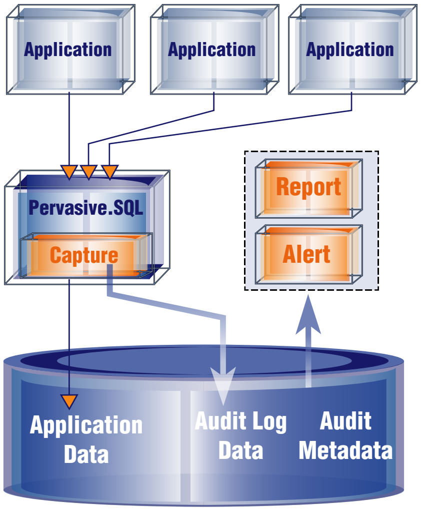
Pervasive AuditMaster™: Data Access Security and Accountability

Attain a new level of security in your applications with the transaction intelligence and proactive monitoring capabilities of Pervasive AuditMaster, without changing your code or database. Never again worry if your data's safe, or if your compliance with privacy and accountability practices has been compromised: *AuditMaster can tell you who's doing what to your data in real time.*

> *"Cost-effective regulatory compliance, accounting fraud detection and procedural best practices are growing concerns among small and mid-sized firms around the world. Organizations must consider their options for implementing solutions that address the concern but aren't cost or deployment prohibitive."*
> – Mark Shainman
> Senior Research Director
> META Group

Pervasive Software® has responded to the growing need for security and accountability in managing mission-critical data by introducing Pervasive AuditMaster, which captures events involving any user touching any data in your Pervasive.SQL™ database, down to a single byte, in any application you're using. Whether you're striving to meet legislated requirements for electronic security and privacy, or raising the standards of corporate governance to satisfy customer and shareholder expectations, AuditMaster gives you the competitive edge.

Security and auditing are critical across virtually all industries – from the Sarbanes-Oxley Act to the Health Insurance Portability and Accountability Act to the Patriot Act, every market is now affected by the need for increased security, and the ability to know who is interacting with data, and how. Proactively monitor data access with alerts that are easily customized to your business rules. Or, track what happened when by way of an audit trail. It's up to you - AuditMaster enables you to always know who's doing what, when, where and how. In most data management systems, security settings authorize user access to data, but within those boundaries, everyone is on the honor system. Unfortunately, not everyone is honorable. Database access control is never enough.



Auditing access below the application level provides a third-party view of data access.

AuditMaster advantages over other auditing options:

AuditMaster vs. Trigger-Based Auditing

▲ More information is captured – contextual information like originating IP address and non-DML events like error messages are logged.
▲ No trigger code to maintain – triggers do not have to be created for each monitored table.
▲ Full DDFs are not required – AuditMaster can log partly described or non-SQL compliant data.
▲ Works with Btrieve – the capture module plugs into the MicroKernel, not the relational engine.

AuditMaster vs. Application-Level Auditing

▲ More information is captured – contextual information like originating IP address and non-DML events like error messages are logged.
▲ No coding is required – auditing occurs below the application level
▲ The audit log is more complete – the capture module logs all database events, including ones originating outside your application (3rd party integrations, VAR customizations).

Data Access Accountability Features

AuditMaster provides strong data access accountability by means of three modules:

Capture
Report
Alert

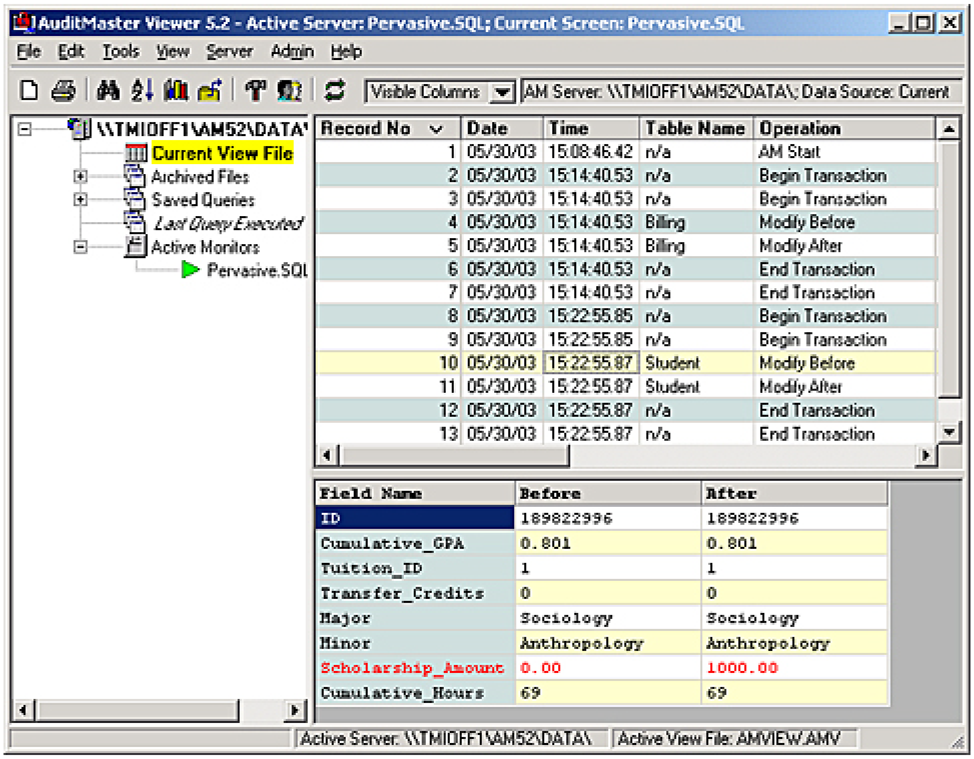
The *Capture* module is an easily installed database plug-in. It serves as an all-seeing flight recorder, trapping every event in the database in a detailed trail. It's installed at the database level, so when the database is running, AuditMaster Capture is running, and the log record is always complete.

Once the Capture module establishes the audit trail, the *Report* module allows queries on it, enabling a security administrator to verify past activities or analyze patterns and trends. A simple graphical interface and drop-down lists simplify rapid building of queries. AuditMaster reports can also conveniently supply evidence of compliance with best or required practices.

While reports are historical, the *Alert* module offers proactive surveillance on future data activity. Once defined in AuditMaster, alert triggers wait for specific events of interest based on the entire range of user actions, including creating, updating and deleting data, or even simply reading it. When a watched-for event occurs, AuditMaster immediately triggers an alert, which can take the form of an email to one or more recipients, a call to another application, or the start-up of a new application.

Complete Audit Trails, Automatically

Along with application data, Pervasive.SQL also saves data captured by AuditMaster and stores them in tables in their own directory. These files hold all audit information, such as user ID, network station ID, time and date of operation, application name, database table name, and operation type.



AuditMaster Viewer 5.2 - Active Server: Pervasive.SQL; Current Screen: Pervasive.SQL

Record No	Date	Time	Table Name	Operation
1	05/30/03	15:08:46.42	n/a	AM Start
2	05/30/03	15:14:40.53	n/a	Begin Transaction
3	05/30/03	15:14:40.53	n/a	Begin Transaction
4	05/30/03	15:14:40.53	Billing	Modify Before
5	05/30/03	15:14:40.53	Billing	Modify After
6	05/30/03	15:14:40.53	n/a	End Transaction
7	05/30/03	15:14:40.53	n/a	End Transaction
8	05/30/03	15:22:55.85	n/a	Begin Transaction
9	05/30/03	15:22:55.85	n/a	Begin Transaction
10	05/30/03	15:22:55.87	Student	Modify Before
11	05/30/03	15:22:55.87	Student	Modify After
12	05/30/03	15:22:55.87	n/a	End Transaction
13	05/30/03	15:22:55.87	n/a	End Transaction

Field Name	Before	After
ID	189822996	189822996
Cumulative_GPA	0.801	0.801
Tuition_ID	1	1
Transfer_Credits	0	0
Major	Sociology	Sociology
Minor	Anthropology	Anthropology
Scholarship_Amount	0.00	1000.00
Cumulative_Hours	69	69

Active Server: \\TMIOFF1\AM52\DATA\ | Active View File: AMVIEW.AMV

Comparing before-and-after images in AuditMaster Viewer.

The database also stores report queries and their results, triggers for alerts and metadata.

AuditMaster also provides before-and-after transaction imaging. Each time a user changes data, AuditMaster captures both the original and the new record. This powerful capability allows database rollback or fine-grain, point-in-time recovery for individual records by undoing changes captured in the audit trail.

AuditMaster works with all Pervasive.SQL data, whether transactional or relational. In addition, AuditMaster can automatically maintain multiple metadata files on your data records to support upgrades to new versions of your client application, even when data definition files (DDFs) change. AuditMaster metadata support auditing even if your DDFs are missing or incomplete. In addition, if your system uses variant records, AuditMaster still performs all of the same capture, report and alert functions.

Answering an Industry Need

Across every industry, guidelines for security policy and requirements for data access accountability are on the rise. Code redesign and integration projects are time-consuming for product schedules and hard on your company's balance sheet. Whether your product line is new or well-established, AuditMaster addresses these concerns with easy adoption, high level of automation, low level of maintenance, and no changes to application code or database.

Keeping a Best Foot Forward: Accounting

In the post-Enron era, corporate governance is coming under increased scrutiny by regulators, analysts, shareholders, business partners, clients and, of course, the news media. As never before, monitoring of best practices and detection of fraud and ethical lapses gives a big return on investment in auditing technology.

Fraud often turns on the fact that those who commit it have been given authority to access data so that they can do assigned work. Thus, the challenge is to detect work that they have “assigned themselves,” such as accessing the payables database while checks are being run.

If an accounting clerk were able to change the pay-to recipient for a large check, then, after the check is printed and intercepted, update the record to once again show the originally intended recipient, then how long might it take to discover this redirection of funds?

AuditMaster triggers can be custom set to watch for precisely this type of activity, as well as a wide range of others, depending on the specific needs of your workplace and policies.

Meeting Federal Standards: Healthcare

With the adoption of the Internet and the transition of the patient record to an electronic format, privacy concerns have gone mainstream. When it comes to who, what, when, where and how data is accessed to deliver healthcare, new rules abound to protect confidentiality and ensure accountability on the part of healthcare providers. Public sector ideas about information technology are catching up with the commercial world, as shown in recent years by a wave of new legislation. In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) is becoming for healthcare providers the foundation and new paradigm of patient record keeping and sharing.

“HIPAA dictates that providers must ensure privacy and security of patient data—a task that requires retrofitting long-used, legacy systems that can consist of millions of customer records.”
– Elizabeth Lipp, Managing Editor, Database Trends and Applications magazine, May 2003

Since AuditMaster is a quickly installed plug-in for Pervasive.SQL and Btrieve databases, the retrofitting of applications built on those systems need not carry the sense of foreboding that's making headlines in IT news media.

HIPAA requires administrative, physical and technical safeguards. Healthcare providers, such as hospitals or group practices, must complete an assessment of their data vulnerabilities and ensure that roles and responsibilities for data access are clearly defined.

In addition, healthcare providers will be held accountable to provide an audit trail documenting who accesses or modifies patient data. Compliance will depend on preparedness to provide this documentation accurately and rapidly.

AuditMaster retains all audit items, provides the technical means to implement your audit trail policy, and enables your HIPAA security officer to monitor the audit trail. It can play a key role in establishing the safeguards, accuracy and speed required to meet HIPAA compliance and enter the chain of trust with other HIPAA-compliant organizations.

For more information
To learn more about Pervasive Software and our solutions, please visit **www.pervasive.com.** To reach the North American sales office, call **1.800.287.4383, extension 2**. For Latin, Central and South America, Australia and New Zealand, call **+1.512.231.6000**. In Europe, for Belgium, France, Germany, Italy, Luxembourg, The Netherlands, Spain, Sweden, Switzerland and the United Kingdom, call **+800.12.12.34.34**. For any other European, Middle Eastern, African or Asian countries (excluding Japan), call **+32.70.23.37.61**. For Japan, please call **+81.3.3293.5300**, or visit **www.pervasive.co.jp**.

About Pervasive Software
Pervasive Software is a leading global data-management company powering the success of application developers by providing solutions that deliver the industry's best combination of performance, reliability and low administration costs. Pervasive's strength is evidenced by the size and diversity of its customer base, serving tens of thousands of customers with hundreds of thousands of end-users in nearly every vertical market around the world. Founded in 1994, Pervasive® sells its products into more than 150 countries and is based in Austin, Texas, with offices in Europe.

PERVASIVE®
Powering Success