

## Software vs. Appliances

# Cost Considerations When Evaluating Database Activity Monitoring Solutions

### INTRODUCTION

When evaluating database activity monitoring (DAM) solutions, the total cost of ownership (TCO) should be factored into the decision process. DAM total cost of ownership includes:

- Capital costs
- Installation and set up costs
- Monitoring operation costs

Software-based solutions differ widely from appliance-based solutions in these costs. When they are not properly factored into the purchasing decision, organizations may find themselves spending more money on equipment and services than they planned, as well as wasting valuable IT resources.

The purpose of this white paper is to identify the cost components that should be considered when selecting a database activity monitoring solution.

### CAPITAL COSTS

List prices differ across DAM solutions and vendors often discount their pricing in order to win business. However, the initial DAM investment is just the tip of the iceberg, as organizations are often required to spend additional and unplanned capital. This is especially true with appliance-based solutions.

The first problem organizations face is sizing the DAM solution to meet their capacity requirements. This is not an exact science. Appliance vendors will cite a rule of thumb – one appliance will support X number of databases. In most cases

this is not accurate. As a result, organizations must purchase and deploy additional appliances to satisfy their capacity demands. Application Security (AppSec) solves this problem with flexible software licensing and our price guarantee. If AppSec underestimates capacity requirements, we provide additional software licensing free of charge.

Appliances can become resource constrained by the policies they are enforcing. Changes in database activity and compliance requirements may require upgrades to the appliance CPU, memory and/or storage. This entails additional hardware costs as well as the costs associated with field retrofitting the appliances.

Because appliances employ nonspecific monitoring of activity, collecting all database activity, they don't scale cost-effectively. Supporting an organization's database ecosystem growth will require purchasing and deploying additional appliances. AppSec's DbProtect utilizes precision monitoring, and thereby collects only relevant data. This significantly reduces the amount of data it collects. Precision monitoring combined with flexible software licensing, provides for greater scalability at a much lower cost.

Appliance technology refresh costs can also be prohibitive as appliance vendors turn over hardware platforms every three to four years. Eventually organizations are forced to swap out their existing appliances at a significant cost and disruption to their operations. These costs are avoided with DbProtect's software-only architecture as technology refreshes are a simple software download and don't require attendance at remote sites.

## INSTALLATION AND SETUP COSTS

Appliance vendors hype plug-and-play. One appliance connected to one database may be plug-and-play, however, multiple appliances supporting enterprise-wide databases are not. Appliances are deployed in a multi-tiered network architecture. “Dumb” copy and forward host-based agents transmit monitored activity to data collection appliances, which in turn sends data to management consoles and storage devices. Because of this and the high volume of traffic appliance-based solutions generate (nonspecific monitoring), the networking team needs to participate in the installation process to ensure this increased traffic does not impact network performance and introduce latency to critical business systems.

AppSec’s DbProtect is deployed in a single tiered network architecture. Intelligent host-based agents send data direct to management consoles and storage devices. Also, DbProtect filters data on the database host, and only transmits business relevant data (precision monitoring). Because of this simple

network architecture and significantly reduced volume of data, the network does not need to be reconfigured, freeing networking team resources for other important projects.

Policy development can be time-consuming and tie up valuable DBA resources. Appliance vendors will claim that learning-based policy development simplifies this process, when in reality, learning-based policy development does the exact opposite. In order to collect a valid sampling of data, you need to run learning mode for two to three months. However, the “baseline” policy generated is populated with false positives and negatives. Eliminating these false positives and negatives requires dedicating one or more DBA resources to analyze two to three months of data to modify the baseline policy.

DbProtect employs a knowledge-based policy development process. This simple top-down approach creates policy and business filters that eliminate false positives and negatives.

An easy-to-use wizard, featuring compliance templates and a validated library of rules, enables non-DBAs to do much of the work developing policy—therefore minimizing valuable DBA resources.

DbProtect draws upon the TeamSHATTER knowledgebase of database threats and vulnerabilities. With over 100 man-years of research, the TeamSHATTER knowledgebase provides the most comprehensive database vulnerability coverage. The TeamSHATTER knowledgebase frees DBA resources from time-consuming vulnerability research.

## Summary of Costs

	DbProtect™	Appliances
<b>CAPITAL COSTS</b>		
Cost protection from errors in capacity planning	Yes	No
May require CPU, memory and/or storage upgrades with increase in Db activity or changes to compliance regs	No	Yes
Scalable with growth of DB ecosystem	Low Cost	High Cost
Technology refresh costs	Low	High
<b>INSTALLATION AND SETUP COST</b>		
Network traffic	Low Traffic	High Traffic
Network reconfiguration required	No	Yes
Policy Development	Low Cost	High Cost
Vulnerability Knowledgebase	TeamSHATTER	Limited
<b>MONITORING OPERATION COSTS</b>		
Remediation costs	Low	High
Storage management costs	Low	High

## MONITORING OPERATIONS COSTS

The time spent remediating DAM findings requires highly skilled DBA’s. If the DAM implementation is populated with false positives and negatives, as described above:

- Acceptable and authorized behavior may be incorrectly flagged and require unnecessary analysis and policy modification. If blocking is enabled, this will result in disruption of services.

- Unacceptable and unauthorized behavior may pass undetected. This can result in costly compliance violations and even more costly database security breaches.

AppSec's DbProtect knowledge-based policy development reduces remediation costs by eliminating false positives and negatives. This combined with the TeamSHATTER knowledgebase increases the effectiveness of the DbProtect blocking solution by providing:

- More accurate identification of unacceptable and unauthorized behavior to be blocked.
- Maximum vulnerability coverage.

TeamSHATTER vulnerability checks are written with a focus on remediation. Each check is described in detail to provide a common understanding between DBAs, IT SEC, and other organizations. Each check provides proven remediation recommendations, helping organizations to resolve vulnerabilities quickly and at a lower cost.

As mentioned above, appliances collect all database activity. In a high activity database this can rapidly eat up the appliance storage capacity. As a result, organizations may require dedicating DBA resources to frequently backup and purge appliance storage. Because DbProtect only collects the business relevant data, we significantly reduce storage requirements.

## ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: [www.appsecinc.com](http://www.appsecinc.com) | [www.teamshatter.com](http://www.teamshatter.com)

For a free database vulnerability assessment visit: [www.appsecinc.com/downloads/appdetectivepro](http://www.appsecinc.com/downloads/appdetectivepro)

Follow us on Twitter: [www.twitter.com/appsecinc](http://www.twitter.com/appsecinc) | [www.twitter.com/teamshatter](http://www.twitter.com/teamshatter)

**APPLICATION  
SECURITY, INC.**<sup>®</sup>  
[www.appsecinc.com](http://www.appsecinc.com)