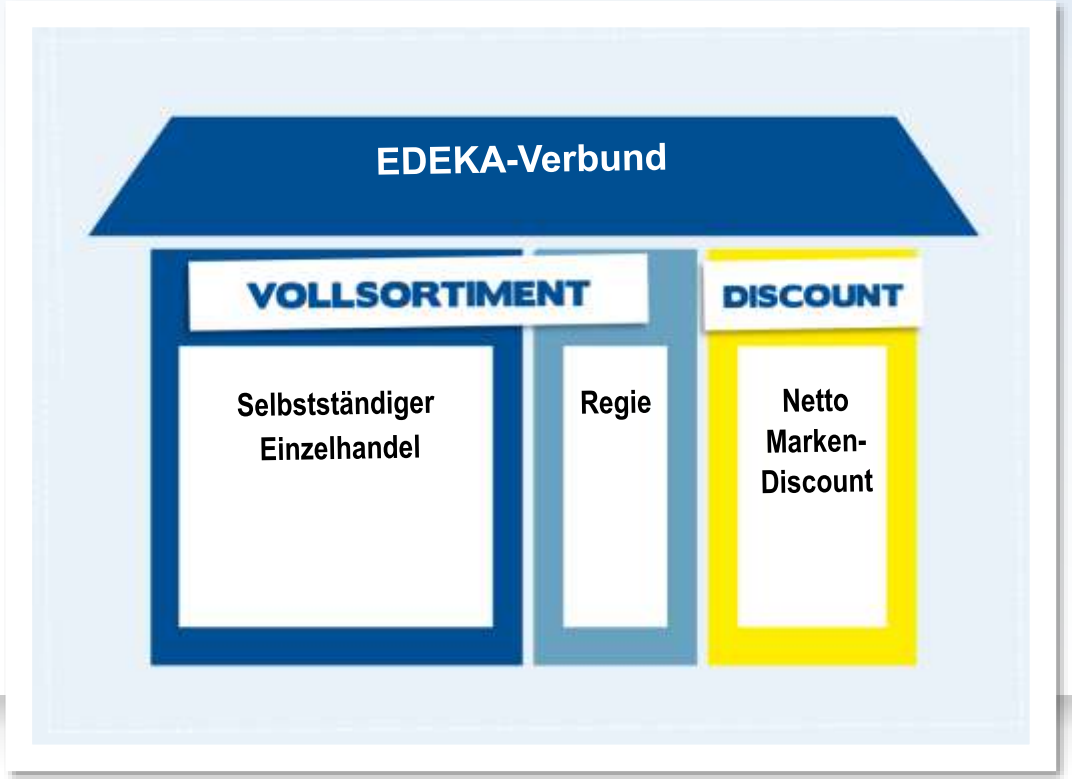
Brauche ich ein Database Activity Monitoring?

DOAG SIG Monitoring | 26.06.2018 | Sebastian Kilchert | Lunar GmbH

EDEKA

Unternehmergeist auf allen Ebenen



- EDEKA steht seit über 100 Jahren für das genossenschaftliche Prinzip der Eigenverantwortung
- Kerngeschäftsfeld ist das von rund 3.800 selbstständigen Unternehmern geführte Vollsortimentsgeschäft
- Zweite Säule: Netto Marken-Discount

Qualifizierte Nahversorgung für Deutschland

Daten & Fakten 2017

- EDEKA ist ausschließlich in Deutschland aktiv
- 7.227 EDEKA-Märkte &
  4.200 Netto Marken-Discount-Filialen
  - bis zu 50.000 Produkte
  - 12 Mio. Kundenkontakte täglich
- 369.300 Mitarbeiter
- 17.150 Auszubildende in rund 40 Ausbildungsberufen
- 58 Existenzgründer
- das größte Markenartikelsortiment im deutschen Handel

Die LUNAR GmbH ist der IT-Dienstleister des EDEKA Verbunds

Die LUNAR GmbH…

- beeinflusst maßgeblich die IT-Strategie der EDEKA-Verbund
- ist der IT-/Prozessdienstleister in der EDEKA-Verbund
- realisiert und betreut innovative Templatelösungen
- verzahnt die Prozesse des Einzel- und Großhandels sowie der EDEKA-Zentrale
- deckt diverse IT-Leistungen für die EDEKA-Verbund ab
- beschäftigt ca. 600 MitarbeiterInnen an den Standorten Mannheim und Hamburg

Agenda

01 Was ist ein Database Activity Monitoring (DAM)?

02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern

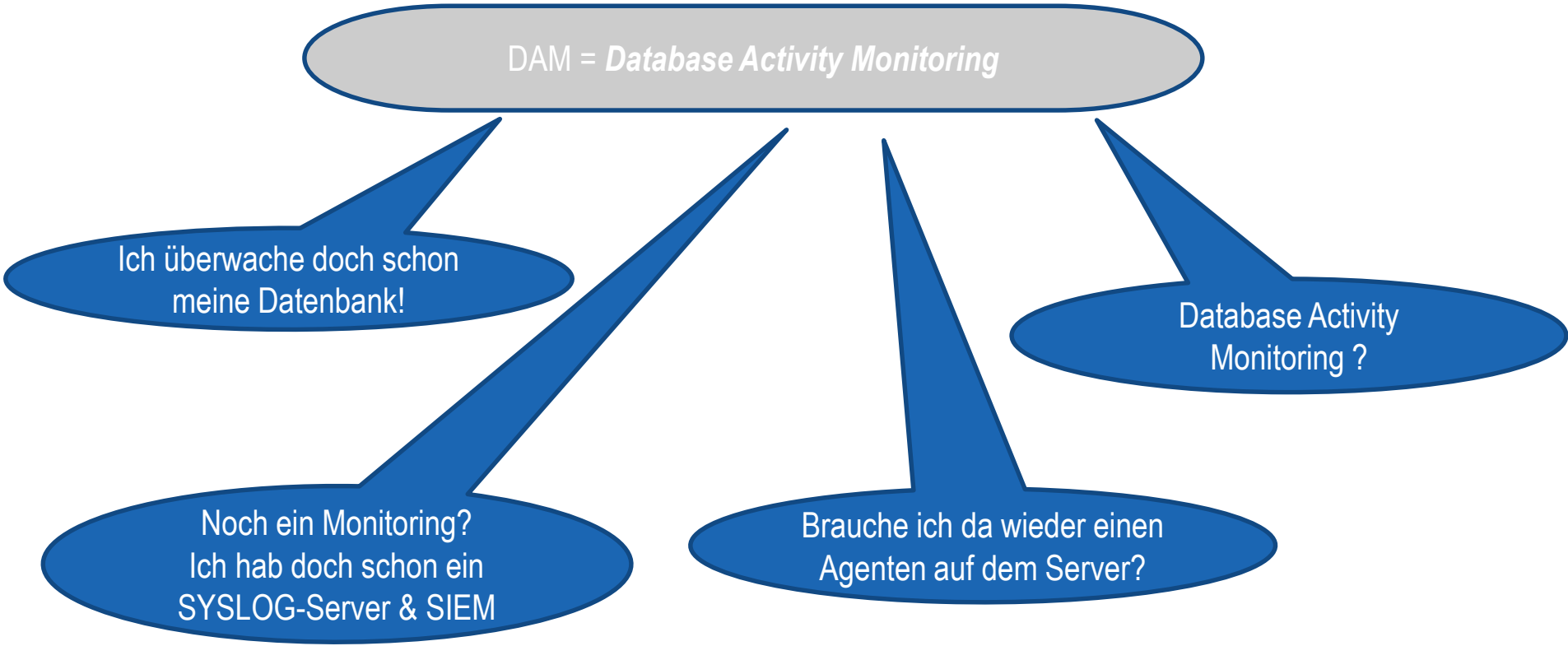
Agenda

01 **Was ist ein Database Activity Monitoring (DAM)?**

02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern

Was ist ein DAM?



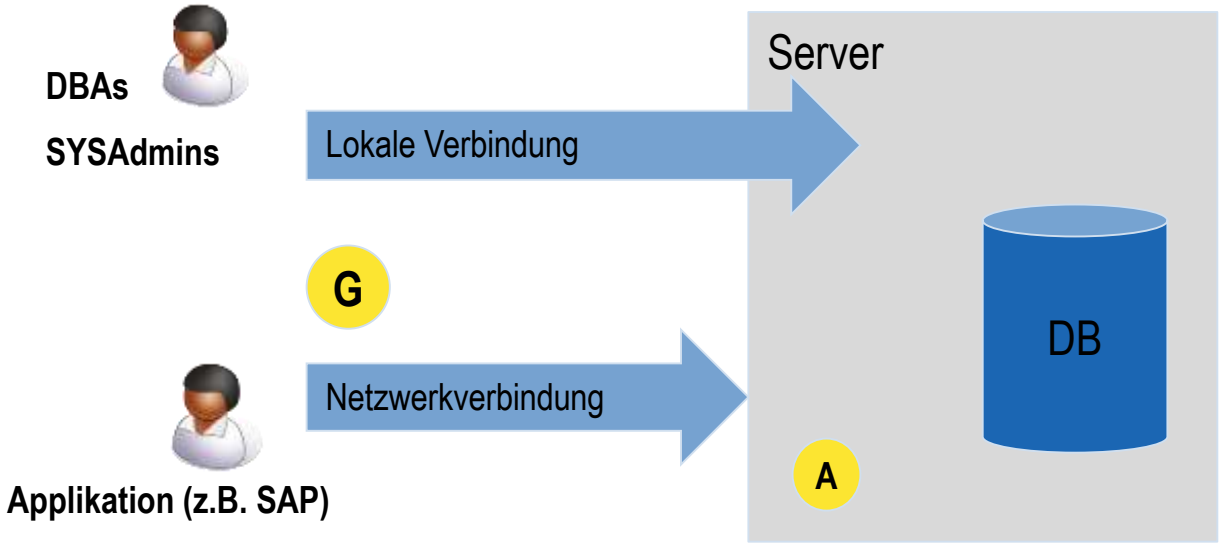
Auditing oder Security-Maßnahmen bringen ohne entsprechendes Monitoring nichts!

Wie unterscheidet sich ein „DAM“ von einem „normalen“ Monitoring?

Was ist Database Activity Monitor

- Kombiniert Auditing (Protokollierung) und Firewall/Alerting für die DATENBANK
- Sinnvolle und wichtige Ergänzung zu anderen Sicherheitsprodukten
- Dient der Sichtbarkeit und dem Aufdecken von Auffälligkeiten oder Angriffen
- Aktives Einwirken möglich
- Agent- und/oder Netzwerkbasiert
- Zugriffe auf Objekte für alle Benutzerarten einschränkbar
- Abgrenzung von Verantwortungsbereichen möglich
- Auswertung/Reporting bzw. Analysemöglichkeiten
- Generell für die gängigsten Datenbanken verfügbar
- Zusätze Sicherheitsprüfungen (Compliance Checks) möglich

Kurzübersicht



Verbindungsmöglichkeiten

- **Aus der DB**
- **Vom Server aus**
- **Über das Netzwerk**

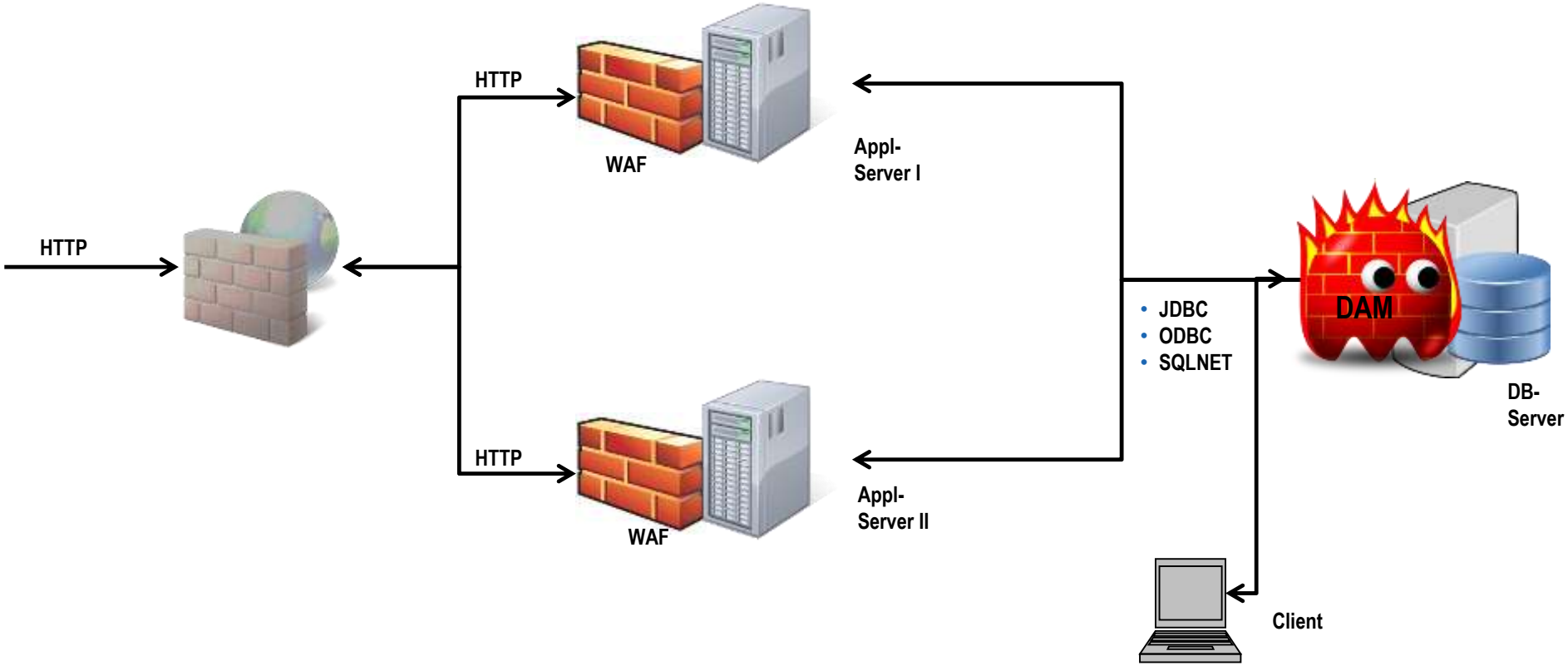
G = Gateway
A = Agent

Unterschiede DAM, Syslog-Server und WAF (Web Application Firewall)

Database Activity Monitoring	Syslog-Server	Wep Application Firewall
Kann Angriffe mitbekommen, bevor sie in der Datenbank ausgeführt werden	Bekommt die Informationen erst wenn Sie passiert sind	Sitzt zw. Client und Applikationsserver
Kann aktiv einwirken und ggf. Session beenden oder ins Leere laufen lassen	Kann nicht direkt Angriffe verhindern	Firewall für Webanwendungen – Nicht für Datenbanken
Kann Konfigurationen gegen einen „Standard“ prüfen (Compliance)	-	Für statische Requests geeignet
Zieht Daten direkt über den Agent und/oder im Netzwerk ab. Braucht größtenteils keine/wenig extra Mechanismen	Oftmals müssen extra Logging etc. eingeschaltet werden	
Dient einer revisionssicheren Protokollierung		
Versteht die SQL-Sprache und kann somit verdeckten Angriffen zuvor kommen		

Kombination DAM & WAF empfohlen!

Ansatzpunkte WAF & DAM



Agenda

01 Was ist ein Database Activity Monitoring (DAM)?

02 **Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?**

03 Übersicht/Unterschiede von drei größeren Anbietern

In der Regel sind Daten in Datenbanken gespeichert…

Einsatzszenarien

Geschäftsinteressen

- Schutz vor gezielten Angriffen
- Schutz der geschäftskritischen Daten
- Verfügbare Systemabläufe

Betrieb

- Verfügbarkeit der Datenbanken
- Änderungsnachvollziehbarkeit
- Schutz der Datenbanken

Compliance & rechtl. Verpflichtungen

- Schutz sensitiver Daten
- Schutz vor Datendiebstahl
- Ggf. grenzüberschreitender Datenverkehr

Bei einem Einsatz eines DAMs werden die folgenden TOMs* (Auszug) gemäß BDSG-neu §64 erfüllt

FOKUS DATENBANK

Zugangskontrolle *(Zutrittskontrolle)*
– Meistens kein DB Thema

Zugangskontrolle
✓ Zuordnung Benutzerrechte
✓ Passwortvergabe
✓ Authentisierung
✓ Protokollierung
✓ Einsatz IDS
✓ Erstellung Benutzerprofilen
✓ Einsatz Firewalls

Datenträgerkontrolle *(Weitergabekontrolle)*
✓ Anonymisierung vor Weitergabe
✓ Kontrolle der Zugriffberechtigungen von Datenträgern

Speicherkontrolle *(ehem. Teil der Zugriffskontrolle)*
✓ Verschlüsselung von Datenträgen
✓ Protokollierung
✓ Protokollierung von Zugriffen
✓ Rechteverwaltung

Benutzerkontrole *(Weitergabekontrole)*
✓ Übersicht der Abrufe
✓ Anonymisierung vor Weitergabe
✓ Rechteverwaltung

Zugriffskontrolle
✓ Protokollierung von Zugriffen
✓ Verschlüsselung von Datenträgen
✓ Rechteverwaltung
✓ PW-Konzepte/Richtlinien

Übertragungskontrolle *(Weitergabekontrolle)*
✓ Protokollierung von Zugriffen

Eingabekontrolle
✓ Protokollierung, Wer hat wann, was gemacht
✓ Vergabe von Rechten

Transportkontrolle *(Weitergabekontrolle)*
✓ Anonymisierung vor Weitergabe
✓ Netzwerkverschlüsselung
✓ Integritätsprüfung

Wiederherstellbarkeit (Neu)
✓ Backup & Recovery Tests
✓ Hochverfügbarkeit

Zuverlässigkeit (Neu)
✓ Monitoring von Fehlern
✓ Hochverfügbarkeit

Datenintegrität (Neu)
✓ Protokollierung
✓ Bildung von HASH-Werten

Auftragskontrolle
✓ Sicherstellung der Vernichtung von Daten nach Auftrag
✓ Laufende Überprüfung des Auftragsnehmers
– Meistens kein reines DB Thema

Verfügbarkeitskontrolle
✓ Testen Datenwiederherstellung
✓ Aufbewahrung Datensicherung an sicheren Ort
✓ Backup & Recovery
✓ Protokollierung / Monitoring von Fehlern
✓ Hochverfügbarkeit

Trennungsgebot
✓ Physikalisch getrennte Speicherung
✓ Versehen Datensätze mit Zwecktrennung Attribute
✓ Mandantentrennung
✓ Verschlüsselung von Datensätzen
✓ Pseudonymisierung
✓ Trennung Prod. und Test-Umgebung
✓ Separate Tabelle, getrennte DBs

*TOM = technisch und/oder organisatorische Maßnahmen

**Blau gefärbter Text = Erfüllte TOMs durch DAM-Einsatz

Vorteile eines Database Activity Monitorings (1)

- DAM ist Auditing und Alerting mit Weiterleitungsfunktion an einen SIEM und/oder Syslog-Server
- DAM wertet das Ergebnis des „Execution Plans“ aus bzw. versteht SQL
  - Es sieht somit, was wirklich passiert
- Unterschiedliche Datenbankhersteller werden unterstützt mit einer zentralen Lösung
- DAM bietet einen direkten Schutz der Datenbanken, während Firewalls und Network Security die Infrastruktur schützen. DAM kann als "letzte" Verteidigungslinie betrachtet werden
- Minimierung des Risikos der Haftbarkeit, in dem man Angriffe sofort erkennt
- Eigene Compliance-Regeln können erstellt werden
- Im Zweifel fachgerechte Beurteilung und ggf. Eingreifen durch den DBA statt nur im Nachgang durch Analyse

Vorteile eines Database Activity Monitorings (2)

- DBA‘s und andere User können von den Applikationsdaten ferngehalten werden
- Absicherung der DBAs durch die Protokollierung (Auditing)
- unerlaubte Zugriffe auf die Applikationsdaten können protokolliert werden
- geringer Einfluss auf die Performance
- einfache Formulierung der Monitoring Regeln
- hunderte mögliche Regeln können definiert werden
- umfangreiche Reporting Möglichkeiten
- große Infrastrukturen werden unterstützt (skalierbar)
- Oft kann ein DAM mit weiteren Komponenten des Herstellers aufgestockt und ergänzt werden
- Oft sind zusätzliche Prüfungen und Scans durch‘s DAM möglich

Agenda

01 Was ist ein Database Activity Monitoring (DAM)?

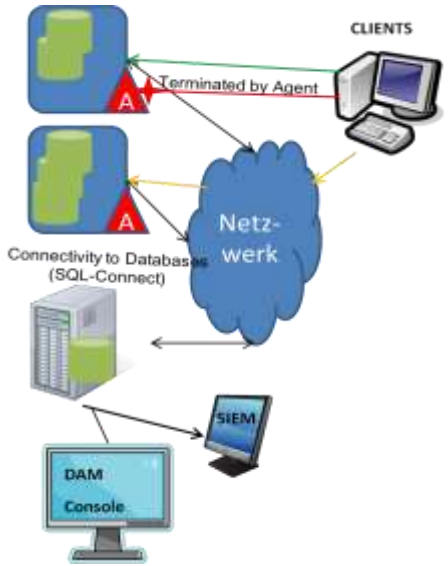
02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 **Übersicht/Unterschiede von drei größeren Anbietern**

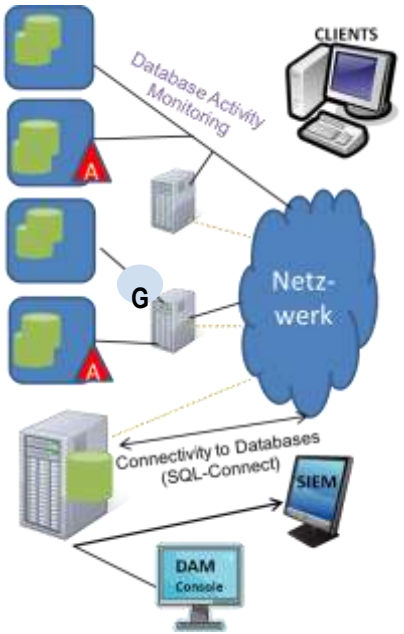
Drei größere Anbieter für Activity Monitoring

Architekturunterschiede der Anbieter

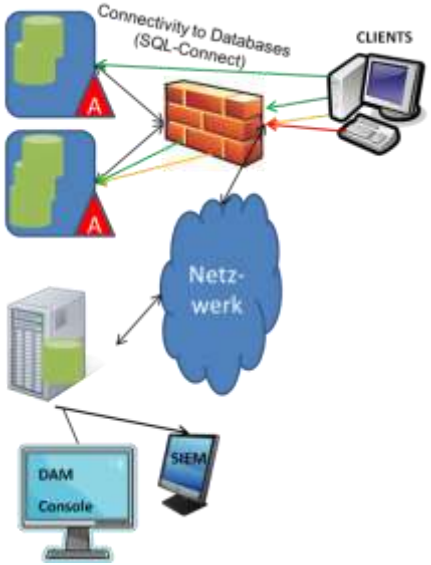
McAfee
Together is power.



IMPERVA



ORACLE



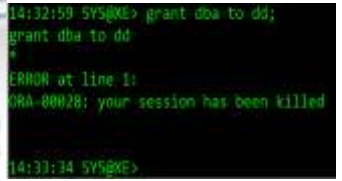
Unterstütze DB-Plattformen der Anbieter

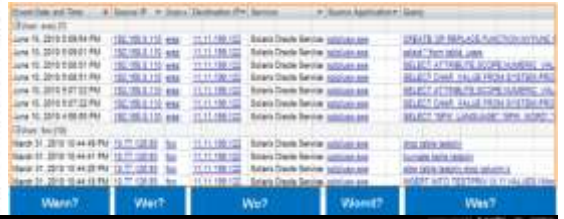
	McAfee Together is power.	IMPERVA	ORACLE
Oracle	✓	✓	✓
MySQL	✓	✓	✓
Microsoft SQL Server	✓	✓	✓
DB2	✓+	✓+	✓+
SYBASE	✓	✓	✓
TERADATA	✓	✓	
Maria DB	✓	✓	
PostgreSQL	✓	✓	
Progress OpenEdge		✓	
IBM Informix, Netezza		✓	
SAP HANA	✓	✓	

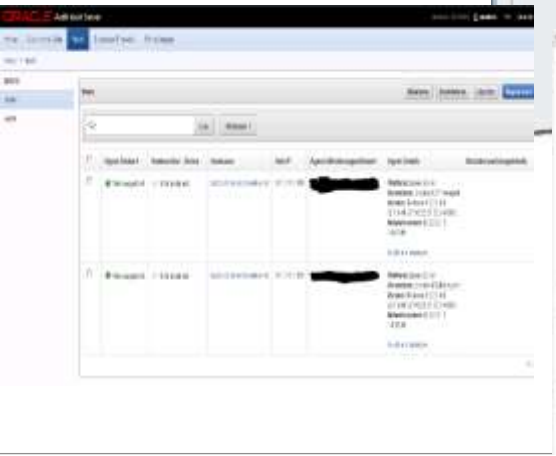
Webkonsolen

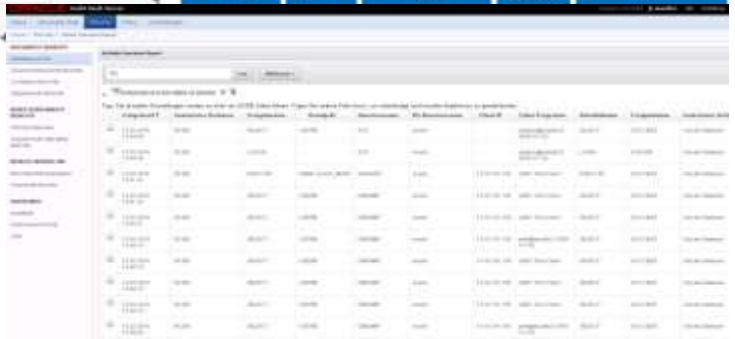
Die Ansicht, Menüführung und Steuerung der Konsolen ist Geschmackssache….

Webconsolen









Überlegungen für den Einsatz eines Database Activity Monitorings

- Definieren Sie die Systeme / Datenbanken die geschützt werden sollen
- Definieren Sie die Plattformen für Betriebssystem / Datenbank
- Prüfen Sie die Voraussetzungen für Compliance Checks
- Definieren Sie Reports- und Analyseanforderungen
- Prüfen Sie Anforderungen aus Datenschutzgesichtspunkten / Sicherheitsanforderungen
- Definieren Sie Prozessuale Abläufe zwischen DBA, Sicherheits-Admin und Sicherheitsabteilung
- Gewichten Sie Ihre Anforderungen und Bewertungen der Anbieter

Passendes Produkt für Ihre Anforderung

Einführung oder Durchführung eines Proof of Concept (PoC) mit einem Hersteller

…aber

ohne eine Überwachung/Monitoring…

Haben Sie Fragen?