritmaları, geleneksel düz dosya tabanlı yaklaşımlara göre 100 kat daha iyi depolama verimliliği sağlar.
- Müdahale edilemeyen denetim havuzu: kök dizini olmaksızın güçlü kimlik doğrulaması ve şifreli arşivler.
- Görev tabanlı: modüllere ve verilere erişim, kurumsal görevler doğrultusunda denetlenir.



Ölçeklenebilir Çok Katmanlı Mimari

InfoSphere Guardium'un ölçeklenebilir mimarisi, denetim verilerinin merkezi olarak birleştirilmesi ve normalleştirilmesi ve kuruluş çapındaki güvenlik ilkelerinin bir Web konsolu aracılığıyla merkezi olarak yönetilmesi yoluyla hem büyük, hem de küçük ortamları destekler. S-TAP'lar, hafif, ana bilgisayar tabanlı algılayıcılardır. Bunlar, ayrıcalıklı kullanıcıların yerel erişimi dahil olmak üzere tüm veritabanı trafiğini izler ve analiz ile raporlama için bu bilgileri InfoSphere Guardium toplayıcı aygıtlarına yönlendirir. Toplayıcı aygıtlar, izlenen verileri S-TAP'lardan alır ve/veya doğrudan ağ anahtarlarındaki SPAN kapılarına bağlanır. Birleştiriciler, çok sayıda toplayıcı aygıtından denetim verilerini otomatik olarak birleştirir. En yüksek düzeyde ölçeklenebilirlik ve esneklik için çok sayıda birleştirici katmanı yapılandırabilirsiniz. S-TAP'lara genişletme olarak uygulanan InfoSphere Guardium Data-Level Access Control olanağı da güvenliği güçlendirir ve veritabanı yöneticilerinin yeni veritabanı hesapları oluşturmak ve mevcut hesaplar için ayrıcalıkları artırmak gibi güvenlik işlemleri gerçekleştirmesini önleyerek görevlerin ayrılmasını sağlar.

Uyumluluk iş akışı otomasyonu

Endüstride benzersiz olan InfoSphere Guardium Uyumluluk İş Akışı Otomasyonu uygulaması, tüm uyumluluk iş akışı sürecini optimize eder ve denetim raporu oluşturma sürecinin, önemli paydaşlara dağıtımın, elektronik onayların ve üst seviyelere yükseltmelerin otomatikleştirilmesine yardımcı olur. İş akışı süreçleri, ayrıntılı bir düzeyde tamamen kullanıcı tarafından özelleştirilebilir ve belirli denetim başlıklarının bağımsız olarak yönlendirilmesine ve onaya kadar takip edilmesine olanak sağlar.

Türdeş Olmayan Ortamlar için Birleşik Çözüm

Geniş platform desteği

InfoSphere Guardium'un platformlar arası çözümü, tüm önde gelen işletim sistemleri (Windows, UNIX, Linux, z/OS) üzerinde çalışan tüm önde gelen DBMS platformlarını, iletişim kurallarını ve aynı zamanda Microsoft SharePoint ve FTP ortamlarını destekler:

Desteklenen Platform	Desteklenen Sürümler
Oracle Database	8i, 9i, 10g (r1, r2), 11 g, 11 gR2
Oracle Database (ASO, SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2003, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10, 11,11.50
Sun MySQL ve MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.X, 12, 13
FTP	

Ana bilgisayar tabanlı izleme

Endüstride benzersiz olan S-TAP'lar, veritabanı sunucusu işletim sistemi düzeyinde hem ağ, hem de yerel veritabanı iletişim kurallarını (paylaşılan bellek, adlandırılmış kanallar, vs.) izleyen hafif yazılım algılayıcılarıdır. S-TAP'lar, günlük verilerinin işlenmesi ve depolanması için veritabanının kendisine güvenmek yerine tüm trafiği gerçek zamanlı analiz ve raporlama için ayrı InfoSphere Guardium aygıtlarına yönlendirerek sunucu performansı üzerindeki etkiyi en aza indirger. S-TAP'lar genellikle uzak konumlarda özel olarak ayrılmış donanım aygıtlarına veya veri merkezinizdeki kullanılabilir SPAN kapılarına olan gereksinimi ortadan kaldırmaları nedeniyle tercih edilir.

İşletim Sistemi Tipi	Sürüm	32-Bit ve 64-Bit
AIX	5.1, 5.2, 5.3,	Her ikisi
	6.1	64-Bit
HP-UX	11.00, 11.11, 11.23, 11.31	Her ikisi
Red Hat Enterprise Linux	3, 4, 5	Her ikisi
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Her ikisi
SUSE Enterprise Linux for System z	9, 10, 11	
Solaris - SPARC	8, 9, 10	Her ikisi
Solaris - Intel/AMD	10	Her ikisi
Tru64	5.1A, 5.1B	64-Bit
Windows	2000, 2003, 2008	Her ikisi
iSeries	i5/OS*	

Uygulama izleme

InfoSphere Guardium, kritik tablolara doğrudan veritabanına erişim yerine çok katmanlı kurumsal uygulamalar aracılığıyla erişen son kullanıcıların etkinliklerini izleyerek potansiyel dolandırıcılık girişimlerini tanımlar. Kurumsal uygulamalar genellikle "bağlantı havuzu oluşturma" adı verilen bir optimizasyon mekanizması kullandığından bu gereklidir. Havuz oluşturulan bir ortamda, tüm kullanıcı trafiği sadece genel bir hesap adı ile tanımlanan ve buna bağlı olarak son kullanıcıların kimliğini gizleyen birkaç veritabanı bağlantısında birleştirilir. InfoSphere Guardium, tüm önde gelen kullanıma hazır kurumsal uygulamalar için uygulama izlemeyi destekler. Şirket içi uygulamalar dahil olmak üzere diğer uygulamalar için destek, işlemlerin uygulama sunucusu düzeyinde izlenmesi ile sağlanır.

Desteklenen Kurumsal Uygulamalar	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
Desteklenen Uygulama Sunucusu Platformları	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform

IBM InfoSphere Guardium Hakkında

Guardium, sistemleriniz çapında güvenilir bilgilerin tanımlanmasına, bütünleştirilmesine, korunmasına ve yönetilmesine yönelik bütünleştirilmiş bir platform olan IBM InfoSphere'in bir parçasıdır. InfoSphere Platformu, veri bütünleştirme, veri ambarlama, ana veri yönetimi ve bilgi yönetişimi gibi bir paylaşılan üstveri ve modeller çekirdeği çevresinde bütünleştirilmiş temel güvenilir bilgi yapı taşlarını sağlar. Portföy modülerdir ve herhangi bir yerden başlamanıza ve InfoSphere yazılımı yapı taşlarını diğer satıcı firmaların bileşenleri ile birleştirmenize veya daha yüksek hız ve değer için çok sayıda yapı taşını bir arada devreye almayı tercih etmenize olanak sağlar. InfoSphere Platformu, zorlukların basitleştirilmesi ve işiniz için güvenilir bilgilerin daha hızlı sağlanması için gerekli olan performansı, ölçeklenebilirliği, güvenilirliği ve hızlandırmayı sağlayarak, bilgi yoğun projeler için kurumsal standartlarda bir temel sunar.

IBM Corporation
Route 100
Somers, NY 10589

Amerika Birleşik Devletleri'nde hazırlanmıştır.

Mayıs 2010

InfoSphere®
software