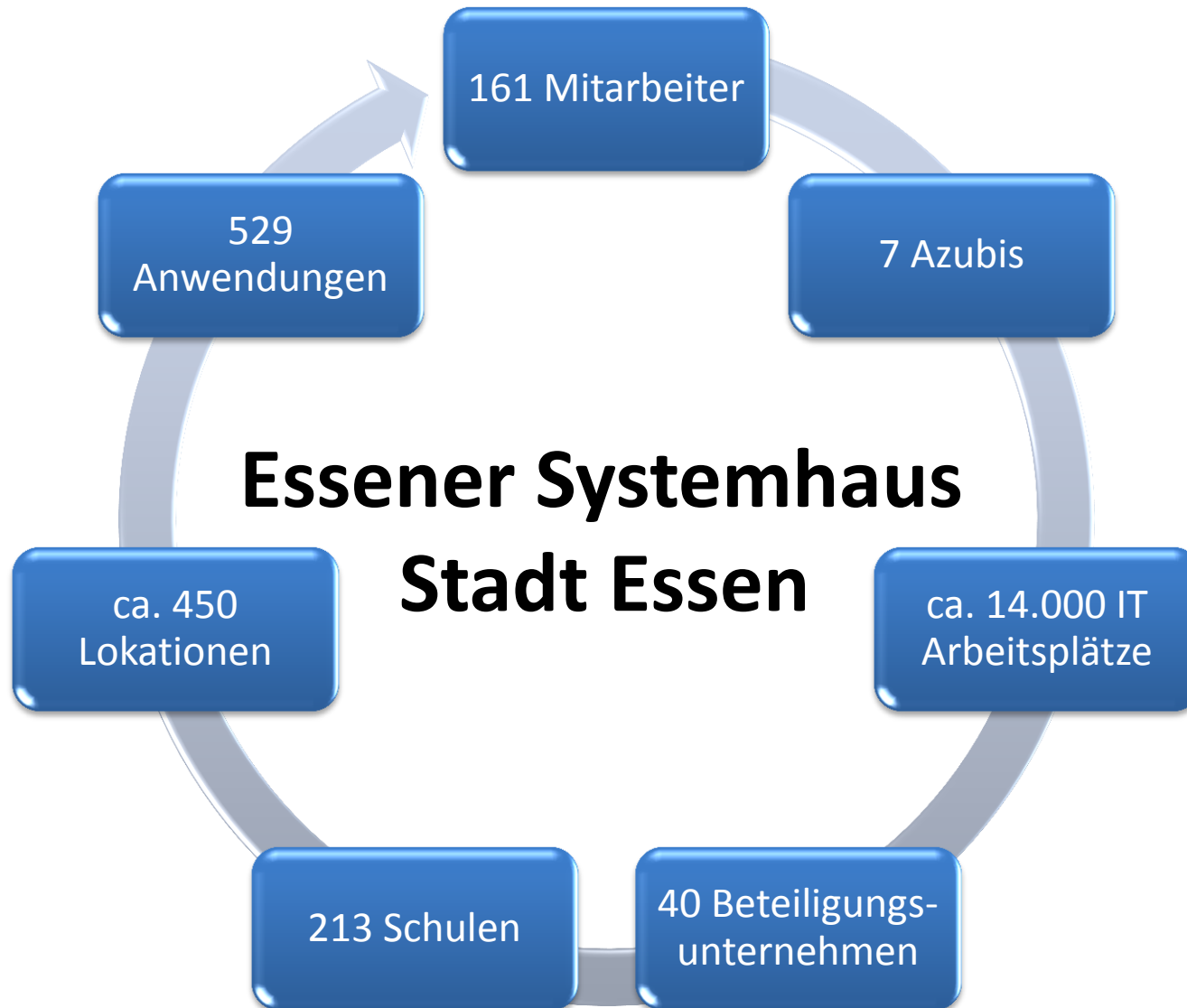


von

Torsten Husmann
Essener Systemhaus
Stadt Essen

Suvad Sahovic
Oracle Deutschland B.V. & Co. KG
Potsdam



- **Einführung**
 - Was war die Ausgangssituation?
 - Welche Probleme und Sorgen hatten wir?
 - Welche Lösungsansätze gab es?
 - Gründe für Audit Vault
- **Installation**
 - Einfachheit und Zeitaufwand
 - Komponente Audit Vault Server auf verschiedenen Maschinen
- **Aufgabenbereiche**
 - Rollenverteilung
 - Module unterhalb der Rollen

- **Erfahrungen**
 - Betriebserfahrungen
 - Betriebsprobleme
 - Cleaning
 - Patching
 - Strategie der Policies
 - Berichtswesen & Benachrichtigung
 - Umgang mit Alt-Daten
 - Ausblick in der Zukunft

- **Einführung**

- **Was war die Ausgangssituation?**

- Betrachtung der Betriebssicherheit im Oracle-Umfeld und Analyse aller Möglichkeiten zur Optimierung

- **Welche Probleme und Sorgen hatten wir?**

- Status einer öffentlichen Einrichtung mit entsprechenden Datenschutzbestimmungen

Vollständige und vielfältige Überwachung der Systeme , um Angriffe oder Versuche der Manipulation zu erkennen und nachzuweisen

- **Welche Lösungsansätze gab es?**

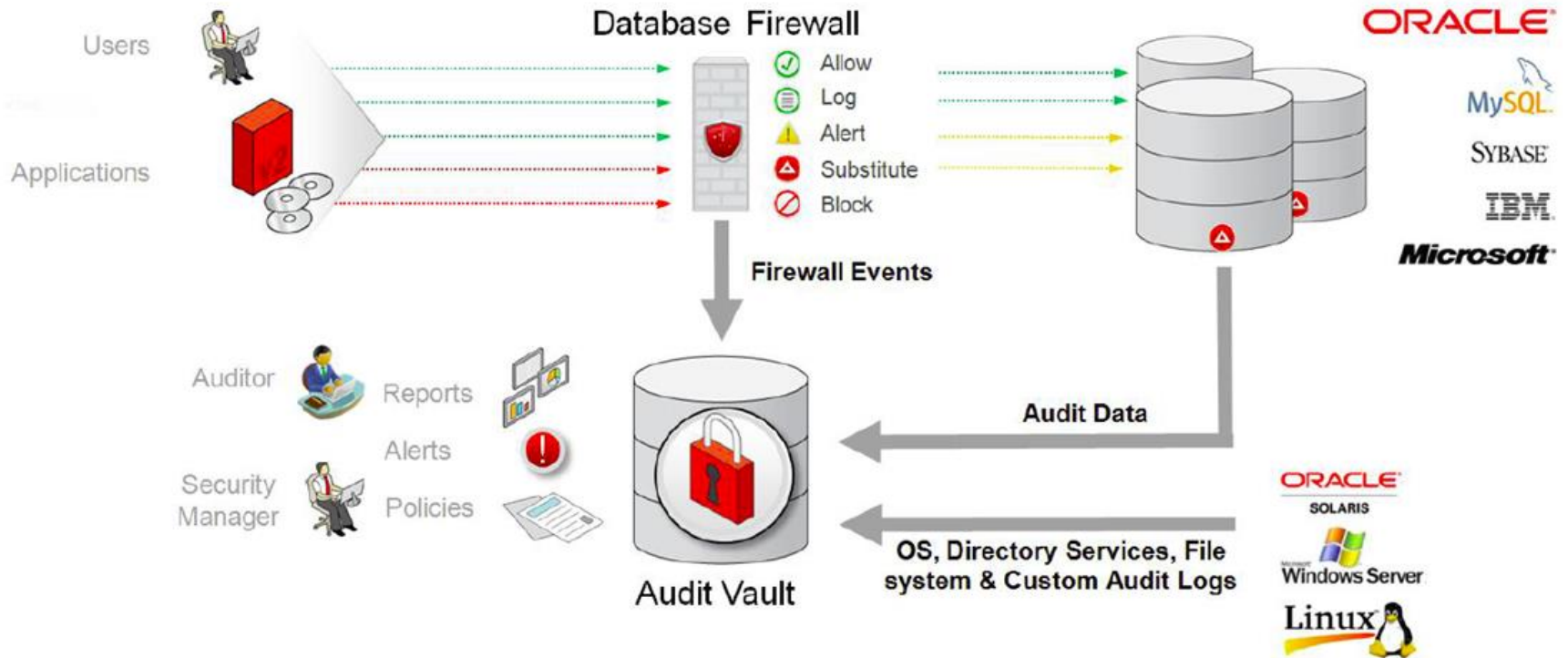
- Bordmittel, Syslog-Server, eingeschränkte User oder AuditVault

- **Gründe für AuditVault**

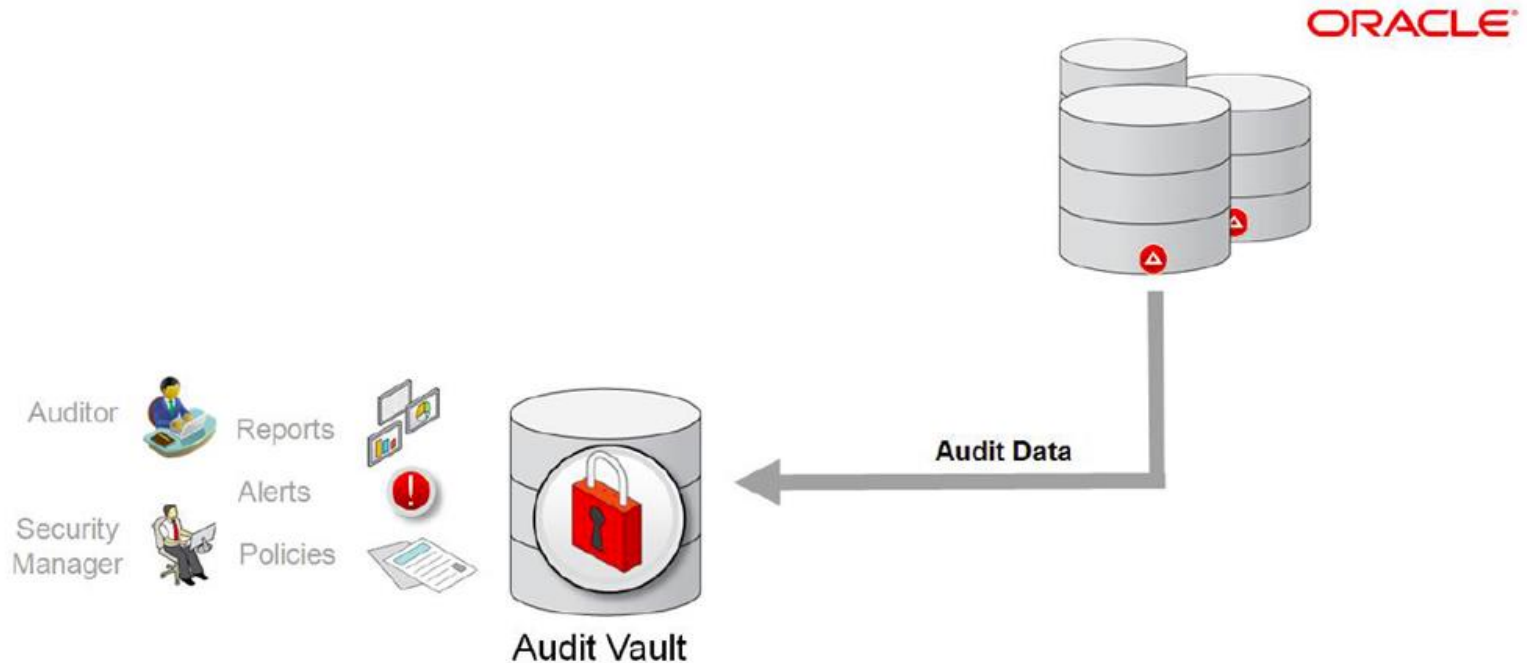
- Engpässe in der Verwaltung, proaktive Arbeit, unübersichtliche Datenbanken und ein gezieltes Logging

Zeitersparnis und Prinzip „Alles aus einer Hand“

Oracle Audit Vault & Database Firewall Architecture



Oracle Audit Vault & Database Firewall Architektur



- **Installation**

- **Einfachheit und Zeitaufwand**

- Einfache Installation: „Out of the Box“-Technik

- **Komponente Audit Vault Server auf verschiedenen Maschinen**

- Universelle Agenten auf den zu überwachenden PCs

- **Aufgabenbereiche**
 - **Rollenverteilung nach Aufgaben und Berechtigungen**
Zwecktrennung zwischen Administration und Datenverwaltung
 - **Module unterhalb der Rollen**
Admin-User: Verwaltung der Dienste und der Server
Audit-User: Verwalter der Daten und Berichte

- **Erfahrungen**

- **Betriebserfahrungen**

- Erste Erkenntnisse und Erfolge

- Hilfestellungen durch Audit Vault

- **Betriebsprobleme**

- Probleme durch Agentenstatus und falsche Keys

- **Cleaning**

- Umgang mit den gesammelten Daten

- **Patching**

- Patching von Linux, des Audit Vault Servers sowie der Agenten

- **Erfahrungen**

- **Strategie der Policies**

- Unterschiede zwischen einer User-Protokollierung und einer Befehls-Protokollierung

- **Berichtswesen & Benachrichtigung**

- Berichtswesen & Benachrichtigung

- **Umgang mit Alt-Daten**

- Grundsatzentscheidung: Löschen, archivieren oder halten

- **Ausblick in der Zukunft**

- Ausblick in der Zukunft

- **Kontaktadressen:**
 - **Torsten Husmann**
 - Systemadministrator
 - Essener Systemhaus / Stadt Essen
 - Kruppstraße 82-100
 - 45145 Essen

 - Telefon: +49 (0)201-88 17 342
 - Fax: +49 (0) 201-88 91 17 342
 - E-Mail: torsten.husmann@esh.essen.de
 - Internet: www.essen.de

 - **Suvad Sahovic**
 - Leitender Systemberater
 - Oracle Deutschland B.V. & Co. KG
 - Schiffbauergasse 14
 - 14467 Potsdam

 - Telefon: +49 (0) 331-2007-181
 - Fax: +49 (0) 331-2007-561
 - E-Mail: suvad.sahovic@oracle.com
 - Internet: <http://www.oracle.com>