Trustwave Database Security Solutions Prospecting Guide

Solution Description

Trustwave Database Security Solutions (DBSS) scan database and big data stores to identify configuration mistakes, identification and access control issues, missing patches, highly privileged users and any toxic combination of settings that could lead to escalation of privilege attacks, data leakage, denial-of-service (DoS), or the unauthorized modification of data held within data stores.

- Trustwave AppDetectivePRO is a security and audit practitioner tool that helps easily identify and fix database security issues, identify and eliminate excessive user permissions, and document compliance.
- Trustwave DbProtect is an enterprise-class database security risk and compliance solution that helps organizations quickly identify and reduce risk, manage access and protect sensitive data across all of its databases.

Key Buyers and Discovery Questions

SecOps	CRO/Audit/Compliance	IT Ops
• Work with development operations teams to ensure that systems are up to date • Security engineers document: • Requirements • Procedures • Protocols • Policy • Uncover hidden risks	• Enterprise-wide Certification and Accreditation or Authority to Operate • Comply with data security and privacy regulations such as HIPAA, GDPR, SOX, DISA-STIG. • Auditors document: ○ Audit Failures ○ Risk Mitigation ○ Regulatory Compliance	• Ensure that other users have the right resources • Create a set of processes and services for their internal or external clients • Conduct software deployments • Maintenance operations
	Discovery Questions	
• What is your company's approach to database security? • How do you protect databases from cyber threats today? • How do you identify database vulnerabilities today? • Are you worried about what information your users (privileged or not) have access to? Do you have a comprehensive program in place to manage user rights/entitlements?	• How confident are you that critical databases are compliant with government, regulatory or 3rd party requirements at any given time? • Are you worried about what information your users (privileged or not) have access to?	• How many databases do you maintain in various environments and how do you maintain a consistent inventory? • How well are you able to maintain a database inventory where business-criticality is associated to risk exposure? • How easy is it to consistently measure database vulnerabilities after each code change or patch release?
	Keywords to Listen For	
• It's very manual • It's not scalable • It's hard to track user privileges	• Reporting is inaccurate/incomplete/not timely • We have failed audits	• It's manual • It's not scalable • Concerned about consistently patching or addressing misconfigurations

Trustwave DBSS Value Proposition

Trustwave DBSS automates the security of critical data where it's stored, by performing three critical functions: uncovering vulnerabilities that would-be attackers could exploit, limiting user access to the most sensitive data and alerting on suspicious activities, intrusions and policy violations. Trustwave DbProtect will also take corrective action, as your team investigates the incident. Trustwave DBSS makes it easy to provide business leadership with the high-level risk trending, while also providing administrators and analysts the ability drill down into individual or groups of databases to address specific concerns.

Trustwave Database Security Solutions Prospecting Guide

Competitive Positioning by Key Competitor

Competitor	Strengths	Weaknesses	Positioning
IBM Guardium	• Most feature rich DBS portfolio in the market. • Significant corporate support • Huge existing customer base, easier cross-sell and ELA.	• Most expensive solution on the market. • Activity Monitoring requires network or Operating System reconfiguration • Cumbersome User Rights capabilities requires custom reporting.	• More cost effective • Easier to use, navigate • Shorter time frame from install to production
Imperva SecureSphere	• Strong database Activity Monitoring. • Aggressive in the market, massive marketing budget	• Large amounts of appliances to realize solution value • Activity Monitoring requires network reconfiguration • Rights Management requires 2 licenses to get level of detail we have with a single license	• More cost effective • Easier to use, navigate • Shorter time frame from install to production
Oracle	• Complete and natural integration into Oracle's Databases. • Oracle's AuditVault comes when you install the database and is a flip of switch type license.	• Only supports a very limited number of databases. • AuditVault and DataVault require additional licenses and specially trained DBAs on staff (more cost)	• More robust support of database types. Unless the customer is solely an Oracle shop, they'll need additional database support that Oracle cannot provide.
Nessus Tenable Professional	• Well known company with large customer base; brand recognition and easy cross sell to existing customers. • Modern, feature-rich SW. Especially strong in APAC • Scanning might be seen as "good enough" by some customers	• Knowledgebase not as comprehensive.	• We have four times the amount of security checks for databases, more built-in policies. • Tenable does not offer rights management nor Fix Scripts which offers how to fix issues that were identified
Qualys	• Robust cloud scanning suite. • Cloud-based with virtual or physical appliance needed for internal scanning. • Scanning is being pitched to customers as "good enough" for compliance, CIS.	• May require multiple modules depending on your platform needs.	• ADP does not require additional configuration as it's an all-in-one application. • Fix Scripts shows how to fix issues that were identified.

Objection Handling

I'm already protecting my most important database.
While you may have "better" security around your critical databases what are you doing for your databases used in development or embedded into applications? Do you know they exist? Do you know if they contain sensitive data? Do you know if they are vulnerable?

We don't have a database security problem because our IT auditor didn't find anything.
Often an audit is a solid first step into exploring database security. However, many clients I speak with have found that sometimes the goals of the IT audit were not directly related to the database controls, so nothing was found, leaving them with risks they were unaware of. Trustwave database security solutions can help you quickly identify your issues with risk-ranked association that will empower you to take the appropriate measure for mitigating risk.

Customer Success Story

A major energy company with numerous, disparate databases was regularly subject to industrial espionage attempts threatening exposure of intellectual property and data. Database audits were continually generating findings. Trustwave Database Solutions were leveraged to deploy enterprise-wide vulnerability and rights management as well as continuous monitoring to resolve audit findings. Security and compliance objectives were achieved, while easing the burden on IT Security and database administrator teams.