DB Networks and CyberArk Deliver Lower Systems Impact and Reliable Compliance with Agentless Database Management

A Brief ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Analysis
Prepared by David Monahan

December 2016

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

DB Networks and CyberArk Deliver Lower Systems Impact and Reliable Compliance with Agentless Database Management

Table of Contents

DB Networks and CyberArk Deliver Lower Systems Impact and Reliable Compliance with Agentless Database Management

Key Takeaways

Database Activity Monitoring (DAM) should be a part of the security strategy for every organization using databases for critical information. However, in determining the level of need and the representative investment for the solution, decision makers should consider three key points when generating their requirements and estimating their investment:

- Agentless DAM is a highly robust and reliable solution option
- Because agentless DAM does not need to touch the databases, deployment and lifecycle management are far easier and less complex than agent-based solutions
- Agentless DAM provides security services beyond traditional DAM and thus offers additional value

The following analysis discusses these issues and why the release of Agentless DAM will make a significant impact on database-dependent organizations.

The Need for Database Access Monitoring

Database monitoring is a common need across virtually every industry vertical. Most companies are now highly aware that their information is valuable, not only to themselves for legitimate business purposes, but also to others for one nefarious purpose or another. Being aware of the value of the data is only the first step in protecting it, and the one that keeps you up at night. These databases are rich with employees' personal information, customer data, payments data, trade secrets, and other intellectual property, and are literally gold to attackers. If left unmonitored, they are a lawsuit waiting to happen.

Figure 1: Risky Activities Identified by Agentless DAM

Industries from government agencies and large financial firms to retail, manufacturing, and educational institutions all have databases that need protecting. Data owners, insiders, hackers, database administrators, and normal users all have the possibility of inappropriately accessing, modifying, or destroying information. Once a breach occurs, a reckoning must be made regardless of whether the inappropriate action(s) was malicious or not. This reckoning may be nothing more than an internally-driven reprimand and a change in access controls, but if the data is governed by legislative or other compliance mandates, the reckoning could mean millions of dollars in costs for notification, fines, and reputation and revenue loss.

A 2012 IOUG database security study identified that 67% of organizations were leveraging native database auditing for some to all of their critical databases. Though better than nothing, native database monitoring lacks certain core capabilities that are required for best practices. Native database auditing falls under the control of the database and system administrators. This means that it is susceptible to possible tampering by attackers who get access to the system, and it fails in the need for separation of duties required by best practices and compliance standards because those making the changes to the database can modify the logs. Native auditing also fails to provide alerting. It provides for log actions only.

Database activity monitoring (DAM) was invented to address these issues. DAMs provide policy-driven, real-time alerting for policy violations to meet separation of duties and other compliance requirements. They create less internal overhead than native auditing and provide heterogeneous database support for consistent alerting across platforms.

Traditional DAMs use an agent that resides on the database system. The agent collects information and interacts with the system based on the rules or policies that were pushed to it from the DAM management system. Policies and rules can range from very simple, such as "log every command," to very complex based on the user, database, table, attribute, and command issued.

Common DAM Problems and Limitations

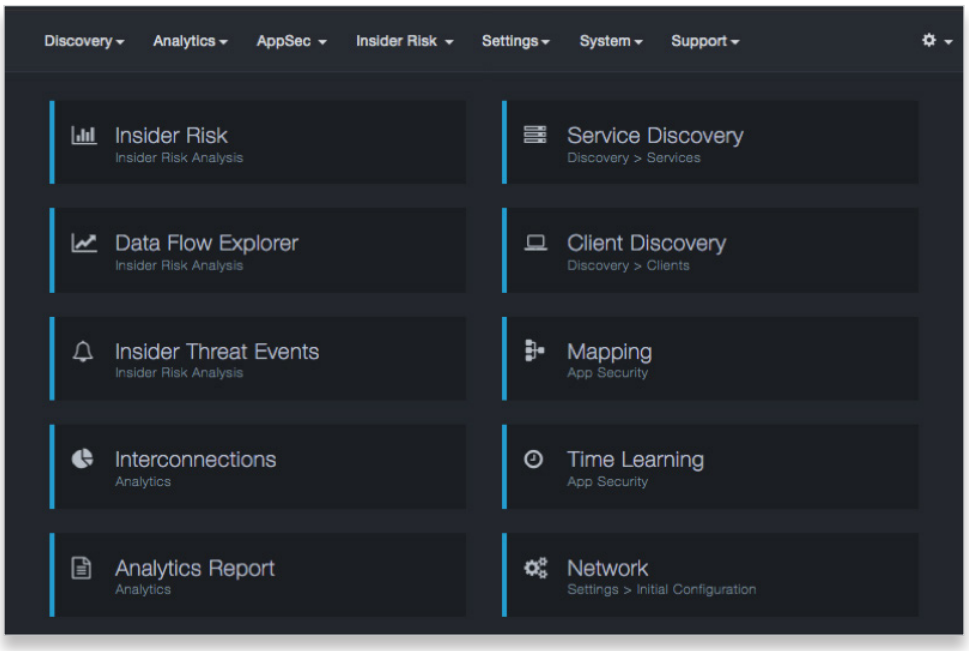

Figure 2: Agentless DAM Coverage and Reporting

With so many businesses relying on their databases for their business advantage and with many industries under compliance requirements for much of that data, monitoring and tracking access and commands, especially on those with administrative powers, is critical. Both best practices and legislation dictate a watchful eye to know the who, what, and when of any interactions with any sensitive information. However, DAMs are commonly susceptible to three main issues that drastically affect their value proposition. These three common problems are policy or agent misconfiguration, agent failure, and failure to identify and monitor new databases.

Each of these problems can go unnoticed for an extended length of time, creating a failure to comply with company policy and mandated regulations that leave private or otherwise confidential data exposed. Though each of these issues results from a different root, they can each put the organization in jeopardy. Policy and agent misconfigurations, though they are undesirable and may exist for some time before detection, produce a consistent result, so they are the easiest to audit and correct. The latter two are much more insidious.

Agent failure can happen at any time. After all, agents are just another program running on the system and are susceptible to the same problems any other software can encounter. When agent failure occurs, monitoring on the affected system ceases. The DAM manager may or may not detect the agent failure, and often they do not, so the affected databases go unmonitored until some form of audit occurs. This audit usually happens during some major reporting timeframe, such as yearly compliance or security audits. That leaves that system out of compliance and unprotected from undesirable actions.

Failure to identify databases is the most common problem encountered. In most organizations, spinning up a new database is a simple matter of a change request. At that point the new database is populated and activity begins. The problem is that without rigorous change processes, new databases are often not sufficiently vetted to determine if they need to be monitored. Though all of the major agent-based DAMs have a database discovery feature, this feature is often turned off due to the impacts it has on the network and the database systems. The discovery tools operate much like vulnerability scanners, using a significant amount of network bandwidth and system resources to discover the new databases. The performance impacts this invasiveness on systems, especially high-volume transaction databases and applications, and is unacceptable to application owners. Therefore, it is permitted only in select maintenance windows, if at all.

Agentless DAM Provides Better Visibility and Control for Databases

DB Networks partnered with CyberArk to deliver the first fully effective agentless DAM architecture. This partnership is a key step forward in providing less intrusive, more in-depth coverage for both database access and changes. The DB Networks' DBN-6300 and CyberArk's Privileged Account Security Solution (PASS), used in combination with native auditing, do not use an agent and are therefore not susceptible to any agent-related issues traditional DAM architectures face. The solution includes DB Networks' machine learning-based database security and also eliminates the issues with database discovery.

This DBN-6300 uses machine learning together with behavioral analysis to immediately and accurately alert on database policy violations and database attacks. This ensures an organization's sensitive data stores are not unknowingly tampered with.

The DBN-6300 locates databases by monitoring network traffic for communications with databases, not by scanning. When a new database is identified it logs and alerts on both the database location and the application communicating with it. Because it is not scanning, it does not generate the same network and system load

"We are excited to have one solution to meet our multiple compliance regulations. DB Networks and CyberArk's Agentless DAM solution provides my organization with more reliable database discovery and monitoring than the two industry-leading agent-based DAM solutions we previously deployed," said Jeff Weeks, SVP/CISO of a large, privately-held bank. "After testing Agentless DAM, our intent is to remove those DAM solutions."

impacts that a resident DAM causes when scanning. The DBN-6300 also detects unusual database read and update activity, further improving native database logging.

Traditional DAMs do not provide access control for the databases or their underlying infrastructure systems. They are reactive in logging and alerting for the database only. The addition of CyberArk PASS to the solution creates a proactive compensating control for privileged user separation-of-duties by managing and monitoring access and use of privileged access credentials for both the database and the underlying infrastructure systems. CyberArk authenticates the requesting user and, if successful, uses the administrator credential on his or her behalf to provide access to the database. The user never controls the privileged credential.

Using all three components effectively provides log tamper prevention, privileged account security and auditing, complete database identification and monitoring, database attack identification, credential protection, access abuse detection, infrastructure administrative credential protection, separation of duties enforcement for change and audit functions, and meets compliance requirements for numerous standards like PCI, HIPAA, and SOX.

About DB Networks

DB Networks innovates database cybersecurity products. Its customers include the world's largest financial institutions, healthcare providers, manufacturers, and governments. DB Networks technology non-intrusively assesses database infrastructures through deep protocol extraction, machine learning, and behavioral analysis. Customers gain insights by discovering all active databases, identifying tables being accessed, and the specific applications accessing the databases. In addition, analyzing application database access that deviates from the model of normal application behavior immediately identifies compromised credentials and database attacks. DB Networks is a privately held company headquartered in San Diego, Calif. For more information, call (800) 598-0450 or visit the company's website at http://www.dbnetworks.com/.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3497.121316