Database Activity Monitoring Is Evolving Into Database Audit and Protection

22 February 2012 ID:G00230083

Analyst(s): Jeffrey Wheatman

VIEW SUMMARY

Database security concerns, regulatory requirements and expanded vendor capabilities are driving the emergence of a class of technologies that Gartner now identifies as database audit and protection tools. Database activity monitoring tools are transforming into DAP suites.

Overview

Database audit and protection (DAP) represents an important evolutionary advance from earlier database activity monitoring (DAM) tools. Security managers, database administrators (DBAs) and other stakeholders who are concerned with protecting sensitive data in databases should evaluate these increasingly mature suites.

Key Findings

- Enterprises are increasingly concerned with database security as they grapple with repositories containing huge and growing amounts of regulated and otherwise sensitive or critical data.
- The DAP market continues to mature, with vendors expanding their offerings and targeting a broader range of use cases. However, it is not yet clear whether enterprises will be willing or able to adopt some of the more advanced functions of DAP.
- Many enterprises do not possess the necessary program maturity, resources and skills to implement some of the more sophisticated DAP features that are becoming available.
- Legal and regulatory compliance drivers are still the most prevalent drivers for DAP investments, and Gartner expects this to be the case through the midterm.

Recommendations

- Implement DAP functionality to mitigate the high levels of risk resulting from database vulnerabilities, and to address audit findings in areas such as database segregation of duties and change management.
- Develop a database security strategy that incorporates short-term and long-term goals and requirements. Evaluate DAP offerings as part of a database security program.
- Consider alternative solutions for DAP functions in which full functionality may not be required. Recognize that the viability of alternatives will be subject to cost-benefit trade-offs.

What You Need to Know

Enterprises are increasingly and understandably concerned with the risks associated with their fast-growing use of relational database management systems (RDBMSs). Auditors are looking more closely at how access to the huge data stores in these systems is controlled, and enterprises are being pressured to adopt more aggressive and expansive data controls. DAP tools can provide a comprehensive solution for database security requirements, but current vendor offerings exceed the needs of mainstream technology adopters. Nonetheless, leveraging the core capabilities of a DAP suite and mapping future investments to the vendor's road maps will set the stage for better future data security. Enterprises that are considering investments in DAP should be aware of alternative and complementary capabilities from other data security tools and vendors.

Return to Top

Analysis

Technology Description

DAP — a term Gartner has developed to replace the earlier DAM concept — refers to suites of tools that are used to support the identification of and reporting on inappropriate, illegal or otherwise undesirable behavior in RDBMSs, with minimal impact on user operations and productivity. These suites have evolved from DAM tools — which offered analysis of user activity in and around RDBMSs — to encompass a more comprehensive set of capabilities, including:

- Discovery and classification
- Vulnerability management
- Application-level analysis
- Intrusion prevention
- Support for unstructured data security
- Identity and access management integration

EVIDENCE

More than 100 client inquiries have indicated a shifting set of requirements — moving from basic monitoring to more advanced needs such as discovery, prevention and vulnerability management. Vendor briefings and other discussions with vendors have indicated aggressive road maps with expanded capabilities for the short term, midterm and long term.

Risk management support

Return to Top

Technology Definition

Today, DAP suites deliver a broad range of functions built around the core functions of what Gartner previously identified as DAM technology: collecting, normalizing and analyzing database traffic and activities. Gartner has seen the capabilities of these suites extended significantly, particularly during the past 12 months, with the addition of complementary and peripheral functionality. These ongoing improvements and extensions have resulted in higher levels of product maturity and better support for more use cases — and have expanded the potential market to include enterprises that take a strategic approach to data security. Vendors in this market will need to expand their real-time prevention capabilities, possibly through relationships with dynamic data masking, encryption or tokenization tools. DAP provides better auditing and monitoring support than native logging, which can add significant overhead and does not provide the same level of granularity as DAP tools do. DAP, moreover, provides comprehensive cross-platform support in heterogeneous database environments, and can serve as an effective addition to identity and access analytics.

Core DAP Capabilities

Event Collection, Analysis and Reporting
DAP tools, like other security monitoring technologies — such as security information and event management (SIEM) tools and intrusion detection systems — collect, aggregate, normalize and analyze information from a number of disparate database and application sources, and provide a mechanism for response and workflow (that is, to define what should happen when a potential security incident occurs).

Management and Auditing of the Database Security Policy
Centralized management is an important value proposition for DAP tools compared with native logging solutions. Such management provides the ability to standardize policy, configuration and reporting across all supported platforms, while providing role-based controls for configuration and reporting to support the segregation of duties.

Privileged User Monitoring
Gartner client interactions make it clear that the majority of DAP investments are being driven by the need to monitor privileged user activity. The primary goal is to review administrator activity on a periodic or as-needed basis. A secondary goal is to perform real-time monitoring and alerting to catch inappropriate administrative activity, whether deliberate (for example, looking at protected data) or accidental (for example, granting excessive access to users).

Secondary DAP Capabilities

Prevention and Blocking of Access/Attacks
One increasingly important use case is the ability to provide real-time blocking of obviously inappropriate or malicious activity. Some examples include preventing a DBA from reading the contents of a table with credit card numbers in it, preventing SQL injection attacks or buffer overflows, and implementing virtual patching in cases of known but unpatched vulnerabilities. Blocking must be used with great care, however, because of the potential impact of false positives.

Discovery and Classification
Enterprises are often unclear about what RDBMSs exist in their environments and what data is stored in them. This can make keeping track of changes in databases and the data they house a challenging task. DAP tools' ability to "crawl through" the enterprise infrastructure, discover databases and classify the data in them can be a significant aid to data security program efforts.

Vulnerability and Configuration Management
Vulnerability assessment tools are an integral part of any threat and vulnerability management program. Many DAP suites have deeper scanning capabilities than network vulnerability management tools do, including scanning for missing patches and other misconfigurations, as well as the capability to compare the current configuration with the baseline, and sometimes with change and configuration management tools, to ensure that changes are preapproved.

Auditing and Monitoring of Users and Applications
The ability to collect and analyze the data access components of application traffic is challenging for most enterprises. Shared IDs and connection pooling are often implemented at the application layer to speed up performance, but they add a level of abstraction. A pooled connection will aggregate numerous requests into one SQL query against the RDBMS; this request may contain SQL commands that violate a policy, mixed in with SQL commands that do not. DAP tools continue to add capabilities for maintaining context and for mapping SQL commands back to individual user requests.

Assessment of Users and Permissions
Databases maintain their own identity and policy stores, and because user permissions are often assessed at the application level — rather than in the underlying repositories — general-purpose identity management software does not cover databases well. Some DAP vendors can extract and report on these permissions so that security, compliance, and even application and database teams can assess the access control model.

Return to Top

Operating Requirements

DAP can be deployed using a combination of two basic architectures:

Network Collectors: These are fast and centralized and add no overhead at the database server layer, but miss activity such as direct or remote console activity as well as database triggers and stored procedures.

Agent Collectors: These small pieces of code capture local activities or log data and send it to a centralized location for aggregation and analysis. The agents "see" more, but they add server overhead. If installing local agents is impractical, then pure network collector deployments can be used.

Return to Top

Uses

Gartner has identified two primary DAP use cases:

Privileged user monitoring (the more common use case) focuses on monitoring, analyzing and reporting on the actions undertaken by users (such as DBAs and application managers) with a high level of access to the data within the database. DAP is used to identify and prevent privileged users from accessing data, modifying the RDBMS, or creating or modifying user accounts or permissions.

Application user monitoring (less common, but growing in importance) focuses on activity from end users and applications that connect to the database. The purpose of this monitoring is to detect deliberate or inadvertent abuses of legitimate access privileges. Some auditors and security teams are evaluating or implementing DAP technologies to fulfill contractual and regulatory requirements, enhance overall risk management, and achieve data governance goals.

A third use case relates to attack detection and prevention. This may seem to be a third primary use case, but the attack is typically targeted at compromising privileged user accounts or application-level access. This use case is not really the endgame, but rather an intermediary step that may be necessary before full system or data compromise takes place.

Regulatory compliance requirements — for example, those of the PCI Data Security Standard, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and global privacy regulations — continue to be the main driver for DAP investment. Gartner is, however, seeing increasing investment as part of a data security program.

Return to Top

Benefits and Risks

DAP has not yet reached its full potential, but it represents a worthwhile investment for enterprises with databases containing confidential data, intellectual property, or any data that is subject to legal and regulatory protection requirements. These tools will continue to grow in maturity, function and usability, and will continue to deliver benefits as part of an enterprise data security program. DAP can also benefit risk management programs. Many installations start small and grow in size and complexity over time as enterprises see increased value from their investments.

Return to Top

Technology Alternatives

SIEM tools can be used for database monitoring. SIEM provides broader monitoring and, in some cases, "good enough" support for RDBMSs.

Content-aware data loss prevention (DLP) tools can provide visibility into data access, and can be used as an alternative to DAP in data-centric use cases; however, these tools do not have embedded knowledge of how RDBMSs "work," and they lack visibility into administrative activities such as schema modifications or account management.

Financially constrained enterprises can leverage native RDBMS auditing and logging using homegrown tools or scripts. However, this approach is limited by the high overhead of native auditing and the difficulty of creating homegrown solutions in heterogeneous environments.

Network vulnerability scanners provide a limited subset of RDBMS tests and are often sufficient for audits. These scanning tools are often already deployed with the necessary head count to manage and respond to findings, thereby providing a less expensive (albeit less effective) solution.

Encryption, tokenization and masking can be used to protect the data from inappropriate access, but they are insufficient to identify inappropriate access (for example, accessing too much data too fast) by legitimate users.

Identity and access governance tools have a limited set of functions that are used for monitoring and analytics of data, but they lack the granularity and visibility into structured data environments, and are predominantly application-centric in their feature sets.

Return to Top

Selection Guidelines

DAP tool selection is relatively straightforward, with the most important constraint tending to be platform support. All DAP tools support the most common RDBMS platforms — Microsoft SQL Server, Oracle and DB2 — but support for other platforms may not be as consistent or comprehensive. Longer-term client requirements must be mapped against vendors' road maps. The flexible architectures provided by most platforms allow simple decisions, and can meet the needs of the majority of clients, although ease and scalability of deployments can vary greatly from one vendor to another.

Return to Top

Price Performance

Pricing for DAP suites is fairly consistent, with an entry-level deployment typically costing less than $100,000 for a single data center and a small number of databases with a "normal" transaction volume using core monitoring capabilities. Larger installations with expansive footprints (in geographical and database/transaction volume terms) and added functionality can cost $1 million or more. Pricing scales fairly linearly with requirements, and enterprises typically start with limited-scope deployments, then ramp up to larger deployments over 12 to 18 months.

Return to Top

Technology Providers

Application Security's DbProtect suite combines the company's monitoring product with its user rights management tool and its market-leading vulnerability scanning product. Application Security closed a functionality gap in 2011 by adding prevention to the suite. The company has a strong installed base on the vulnerability side and has leveraged it into monitoring sales.

BeyondTrust acquired the assets of Lumigent, one of the earlier DAM vendors and an early market leader. The Lumigent offering fits well with BeyondTrust's portfolio, but the limited development of the old Lumigent product has resulted in some functionality gaps in its offering. BeyondTrust has closed some of the gaps with its latest release and has committed to addressing others in future releases.

IBM InfoSphere Guardium is the market leader in terms of revenue and number of clients. Its offering has the widest platform coverage and the most robust set of features, and the company has demonstrated the ability to leverage the IBM sales model with its DAP offering.

Imperva is second in DAP market share, with scope and offerings similar to IBM's offering. The company sells DAP as part of a data security suite that includes a Web application firewall and a product for unstructured data security.

McAfee acquired the Sentrigo DAM product and is making a major push into the database security market. If McAfee can leverage its large customer base and sales force, then it could be a strong player in this market.

Oracle has a strong market presence, especially in its client base. Oracle provides much DAP functionality with two separate products: Audit Vault and Database Firewall, which provide support for Oracle and non-Oracle database management systems. Oracle offers numerous separately branded database security tools that map to extended DAP capabilities, some of which are cross-platform and some of which only have support for Oracle RDBMSs.

WareValley, a South Korean vendor with a strong focus and presence in the Asia/Pacific market, has an offering that consists of encryption, monitoring, vulnerability management and RDBMS management. The company has recently indicated an increased desire to move into the North American and European Union markets with aggressive pricing.

Return to Top